GTA SSL Client & Browser Configuration

SSL201607-01

Global Technology Associates, Inc.

Global Technology Associates
3361 Rouse Rd, Suite 240
Orlando, FL 32817

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

Table of Contents

Introduction

The purpose of this document is to assist GB-OS users in the installation, configuration and use of the GTA Firewalls SSL Service. GTA's SSL Service has two components:

- **Browser** – The SSL Browser provides client-less remote network access. Using a standard Web browser, users launch a customized Web portal (the SSL Browser) for access to files, applications and internal and external web sites. Supported protocols include http, https, ftp, ftps, and cifs.
- **Client** – The SSL Client is a remote access VPN client that uses SSL to establish a secure, encrypted connection to the network firewall. Via the SSL Browser, the SSL Client is downloaded and installed to the authorized remote user's machine.

Browser access for SSL users is determined by their group privileges. Some users may only have access to browse files and only use bookmarks. While other users may have access to browse any internal host using http, https, CIFS or ftp. In addition, users may be restricted to read only access for browsing or have upload and download access.

Client access is also determined by group privileges. A user must have SSL Browser capability in order to have Client access. The SSL Client is downloaded via the SSL Browser interface for each user.

Requirements

- GB-OS version 6.1 or higher

Firewall Configuration

SSL has seven (7) configuration sections:

1. Creating a Certificate Authority (CA) Certificate
2. Defining Bookmarks
3. Defining Groups
4. Defining Users
5. Defining Remote Access Preferences
6. Enabling the SSL Client
7. Creating Security Policies for SSL Client Access

Creating a Certificate Authority (CA) Certificate

Create a Certificate Authority (CA) Certificate to sign all other Certificates.

1. Navigate to **Configure>VPN>Certificates**.
2. Set the section to default. The firewall will automatically generate a new CA and Remote Administration certificate, and assign them as CA, Remote Administration, and VPN certificate. Below is an example of the CA, Remote Administration, and VPN certificates.

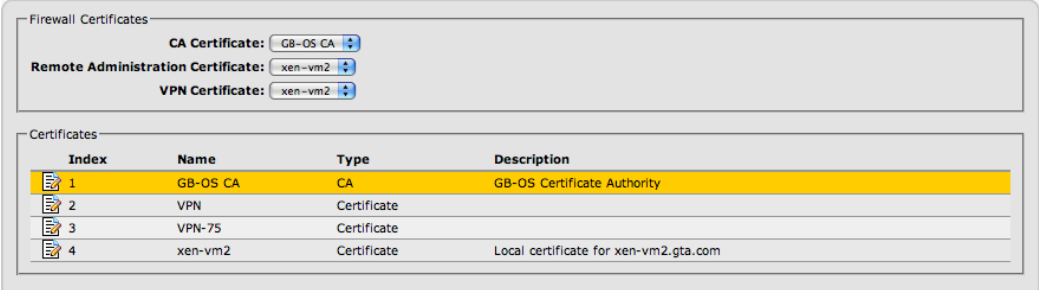

Figure 1: *Creating Certificates*

Note

See the *GB-OS Users Guide* for more information on creating firewall certificates.

Defining Bookmarks

Bookmarks are shortcuts for users when logged in to the SSL Browser.

1. Navigate to **Configure>Objects>Bookmark Objects.**
2. Edit an existing bookmark or create a new one.

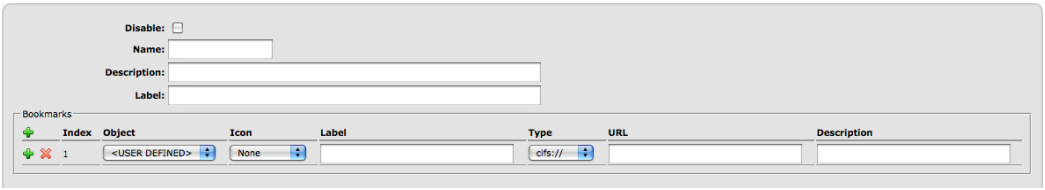

Figure 2: *Defining Bookmarks*

Table 1: Bookmarks

Field	Default	Description
Disable	Unchecked	Disables bookmarks.
Name	Blank	Object name referenced in groups section and in other bookmarks.
Description	Blank	Brief description of the bookmark object's purpose.
Label	Blank	Bookmark label displayed to the user when logged into the SSL Browser interface.

