GB-OS

Certificate Management

GBOSCM201311-01

Global Technology Associates, Inc.

Global Technology Associates
3505 Lake Lynda Drive Suite 109
Orlando, FL 32817

Tel: +1.407.380.0220
Fax. +1.407.380.6080
Email: info@gta.com
Web: www.gta.com

Table of Contents

GB-OS Certificate Management

GB-OS 5.3 and above can create signing Certificate Authorities (or CA's) for creating GTA firewall certificates. These CA's can be used for remote firewall administration, SSL Browsers, and Remote Administration Certificates — which are used for the SSL Client and both Mobile IPSec VPN Clients and Firewall to Firewall IPSec VPN's.

GB-OS will automatically create a GB-OS CA, Remote Administration and VPN certificate under the following conditions:

- Basic Setup Wizard is employed to configure the firewall
- Certificate section is defaulted (Automatically configured based on firewall configuration)

GB-OS will automatically create user certificates when:

- Administrator is defined during the Basic Setup Wizard
- A new user is created and the certificate field is set to **GENERATE**
- During upgrade, if no user certificate has been created on previous versions

Creating a Certificate Authority

To manually create a signing CA click **NEW** in **Configure >VPN >Certificates.** Enter information for the following fields:

Table 1: Creating a GB-OS CA

Field	Description
Disable	A selection to disable the certificate. Default is unselected
Name	A unique name used to identify the certificate.
Description	A brief description of the certificate.
Certificate	Select Generate to allow the firewall to generate a new GB-OS CA.
Generate	
Type	Set certificate type to CA.
Common Name	Enter a common name for the certificate.
Subject Alt Name	The subject alternative name extension allows various literal values to be included in the configuration file. These include email (an email address) URI a uniform resource indicator, DNS (a DNS domain name), RID (a registered ID: OBJECT IDENTIFIER), IP (an IP address), dirName (a distinguished name) and otherName
Email Address	Pre-populated field with Administrator's email address.
Country	Select the CA country.
State/Region	Enter the CA's state or region.
City/Locality	Enter the CA's city or locality.
Organization	Enter the CA's organization.
Organizational Unit	Enter the CA's organizational unit.
Duration	The amount of time for which the CA is valid. Default is 5 years.
Key Size	A selection for the key size of the CA, in bits.

Once the new CA is created, select it as the Firewall's CA Certificate. All new GB-OS certificates generated via firewall will use this CA as their signing CA.

Note

Only CA's generated on target firewall may be selected as Local CA.

Creating a CSR

To create a CSR Request for the firewall, click **NEW** in **Configure >VPN>Certificates**. Enter information for the following fields.

Table 2: Creating a CSR

Field	Description
Disable	A selection to disable the certificate. Default is unselected
Name	A unique name used to identify the certificate.
Description	A brief description of the certificate.
Certificate	Select Generate to allow the firewall to generate a new certificate request.
Generate	
Type	Set certificate type to CSR.
Common Name	Enter a common name for the certificate.
Subject Alt Name	The subject alternative name extension allows various literal values to be included in the configuration file. These include email (an email address) URI a uniform resource indicator, DNS (a DNS domain name), RID (a registered ID: OBJECT IDENTIFIER), IP (an IP address), dirName (a distinguished name) and otherName
Email Address	Pre-populated field with Administrator's email address.
Country	Select the CA country.
State/Region	Enter the CA's state or region.
City/Locality	Enter the CA's city or locality.
Organization	Enter the CA's organization.
Organizational Unit	Enter the CA's organizational unit.
Duration	The amount of time for which the CA is valid. Default is 5 years.
Key Size	A selection for the key size of the CA, in bits.

Once the CSR request is completed, export the CSR and submit to your Certificate Authority. See Exporting Certificates for more information.

Creating a Certificate

To manually create a certificate for use by the firewall or a client, in the firewall web administration interface, click **NEW** in **Configure >VPN >Certificates**. Enter information for the following fields.

