

Serial-to-WiFi AT Commands Configuration Examples

To Create HTTP, HTTPS, and EAP Connections

User Guide

GS2K-HTTP-EAP-UG-001213

Modules

GS2011M and GS2100M

GainSpan[®] 802.11b/g/n Ultra-Low Power Wi-Fi[®] Series Modules

Copyright Statement	<p>This GainSpan manual is owned by GainSpan or its licensors and protected by U.S. and international copyright laws, conventions, and treaties. Your right to use this manual is subject to limitations and restrictions imposed by applicable licenses and copyright laws. Unauthorized reproduction, modification, distribution, display or other use of this manual may result in criminal and civil penalties.</p> <p>GainSpan assumes no liability whatsoever, and disclaims any express or implied warranty, relating to sale and/or use of GainSpan products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. GainSpan products are not authorized for use as critical components in medical, lifesaving, or life-sustaining applications</p> <p>GainSpan may make changes to specifications and product descriptions at any time, without notice.</p>
Trademark	<p>GainSpan is a registered trademark of GainSpan Corporation. All rights reserved. Other names and brands may be claimed as the property of others.</p>
Contact Information	<p>In an effort to improve the quality of this document, please notify GainSpan Technical Assistance at 1.408.627.6500 in North America or +91 80 42526503 outside North America .</p>

Table of Contents

Chapter 1 HTTP Examples	15
1.1 Requirements	15
1.2 Installing Apache Server	15
1.2.1 Install Apache Server in Windows	16
1.2.2 Run Apache Web Server	17
1.3 HTTP GET Examples	22
1.3.1 HTTP GET on Local Apache Server	22
1.3.2 HTTP GET on GainSpan.com	24
1.3.2.1 HTTP GET on Gainspan.com Tera Term Output	25
1.4 HTTP POST Examples	27
1.4.1 HTTP POST on Local Apache Server	27
Chapter 2 HTTPS Examples	29
2.1 Requirements	29
2.2 Installing Apache Server	29
2.2.1 Install Apache Server in Windows	30
2.2.2 Run Apache Web Server	31
2.2.3 HTTPS Server Configuration	36
2.2.3.1 How To Install OpenSSL	36
2.2.4 Generating Certificates	39
2.2.4.1 Creating Own Certificate Authority	40
2.2.4.2 Generating Server Certificate	42
2.2.4.3 Generating Client Certificate	45
2.3 HTTPS GET Example	48
2.4 HTTPS POST Example	51
2.5 Using SSLOPEN Command	53
2.5.1 Starting a SSL Server	53
2.5.2 Configuring GS Node as HTTPS Client (One-way Authentication)	54
2.5.3 Configuring GainSpan Node as HTTPS Client (Mutual Authentication)	56
2.5.4 HTTPS POST Using AT+SSLOPEN Command	58
Chapter 3 EAP Examples	61
3.1 PEAP Without Certificate	61
3.2 PEAP With Certificate	63
3.3 EAP-TLS	66

- This page intentionally left blank -

About This Manual

This manual provides GS2000 based module evaluation kit examples for using Serial-to-WiFi AT commands to create HTTP, HTTPS, and EAP connections.

Refer to the following sections:

- [Revision History, page 5](#)
- [Audience, page 5](#)
- [Standards, page 5](#)
- [Documentation Conventions, page 6](#)
- [Documentation, page 9](#)
- [References, page 11](#)
- [Contacting GainSpan Technical Support, page 12](#)
- [Returning Products to GainSpan, page 13](#)
- [Accessing the GainSpan Portal, page 14](#)

Revision History

This version of the *GainSpan GS2000 Based Module Configuration Examples User Guide (for using Serial-WiFi AT Commands to Create HTTP, HTTPS, and EAP Connections)* contains the following new information listed in [Table 1, page 5](#).

Table 1 Revision History

Version	Date	Remarks
1.0	January 2014	Initial Release

Audience

This manual is designed to setup, create, and run connection examples for HTTP, HTTPS, and EAP.

Standards

The standards that are supported by the GainSpan GS module supports IEEE 802.11b/g/n.

Documentation Conventions

This manual uses the following text and syntax conventions:

- Special text fonts represent particular commands, keywords, variables, or window sessions
- Color text indicates cross-reference hyper links to supplemental information
- Command notation indicates commands, subcommands, or command elements

[Table 2, page 6](#), describes the text conventions used in this manual for software procedures that are explained using the AT command line interface.

Table 2 Document Text Conventions






Convention Type	Description
command syntax monospaced font	This monospaced font represents command strings entered on a command line and sample source code. AT XXXX
Proportional font description	Gives specific details about a parameter. <Data> DATA
UPPERCASE Variable parameter	Indicates user input. Enter a value according to the descriptions that follow. Each uppercased token expands into one or more other token.
lowercase Keyword parameter	Indicates keywords. Enter values exactly as shown in the command description.
[] Square brackets	Enclose optional parameters. Choose none; or select one or more an unlimited number of times each. Do not enter brackets as part of any command. [parm1 parm2 parm3]
? Question mark	Used with the square brackets to limit the immediately following token to one occurrence.
<ESC> Escape sequence	Each escape sequence <ESC> starts with the ASCII character 27 (0x1B). This is equivalent to the Escape key. <ESC>C
<CR> Carriage return	Each command is terminated by a carriage return.
<LF> Line feed	Each command is terminated by a line feed.
<CR> <LF> Carriage return Line feed	Each response is started with a carriage return and line feed with some exceptions.

Table 2 Document Text Conventions (Continued)

Convention Type	Description
<> Angle brackets	Enclose a numeric range, endpoints inclusive. Do not enter angle brackets as part of any command. <SSID>
= Equal sign	Separates the variable from explanatory text. Is entered as part of the command. PROCESSID = <CID>
. dot (period)	Allows the repetition of the element that immediately follows it multiple times. Do not enter as part of the command. .AA:NN can be expanded to 1:01 1:02 1:03.
A.B.C.D IP address	IPv4-style address. 10.0.11.123
X:X::X:X IPv6 IP address	IPv6-style address. 3ffe:506::1 Where the :: represents all 0x for those address components not explicitly given.
LINE End-to-line input token	Indicates user input of any string, including spaces. No other parameters may be entered after input for this token. string of words
WORD Single token	Indicates user input of any contiguous string (excluding spaces). singlewordnospaces

Table 3, page 8, describes the symbol conventions used in this manual for notification and important instructions.

Table 3 Symbol Conventions

Icon	Type	Description
	Note	Provides helpful suggestions needed in understanding a feature or references to material not available in the manual.
	Alert	Alerts you of potential damage to a program, device, or system or the loss of data or service.
	Caution	Cautions you about a situation that could result in minor or moderate bodily injury if not avoided.
	Warning	Warns you of a potential situation that could result in death or serious bodily injury if not avoided.
	Electro-Static Discharge (ESD)	Notifies you to take proper grounding precautions before handling a product.

Documentation

The GainSpan documentation suite listed in [Table 4, page 9](#) includes the part number, documentation name, and a description of the document. The documents are available from the GainSpan Portal. Refer to [Accessing the GainSpan Portal, page 14](#) for details.

Table 4 Documentation List

Part Number	Document Title	Description
GS2K-QS-001205	GainSpan GS2000 Based Module Kit Quick Start Guide	Provides an easy to follow guide on how to unpack and setup GainSpan GS2000 based module kit for the GS2011M and GS2100M modules.
GS2K-EVB-FP-UG-001206	GainSpan GS2000 Based Module Programming User Guide	Provides users steps to program the on-board Flash on the GainSpan GS2000 based modules using DOS or Graphical User Interface utility provided by GainSpan. The user guide uses the evaluation boards as a reference example board.
GS2K-SMP-EXP-UG-001207	GainSpan GS2000 Based Module Sample Examples for using Serial-to-WiFi AT Commands to Create TCP or UDP Connection User Guide	Provides an easy to follow instructions on how to setup, create, and run connection examples for UDP client/server and TCP client/server. This manual also provides instructions for provisioning the board, setting up Limited AP mode, and WiFi Protected Setup (WPS), and Web provisioning over Ad-hoc.
GS-S2W-APP-PRG-RG-001208	GainSpan Serial-to-WiFi Adapter Application Programmer Reference Guide	Provides a complete listing of AT serial commands, including configuration examples for initiating, maintaining, and evaluating GainSpan WiFi series modules.
GS2K-SDK-DB-UG-001209	GS2000 Based Module Software Development Kit and Debugging User Guide	This manual provides SDK user installation instructions, IAR IDE workbench application, and I-Jet hardware used for JTAG Serial-to-WiFi (S2W) and TLS application development and debugging.
GS2K-EVB-HW-UG-001210	GainSpan GS2000 Based Module Evaluation Board Hardware User Guide.	Provides instructions on how to setup and use the GS2000 based module evaluation board along with component description, jumper settings, board specifications, and pinouts.

Table 4 Documentation List (Continued)

Part Number	Document Title	Description
GS2011M-DS-001211	GainSpan GS2011M Low Power WiFi Module Data Sheet	Provides information to help WiFi system designers to build systems using GainSpan GS2011M module and develop wireless applications.
GS2100M-DS-001212	GainSpan GS2100M Low Power WiFi Module Data Sheet	Provides information to help WiFi system designers to build systems using GainSpan GS2100M module and develop wireless applications.
GS2K-HTTP-EAP-UG-001213	GainSpan GS2000 Based Module Configuration Examples for using Serial-to-WiFi AT Commands to Create HTTP, HTTPS, and EAP Connection User Guide	Provides an easy to follow instructions on how to setup, create, and run connection examples for HTTP, HTTPS, and EAP.
GS2011MxxS-DS-001214	GainSpan GS2011MxxS Low Power WiFi Module Data Sheet	Provides information to help WiFi system designers to build systems using GainSpan GS2011MxxS module and develop wireless applications.
GS2K-SDK-BLDR-UG-001223	GainSpan GS2000 Based Module Software Developer Kit (SDK) Builder User Guide	Allows OEMs and system developers to configure and generate custom firmware binary images for GainSpan low power embedded GS2000 based WiFi modules. The SDK Builder supports the GainSpan GEPS software released, including the corresponding WLAN firmware.
GS2K-SDK-QS-001225	GainSpan GS2000 Based Module Software Development Kit Quick Start Guide	Provides an easy to follow guide that will walk you through easy steps to setup, evaluation, develop, and debug the full capabilities and features of the GS2011M or GS2100M embedded platform software.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments by logging into [GainSpan Support Portal](#). If you are using e-mail, be sure to include the following information with your comments:

- Document name
- URL or page number
- Hardware release version (if applicable)
- Software release version (if applicable)

References

The GainSpan references listed in [Table 5, page 11](#) are available on the GainSpan Portal. Refer to [Accessing the GainSpan Portal, page 14](#) for details.

Table 5 Other Documents and References

Title	Description
Schematics	GS2000 Based Module Evaluation Board schematics supporting: <ul style="list-style-type: none">• GS2011M• GS2100M
Module Firmware and Programming Utilities	<ul style="list-style-type: none">• Serial-to-WiFi (S2W) based firmware• Temperature and Light Sensor (TLS) based firmware<ul style="list-style-type: none">– For use with GS2011M EVK only• Firmware Release Notes• GSFlashprogram utility for programming the modules
Smart Phone Applications	<ul style="list-style-type: none">• Smart Phone applications for iOS and Android to evaluate and demonstrate the Temperature and Light Sensor (TLS) firmware.<ul style="list-style-type: none">– For use with GS2011M EVK only
Software Utilities	Serial terminal program to evaluate and demonstrate Serial-to-WiFi (S2W) applications

Contacting GainSpan Technical Support

Use the information listed in [Table 6, page 12](#), to contact the GainSpan Technical Support.

Table 6 GainSpan Technical Support Contact Information

North America	1 (408) 627-6500 - techsupport@gainspan.com
Outside North America	Europe: EUsupport@gainspan.com China: Chinasupport@gainspan.com Asia: Asiasupport@gainspan.com
Postal Address	GainSpan Corporation 3590 North First Street Suite 300 San Jose, CA 95134 U.S.A.

For more Technical Support information or assistance, perform the following steps:

1. Point your browser to <http://www.gainspan.com>.
2. Click **Contact**, and click **Request Support**.
3. Log in using your customer **Email** and **Password**.
4. Select the **Location**.
5. Select **Support Question** tab.
6. Select **Add New Question**.
7. Enter your technical support question, product information, and a brief description.

The following information is displayed:

- Telephone number contact information by region
- Links to customer profile, dashboard, and account information
- Links to product technical documentation
- Links to PDFs of support policies

Returning Products to GainSpan

If a problem cannot be resolved by GainSpan technical support, a Return Material Authorization (RMA) is issued. This number is used to track the returned material at the factory and to return repaired or new components to the customer as needed.



NOTE: Do not return any components to GainSpan Corporation unless you have first obtained an RMA number. GainSpan reserves the right to refuse shipments that do not have an RMA. Refused shipments will be returned to the customer by collect freight.

For more information about return and repair policies, see the customer support web page at: <https://www.gainspan.com/secure/login>.

To return a hardware component:

1. Determine the part number and serial number of the component.
2. Obtain an RMA number from Sales/Distributor Representative.
3. Provide the following information in an e-mail or during the telephone call:
 - Part number and serial number of component
 - Your name, organization name, telephone number, and fax number
 - Description of the failure
4. The support representative validates your request and issues an RMA number for return of the components.
5. Pack the component for shipment.

Guidelines for Packing Components for Shipment

To pack and ship individual components:

- When you return components, make sure they are adequately protected with packing materials and packed so that the pieces are prevented from moving around inside the carton.
- Use the original shipping materials if they are available.
- Place individual components in electrostatic bags.
- Write the RMA number on the exterior of the box to ensure proper tracking.



CAUTION! Do not stack any of the components.

Accessing the GainSpan Portal

To find the latest version of GainSpan documentation supporting the GainSpan product release you are interested in, you can search the GainSpan Portal website by performing the following steps:



NOTE: *You must first contact GainSpan to set up an account, and obtain a customer user name and password before you can access the GainSpan Portal.*

1. Go to the [GainSpan Support Portal](#) website.
2. Log in using your customer **Email** and **Password**.
3. Click the **Getting Started** tab to view a Quick Start tutorial on how to use various features within the GainSpan Portal.
4. Click the **Actions** tab to buy, evaluate, or download GainSpan products.
5. Click on the **Documents** tab to search, download, and print GainSpan product documentation.
6. Click the **Software** tab to search and download the latest software versions.
7. Click the **Account History** tab to view customer account history.
8. Click the **Legal Documents** tab to view GainSpan Non-Disclosure Agreement (NDA).

Chapter 1 HTTP Examples

This chapter describes the Serial-to-WiFi procedures on how to setup, test, and evaluate HTTP connection examples on GainSpan® GS2011M and GS2100M.

- [Requirements, page 15](#)
- [Installing Apache Server, page 15](#)
- [HTTP GET Examples, page 22](#)
- [HTTP POST Examples, page 27](#)

1.1 Requirements

The Serial-to-WiFi application firmware binaries must be loaded onto the GainSpan GS2011M or GS2100M module. For details on how to install the firmware and binaries. Refer to *GainSpan Serial-to-WiFi Adapter Application Programmer Reference Guide*.