Table 1: Bookmarks		
Field	**Default**	**Description**
Bookmarks		
Object	User Defined	Set to <user define> to define the bookmark or reference other bookmarks.
Icon	None	Select an icon to represent the bookmark object. Options include None, Browser, Document, Email, Folder, Network and Web.
Label	Blank	Link label as displayed to the user in the SSL Browser.
Type	cifs	Select the protocol to be used to connect to the URL. Specify http, https, ftp, or cifs.
URL	Blank	IP address or host name.
Description	Blank	User defined. Briefly description of the bookmark's purpose.

Defining a Group for the SSL Client

1. Navigate to **Configure>Accounts>Groups**.
2. Create a NEW group, or edit an existing group.
3. Enable SSL.
4. Enable BOOKMARKS ONLY and READ ONLY as applicable. BOOKMARKS ONLY will authorize users to only access configured bookmarks and will not allow browsing of internal networks. READ ONLY will only allow users to download files, disabling the upload feature.
5. Select the group bookmarks authorized for the user in the BOOKMARKS pulldown.
6. Enable the CLIENT to authorize SSL Client access for the configured group.

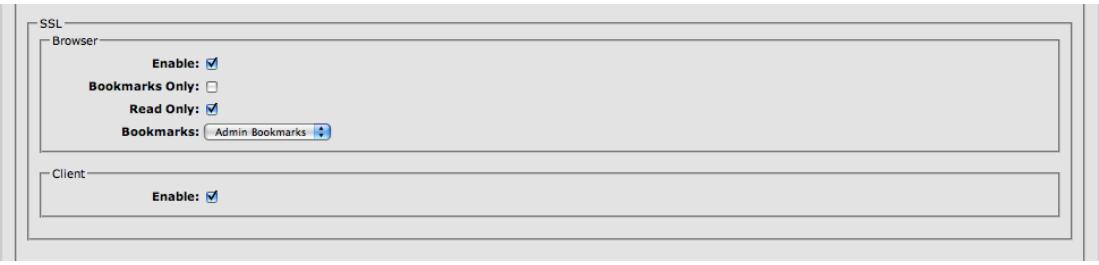

Figure 3: *Defining a Group*

Table 2: Defining Groups		
Field	**Default**	**Description**
SSL		
Browser		
Enable	Unchecked	Enables SSL Browser access.
Bookmarks Only	Checked	Displays only Bookmarks for SSL Browser access.
Read Only	Checked	Read only access. Users can only download files via the browser.
Bookmarks	Not Selected	Displays the defined bookmarks for the group.
Client		
Enable	Unchecked	Allows SSL Client access.

Defining a User on the Firewall

1. Navigate to **Configure>Accounts>Users**
2. Select the SSL group previously configured.
3. Assign the SSL certificate previously defined or generate a new certificate.
4. Enter the password the user will use to login to both SSL Browser, and SSL Client.

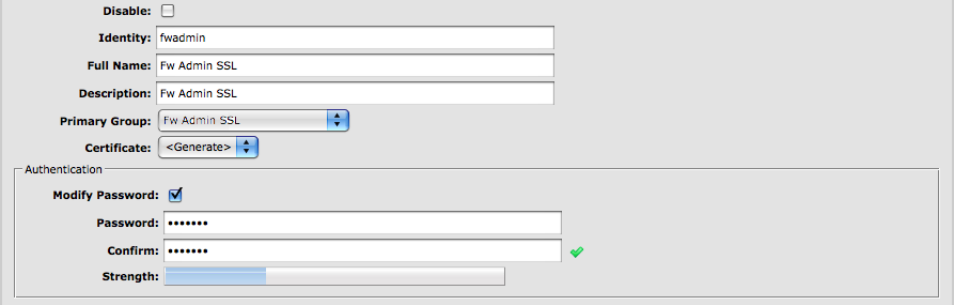

Figure 4: *Defining a User*

Note

User certificates used for the SSL Client MUST be signed by a CA.