Table 3: Creating a Certificate

Field	Description
Disable	A selection to disable the certificate. Default is unselected
Name	A unique name used to identify the certificate.
Description	A brief description of the certificate.
Certificate	Select Generate to allow the firewall to generate a new certificate.
Generate	
Type	Set certificate type to Certificate.
Common Name	Enter a common name for the certificate.
Subject Alt Name	The subject alternative name extension allows various literal values to be included in the configuration file. These include email (an email address) URI a uniform resource indicator, DNS (a DNS domain name), RID (a registered ID: OBJECT IDENTIFIER), IP (an IP address), dirName (a distinguished name) and otherName
Email Address	Pre-populated field with Administrator's email address.
Country	Select the certificate's country.
State/Region	Enter the certificate's state or region.
City/Locality	Enter the certificate's city or locality.
Organization	Enter the certificate's organization.
Organizational Unit	Enter the CA's organizational unit.
Duration	The amount of time for which the CA is valid. Default is 5 years.
Key Size	A selection for the key size of the CA, in bits.

Exporting Certificates

When exporting certificates from the configuration, the following file formats are available:

- **DER**: A binary certificate and its private key are exported as separate DER files. Certificates have a .der file extension and private keys have a .key file extension.
- **PEM**: A Base64 encoded certificate and its private key are exported as separate PEM file. Certificates have a .crt file extension and private keys have a .key file extension.
- **PKCS#7 DER:** A certificate along with the certificate chain are exported as a single PKCS#7 file in binary format. PKCS#7 files have a .p7b file extension.
- **PKCS#7 PEM:** A certificate along with the certificate chain are exported as a single PKCS#7 file in Base64 encoded format. PKCS#7 files have a .p7b file extension.
- **PKCS#12**: The certificate and its private key, along with the certificate chain used are exported as a single PKCS#12 file. PKCS#12 files have a .p12 file extension. Private key may be password protected.
-

Note

PEM and DER file formats require that certificates and private keys are downloaded separately.

1. Navigate to **Configure>VPN>Certificates**.
2. Select a previously defined certificate and click the **Edit** button to bring up the **Edit Certificate** screen.
3. Select the desired file formats for the VPN certificate and its private key.
4. Click the **Download** buttons to export the files.

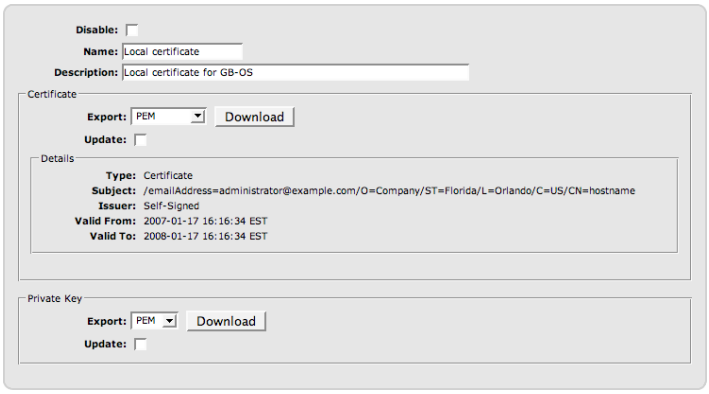

Figure 1: *Exporting a Certificate*

Table 4: Exporting a Certificate	
Field	**Description**
Disable	A toggle to disable the configured certificate.
Name	A unique name used to identify the configured certificate.
Description	A brief description to describe the function of the configured certificate.
Certificate	
Export	Select the file format for the certificate. Click the **Download** button to export the file.
Update	Toggle the Update checkbox if you wish to update the certificate's definition with an existing certificate, or generate a new certificate.
PKCS#12 Password	If the certificate is to be exported as a PKCS#12 file, an optional password can be set to secure the certificate. The PKCS#12 Password field is case sensitive.
Private Key	
Export	Select the file format for the private key. Click the **Download** button to export the file.
Update	Toggle the Update checkbox if you wish to update the private key with an existing private key.

Importing Certificates

1. To import a certificate into GB-OS for use in configuration or user account definition, navigate to **Configure>VPN>Certificates** and select the **New** icon.
2. The **Edit Certificate** screen will then be displayed. Select the **Import** toggle in the Certificate field to import a certificate.