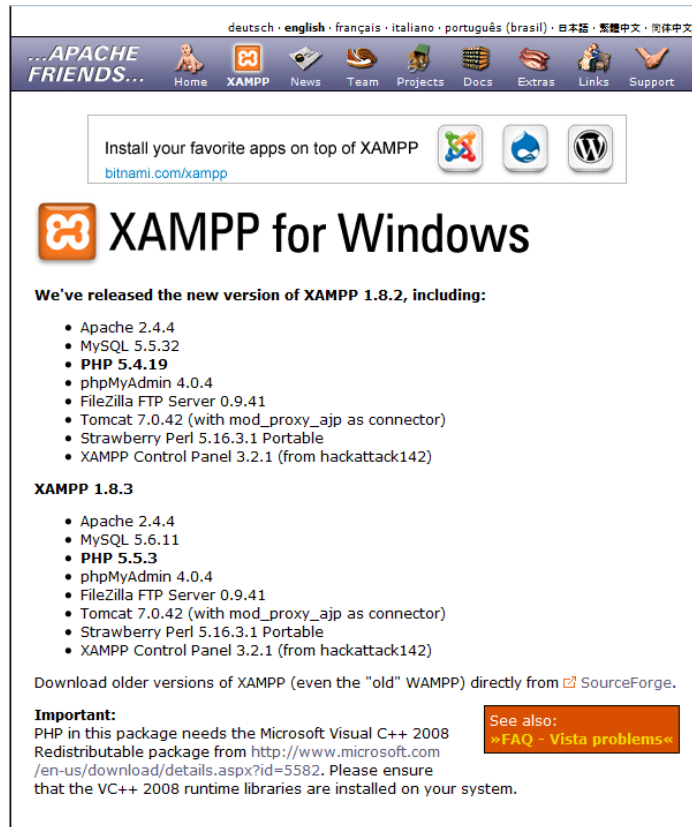
1.2 Installing Apache Server

This section provides instructions on how to install the Apache server in a Windows environment and provides several HTTP GET/POST examples using the Serial-to-WiFi application.

1.2.1 Install Apache Server in Windows

1. Open a Windows browser and download the XAMPP program from the <http://www.apachefriends.org/en/xampp-windows.html> (see Figure 1, page 16).

Figure 1 Download Apache Server Program



2. Run the setup file to install XAMPP. All the files would be extracted to **C:\xampp**.

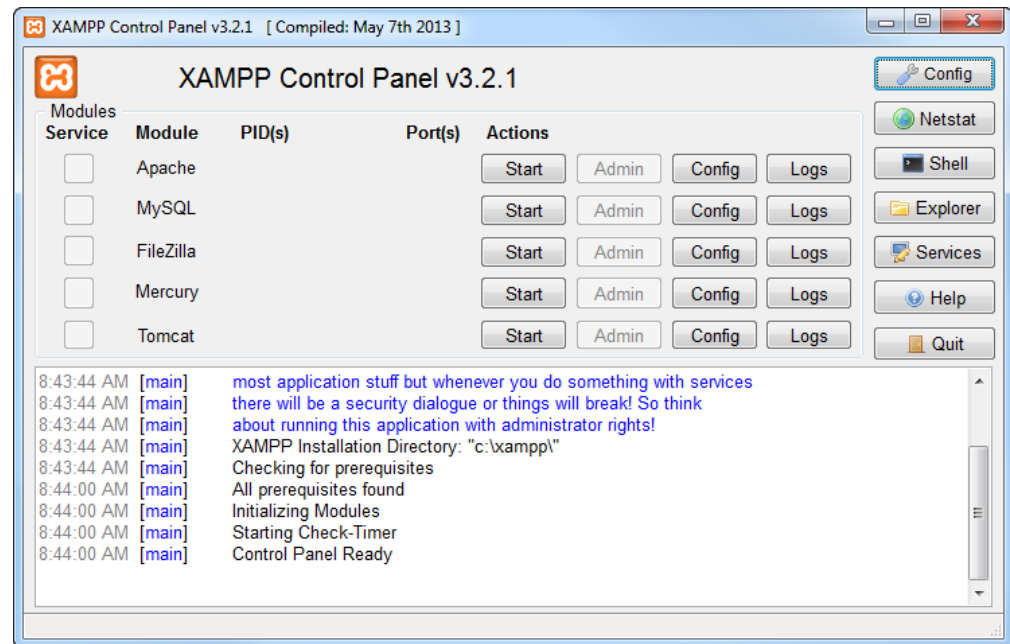


NOTE: Turn off your network connections and close all web browsers to avoid any error during the installation process.

1.2.2 Run Apache Web Server

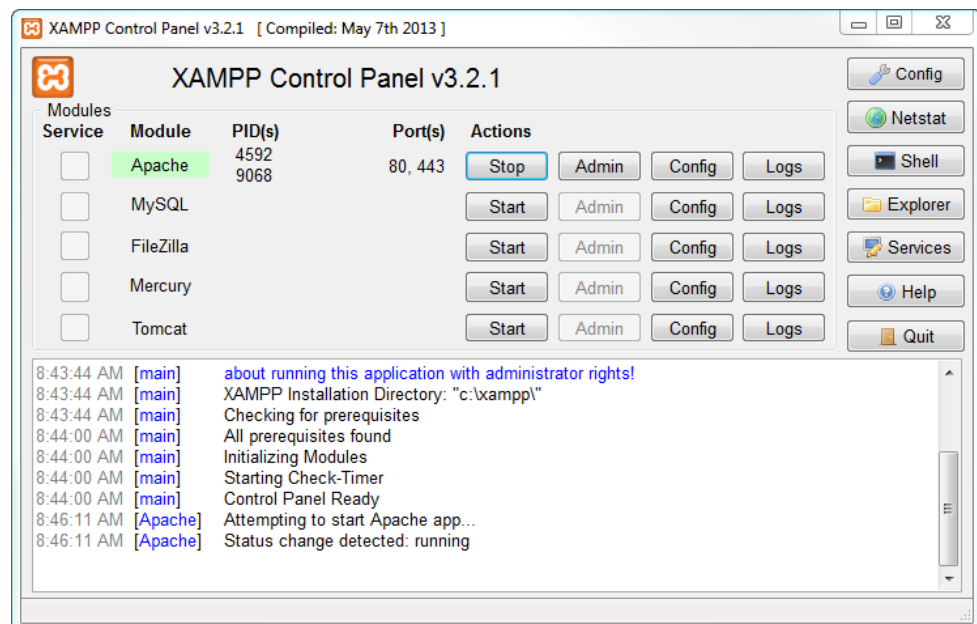
1. Browse to **C:\xampp** and download the latest XAMPP application. The XAMPP Control Panel will display (see Figure 2, page 17).

Figure 2 XAMPP Control Panel



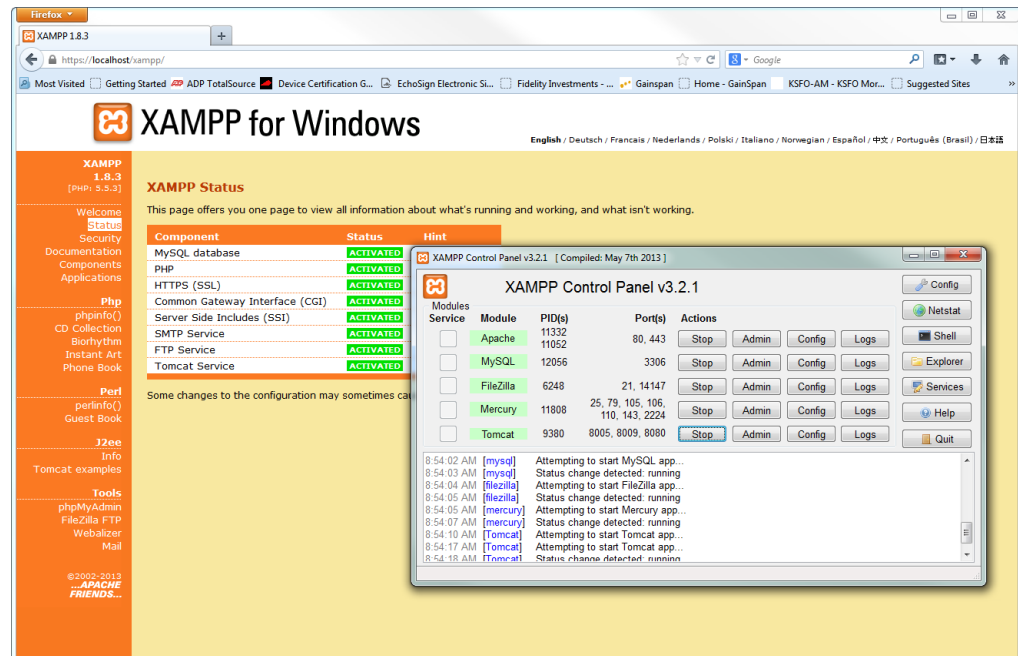
2. Click the **Start** button to start the Apache Web server (see Figure 3, page 17).

Figure 3 Starting the Apache Web Server



- After starting Apache, go to the web address: <http://localhost/> or <http://127.0.0.1/> in your browser. This will verify that the web server is running properly (see Figure 4, page 18).

Figure 4 Verifying Web Server Running



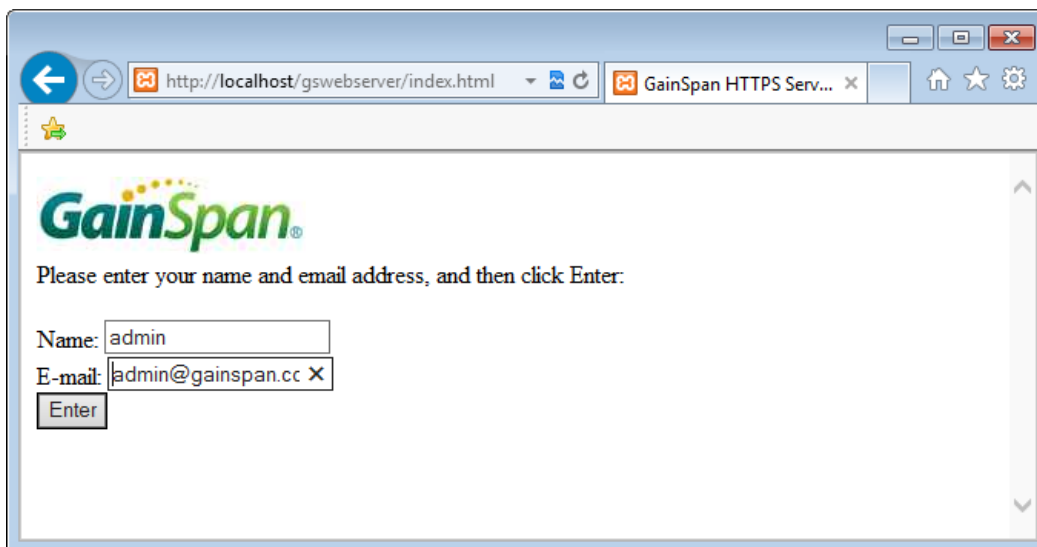
- GainSpan provides several example web pages for users to verify that the Apache Server is configured properly to access these web pages. Copy the GainSpan example: "gswebserver" folder into **C:\xampp\htdocs**.



NOTE: The "gswebserver" folder is bundled with under the SW Utilities folder in the EVK package.

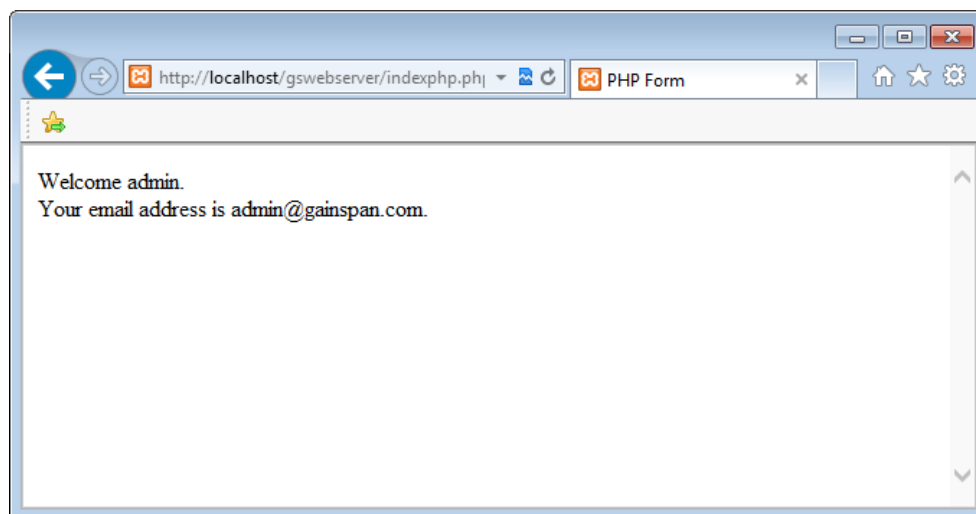
5. To test the **index.html** web page, open a web browser and go to one of the following addresses:
 - <http://localhost/gswebserver/index.html> or
 - <http://127.0.0.1/gswebserver/post.html>
6. Enter the **Name** and **Email address** details and click the **Enter** button (see Figure 5, page 19).

Figure 5 Enter Name and Email Address Information



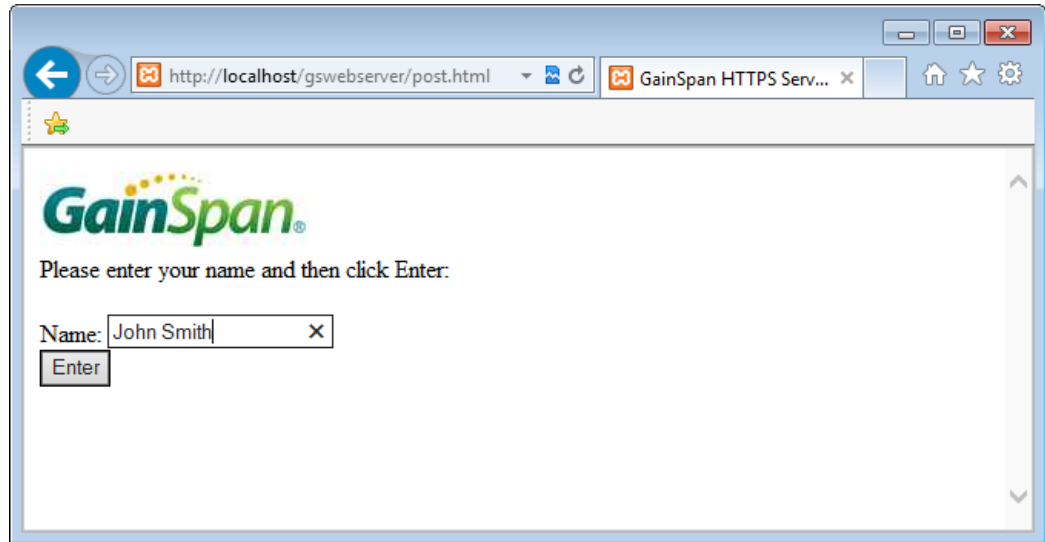
7. The GainSpan Name and Email address will display (see Figure 6, page 19).

Figure 6 GainSpan Server Email Address Displayed



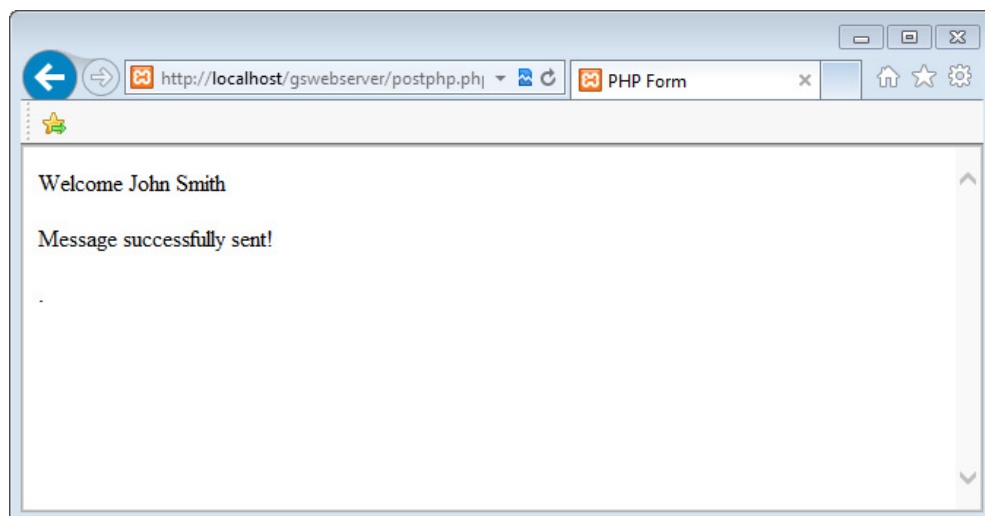
8. Test the **post.html** web page, by opening a web browser and go to one of the following addresses:
 - <http://localhost/gswebserver/post.html> or
 - <http://127.0.0.1/gswebserver/post.html>
9. Enter the **Name** and click the **Enter** button (see Figure 7, page 20).