Table 3: Defining Users

Field	Default	Description
Disable	Unchecked	Disables the user.
Identity	Blank	The name used to authenticate the connecting user. This must be a unique name. Minimum of 3 characters.
Full Name	Blank	Name to identify the user. Minimum of three (3) characters.
Description	Blank	User defined description for the user.
Primary Group	Users	Primary group for specifying the type of access allowed for SSL. Also used in security policies for authentication.
Certificate	Generate	Generate automatically creates a user certificate based on user definition, or select a predefined certificate.
Authentication		
Password	Blank	Password for user to authenticate with the firewall. Minimum of four (4) characters.

Defining Remote Access Preferences

1. Navigate to **Configure>VPN>Remote Access>Preferences**
2. Enable an ALTERNATIVE PORT. By default, the SSL Browser is listening on TCP port 443. Administrators may choose to allow browser access on an alternate port and restrict 443 to firewall administrators only, or change the Administrator port.
3. Select and enable authentication methods LDAPv3 or RADIUS.
4. Select the encryption level to be used.
5. Define the time out range for the SSL Browser. Valid time out range is 5 - 1440 minutes.
6. Select the desired use of the virtual keyboard for logins. The virtual keyboard can be required, enabled to use or not use, or disabled and turned off.
7. Enable automatic policies as desired and select the zone and source address for connections.
8. Optionally, create a customized login screen for the Remote Access Portal — displaying a title, logo and disclaimer message which will appear upon login.