Note

When importing a certificate that is a PKCS#12 file, all certificates used in the certificate chain as well as the certificate's private key are imported into the configuration.

When importing a certificate that is a PKCS#7 file, all certificates used in the certificate chain are imported into the configuration.

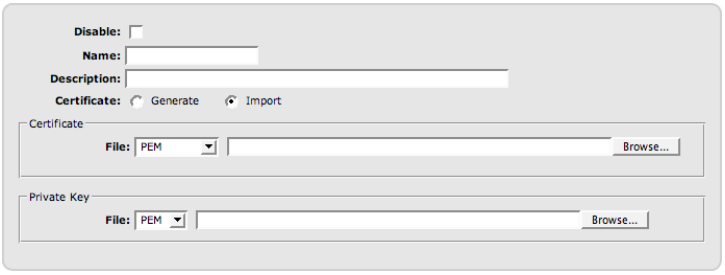

Figure 2: *Importing VPN Certificates*

Table 5: Importing VPN Certificates	
Field	**Description**
Disable	A toggle to disable the configured certificate.
Name	A unique name used to identify the certificate.
Description	A brief description for the function of the certificate.
Certificate	Import
Certificate	
File	Select the **Browse** button to locate the certificate file.
Private Key	
File	Select the **Browse** button to locate the associated private key.

Updating Certificates

1. To update a certificate, navigate to **Configure>VPN>Certificates**, select the certificate to be updated, and double click or click the **EDIT** button.
2. Select the **Update** toggle under Certificate.

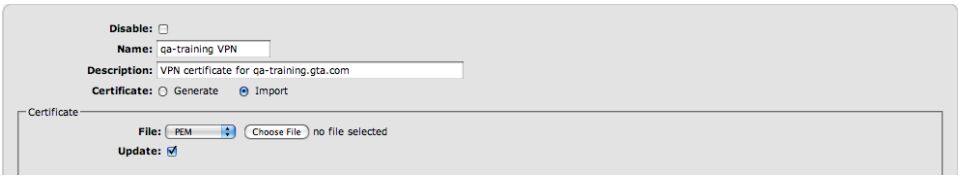

Figure 3: *Update Certificate*

3. In the top section, select the **Generate** toggle in the CERTIFICATE field.
4. The generate fields will auto populate. Select the **OK** button at top.