Figure 7 Test the Post HTML Web Page



10. A welcome message will display (see [Figure 8, page 21](#)).

Figure 8 Message Sent



1.3 HTTP GET Examples

This section describes how to setup the HTTP GET using the Serial-to-WiFi application.

For a list of available HTTP Client Configuration commands, refer to the *GainSpan Serial-to-WiFi Adapter Application Programmer Reference Guide*.

1.3.1 HTTP GET on Local Apache Server

This example shows how to perform HTTP GET on a local Apache Server.

Before you begin, you will first need to setup a GainSpan Network (GSN) as HTTP Client and access the HTTP Server running on a Windows PC (see [Figure 9, page 23](#)).

1. Open a Tera Term window.
2. Associate with an Access Point (AP).

```
AT+NDHCP=1
OK
```

```
AT+WA=GainSpanDemo,,6
OK
```

3. Configure the HTTP parameters.

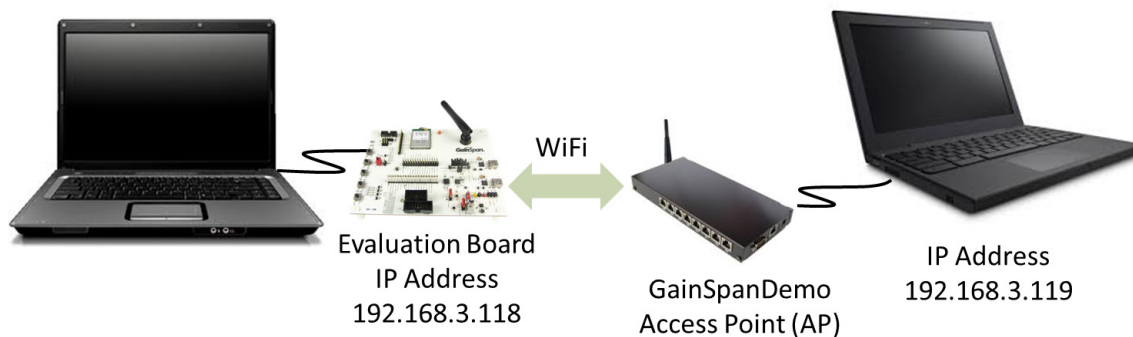
```
AT+HTTPCONF=20,Mozilla/5.0 (Windows; U; Windows NT 5.1;
en-US) AppleWebKit/534.7 (KHTML, like
Gecko) Chrome/7.0.517.44Safari/534.7
AT+HTTPCONF=7,application/x-www-form-urlencoded
AT+HTTPCONF=11,192.168.3.119
AT+HTTPCONF=3,keep-alive
```

4. Initiate HTTP client connection to the server.

```
AT+HTTPOPEN=192.168.3.119,80
```

5. Perform HTTP GET.

```
AT+HTTPSEND=0,1,10,/gswebserver/index.html
```

Figure 9 Example HTTP GET Configuration Setup**Figure 10 HTTP GET on Local Apache Server**

```

COM5:9600baud - Tera Term VT
File Edit Setup Control Window Help
Serial2WiFi APP
AT+NDHCP=1
OK
AT+WA=GainSpanDemo,,6
IP SubNet Gateway
192.168.3.118 255.255.255.0 192.168.3.1
OK
AT+HTTPCONF=20,Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.7 (KHTML, like Gecko)Chrome/7.0.517.44Safari/534.7
OK
AT+HTTPCONF=7,application/x-www-form-urlencoded
OK
AT+HTTPCONF=11,192.168.3.119
OK
AT+HTTPCONF=3,keep-alive
OK
AT+HTTPOPEN=192.168.3.119,80
0
OK
00449200 OK=0,1,100,/gswebserver/index.html
<html>
<head>
<title>GainSpan HTTPS Server GET Method</title>
<link rel="shortcut icon" href="/favicon.ico" />
</head>
<body>
<IMG src="logo.gif"> </br>
Please enter your name and email address, and then click Enter: </br>
<form action="index.php" method="get">
Name: <input type="text" name="name" /> </br>
E-mail: <input type="text" name="email" /> </br>
<input type="submit" value="Enter" />
</form>
</body>
</html>
OK

```

1.3.2 HTTP GET on GainSpan.com

This example shows how to perform an HTTP GET on GainSpan web site.

1. Disassociate from the current network.

```
AT+WD
```

2. Enable DHCP.

```
AT+NDHCP=1
```

3. Associate to a specified SSID, BSSID, and Channel.

```
AT+WA=<SSID>,<BSSID>,<CHANNEL>
```

```
AT+WA=GainSpanDemo,,6
```

4. Query DNS Server for the IP address of hostname URL.

```
AT+DNSLOOKUP=www.gainspan.com
```

5. Configure the HTTP header parameter “GSN_HTTP_HEADER_USER_AGENT”

```
AT+HTTPCONF=20,User-Agent: Mozilla/5.0 (Windows; U;  
Windows NT 5.1; en-US; rv:1.9.1.9) Gecko/20100315  
Firefox/3.5.9
```

6. Configure the HTTP header connection parameter “GSN_HTTP_HEADER_CONNECTION”. If it is a one-time HTTP GET, set the parameter to “close”.

```
AT+HTTPCONF=3,close
```

If user wants to do consecutive HTTP GET on the same CID, and given that a server do keep the connection open after HTTP GET is complete, set the parameter to “keep alive”

```
AT+HTTPCONF=3,keep-alive
```

7. Configure the HTTP header host parameter “GSN_HTTP_HEADER_HOST”

```
AT+HTTPCONF=11,23.23.181.241
```

8. Open HTTP client connection. This will return a unique CID.

```
AT+HTTPOPEN=23.23.181.241,80
```

9. Send HTTP request to the server using the CID from the previous step.

```
AT+HTTPSEND=<CID>,<type: get=1, post=3>,<timeout>,<page>[,size of the  
content]
```

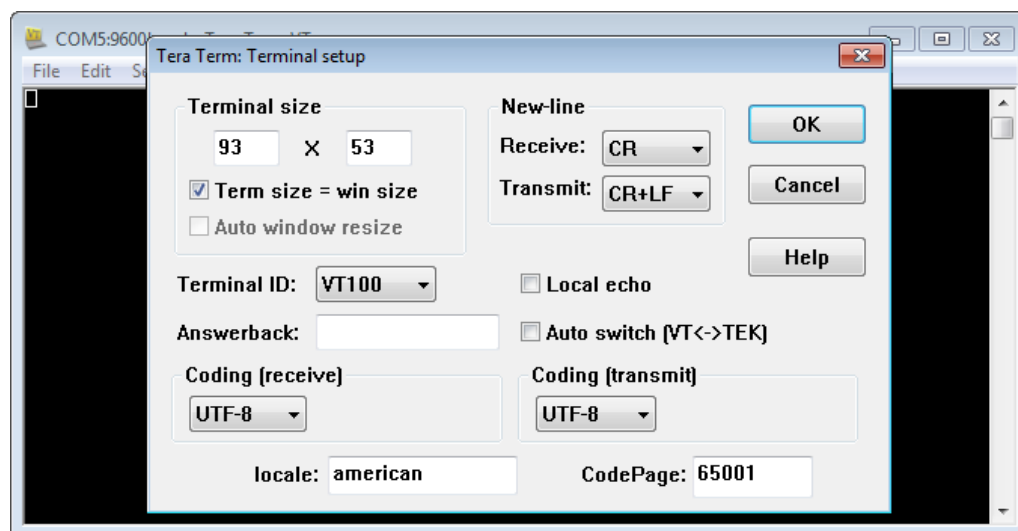
```
AT+HTTPSEND=1,1,10,/
```


1.3.2.1 HTTP GET on Gainspan.com Tera Term Output

This example shows how to perform an HTTP GET on GainSpan with Tera Term output.

1. Change the Tera Term New-line Transmit to: **CR+LF** (see [Figure 11, page 25](#)). Click the **OK** button.

Figure 11 Changing Tera Term Settings



2. Associate with AP.

```
AT+NDHCP=1
AT+WWPA=password
AT+WA=GainSpanDemo,,11
```

3. Start TCP Client to the GainSpan IP and port 80.

```
AT+NCTCP=192.168.3.117,80
```

4. Send data to remote server by using the <ESC>S sequence and the CID number.

- Enter the [ESC] key
- Enter the [S] key
- Enter the [CID number from Step 3]

5. Copy the highlighted text (the new line should also be copied), and paste it on Tera Term (via the Edit menu, choose Paste option).

```
GET/HTTP/1.1
User-Agent:Mozilla/5.0 (Windows;U;Windows NT
5.1;en-US;rv:1.9.1.0) Gecko/20100315
Firefox/3.5.9
Host:192.168.3.124:80
Accept: */*
```

```
Connection:keep-alive  
[new line]  
[new line]
```

6. Indicate end of transmission by using the <ESC>E sequence.
 - Enter the [ESC] key
 - Enter the [E] key
7. The output of HTTP GET will now be displayed as output in the Tera Term window. Since the GainSpan HTTP server closes the connection after HTTP GET is complete, you will see the following output message:

```
DISCONNECT<cid>
```

8. To issue another HTTP GET, repeat Steps 2 through 6. If the HTTP server closes the connection after the HTTP GET is complete, then you must issue a HTTP OPEN prior to every HTTP GET. Gainspan.com is an example of such a server.

1.4 HTTP POST Examples

This section describes the steps to perform a HTTP POST command using the Serial-to-WiFi application.

1.4.1 HTTP POST on Local Apache Server

1. Associate with AP (see [Figure 12, page 28](#)).

```
AT+NDHCP=1
```

```
AT+WA=GainSpanDemo,,6
```

2. Configure the HTTP parameters.

```
AT+HTTPCONF=20,Mozilla/5.0 (Windows; U; Windows NT 5.1;  
en-US) AppleWebKit/534.7 (KHTML, like Gecko)  
Chrome/7.0.517.44 Safari/534.7  
AT+HTTPCONF=7,application/x-www-form-urlencoded  
AT+HTTPCONF=11,192.168.3.116  
AT+HTTPCONF=3,keep-alive
```

3. Initiate HTTP client connection to the server.

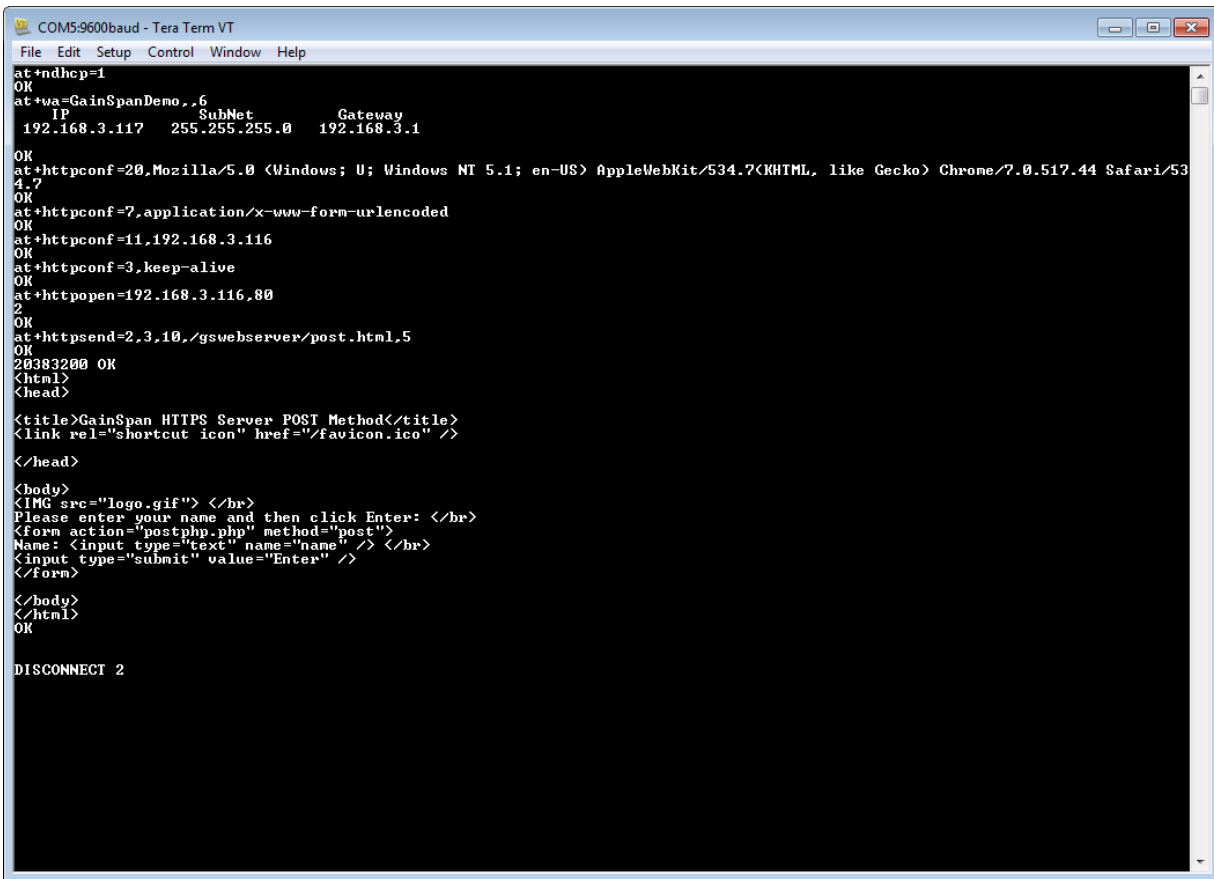
```
AT+HTTPOPEN=192.168.3.116,80
```

4. Perform HTTP POST.

```
AT+HTTPSEND=2,3,10,/gswebserver/post.html,5
```

- Enter the [ESC] key
- Enter the [H] key
- Enter the CID
- Enter the text you want to POST

Figure 12 HTTP POST Command Using Serial-to-WiFi Application



```
COM5:9600baud - Tera Term VT
File Edit Setup Control Window Help
at+ndhcp=1
OK
at+wa=GainSpanDemo,,6
IP SubNet Gateway
192.168.3.117 255.255.255.0 192.168.3.1
OK
at+httpconf=20,Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.7(KHTML, like Gecko) Chrome/7.0.517.44 Safari/534.7
OK
at+httpconf=7,application/x-www-form-urlencoded
OK
at+httpconf=11,192.168.3.116
OK
at+httpconf=3,keep-alive
OK
at+httpopen=192.168.3.116,80
2
OK
at+httpsend=2,3,10,/gswebserver/post.html,5
OK
20383200 OK
<html>
<head>
<title>GainSpan HTTPS Server POST Method</title>
<link rel="shortcut icon" href="/favicon.ico" />
</head>
<body>
<IMG src="logo.gif"> </br>
Please enter your name and then click Enter: </br>
<form action="postphp.php" method="post">
Name: <input type="text" name="name" /> </br>
<input type="submit" value="Enter" />
</form>
</body>
</html>
OK
DISCONNECT 2
```

Chapter 2 HTTPS Examples

This chapter describes the Serial-to-WiFi procedures on how to setup, test, evaluate, and generate self-signed certificates for HTTPS GET/POST connection examples on GainSpan® GS2011M and GS2100M.

- [Requirements, page 29](#)
- [Installing Apache Server, page 29](#)
- [HTTPS GET Example, page 48](#)
- [HTTPS POST Example, page 51](#)
- [Using SSLOPEN Command , page 53](#)

2.1 Requirements

The Serial-to-WiFi application firmware binaries must be loaded onto the GainSpan GS2011M or GS2100M module. For details on how to install the firmware and binaries. Refer to *GainSpan Serial-to-WiFi Adapter Application Programmer Reference Guide*.