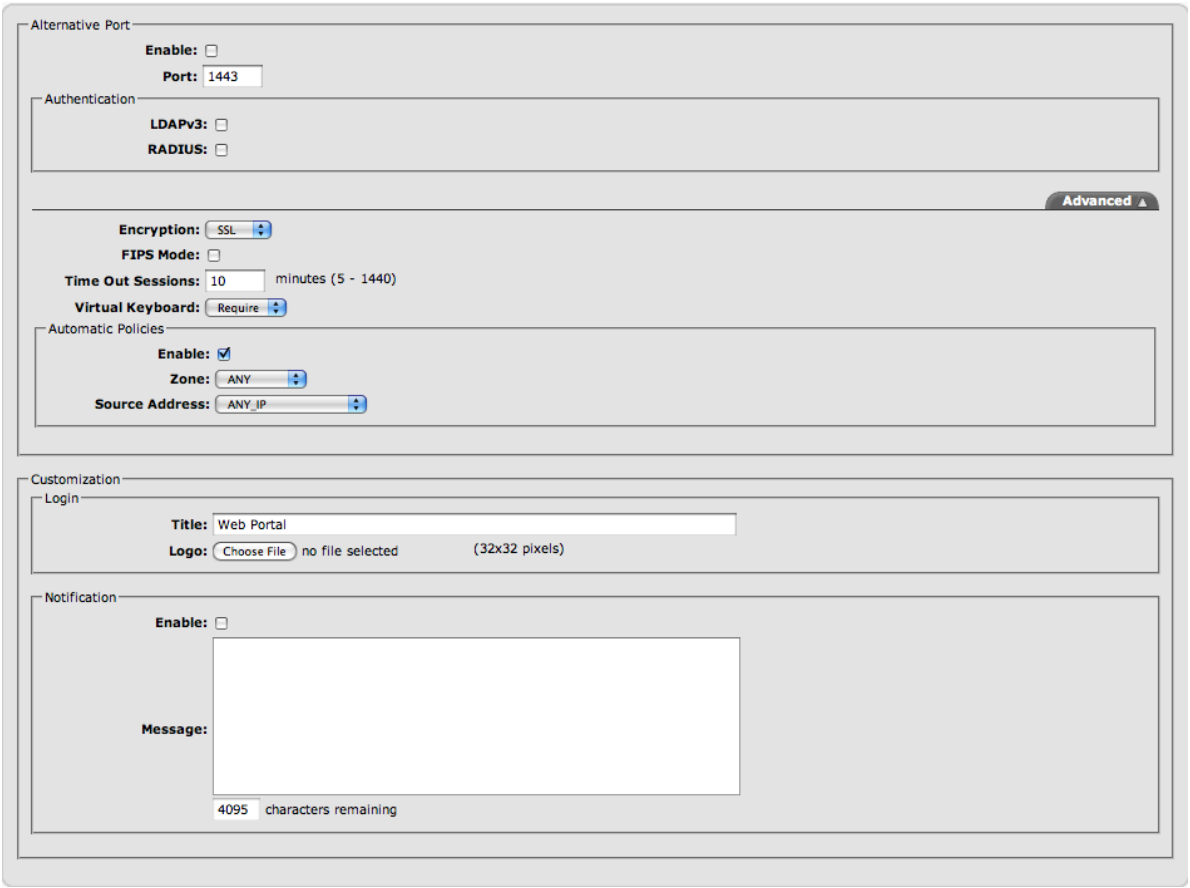

Figure 5: *Enabling the SSL Browser*

Table 4: Remote Access Preferences

Field	Default	Description
Alternative Port		
Enable	Unchecked	Starts the SSL Browser service.
Port	443	Port through which browser access will be allowed. Default is TCP port 1443.
Authentication		
LDAP	Unchecked	Enables LDAP users.
RADIUS	Unchecked	Enables RADIUS users.

Table 4: Remote Access Preferences		
Field	**Default**	**Description**
Advanced		
Encryption	High	Level of encryption to be used. See table below for more information.
FIPS Mode	Unchecked	Enables FIPS mode for Remote Access. When enabled, SSL is forced.
Time out Sessions	10 minutes	Define the time out range. Valid range is 5 - 1440 minutes.
Virtual Keyboard	Require	Require: requires users to use the virtual keyboard for logins to the browser interface; Enable: allows users to use or not use the virtual keyboard; Disable: turn off the virtual keyboard
Automatic Policies		
Enable	Checked	Allows the firewall to automatically create policies for SSL Browser access.
Zone	ANY	Specifies the Zone which will be allowed to connect. Options are External, Protected, and PSN.
Source Address	ANY_IP	Specifies the source address allowed to connect.
Customization		
Login		
Title	User Define	Enter a customized title for the SSL Browser.
Logo	User Define	Upload a logo to be displayed on the SSL login. Images must be 32 x 32 pixels and 100 KB or less. JPEG, PNG, or GIF formats are accepted.
Disclaimer		
Enable	Unchecked	Enable the disclaimer message to appear upon login.
Message	User Define	Enter a disclaimer, note or welcome to appear when users login to the SSL Browser.
Characters Remaining	Uneditable	Character count field detailing the number of characters remaining for the disclaimer message. Maximum characters is 4095.

Table 5: Encryption Levels		
Level	**Key Strength**	**Description**
None	N/A	Disables SSL encryption
All	N/A	Accepts low, medium and high levels of encryption
Low	40-, 56-, 64-bit	A low level SSL encryption
Medium	128-bit	A medium level SSL encryption
High	168-bit	A high level SSL encryption

Enabling the SSL Client

1. Navigate to **Configure>VPN>Remote Access>SSL Client**
2. Check the ENABLE check box to enable the SSL Client Service
3. For ACCESSIBLE NETWORK, select an object or enter a user defined address for the networks accessible through the SSL Client Tunnel
4. For CLIENT DHCP NETWORK, select an object or enter a user defined address for the network that will be used as the Client DHCP Address Pool.

Note

The first address in the range will be reserved and assigned to the firewall as `tun0` interface.