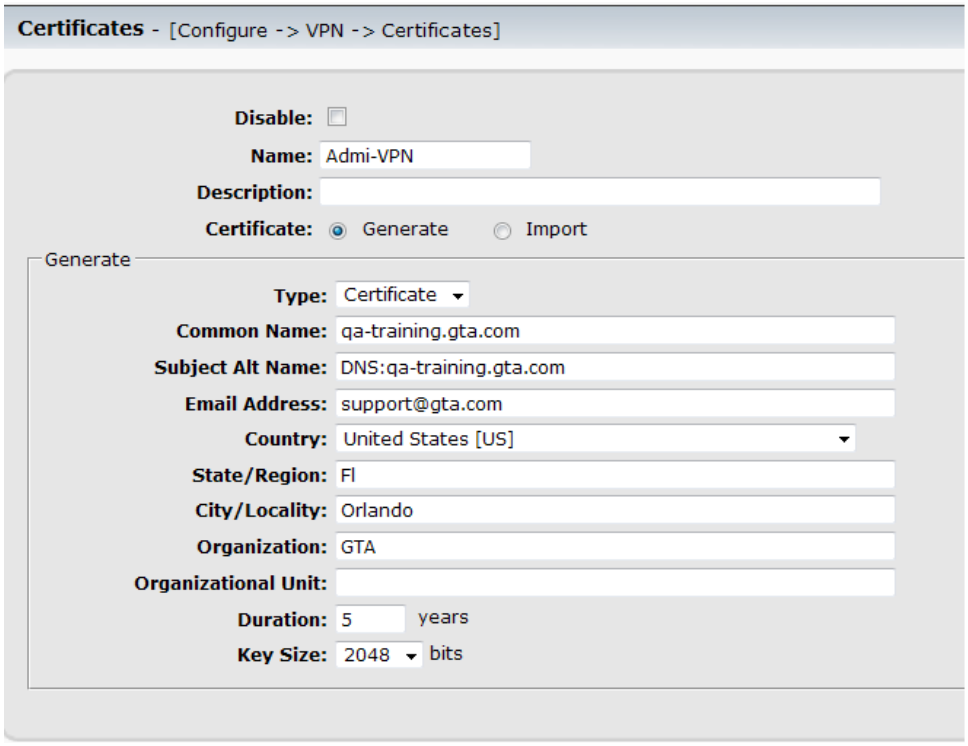

Figure 4: Generate Updated Certificate.

Note

If the firewall's VPN certificate is updated and it is used in a Site to Site IPSec Tunnel, the remote firewall will need to have the updated certificate.

If a user's certificate is updated and they use an SSL VPN, IPSec RSA, or IPSec RSA+XAuth VPN configuration they will need to download new VPN configurations.

Note

When updating certificates due to verification errors, DO NOT regenerate the CA unless necessary - doing so will invalidate all other certificates. Regenerate all other certificates as necessary. If the firewall CA certificate is updated, ALL certificates generated using the CA will need to be updated. See Troubleshooting for more details.

Revoking Certificates

To revoke a certificate, navigate to **Configure>VPN>Certificates**, select the certificate to be updated, and click the **REVOKE** button in the action menu.

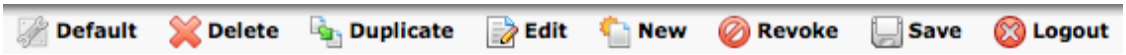

Figure 5: Revoking Certificates

Using Intermediate and Chained Certificates

If the firewall uses intermediate and chained certificates, Policy Compatibility, located at **Configure>Accounts>Remote Administration>Advanced**, must be unchecked.

Figure 6: Remote Administration Policy Compatibility

The following is an example of an intermediate/chained certificate. The certificate `qa-training.gta.com` is issued by RapidSSL, which is in turn issued by GeoTrust Global CA.

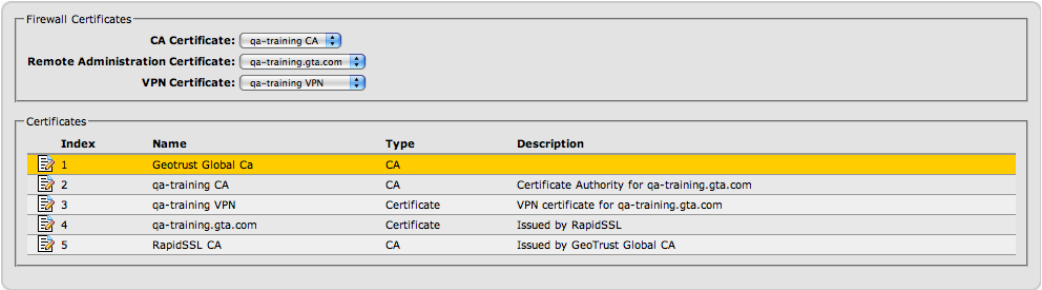

Figure 7: Example of Intermediate/Chained Certificates

Defaulting the Certificate Section

Clicking the **DEFAULT** button at the top of the screen in **Configure >VPN >Certificates** will create the following certificates:

- CA Certificate
- Remote Administration Certificate
- VPN Certificate

The certificates will be created using the host name configured in **Configure >Network>Interfaces>Settings** and the contact information configured in **Configure >System >Contact information.**

Default Firewall Certificate

The built in Default certificate is non-editable. This certificate is only updated when firewall host name is updated in **Configure>Network>Interface>Settings** or if a new default certificate is generated via the console interface. If all other certificates are removed, the Default certificate will be used by the firewall.