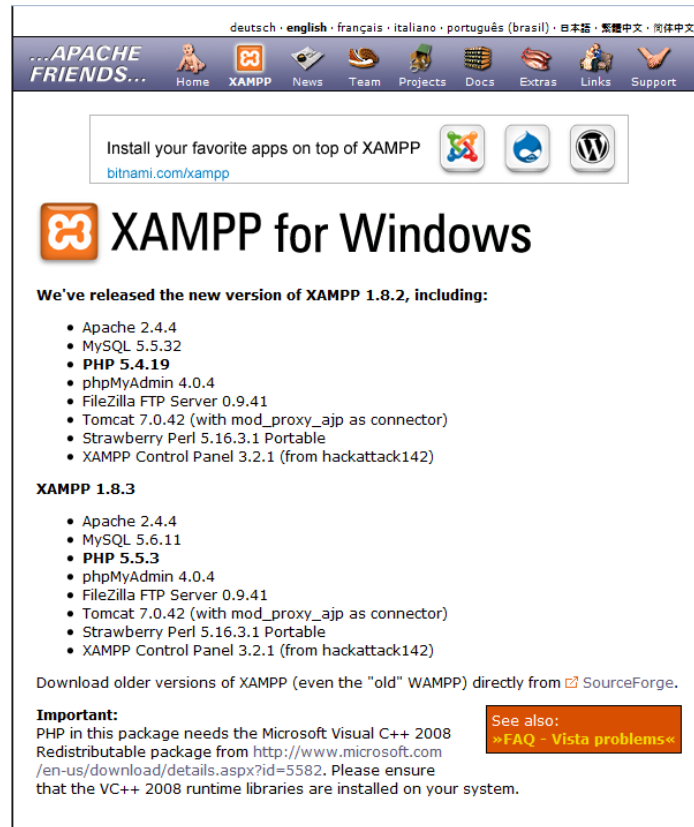
2.2 Installing Apache Server

This section provides instructions on how to install the Apache server in a Windows environment and provides several HTTPS GET/POST examples using the Serial-to-WiFi application.

2.2.1 Install Apache Server in Windows

1. Open a Windows browser and download the XAMPP program from the <http://www.apachefriends.org/en/xampp-windows.html> (see Figure 13, page 30).

Figure 13 Download Apache Server Program



2. Run the setup file to install XAMPP. All the files would be extracted to **C:\xampp**.

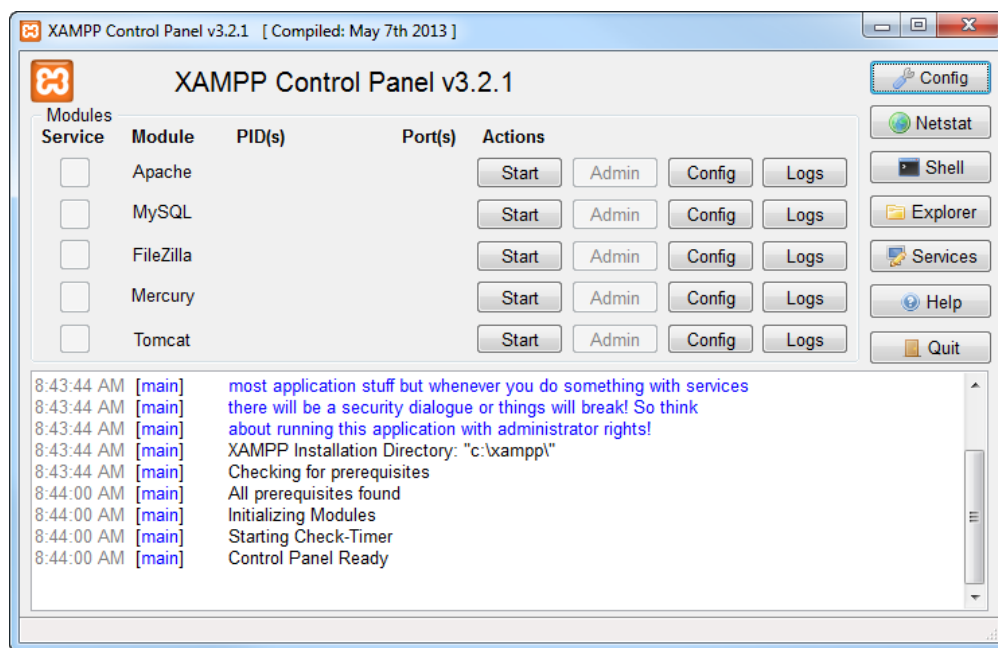


NOTE: Turn off your network connections and close all web browsers to avoid any errors during the installation process.

2.2.2 Run Apache Web Server

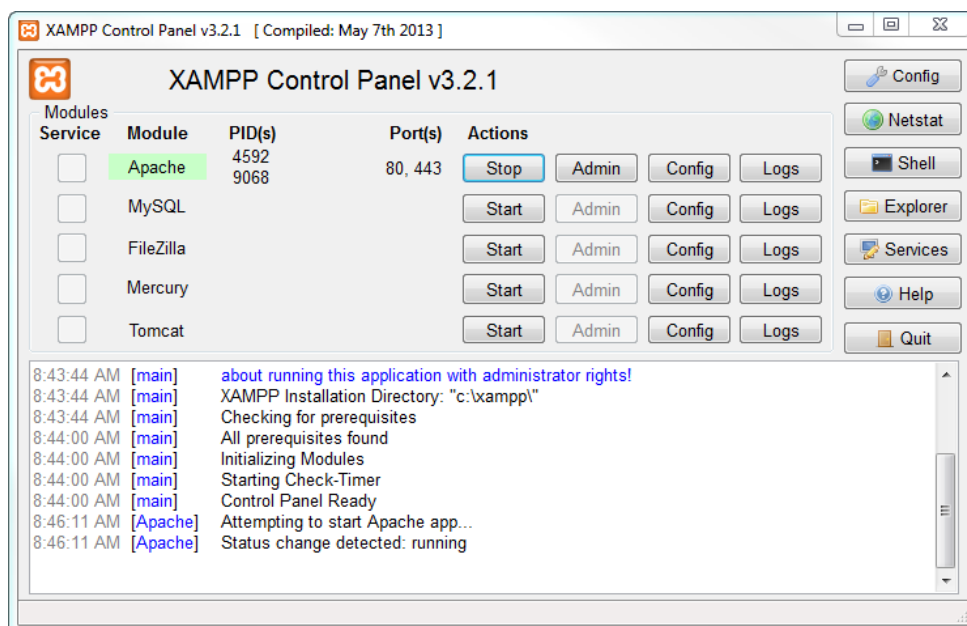
1. Browse to **C:\xampp** and download the latest XAMPP application. The XAMPP Control Panel will display (see Figure 14, page 31).

Figure 14 XAMPP Control Panel



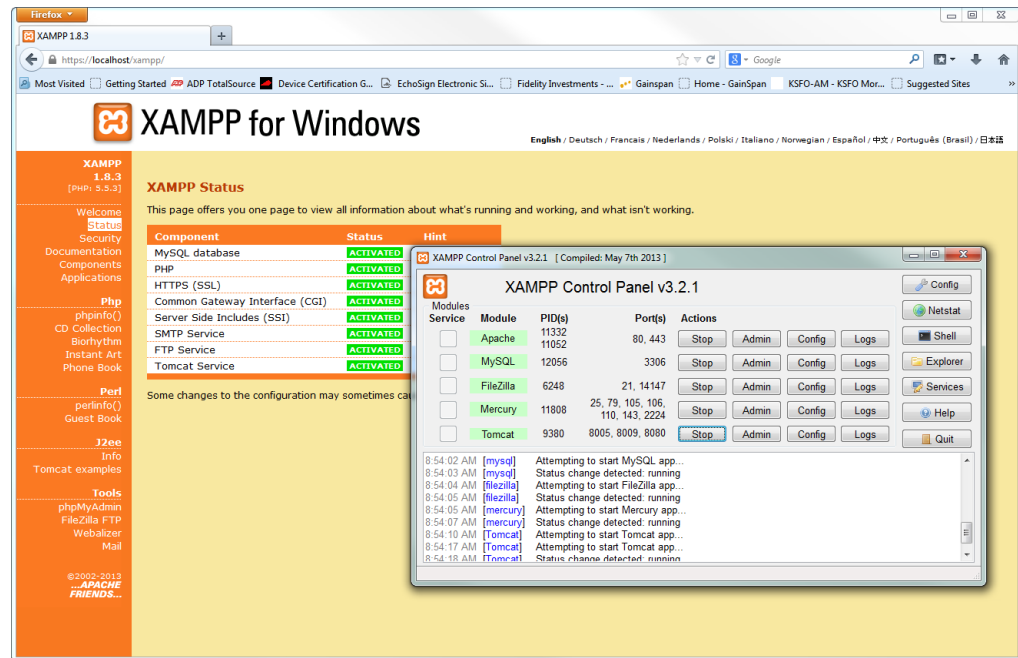
2. Click the **Start** button to start the Apache Web server (see Figure 15, page 31).

Figure 15 Starting the Apache Web Server



- After starting Apache, go to the web address: <http://localhost/> or <http://127.0.0.1/> in your browser. This will verify that the web server is running properly (see Figure 16, page 32).

Figure 16 Verifying Web Server Running



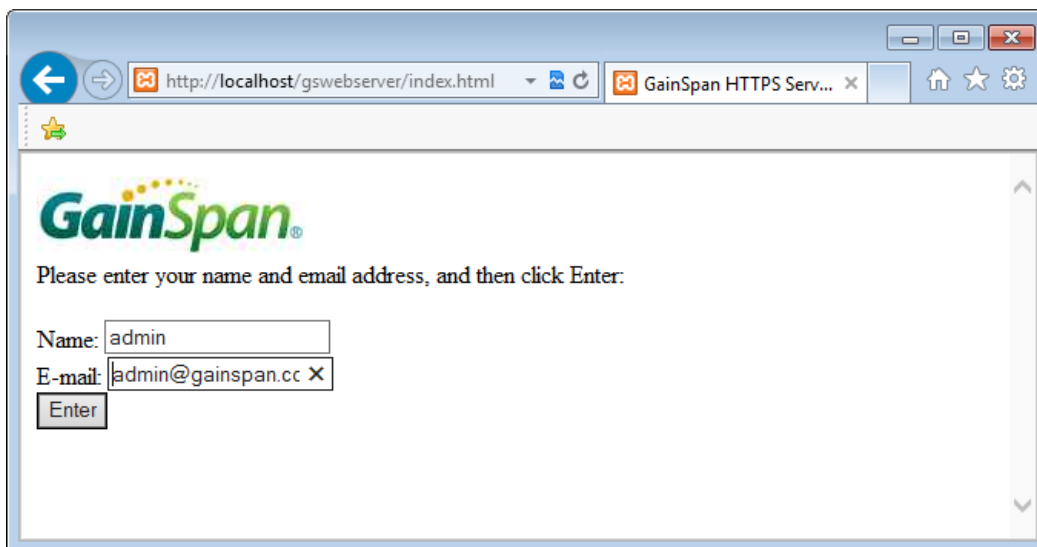
- GainSpan provides several example web pages for users to verify that the Apache Server is configured properly to access the web pages. Copy the GainSpan example: “gswebserver” folder into **C:\xampp\htdocs**.



NOTE: The “gswebserver” folder is bundled with your EVK package.

5. To test the **index.html** web page, open a web browser and go to one of the following addresses:
 - <http://localhost/gswebserver/index.html> or
 - <http://127.0.0.1/gswebserver/post.html>
6. Enter the **Name** and **Email address** details and click the **Enter** button (see Figure 17, page 33).

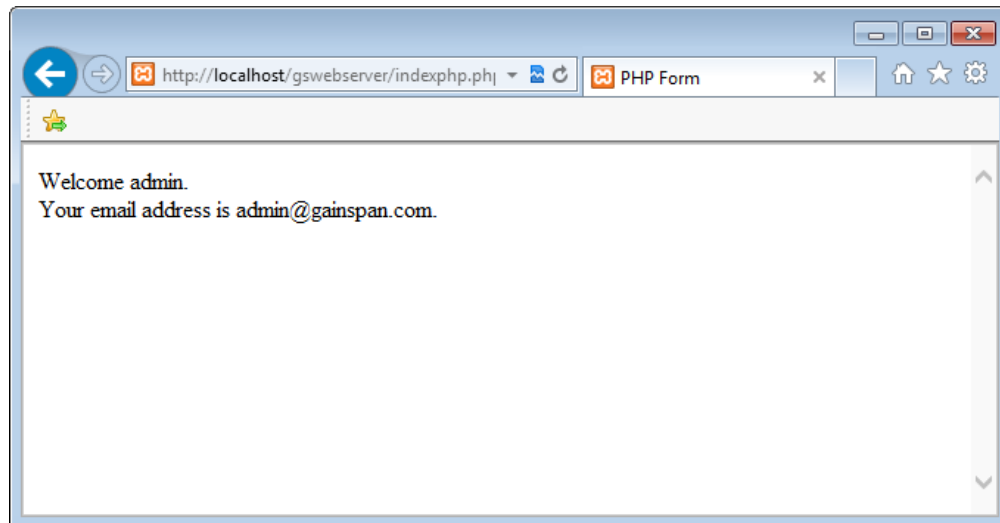
Figure 17 Enter Name and Email Address Information



The screenshot shows a web browser window with the address bar displaying `http://localhost/gswebserver/index.html`. The page features the GainSpan logo and a prompt: "Please enter your name and email address, and then click Enter:". Below this, there are two input fields: "Name:" with the text "admin" and "E-mail:" with the text "admin@gainspan.cc". A small "X" icon is visible next to the email field. An "Enter" button is located below the input fields.

7. The GainSpan Name and Email address will display (see Figure 18, page 33).

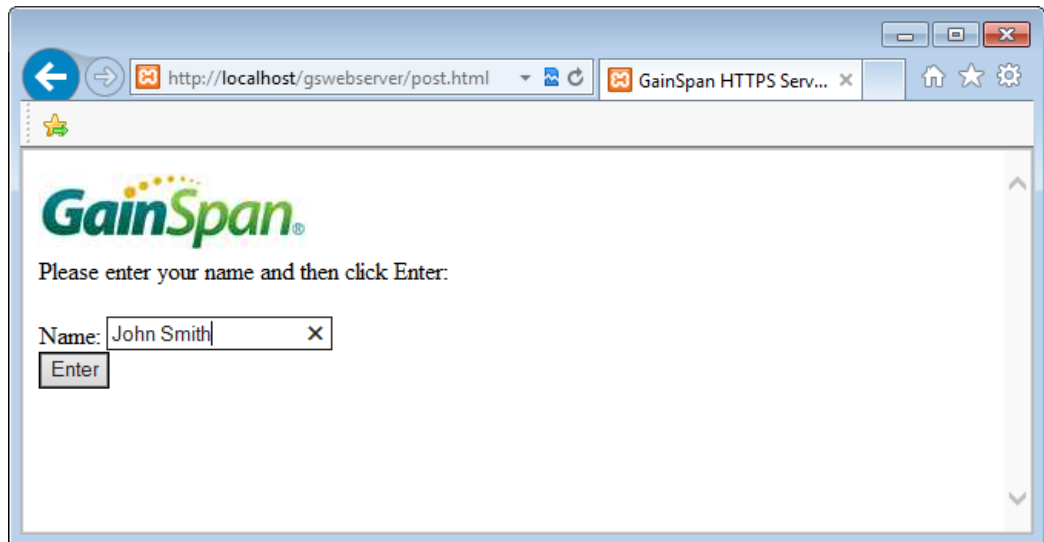
Figure 18 GainSpan Server Email Address Displayed



The screenshot shows a web browser window with the address bar displaying `http://localhost/gswebserver/indexphp.php`. The page displays the text: "Welcome admin." and "Your email address is admin@gainspan.com." The browser tab is labeled "PHP Form".