5. Configure domain, DNS servers and WINS servers that will be assigned to the client.

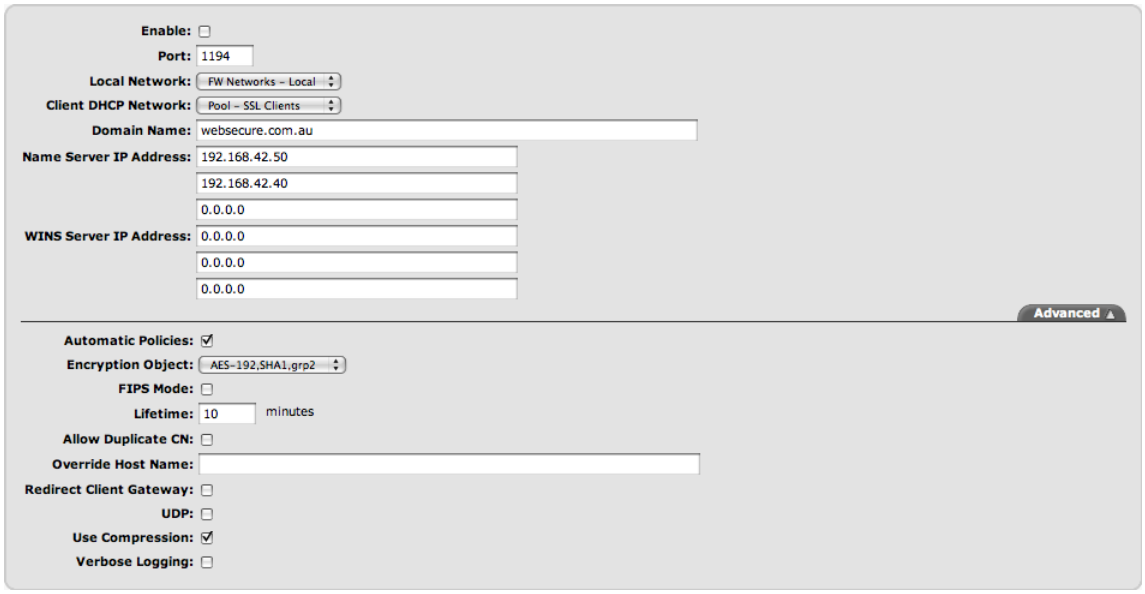

Figure 6: *Enabling the SSL Client*

Table 6: SSL Client

Field	Default	Description
Enable	Enabled	Starts the SSL Client Service.
Port	1194	Port for SSL Client access.
Accessible Networks	FW Network - Local	Default Local Protected Networks.
Client DHCP Network	Pool - SSL	Default DHCP range of 192.168.72.0/24
Domain	User Define	Domain assigned to SSL Client.
Name Server IP Address	User Define	DNS server(s) pushed to SSL Client.
WINS Server IP Address	User Define	WINS server pushed to SSL Client.
Advanced		
Automatic Policies	Enabled	Creates an auto policy based on SSL port.
Encryption Objects	AES-192, sha1, grp2	Encryption used for SSL.
FIPS Mode	Unchecked	Enables FIPS mode for SSL Clients. If FIPS mode is enabled, the firewall only supports 3DES and AES Encryption, and SHA Hash Algorithms.

Table 6: SSL Client		
Field	**Default**	**Description**
Lifetime	480 minutes	Re-key time, in minutes.
Allow Duplicate CN	Unchecked	Allows duplicate certificates.
Override Host Name	Blank	Allows an administrator to override default firewall host name, which is configured in Network Settings. Entry can be an IP address or a fully qualified host name.
Redirect Client Gateway	Unchecked	Force all client connections via VPN.
UDP	Unchecked	Use UDP instead of TCP for SSL connection.
Use Compression	Checked	Disable to not use compression.
Verbose Logging	Unchecked	Increase SSL logging for debug purposes.

Note

Changes to the SSL Client configuration for port, encryption, override host name, and compression will require new client downloads.

Creating Security Policies for SSL Client Access

1. Navigate to **Configure>Security Policies>Policy Editor>VPN>SSL Client**.
2. By default, all in and out is allowed and access to the firewall administration interface using `https` is denied. Pings to the firewall are also allowed.
3. The default SSL Client policies are displayed below. It is recommended that SSL policies are configured based on your corporate security policy.