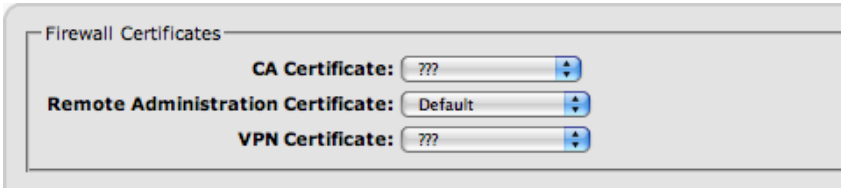

Figure 8: *Default Firewall Certificate*

Certificates and Mobile IPSec VPN Clients and SSL Clients

GTA firewalls are capable of creating user certificates for SSL Clients and Mobile IPSec VPN Clients. The recommended method is to select **GENERATE** in user setup. However, you may manually create a user certificate for SSL and Mobile IPSec VPN's.

SSL Client certificates must use signed certificates. In addition, the firewall VPN certificate must be a signed certificate. Failure to use signed certificates for users with SSL Client configurations will result in failure of the client to connect.

For more information on configuring certificates for SSL Client or the Mobile IPSec VPN Client, see the *GTA SSL Client Guide* or the *Remote Access Guide.*

Certificates and High Availability

Each High Availability firewall must have a unique SSL certificate for web administration. However, the VPN certificate used for IPSec VPN and SSL Clients should be the same on both High Availability firewalls. Additionally, the firewalls should use the same GB-OS CA. For information on syncing the certificates, see the *High Availability Feature Guide.*

Troubleshooting

Lost Web Administration upon GB-OS 6.0.3 Upgrade or Remote Administration Settings Change

Upgrading to GB-OS 6.0.3, or defaulting the remote administration settings screen, may result in remote administration errors due to duplicate certificate serial numbers. These errors may prevent web administration of the firewall via Firefox or Google Chrome. A connection error will be displayed in the web browser.

To preserve remote administration settings and maintain web administration access, enable Policy Compatibility in **Configure>Accounts>Remote Administration>Advanced** via Internet Explorer or Safari. Administration is also available via the Console Interface.

GTA strongly recommends resolving the certificate verification error.

Duplicate Serial Numbers Including CA

```
ERROR: Certificate 4, has same serial number as CA certificate 3
```

This verification message indicates that certificate #4 has the same serial number as the firewall CA certificate. This error can cause loss of remote administration using some browsers. To resolve, update the NON-CA certificate. In this case, certificate #4. DO NOT regenerate the firewall CA unless absolutely necessary. If the firewall CA is re-generated or updated ALL certificates created with the CA will then need to be updated.

Duplicate Serial Numbers

```
Warning: Certificate 3, has same serial number as certificate 4
Warning: Certificate 4, has same serial number as certificate 3
```

Regarding these example certificates:

3. Name: fwadmin
   Description: Automatically added
   Type: Certificate
   Serial Number: 1269432400 (0x4baa0050)
   Subject: emailAddress = fwadmin, CN = fwadmin, O = GTA, C = US
   Issuer: emailAddress = support@gta.com CN = qa.gta.com CA, O = GTA, C = US
   Valid From: 2010-03-24 08:06:40 EDT
   Valid To: 2015-03-23 08:06:40 EDT
   Private Key: Present

4. Name: user
   Description: Automatically added
   Type: Certificate
   Serial Number: 1269432400 (0x4baa0050)
   Subject: emailAddress = user, CN = gbuser, O = GTA, C = US
   Issuer: emailAddress = = support@gta.com, CN = qa.gta.com CA, O = GTA, C = US
   Valid From: 2010-03-24 08:06:40 EDT
   Valid To: 2015-03-23 08:06:40 EDT
   Private Key: Present

This verification message indicates that the certificates have the same serial number. To resolve, update at least one of the two conflicting certificates.

Certificate Signature Failure

```
WARNING: Certificate 1, status "certificate signature failure"
```

This verification message indicates that the firewall CA has been updated and thus all certificates generated by the CA are now invalid. To resolve, update ALL certificates created by the affected firewall CA certificate.

Certificate Not Yet Valid

```
WARNING: Certificate 1, status "certificate is not yet valid"
```

This verification message indicates that the certificate time stamp is later than the firewall current time/date. To resolve, verify NTP is enabled on the firewall and regenerate certificates as needed.