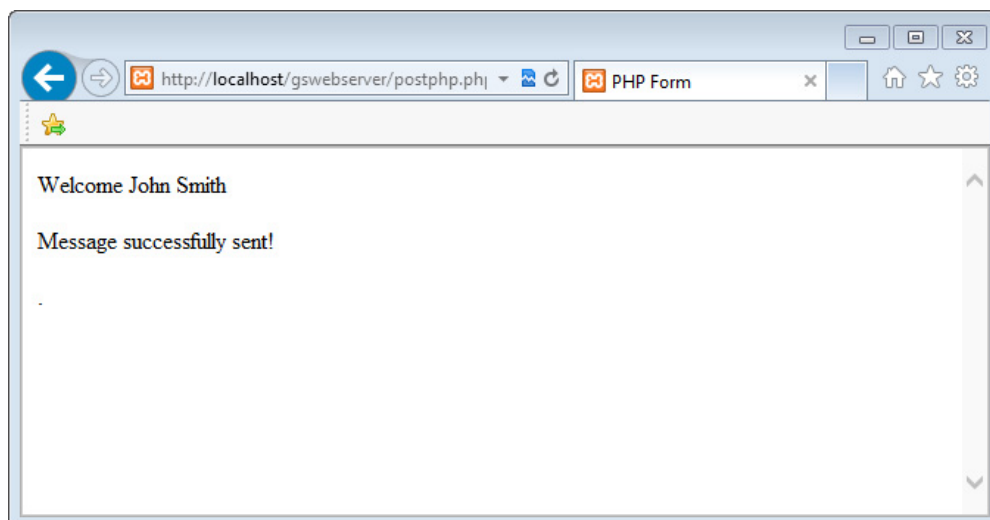
8. Test the **post.html** web page, by opening a web browser and go to one of the following addresses (see Figure 19, page 34):
 - <http://localhost/gswebserver/post.html> or
 - <http://127.0.0.1/gswebserver/post.html>
9. Enter the **Name** and click the **Enter** button (see Figure 20, page 35)

Figure 19 Test the Post HTML Web Page



10. A welcome message will display (see Figure 20, page 35).

Figure 20 Message Sent



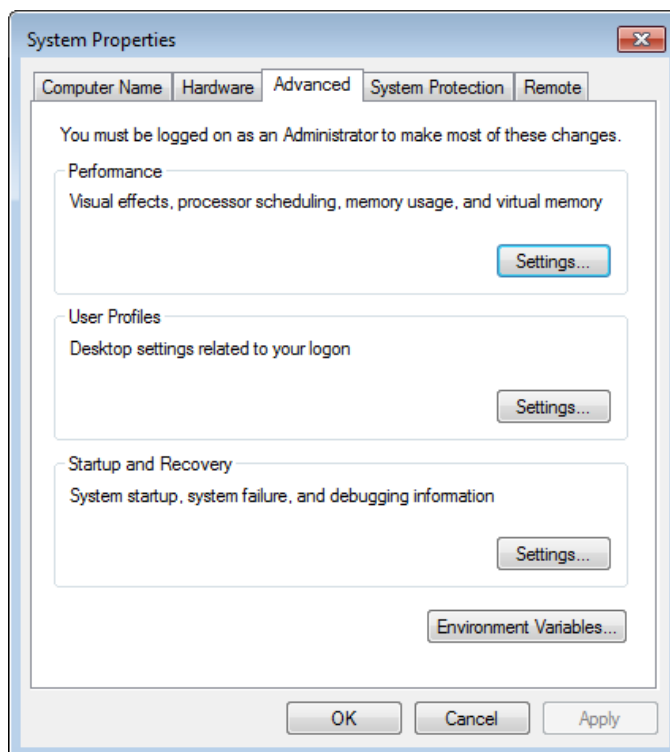
2.2.3 HTTPS Server Configuration

2.2.3.1 How To Install OpenSSL

1. Download and Install Perl from the following link:
<http://activestate.com/Products/activeperl/>
2. Follow the on screen instructions. Download and install Visual C++ 2008 Redistributables from:
<http://www.slproweb.com/products/Win32OpenSSL.html>

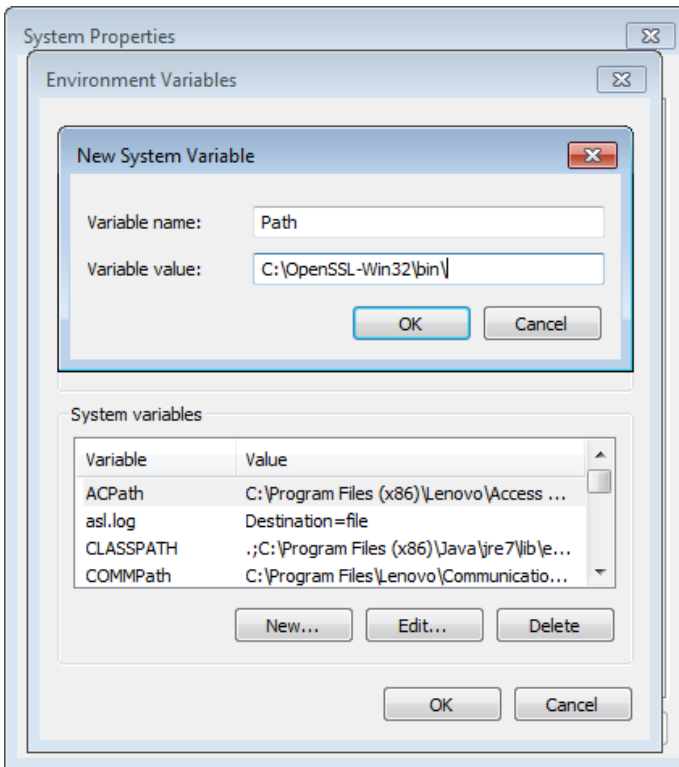
Download the appropriate version for your operating system. For example, if using WinXP 32-bit machine, one would download the “Visual C++ 2008 Redistributables”
3. Download the OpenSSL installer from:
<http://www.slproweb.com/products/Win32OpenSSL.html>

Download the appropriate version for your operating system. For example, if using WinXP 32-bit machine, one would download the “Win32 OpenSSL v1.0.1c”.
4. Add **C:\OpenSSL-Win32\bin** to Windows system PATH variable as shown in the steps below:
 - a. Open the Windows **Start** menu, right click **Computer**, and click **Properties** (see [Figure 21, page 37](#)).
 - b. Open the **Advanced System Settings** and click the **Advanced** tab.

Figure 21 Edit System Variables

- c. Click the **Environment Variables** button. Search for 'Path' in System variables, and add **C:\OpenSSL-Win32\bin** to the Variable value (see [Figure 22, page 38](#)). Click the **OK** button.

Figure 22 Add New System Variable Name and Value



2.2.4 Generating Certificates

This section describes steps to generate the certificates for one-way or two-way authentication (see [Table 7, page 39](#)).

Table 7 Certificates

SSL Entity	Description	Generated Files
Certificate Authority	The CA (Certificate Authority) is the entity that issues trusted digital certificates. The CA issues public key certificates, which is used to verify a certificate's public key and that it belongs to the owner mentioned in the certificate. The CA could be a third party or implemented by the owner.	<ul style="list-style-type: none">• ca.crt• ca.key• cacer.der
Server	The Server provides its certificate to the browser and can also request for a certificate from the Client. The Client validates the Server certificate using the CA's public key.	<ul style="list-style-type: none">• server.crt• server.key
Client	The Client provides its certificates if the Server requests for Client authentication. The Server verifies the Client certificate using the CA's public key.	<ul style="list-style-type: none">• client.crt• client.key.der

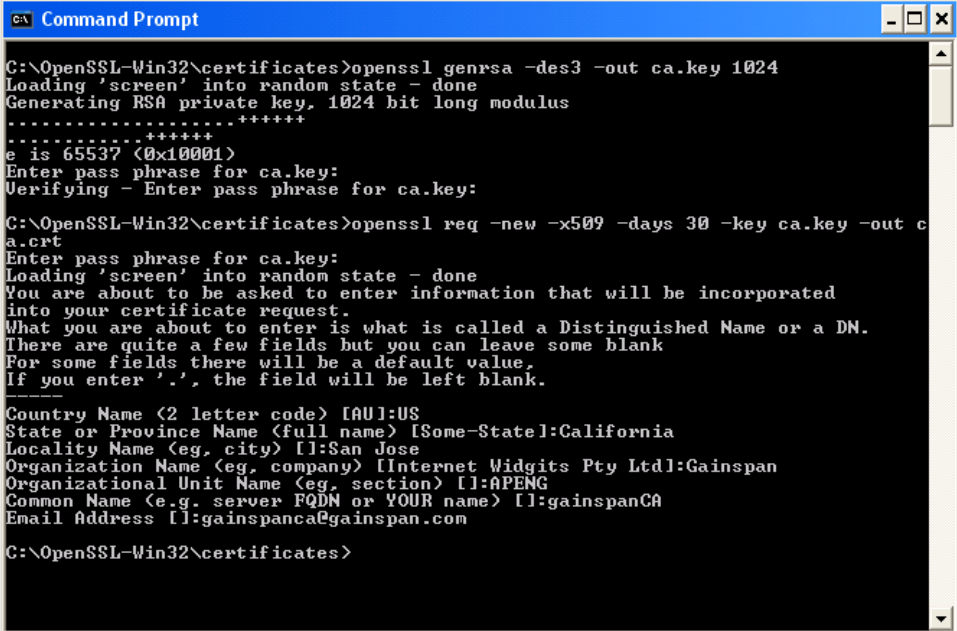
2.2.4.1 Creating Own Certificate Authority

To generate your own certificates on a Windows machine. Open the command prompt and run the following commands.

1. Creating Own Certificate Authority (see [Figure 23, page 40](#)).

```
openssl genrsa -des3 -out ca.key 1024
openssl req -new -x509 -days 30 -key ca.key -out ca.crt
```

Figure 23 Creating Own Certificate Authority



```

C:\OpenSSL-Win32\certificates>openssl genrsa -des3 -out ca.key 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....+++++
e is 65537 (0x10001)
Enter pass phrase for ca.key:
Verifying - Enter pass phrase for ca.key:

C:\OpenSSL-Win32\certificates>openssl req -new -x509 -days 30 -key ca.key -out c
a.crt
Enter pass phrase for ca.key:
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:California
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Gainspan
Organizational Unit Name (eg, section) []:APENG
Common Name (e.g. server FQDN or YOUR name) []:gainspanCA
Email Address []:gainspanca@gainspan.com

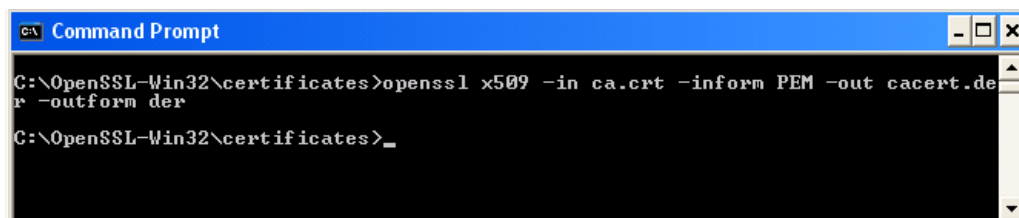
C:\OpenSSL-Win32\certificates>

```


2. Converting the CA Certificate from PEM to DER format (see [Figure 24, page 41](#)).

```
openssl x509 -in ca.crt -inform PEM -out cacert.der  
-outform der
```

Figure 24 Converting CA Certificate from PEM to DER

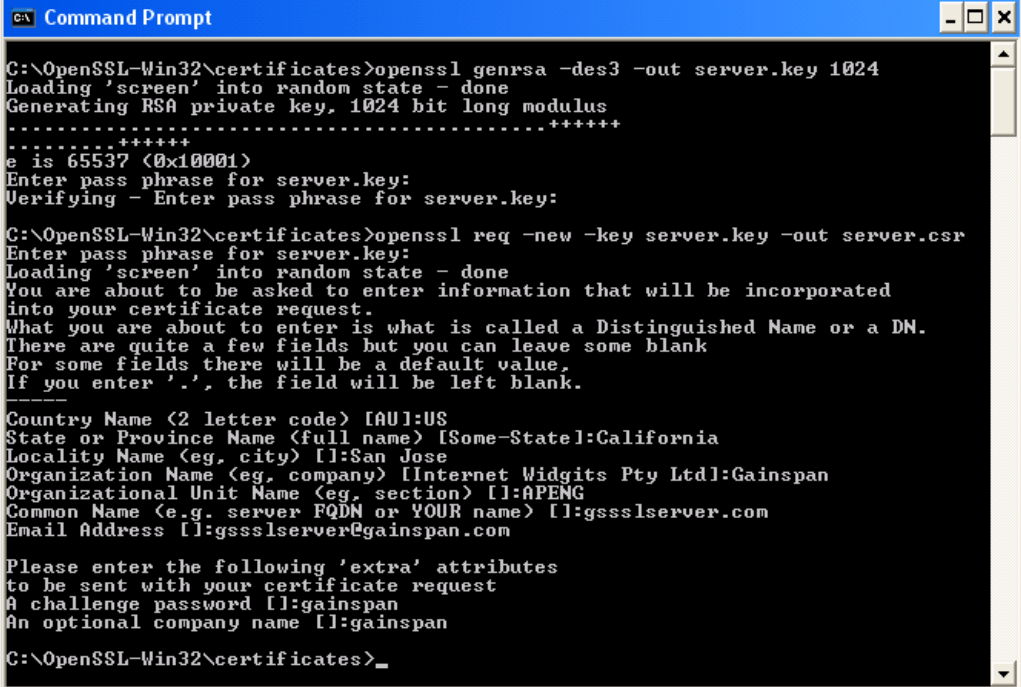


2.2.4.2 Generating Server Certificate

1. Generate Server Certificate (Figure 25, page 42).

```
openssl genrsa -des3 -out server.key 1024
openssl req -new -key server.key -out server.csr
```

Figure 25 Generate Server Certificate



```

C:\OpenSSL-Win32\certificates>openssl genrsa -des3 -out server.key 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....+++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:

C:\OpenSSL-Win32\certificates>openssl req -new -key server.key -out server.csr
Enter pass phrase for server.key:
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:California
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Gainspan
Organizational Unit Name (eg, section) []:APENG
Common Name (e.g. server FQDN or YOUR name) []:gssslserver.com
Email Address []:gssslserver@gainspan.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:gainspan
An optional company name []:gainspan

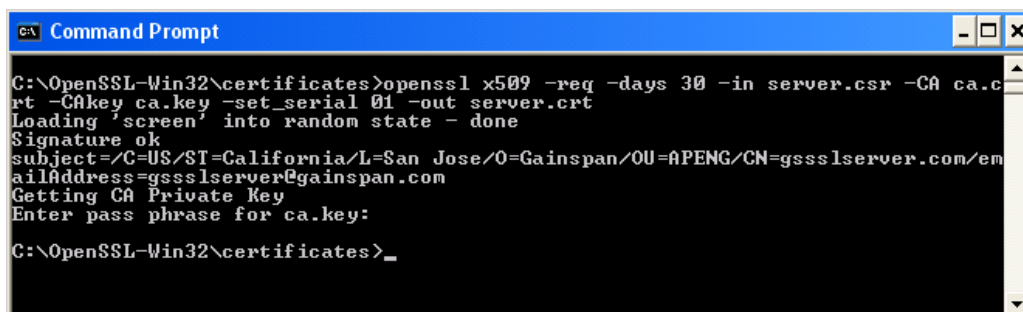
C:\OpenSSL-Win32\certificates>_

```

2. Signing the Server Certificate using own CA (see [Figure 26, page 43](#)).

```
openssl x509 -req -days 30 -in server.csr -CA ca.crt  
-CAkey ca.key -set_serial 01 -out server.crt
```

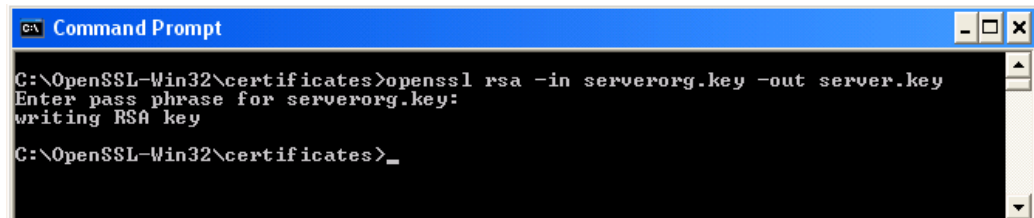
Figure 26 Sign Server Certificate Using Existing CA



3. Remove the password from your key (first rename server.key to serverorg.key), (see [Figure 27, page 44](#)).

```
openssl rsa -in serverorg.key -out server.key
```