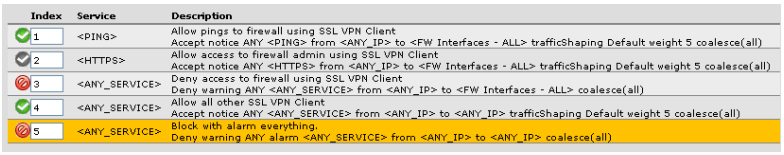

Figure 7: *Creating Security Policies*

Log Messages

Firewall

Licenses Exceeded messages OpenVPN client connections. Default user licenses is 2 users, additional user licenses may be requested via GTA sales.

```
Sep 16 14:33:27 pri=3 msg="OpenVPN: MULTI: new incoming connection would exceed
maximum number of clients (2)" type=mgmt,vpn
```

Close Tunnel OpenVPN:

```
Sep 16 14:33:20 pri=5 msg="Close inbound, openVPN" proto=53/udp src=192.168.72.3
srcport=48517 dst=192.168.71.9 dstport=53 rule=4 duration=22 sent=59 rcvd=130
pkts _ sent=1 pkts _ rcvd=1
```

Block Message Remote Access (Interface tun0 is SSL Client interface):

```
Sep 16 14:23:17 pri=4 pol _ type=RAP pol _ action=block count=12 msg="Block
RAP" duration=30 rule=6 proto=443/tcp src=192.168.72.2 srcport="44323 (3),
44328 (3), 44362 (3), 44363 (3)" dst=192.168.71.254 dstport=443 interface="tun0"
attribute="alarm" flags=0x2
```

User Login Failure:

```
Sep 16 15:59:50 pri=3 msg="OpenVPN: 192.168.73.1:55642 TLS Auth Error: Auth Username/
Password verification failed for peer" type=mgmt,vpn
```

Compression is disabled on firewall and not in the client configuration. Compression is enabled or disabled in **Configure>VPN>SSL Client>Advanced** in firewall interface. The use compression option comp-lzo sets compression for the client.

```
Sep 16 16:32:27 pri=4 msg="OpenVPN: 192.168.73.1:59205 WARNING: 'comp-lzo' is present
in remote config but missing in local config, remote='comp-lzo'" type=mgmt,vpn
```

Compression is enabled on firewall and not in the client configuration. Compression is enabled or disabled in **Configure>VPN>SSL Client>Advanced** in firewall interface. The use compression option comp-lzo sets compression for the client.

```
Sep 16 16:40:21 pri=4 msg="OpenVPN: 192.168.73.1:60094 WARNING: 'comp-lzo' is present
in local config but missing in remote config, local='comp-lzo'" type=mgmt,vpn
```

Firewall and client have mis matched configuration options for Encryption. This is configured in **Configure>VPN>SSL Client>Advanced**, or by setting cipher option on the client.

```
Sep 16 16:47:52 pri=4 msg="OpenVPN: 192.168.73.1:60939 WARNING: 'cipher' is
used inconsistently, local='cipher AES-128-CBC', remote='cipher AES-192-CBC'"
type=mgmt,vpn

Sep 16 16:47:52 pri=4 msg="OpenVPN: 192.168.73.1:60939 WARNING: 'keysize' is used
inconsistently, local='keysize 128', remote='keysize 192'" type=mgmt,vpn
```

Remote server the proxy is attempting to connect to has an invalid certificate.

```
Sep 21 15:21:41 pri=3 msg="SSL: SSL certificate problem, verify that the
CA cert is OK. Details:\\0Aerror:14090086:SSL routines:SSL3 _ GET _ SERVER _
CERTIFICATE:certificate verify failed" type=mgmt proto=http/tcp user="support@
gta.com" src=192.168.73.1 srcport=4869 dst=192.168.73.2 dstport=1443 duration=26
```

SSL Client

User Login Failure: Verify the login credentials.

```
Wed Sep 16 15:59:53 2009 AUTH: Received AUTH _ FAILED control message
```