Missing Referenced Certificate

```
ERROR: VPN Certificate, references missing object ""
ERROR: CA Certificate, references missing object ""
ERROR: User 12, references missing certificate "ipsec-rsa"
```

These verification messages indicates that the referenced certificate is missing. To resolve, edit the configuration by replacing the missing certificates and/or CA certificate.

Certificate Without a Private Key

```
WARNING: Local Certificate, references object "<certificate _ name>" without a private key
```

This verification message indicates that the certificate selected for Remote Administration does not have a private key and cannot be used for Firewall Administration or Remote Access Portal. To resolve, import a private key or select a certificate which has a private key.

Default Certificate Error

```
WARNING: Using the default certificate ERROR:
```

This verification message indicates that the firewall is using the default certificate for remote administration. To resolve, create a new certificate or import a new certificate for remote administration.

Expired Certificate

```
WARNING: Certificate 3, status "certificate has expired"
```

This verification message indicates that the certificate has expired. To resolve, update the certificate.

Missing Certificate Authority (CA) Certificate

```
WARNING: Certificate 3, status "unable to get issuer certificate"
WARNING: Certificate 4, status "unable to get local issuer certificate"
```

This verification message indicates that the firewall's Certificate Authority (CA) certificate is missing. To resolve:

- If it is a firewall created certificate, create a new firewall CA and update all firewall certificates using the new CA.
- If it is an imported certificate, import the certificate CA and any other CA's as needed if it is an intermediate or chain certificate.

Duplicate Certificate Subject

```
ERROR: Certificate 2 ("certificate 2") has same subject as certificate 1 ("certificate 1")
```

This verification message indicates that the two certificates have the same subject. To resolve, update at least one of the two conflicting certificates and change the COMMON NAME.

Legal Notices

Technical Support

GTA includes 30 days “up and running” installation support from the date of purchase. See GTA’s Web site for more information. GTA’s direct customers in the USA should call or email GTA using the telephone and email address below. International customers should contact a local Authorized GTA Channel Partner.

Tel: +1.407.380.0220 **Email:** support@gta.com

Disclaimer

Neither GTA, nor its distributors and dealers, make any warranties or representations, either expressed or implied, as to the software and documentation, including without limitation, the condition of software and implied warranties of its merchantability or fitness for a particular purpose. GTA shall not be liable for any lost profits or for any direct, indirect, incidental, consequential or other damages suffered by licensee or others resulting from the use of the program or arising out of any breach of warranty. GTA further reserves the right to make changes to the specifications of the program and contents of the manual without obligation to notify any person or organization of such changes.

Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation for their use. GTA assumes no responsibility with regard to the performance or use of these products.

Every effort has been made to ensure that the information in this manual is accurate. GTA is not responsible for printing or clerical errors.

Trademarks & Copyrights

GB-OS and GB-Ware are registered trademarks of Global Technology Associates, Incorporated. Global Technology Associates and GTA are service marks of Global Technology Associates, Incorporated.

Microsoft, Internet Explorer, Microsoft SQL and Windows are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe and Adobe Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

UNIX is a registered trademark of The Open Group.

Linux is a registered trademark of Linus Torvalds.

BIND is a trademark of the Internet Systems Consortium, Incorporated and University of California, Berkeley.

WELF and WebTrends are trademarks of NetIQ.

Sun, Sun Microsystems, Solaris and Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Java software may include software licensed from RSA Security, Inc.

Some products contain software licensed from IBM are available at http://oss.software.ibm.com/icu4j/.

Some products include software developed by the OpenSSL Project (http://www.openssl.org/).

Mailshell and Mailshell Anti-Spam is a trademark of Mailshell Incorporated. Some products contain technology licensed from Mailshell Incorporated.

All other products are trademarks of their respective companies.

Global Technology Associates, Inc.

3505 Lake Lynda Drive, Suite 109 • Orlando, FL 32817 USA

Tel: +1.407.380.0220 • **Fax:** +1.407.380.6080 • **Web:** http://www.gta.com • **Email:** info@gta.com