Figure 27 Remove Password from Existing Key

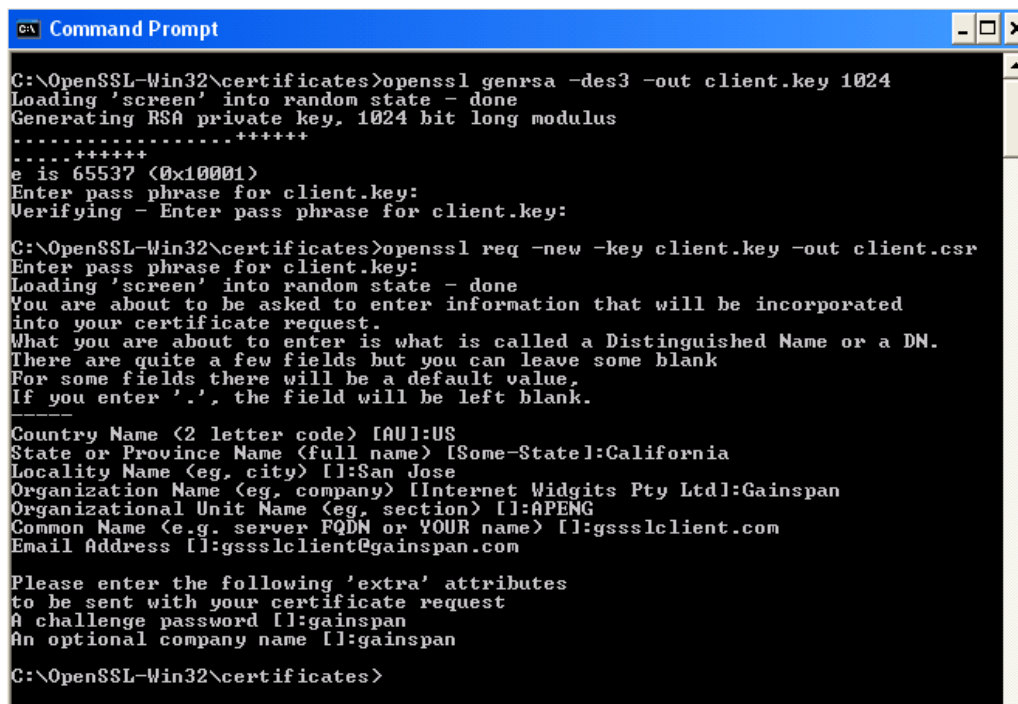


2.2.4.3 Generating Client Certificate

1. Generate Client Certificate (see [Figure 28, page 45](#)).

```
openssl genrsa -des3 -out client.key 1024
openssl req -new -key client.key -out client.csr
```

Figure 28 Generate Client Certificate



```
C:\OpenSSL-Win32\certificates>openssl genrsa -des3 -out client.key 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....+++++
.....+++++
e is 65537 (0x10001)
Enter pass phrase for client.key:
Verifying - Enter pass phrase for client.key:

C:\OpenSSL-Win32\certificates>openssl req -new -key client.key -out client.csr
Enter pass phrase for client.key:
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:California
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Gainspan
Organizational Unit Name (eg, section) []:APENG
Common Name (e.g. server FQDN or YOUR name) []:gssslclient.com
Email Address []:gssslclient@gainspan.com

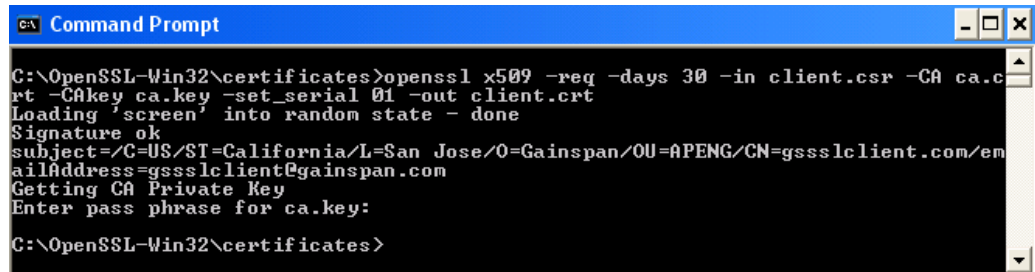
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:gainspan
An optional company name []:gainspan

C:\OpenSSL-Win32\certificates>
```

2. Signing the Client Certificate using own CA (see [Figure 29, page 46](#)).

```
openssl x509 -req -days 30 -in client.csr -CA ca.crt
-CAkey ca.key -set_serial 01 -out client.crt
```

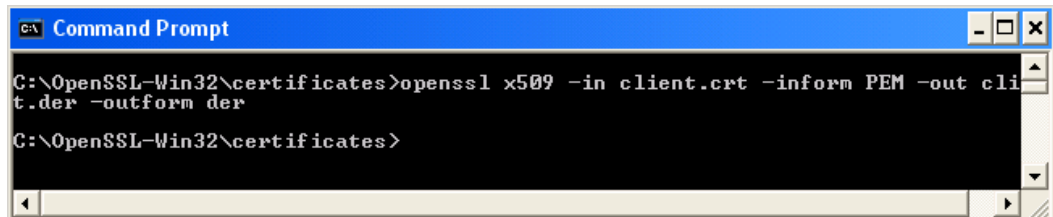
Figure 29 Signing Client Certificate Using Own CA



3. Converting the Client Certificate from PEM to DER format (see [Figure 30, page 46](#)).

```
openssl x509 -in client.crt -inform PEM -out client.der
-outform der
```

Figure 30 Converting Client Certificate from PEM to DER



4. Remove the password from your key (first rename client.key to clientorg.key) (see Figure 31, page 47).

```
openssl rsa -in clientorg.key -out client.key.der
```

Figure 31 Remove Password from Your Key

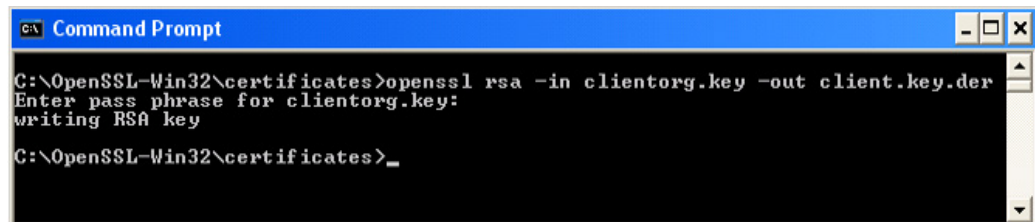
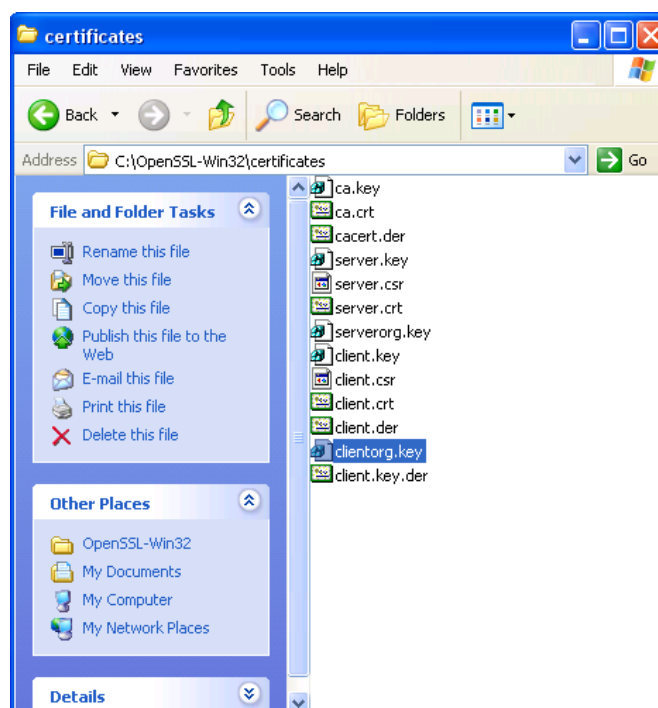


Figure 32, page 47 shows the generated files.

Figure 32 Generated Open SSL Certificate Files



2.3 HTTPS GET Example

To have a secured Apache server you need to put 'server.crt' in `/xampp/apache/conf/ssl.crt` and the 'server.key' in `/xampp/apache/conf/ssl.key`. Make sure that the 'httpd-ssl.conf' configuration file located in `/xampp/apache/conf/extra` is configured to allow SSL connection (SSL Engine should be ON).

1. Configure the certificate for HTTPS connection.

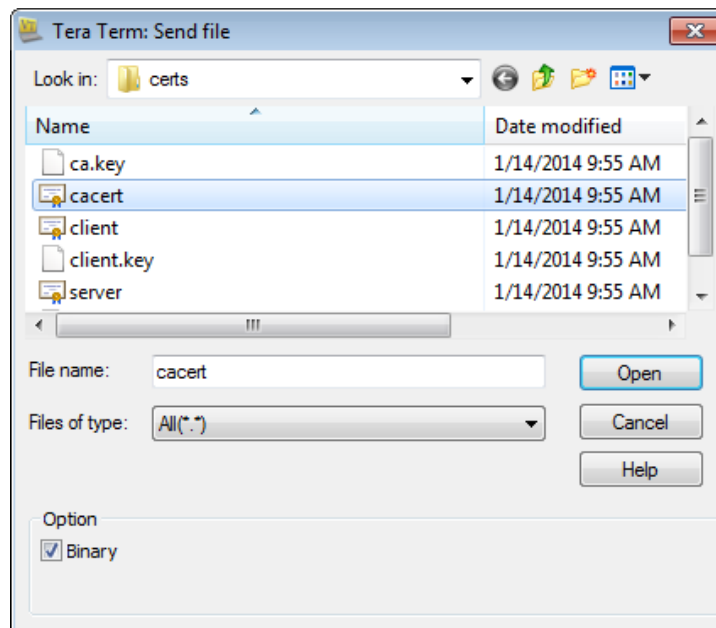
```
AT+TCERTADD=CACERT,0,868,1
```

2. Add the certificate.

- Enter the [ESC] key
- Enter the [W] key

If you are using Tera Term, click on **File** and then select **Send File**. Select the **cacert.der** file. Make sure you check the **Binary option**. Then click **Open** to send the certificate (see Figure 33, page 48).

Figure 33 Tera Term Send File



3. Set the system time (see Figure 34, page 50).

```
AT+SETTIME=7/05/2013,18:00:00
```

4. Associate with AP.

```
AT+NDHCP=1
AT+WA=TEST_AP,,6
```


5. Configure the HTTP parameters (see [Figure 34, page 50](#)).

```
AT+HTTPCONF=20,Mozilla/5.0 (Windows; U; Windows NT 5.1;  
en-US) AppleWebKit/534.7 (KHTML, like Gecko)  
Chrome/7.0.517.44 Safari/534.7  
AT+HTTPCONF=7,application/x-www-form-urlencoded  
AT+HTTPCONF=11,192.168.3.200  
AT+HTTPCONF=3,keep-alive
```

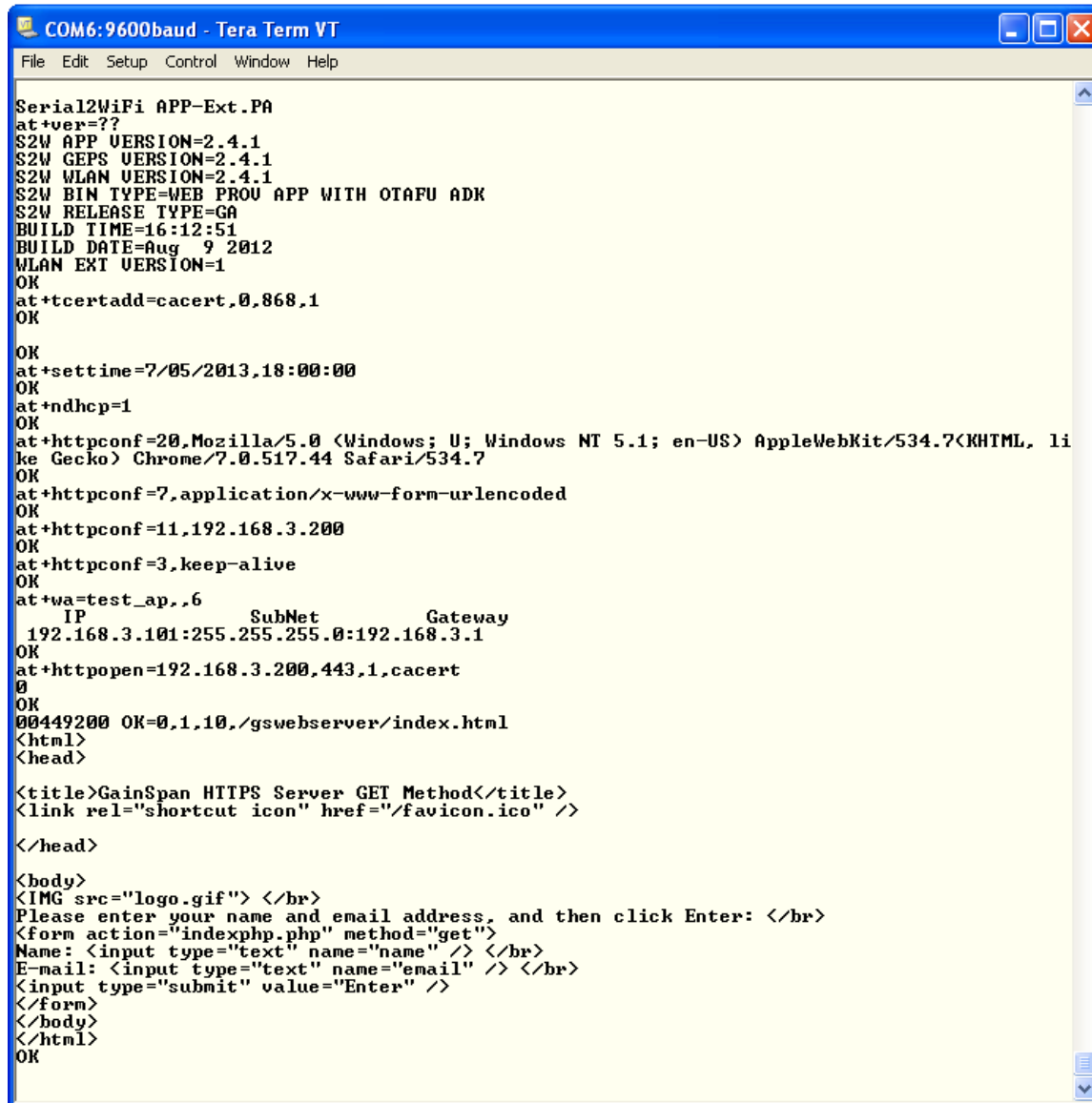
6. Initiate HTTP client connection to the server.

```
AT+HTTPOPEN=192.168.3.200,443,1,cacert
```

7. Perform HTTP GET.

```
AT+HTTPSEND=0,1,10,/gswebserver/index.html
```

Figure 34 Set System HTTP Parameters



```

COM6: 9600baud - Tera Term VT
File Edit Setup Control Window Help

Serial2WiFi APP-Ext.PA
at+ver=?
S2W APP VERSION=2.4.1
S2W GEPS VERSION=2.4.1
S2W WLAN VERSION=2.4.1
S2W BIN TYPE=WEB PROU APP WITH OTAFU ADK
S2W RELEASE TYPE=GA
BUILD TIME=16:12:51
BUILD DATE=Aug 9 2012
WLAN EXT VERSION=1
OK
at+tcertadd=cacert,0,868,1
OK
OK
at+settime=7/05/2013,18:00:00
OK
at+ndhcp=1
OK
at+httpconf=20,Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.7(KHTML, li
ke Gecko) Chrome/7.0.517.44 Safari/534.7
OK
at+httpconf=7,application/x-www-form-urlencoded
OK
at+httpconf=11,192.168.3.200
OK
at+httpconf=3,keep-alive
OK
at+wa=test_ap,,6
      IP          SubNet      Gateway
192.168.3.101:255.255.255.0:192.168.3.1
OK
at+httpopen=192.168.3.200,443,1,cacert
0
OK
00449200 OK=0,1,10,/gswebserver/index.html
<html>
<head>

<title>GainSpan HTTPS Server GET Method</title>
<link rel="shortcut icon" href="/favicon.ico" />

</head>

<body>
<IMG src="logo.gif"> </br>
Please enter your name and email address, and then click Enter: </br>
<form action="indexphp.php" method="get">
Name: <input type="text" name="name" /> </br>
E-mail: <input type="text" name="email" /> </br>
<input type="submit" value="Enter" />
</form>
</body>
</html>
OK

```

2.4 HTTPS POST Example

1. Configure the certificate for HTTPS connection (see [Figure 35, page 52](#)).

```
AT+TCERTADD=CACERT,0,868,1
```

2. Add the certificate.

- Enter the [ESC] key
- Enter the [W] key

If you are using Tera Term, click on **File** and then select **Send File**. Select the **cacert.der** file. Make sure you check the **Binary option**. Then click **Open** to send the certificate.