Compression is enabled on firewall and not in the client configuration. Compression is enabled or disabled in **Configure>VPN>Remote Access>SSL Client>Advanced** in firewall interface. The use compression option comp-lzo sets compression for the client.

```
Wed Sep 16 16:40:22 2009 WARNING: 'comp-lzo' is present in remote config but
missing in local config, remote='comp-lzo'
```

Compression is disabled on firewall and not in the client configuration. Compression is enabled or disabled in **Configure>VPN>Remote Access>SSL Client>Advanced** in firewall interface. The use compression option comp-lzo sets compression for the client.

```
Wed Sep 16 16:46:20 2009 WARNING: 'comp-lzo' is present in local config but missing
in remote config, local='comp-lzo'
```

Firewall and client have mis matched configuration options for Encryption. This is configured in **Configure>VPN>Remote Access>SSL Client>Advanced**, or by setting cipher option on the client.

```
Wed Sep 16 16:50:22 2009 WARNING: 'cipher' is used inconsistently, local='cipher
AES-192-CBC', remote='cipher DES-EDE3-CBC'
```

Client is unable to resolve the address of the firewall. Confirm firewall has fully qualified host name configured in **Network>Interface Settings>Host** name field. The host name resolves correctly.

```
Fri Sep 18 08:24:24 2009 RESOLVE: Cannot resolve host address: dbtest.gta.com:
[HOST _ NOT _ FOUND] The specified host is unknown.
```

SSL Client is unable to use the Self Signed Certificates. To resolve this issue you will need to make sure that both the Client and Firewall VPN Certificates have been signed by a CA. Certificates can be managed in **Configure>VPN>Certificates**.

```
Wed Nov 18 14:43:46 2009 VERIFY ERROR: depth=0, error=self signed certificate: /
emailAddress=support@gta.com/O=GTA/C=US/CN=FW _ VPN _ CERTIFICATE
```

Troubleshooting

If your question is not answered below, please contact GTA Support for more information.

Q: When attempting to download the client I get the message, "Error: Unable to create SSL Client configuration bundle."

Check that the OVERRIDE HOST NAME in **Configure>VPN>Remote Access>SSL Client** is a single IP or name and not a network.

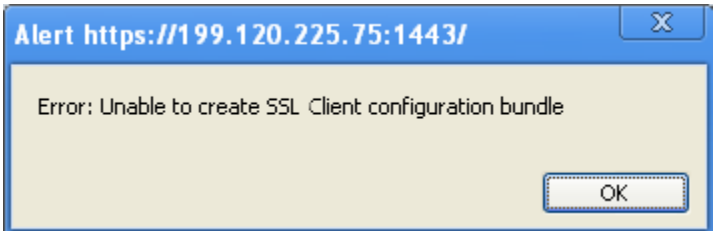

Figure 1: *Client Error Message*

Q: When attempting to download the configuration file, a user gets the message "Error: Unable to create SSL Client configuration bundle."

User has a self signed certificate or the firewall certificate is self signed. Re-create the firewall VPN, users or both certificates using the firewall CA. See the *GB-OS Users Guide* for more information on certificate maintenance.

Q: The firewall logs the following message when users attempt to download the configuration bundle:

```
Mar 12 15:57:26 pri=3 msg="SSL: VPN certificate 'VPN', must be signed by
the CA certificate 'gb-2000x-10-10-1 CA' "type=mgmt user="gtauser"
src=199.201.225.20 srcport=55193 dst=199.120.225.80 dstport=1443 duration=5
Mar 12 15:57:26 pri=3 msg="SSL: User certificate 'gtauser', must be signed
by the CA certificate 'gb-2000x-10-10-1 CA' "type=mgmt user="gtauser"
src=199.201.225.20 srcport=55193 dst=199.120.225.80 dstport=1443 duration=5
```

User has a self signed certificate or the firewall certificate is self signed. Re-create the firewall VPN, users or both certificates using the firewall CA. See the *GB-OS Users Guide* for more information on certificate maintenance.

Copyright

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/).

All other products are trademarks of their respective companies.

Global Technology Associates, Inc.

3361 Rouse Rd, Suite 240• Orlando, FL 32817 USA

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