3. Set the system time.

```
AT+SETTIME=7/05/2013,18:00:00
```

4. Associate with AP.

```
AT+NDHCP=1  
AT+WA=TEST_AP,,6
```

5. Configure the HTTP parameters.

```
AT+HTTPCONF=20,Mozilla/5.0 (Windows; U; WIndows NT 5.1;  
en-US) AppleWebKit/534.7 (KHTML, like Gecko)  
Chrome/7.05.17.44Safari/534.7  
AT+HTTPCONF=7,application/x-www-form-urlencoded  
AT+HTTPCONF=11,192.168.3.200  
AT+HTTPCONF=3,keep-alive
```

6. Initiate HTTP client connection to the server.

```
AT+HTTPOPEN=192.168.3.200,443,1,cacert
```

7. Perform HTTP POST.

```
AT+HTTPSEND=0,3,10,/gswebserver/post.html,5  
– Enter the [ESC] key  
– Enter the [H] key  
– Enter the CID  
– Enter the text you want to POST
```

Figure 35 HTTPS POST Example

```

COM6:9600baud - Tera Term VT
File Edit Setup Control Window Help
Serial2WiFi APP-Ext.PA
at+ver=?
S2W APP VERSION=2.4.1
S2W GEPS VERSION=2.4.1
S2W WLAN VERSION=2.4.1
S2W BIN TYPE=WEB PROU APP WITH OTAFU ADK
S2W RELEASE TYPE=GA
BUILD TIME=16:12:51
BUILD DATE=Aug 9 2012
WLAN EXT VERSION=1
OK
at+tcertadd=cacert,0,868,1
OK
OK
at+settime=7/05/2013,18:00:00
OK
at+ndhcp=1
OK
at+wa=test_ap,,6
IP SubNet Gateway
192.168.3.101:255.255.255.0:192.168.3.1
OK
at+httpconf=20,Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.7 (KHTML, li
ke Gecko) Chrome/7.0.517.44 Safari/534.7
OK
at+httpconf=7,application/x-www-form-urlencoded
OK
at+httpconf=11,192.168.3.200
OK
at+httpconf=3,keep-alive
OK
at+httpopen=192.168.3.200,443,1,cacert
0
OK
at+httpsend=0,3,10,/gswebserver/post.html,5
OK
00383200 OK
<html>
<head>

<title>GainSpan HTTPS Server POST Method</title>
<link rel="shortcut icon" href="/favicon.ico" />

</head>

<body>
<IMG src="logo.gif"> </br>
Please enter your name and then click Enter: </br>
<form action="postphp.php" method="post">
Name: <input type="text" name="name" /> </br>
<input type="submit" value="Enter" />
</form>

</body>
</html>
OK

```

2.5 Using SSLOPEN Command

2.5.1 Starting a SSL Server

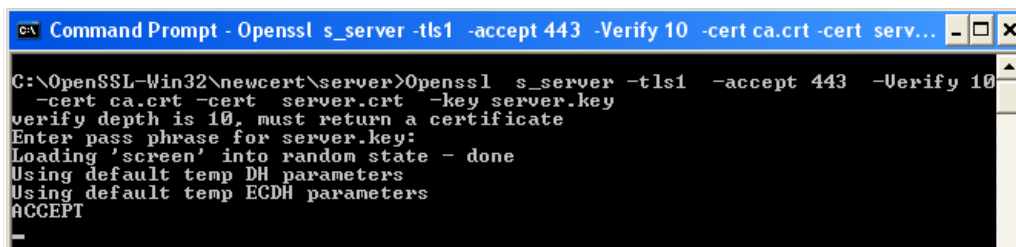


NOTE: *server.crt* is the server certificate. *server.key* is the server key and *cacert.der* is the CA certificate.

To start an SSL server, perform the following (see Figure 36, page 53).

```
$openssl s_server -cert server.crt -key server.key -CA file  
cacert.der -verify 10 -accept 443
```

Figure 36 Starting a SSL Server

A screenshot of a Windows Command Prompt window. The title bar reads "C:\ Command Prompt - Openssl s_server -tls1 -accept 443 -Verify 10 -cert ca.crt -cert serv...". The command prompt shows the execution of the command: `C:\OpenSSL-Win32\newcert\server>openssl s_server -tls1 -accept 443 -Verify 10 -cert ca.crt -cert server.crt -key server.key`. The output text is: `verify depth is 10, must return a certificate`, `Enter pass phrase for server.key:`, `Loading 'screen' into random state - done`, `Using default temp DH parameters`, `Using default temp ECDH parameters`, and `ACCEPT`.

```
C:\OpenSSL-Win32\newcert\server>openssl s_server -tls1 -accept 443 -Verify 10  
-cert ca.crt -cert server.crt -key server.key  
verify depth is 10, must return a certificate  
Enter pass phrase for server.key:  
Loading 'screen' into random state - done  
Using default temp DH parameters  
Using default temp ECDH parameters  
ACCEPT
```

2.5.2 Configuring GS Node as HTTPS Client (One-way Authentication)

To configure GainSpan node as HTTPS Client, perform the following (see [Figure 37, page 55](#)).

1. Load CA Certificate:

AT+TCERTADD=<Name>,<Format>,<Size>,<Location><ESC>W <data of size above>

AT+TCERTADD=cacert,0,760,1

– Enter the [ESC] key

– Enter the [W] key

On Tera Term, click on **File** and then select **Send File**. Select the **cacert.der** file. Make sure you check the **Binary option**. Then click **Open** to send the certificate.

2. Set System Time: *AT+SETTIME=[<dd/mm/yyyy>,<HH:MM:SS>]*

AT+SETTIME=12/03/2012,18:00:00

3. Enable DHCP: *AT+NDHCP=<disable=0/enable=1>*

AT+NDHCP=1

4. Associate to an access point: *AT+WA=<SSID>[,<BSSID>][,<Ch>]]*

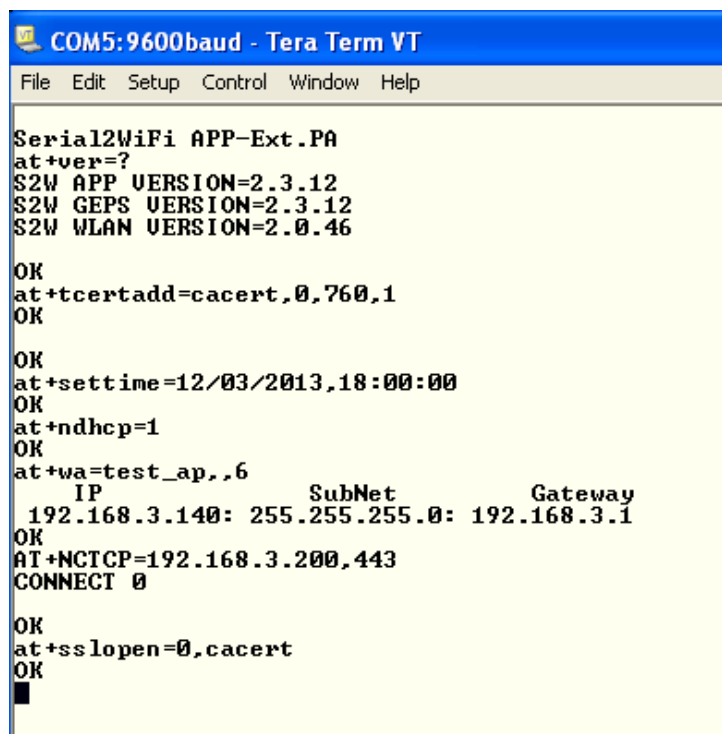
AT+WA=TEST_AP,,6

5. Start a TCP server: *AT+NCTCP=<Dest-Address>,<Port>>[,<Src.Port>]*

AT+NCTCP=192.168.3.200,443

6. Open a SSL Connection: *AT+SSLOPEN=<CID>,<CA certificate name>]*

AT+SSLOPEN=0,cacert

Figure 37 Configuring GainSpan Node as HTTPS Client (One-way Authentication)

```
COM5:9600baud - Tera Term VT
File Edit Setup Control Window Help

Serial2WiFi APP-Ext.PA
at+ver=?
S2W APP VERSION=2.3.12
S2W GEPS VERSION=2.3.12
S2W WLAN VERSION=2.0.46

OK
at+tcertadd=cacert,0,760,1
OK

OK
at+settime=12/03/2013,18:00:00
OK
at+ndhcp=1
OK
at+wa=test_ap,,6
      IP          SubNet      Gateway
192.168.3.140: 255.255.255.0: 192.168.3.1
OK
AT+NCTCP=192.168.3.200,443
CONNECT 0

OK
at+sslopen=0,cacert
OK
█
```

2.5.3 Configuring GainSpan Node as HTTPS Client (Mutual Authentication)

Two way-authentication is supported only in GEPS 2.4.x and GEPS 3.4.x version or later (see [Figure 38, page 57](#)).

1. Load CA Certificate:

AT+TCERTADD=<Name>,<Format>,<Size>,<Location><ESC>W <data of size above>

AT+CERTADD=cacert,0,868,1

- Enter the [ESC] key
- Enter the [W] key

On Tera Term, click on **File** and then select **Send File**. Select the **cacert.der** file. Make sure you check the **Binary option**. Then click **Open** to send the certificate.

2. Load Client Certificate.

AT+TCERTADD=<Name>,<Format>,<Size>,<Location><ESC>W <data of size above>

AT+TCERTADD=clientcert,0,621,1

- Enter the [ESC] key
- Enter the [W] key

On Tera Term, click on **File** and then select **Send File**. Select the **cacert.der** file. Make sure you check the **Binary option**. Then click **Open** to send the certificate.

3. Load Client Key.

AT+TCERTADD=<Name>,<Format>,<Size>,<Location><ESC>W <data of size above>

AT+TCERTADD=AT+TCERTADD=clientkey,0,607,1

- Enter the [ESC] key
- Enter the [W] key

On Tera Term, click on **File** and then select **Send File**. Select the **cacert.der** file. Make sure you check the **Binary option**. Then click **Open** to send the certificate.

4. Set System Time: *AT+SETTIME=[<dd/mm/yyyy>,<HH:MM:SS>]*

AT+SETTIME=15/11/2012,10:15:00

5. Enable DHCP: *AT+NDHCP=<disable=0/enable=1>*

AT+NDHCP=1

6. Associate to an access point: *AT+WA=<SSID>[,<BSSID>][,<Ch>]]*

AT+WA=TEST_AP,,6

7. Start a TCP server: *AT+NCTCP=<Dest-Address>,<Port>>[<,Src.Port>]*

```
AT+NCTCP=192.168.3.200,443
```

8. Open a SSL Connection: *AT+SSLOPEN=<CID>,[<CA certificate name>,Client Certificate>, <Client Key>]*

```
AT+SSLOPEN=0,cacert,clientcert,clientkey
```

Figure 38 Configuring GainSpan Node as HTTPS Client (Mutual Authentication)



```
COM5:9600baud - Tera Term VT
File Edit Setup Control Window Help

Serial2WiFi APP
at+ver=?
S2W APP VERSION=3.4.1.0
S2W GEPS VERSION=3.4.1
S2W WLAN VERSION=3.4.1

OK
at+tcertadd=cacert,0,868,1
OK

OK
at+tcertadd=clientcert,0,621,1
OK

OK
at+tcertadd=clientkey,0,607,1
OK

OK
at+settime=15/11/2012,10:15:00
OK
at+ndhcp=1
OK
at+wa=test_ap,.6
      IP          SubNet      Gateway
192.168.3.124:255.255.255.0:192.168.3.1
OK
at+nctcp=192.168.3.200,443
CONNECT 0

OK
at+sslopen=0,cacert,clientcert,clientkey
OK
█
```

2.5.4 HTTPS POST Using AT+SSLOPEN Command

1. Load CA Certificate:

AT+TCERTADD=<Name>,<Format>,<Size>,<Location><ESC>W <data of size above>

AT+TCERTADD=cacert,0,868,1

- Enter the [ESC] key
- Enter the [W] key

On Tera Term, click on **File** and then select **Send File**. Select the **cacert.der** file. Make sure you check the **Binary option**. Then click **Open** to send the certificate (see [Figure 39, page 59](#)).

2. Set System Time: *AT+SETTIME=[<dd/mm/yyyy>,<HH:MM:SS>]*

AT+SETTIME=09/03/2013,18:00:00

3. Enable DHCP: *AT+NDHCP=<disable=0/enable=1>*

AT+NDHCP=1

4. Associate to an access point: *AT+WA=<SSID>[,<BSSID>][,<Ch>]]*

AT+WA=TEST_AP,,6

5. Start a TCP server: *AT+NCTCP=<Dest-Address>,<Port>>[,<Src.Port>]*

AT+NCTCP=192.168.3.200,443

6. Open a SSL Connection: *AT+SSLOPEN=<CID>,[<CA certificate name>,<Client Certificate>,<Client Key>]*

AT+SSLOPEN=0,cacert

7. Send data to remote server by using the <ESC>S sequence and the CID number:

- Enter the [ESC] key
- Enter the [S] key
- Enter the [CID number from step 5]

8. Copy the highlighted text, and paste it on Tera Term (via the **Edit** menu, choose **Paste** Option)

```
POST /gswebserver/post.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1;
en-US) AppleWebKit/534.7(KHTML, like Gecko)
Chrome/7.0.517.44 Safari/534.7
Content-Type: application/x-www-form-urlencoded
Content-Length: 4
Host: 192.168.3.200
Connection: keep-alive
```

John

9. Indicate end of transmission by using the <ESC>E sequence
 - Enter the [ESC] key
 - Enter the [E] key

Figure 39 HTTPS POST Using AT+SSLOPEN Command

```
COM5:9600baud - Tera Term VT
File Edit Setup Control Window Help

Serial2WiFi APP
at+ver=?
S2W APP VERSION=3.4.1.0
S2W GEPS VERSION=3.4.1
S2W WLAN VERSION=3.4.1
S2W BIN TYPE=WEB PROU APP WITH OTAFU ADK
S2W RELEASE TYPE=GA
BUILD TIME=15:11:50
BUILD DATE=Jul  4 2012
WLAN EXT VERSION=7
OK
at+tcertadd=cacert,0,868,1
OK
OK
at+settime=19/03/2013,18:00:00
OK
at+ndhcp=1
OK
at+wa=test_ap,,6
      IP          SubNet          Gateway
192.168.3.120:255.255.255.0:192.168.3.1
OK
at+nctcp=192.168.3.200,443
CONNECT 0

OK
at+sslopen=0,cacert
OK
```

Over the air capture showing HTTPS POST message will display.

- This page intentionally left blank -

Chapter 3 EAP Examples

This chapter describes the Serial-to-WiFi procedures on how to setup, test, and evaluate EAP association examples on GainSpan® GS2011M and GS2100M.

- [PEAP Without Certificate, page 61](#)
- [PEAP With Certificate, page 63](#)
- [EAP-TLS, page 66](#)

In order to support EAP associations, you must program the Serial-to-WiFi Enterprise Security (EAP) application firmware onto the GainSpan module. The EAP firmware can be found in the official GainSpan software EVK release, or you can build it using the GainSpan SDK-Builder tool.

3.1 PEAP Without Certificate

The example shown in this section is demonstrated with the following authentication server and EAP method:

- **Outer Authentication:** PEAP V0 (25)
- **Inner Authentication:** MSCHAP V2 (26)
- **Authentication Server:** Free Radius Demo v2.2.3 by Enterasys Networks

The following AT command sequence is used.

```
AT+SETTIME=13/6/2013,12:00:00
AT+NDHCP=1
AT+WRXACTIVE=1
AT+WRXPS=0
AT+WEAPCONF=25,26,employee-tls,demo
AT+WA=GainSpanDemo,,6
```

Figure 40, page 62 displays the above AT commands executed in Tera Term.

Figure 40 EAP PEAP Without Certificate AT Commands

```

COM13:9600baud - Tera Term VT
File Edit Setup Control Window Help

Serial2WiFi APP-Ext.PA
at+settime=13/6/2013,12:00:00
OK
at+ndhcp=1
OK
at+wrxactive=1
OK
at+wrxps=0
OK
at+wapconf=25,26,employee-tls,demo
OK
at+wa=GainSpanDemo,,6
IP SubNet Gateway
192.168.3.101: 255.255.255.0: 192.168.3.1
OK

```

Figure 41, page 62 displays the Over-the-Air showing the Key Exchange frame sequence.

Figure 41 EAP PEAP Over-the-Air Showing Key Exchange Frame Sequence

No. -	Time	Source	Destination	Protocol	Info
17181	28.084278	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	EAP	Request, PEAP [Palekar]
17190	28.095023	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	EAP	Response, PEAP [Palekar]
17191	28.095268	Gainspan_aa:bb:cc	Gainspan_aa:bb:cc	(RA IEEE 802	Acknowledgement, Flags=.....C
17206	28.110519	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	EAP	Request, PEAP [Palekar]
17223	28.127392	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	EAP	Response, PEAP [Palekar]
17224	28.127644	Gainspan_aa:bb:cc	Gainspan_aa:bb:cc	(RA IEEE 802	Acknowledgement, Flags=.....C
17229	28.144019	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	TLSv1	Server Hello, Certificate, Server Hello Done
18293	29.876563	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
18294	29.876934	Gainspan_aa:bb:cc	Gainspan_aa:bb:cc	(RA IEEE 802	Acknowledgement, Flags=.....C
18316	29.913434	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	TLSv1	Change Cipher Spec, Encrypted Handshake Message
18325	29.932538	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	EAP	Response, PEAP [Palekar]
18326	29.932783	Gainspan_aa:bb:cc	Gainspan_aa:bb:cc	(RA IEEE 802	Acknowledgement, Flags=.....C
18329	29.942685	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	TLSv1	Application data, Application data
18339	29.951302	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	TLSv1	Application data
18340	29.951675	Gainspan_aa:bb:cc	Gainspan_aa:bb:cc	(RA IEEE 802	Acknowledgement, Flags=.....C
18345	29.960938	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	TLSv1	Application data, Application data
18360	29.980570	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	TLSv1	Application data
18361	29.980936	Gainspan_aa:bb:cc	Gainspan_aa:bb:cc	(RA IEEE 802	Acknowledgement, Flags=.....C
18363	29.990325	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	TLSv1	Application data, Application data
18373	29.998809	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	TLSv1	Application data
18374	29.999182	Gainspan_aa:bb:cc	Gainspan_aa:bb:cc	(RA IEEE 802	Acknowledgement, Flags=.....C
18379	30.009933	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	TLSv1	Application data, Application data
18386	30.016059	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	EAP	Response, PEAP [Palekar]
18387	30.016310	Gainspan_aa:bb:cc	Gainspan_aa:bb:cc	(RA IEEE 802	Acknowledgement, Flags=.....C
18396	30.031421	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	EAP	Success
18402	30.033809	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	EAPOL	Key

Frame 18293 (394 bytes on wire, 394 bytes captured)

Radiotap Header v0, Length 20

IEEE 802.11 QoS Data, Flags:TC

Logical-Link control

802.1X Authentication

3.2 PEAP With Certificate

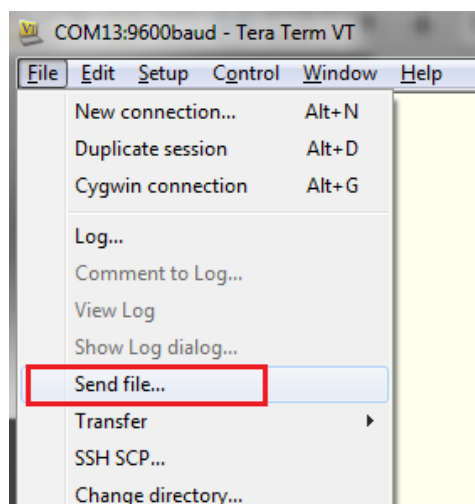
The example shown in this section is demonstrated with the following authentication server and EAP method with certificate.

- **Outer Authentication:** PEAP V0 (25)
- **Inner Authentication:** MSCHAP V2 (26)
- **Authentication Server:** Free Radius Demo v2.2.3 by Enterasys Networks
- **Certificate Format:** DER

The following AT command sequence are used.

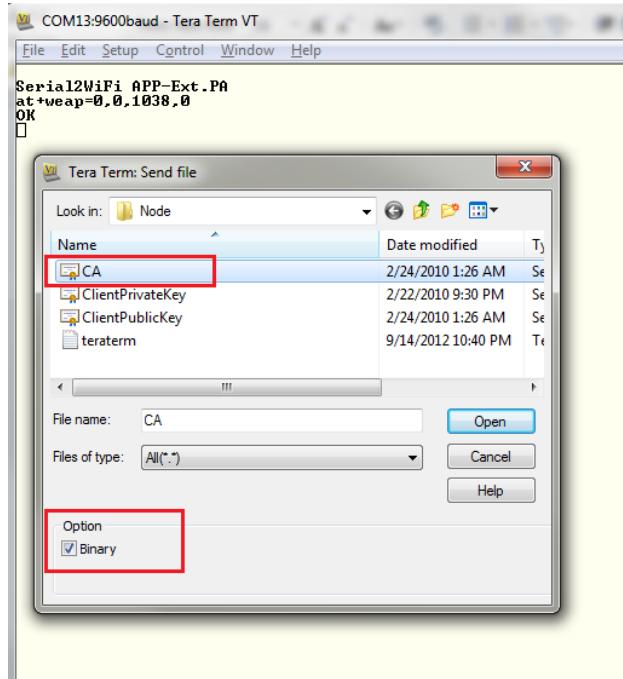
1. AT+WEAP=0,0,1038,0
2. Load the CA certificate into the GainSpan module (see [Figure 42, page 63](#)). If you are using Tera Term, add the certificate by doing the following steps:
 - a. Enter the [ESC] key
 - b. Enter the [shift W] key
 - c. In Tera Term application, click on **File** and then select **Send File**.

Figure 42 EAP PEAP with Certificate Send File



- d. Select the **CA** file. Make sure **Binary option** is checked. Then click **Open** to add the certificate to the GainSpan module (see [Figure 43](#), [page 64](#)).

Figure 43 EAP PEAP Select the CA File



3. Enter the following commands.

```
AT+SETTIME=14/01/2014,12:00:00
AT+NDHCP=1
AT+WRXACTIVE=1
AT+WRXPS=0
AT+WEAPCONF=25,26,employee-tls,demo,1
AT+WA=GainSpanDemo,,6
```


Figure 44, page 65 displays the above AT commands executed in Tera Term.

Figure 44 EAP PEAP With Certificate AT Commands

```

COM13:9600baud - Tera Term VT
File Edit Setup Control Window Help

Serial2WiFi APP-Ext.PA
at+weap=0,0,1038,0
OK

OK
at+settime=13/6/2013,12:00:00
OK
at+ndhcp=1
OK
at+wractive=1
OK
at+wrtps=0
OK
at+weapconf=25,26,employee-tls,demo,1
OK
at+wa=GainSpanDemo,,6
      IP          SubNet      Gateway
      192.168.3.132: 255.255.255.0: 192.168.3.1
OK

```

Figure 45, page 65 displays the Over-the-Air showing the Key Exchange frame sequence.

Figure 45 EAP PEAP Over-the-Air Key Exchange Frame Sequence

No. -	Time	Source	Destination	Protocol	Info
58201	91.983076	Gainspan_aa:00:cc	98:fc:11:7b:f2:b5	SSL	Client Hello
58202	91.983448	Gainspan_aa:bb:cc	Gainspan_aa:bb:cc	(RA IEEE 802	Acknowledgement, Flags=.....C
58215	92.002825	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	EAP	Request, PEAP [Palekar]
58232	92.015059	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	EAP	Response, PEAP [Palekar]
58233	92.015314	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	(RA IEEE 802	Acknowledgement, Flags=.....C
58235	92.031576	Gainspan_aa:bb:cc	Gainspan_aa:bb:cc	EAP	Request, PEAP [Palekar]
58248	92.041319	Gainspan_aa:bb:cc	Gainspan_aa:bb:cc	(RA IEEE 802	Acknowledgement, Flags=.....C
58267	92.054944	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	TLSv1	Server Hello, Certificate, Server Hello Done
59665	94.328432	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
59666	94.328797	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	(RA IEEE 802	Acknowledgement, Flags=.....C
59683	94.360674	Gainspan_aa:bb:cc	Gainspan_aa:bb:cc	TLSv1	Change Cipher Spec, Encrypted Handshake Message
59694	94.380180	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	EAP	Response, PEAP [Palekar]
59695	94.380556	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	(RA IEEE 802	Acknowledgement, Flags=.....C
59699	94.391297	Gainspan_aa:bb:cc	Gainspan_aa:bb:cc	TLSv1	Application Data, Application Data
59710	94.399679	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	TLSv1	Application Data
59711	94.400048	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	(RA IEEE 802	Acknowledgement, Flags=.....C
59722	94.417930	Gainspan_aa:bb:cc	Gainspan_aa:bb:cc	TLSv1	Application Data, Application Data
59743	94.444150	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	TLSv1	Application Data
59744	94.444418	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	(RA IEEE 802	Acknowledgement, Flags=.....C
59750	94.451276	Gainspan_aa:bb:cc	Gainspan_aa:bb:cc	TLSv1	Application Data, Application Data
59758	94.459773	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	TLSv1	Application Data
59759	94.460166	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	(RA IEEE 802	Acknowledgement, Flags=.....C
59766	94.470776	Gainspan_aa:bb:cc	Gainspan_aa:bb:cc	TLSv1	Application Data, Application Data
59770	94.476924	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	EAP	Response, PEAP [Palekar]
59771	94.477653	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	EAP	Response, PEAP [Palekar]
59772	94.478918	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	EAP	Response, PEAP [Palekar]

Frame 59665 (394 bytes on wire, 394 bytes captured)
 Radiotap Header v0, Length 20
 IEEE 802.11 QoS Data, Flags:TC
 Logical-Link Control
 802.1X Authentication

3.3 EAP-TLS

The example shown in this section is demonstrated with the following authentication server and EAP method with certificates:.

- **Outer Authentication:** EAP-TLS (13)
- **Inner Authentication:** MSCHAP V2 (26)
- **Authentication Server:** Free Radius Demo v2.2.3 by Enterasys Networks
- **Certificate Format:** DER

The following AT command sequence is used.

```
AT+WEAP=0,0,1038,0
```

1. Load the **CA certificate** into the GainSpan module. Refer to the example in [PEAP Without Certificate, page 61](#) on how to load the certificate using Tera Term.

```
AT+WEAP=1,0,1305,0
```

2. Load the **client certificate** into the GainSpan module. Refer to the example in [PEAP Without Certificate, page 61](#) on how to load the certificate using Tera Term.

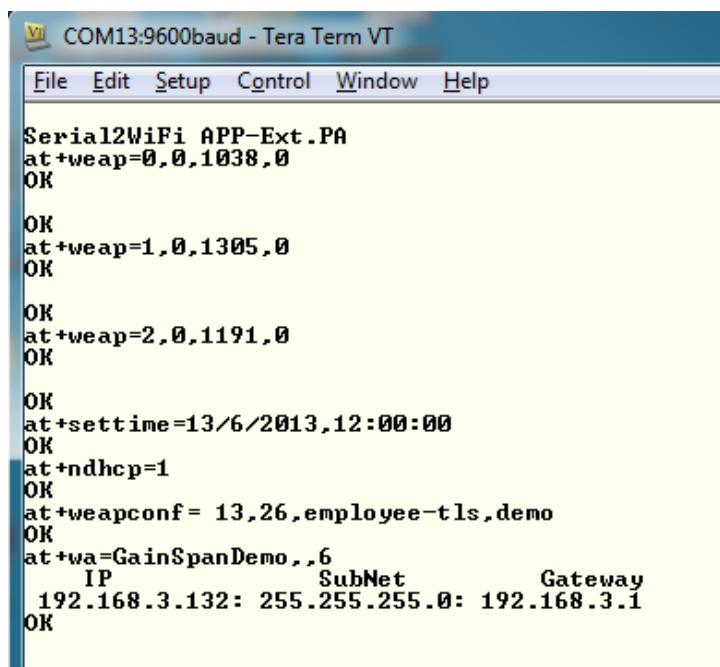
```
AT+WEAP=2,0,1191,0
```

3. Load the **client private key** into the GainSpan module. Refer to the example in [PEAP Without Certificate, page 61](#) on how to load the key using Tera Term.

```
AT+SETTIME=02/01/2013,06:38:00
AT+NDHCP=1
AT+WEAPCONF= 13,26,employee-tls,demo
AT+WA=TEST_AP,,6
```

Figure 46, page 67 displays the above AT commands executed in Tera Term.

Figure 46 EAP-TLS AT Commands



The screenshot shows a Tera Term VT window titled "COM13:9600baud - Tera Term VT". The window contains a series of AT commands and their responses, all of which are "OK". The commands are: "Serial2WiFi APP-Ext.PA", "at+weap=0,0,1038,0", "at+weap=1,0,1305,0", "at+weap=2,0,1191,0", "at+settime=13/6/2013,12:00:00", "at+ndhcp=1", "at+weapconf= 13,26,employee-tls,demo", and "at+wa=GainSpanDemo,,6". The last command is followed by a table of IP, SubNet, and Gateway values: "192.168.3.132: 255.255.255.0: 192.168.3.1".

```
COM13:9600baud - Tera Term VT
File Edit Setup Control Window Help

Serial2WiFi APP-Ext.PA
at+weap=0,0,1038,0
OK

OK
at+weap=1,0,1305,0
OK

OK
at+weap=2,0,1191,0
OK

OK
at+settime=13/6/2013,12:00:00
OK
at+ndhcp=1
OK
at+weapconf= 13,26,employee-tls,demo
OK
at+wa=GainSpanDemo,,6
IP          SubNet      Gateway
192.168.3.132: 255.255.255.0: 192.168.3.1
OK
```

Figure 47, page 68 shows the Over-the-Air wireless capture issuing the Key Exchange frame sequence.

Figure 47 EAP-TLS Over-the-Air Wireless Key Exchange Frame Sequence

No. -	Time	Source	Destination	Protocol	Info
3402	27.789809	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	(RA) IEEE 802	Acknowledgement, Flags=.....C
3404	27.819302	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	TLSv1	Server Hello, Certificate, Certificate Request, Server Hello Done
4956	40.964097	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	EAP	Response, EAP-TLS [RFC2716] [Aboba]
4957	40.964159	Gainspan_aa:bb:cc	Gainspan_aa:bb:cc	(RA) IEEE 802	Acknowledgement, Flags=.....C
4964	41.019337	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	EAP	Request, EAP-TLS [RFC2716] [Aboba]
4966	41.023951	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	TLSv1	Certificate, Client Key Exchange, Certificate verify, Change Cipher Spec
4967	41.024012	Gainspan_aa:bb:cc	Gainspan_aa:bb:cc	(RA) IEEE 802	Acknowledgement, Flags=.....C
4977	41.140035	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	TLSv1	Change Cipher Spec, Encrypted Handshake Message
4983	41.180413	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	EAP	Response, EAP-TLS [RFC2716] [Aboba]
4988	41.209920	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	EAP	Success
4990	41.211671	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	EAPOL	Key
4993	41.223549	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	EAPOL	Key
4994	41.223588	Gainspan_aa:bb:cc	Gainspan_aa:bb:cc	(RA) IEEE 802	Acknowledgement, Flags=.....C
4995	41.228906	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	EAPOL	Key
Frame 4988 (66 bytes on wire, 66 bytes captured)					
+ Radiotap Header v0, Length 20					
+ IEEE 802.11 QoS Data, Flags:F.C					
+ Logical-Link Control					
+ 802.1X Authentication					
Version: 1					
Type: EAP Packet (0)					
Length: 4					
+ Extensible Authentication Protocol					
Code: Success (3)					
Id: 7					
Length: 4					