



Cisco RF Gateway 1 Software
Version 2.5.x Security Features
Addendum

For Your Safety

Explanation of Warning and Caution Icons

Avoid personal injury and product damage! Do not proceed beyond any symbol until you fully understand the indicated conditions.

The following warning and caution icons alert you to important information about the safe operation of this product:

-  You may find this symbol in the document that accompanies this product. This symbol indicates important operating or maintenance instructions.
-  You may find this symbol affixed to the product. This symbol indicates a live terminal where a dangerous voltage may be present; the tip of the flash points to the terminal device.
-  You may find this symbol affixed to the product. This symbol indicates a protective ground terminal.
-  You may find this symbol affixed to the product. This symbol indicates a chassis terminal (normally used for equipotential bonding).
-  You may find this symbol affixed to the product. This symbol warns of a potentially hot surface.
-  You may find this symbol affixed to the product and in this document. This symbol indicates an infrared laser that transmits intensity-modulated light and emits invisible laser radiation or an LED that transmits intensity-modulated light.

Important

Please read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

Notices

Trademark Acknowledgments

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of cisco trademarks, go to this URL: www.cisco.com/go/trademarks.

Third party trademarks mentioned are the property of their respective owners.

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Publication Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing or later issued patent.

Copyright

© 2010, 2012 Cisco and/or its affiliates. All rights reserved. Printed in the United States of America.

Information in this publication is subject to change without notice. No part of this publication may be reproduced or transmitted in any form, by photocopy, microfilm, xerography, or any other means, or incorporated into any information retrieval system, electronic or mechanical, for any purpose, without the express permission of Cisco Systems, Inc.

Contents

Safe Operation for Software Controlling Optical Transmission Equipment	v
Chapter 1 Introduction	1
Chapter 2 Software Version 2.5.x Security Features	3
Software Enhancements.....	4
New Menu Items.....	5
Authentication.....	6
Administrator Password.....	6
Authentication/Radius Settings.....	7
Edit Local Users.....	8
Firewall Settings.....	9
SNMP Trap Destination Port.....	11
Enabling HTTPS on the RF Gateway 1.....	12
Steps for Enabling HTTPS.....	12
Creating a CA.....	12
Creating a CA Certificate.....	13
Creating a Server Key.....	13
Creating a CSR.....	14
Sign the CSR.....	15
Downloading Key and Certificate files to the RF Gateway 1.....	15
Importing the CA Certificate.....	17
Chapter 3 Customer Support Information	20
Glossary	21
Index	23

Safe Operation for Software Controlling Optical Transmission Equipment

If this manual discusses software, the software described is used to monitor and/or control ours and other vendors' electrical and optical equipment designed to transmit video, voice, or data signals. Certain safety precautions must be observed when operating equipment of this nature.

For equipment specific safety requirements, refer to the appropriate section of the equipment documentation.

For safe operation of this software, refer to the following warnings.

**WARNING:**

- **Ensure that all optical connections are complete or terminated before using this equipment to remotely control a laser device. An optical or laser device can pose a hazard to remotely located personnel when operated without their knowledge.**
- **Allow only personnel trained in laser safety to operate this software. Otherwise, injuries to personnel may occur.**
- **Restrict access of this software to authorized personnel only.**
- **Install this software in equipment that is located in a restricted access area.**

1

Introduction

Overview

This document describes the Cisco RF Gateway 1 security features in software version 2.5.x, including Enhanced Authentication, Secret Key, Certificate Signing Requests (CSR), Certificate Authority (CA), and signed certificates using OpenSSL. It also provides procedures for enabling HTTPS and importing a private CA into Firefox.

Who Should Use This Document

This document is intended for authorized service personnel who have experience working with the RF Gateway 1 or similar equipment. The service personnel should have appropriate background and knowledge to complete the procedures described in this document.

Qualified Personnel

Only appropriately qualified and skilled personnel should attempt to install, operate, maintain, and service this product.



WARNING:

Allow only qualified and skilled personnel to install, operate, maintain, and service this product. Otherwise, personal injury or equipment damage may occur.

Document Version

This is the first release of this guide.

2

Software Version 2.5.x Security Features

This chapter describes the Cisco RF Gateway 1 2.5.x security features.

In This Chapter

■ Software Enhancements.....	4
■ New Menu Items	5
■ Authentication.....	6
■ SNMP Trap Destination Port	11
■ Enabling HTTPS on the RF Gateway 1	12

Software Enhancements

Software version 2.5.x contains the following enhancements.

- HTTPS
- GUI support for downloading externally generated keys and certificates to the RF Gateway 1 web server
- Authentication is now multi-level, R/W and R/O
- RADIUS support of service-type and cisco-av-pair
- A firewall has been added to selectively block FTP, HTTPS, HTTP, and Telnet ports
- SNMP trap destination UDP port addresses are now configurable

New Menu Items

The following new menu items have been added to the *System/Configuration* page to provide access to the 2.5.x security features.

- Edit Local Users
- Firewall Settings
- SSL Configuration

The following screen shows the new menu items.

The screenshot displays the Cisco RFGW-1-D Universal Edge QAM web interface in Mozilla Firefox. The browser address bar shows the URL <https://10.90.149.80/#>. The page title is "Cisco RFGW-1-D Universal Edge QAM". The interface includes a navigation bar with tabs for Summary, Monitor, Alarms, QAMS, Maps, and System (selected). A "System Configuration" sidebar on the left lists various configuration options, with "Authentication", "Firewall Settings", "SNMP & Traps", and "SSL Configuration" highlighted with blue boxes. The main content area shows "Device Information" for "rfgw-1d", including fields for Device Description, Device Up Time, Device Name, Device Contact, Device Location, QAM Encoding Type, Frequency Plan, Gratuitous ARP State, Gratuitous ARP Time, DeJitter Buffer Depth, Network PID, Insert Network PID reference in PAT, and Cho Dart CRC Alarm Set Threshold.

Device Information	
Device Description	Cisco RFGW-1-D Universal Edge QAM
Device Up Time	0 Days, 00 Hours, 17 Minutes, 51 Seconds
Device Name	rfgw-1d
Device Contact	Cisco Support
Device Location	here
QAM Encoding Type	ITU-B
Frequency Plan	Standard
Gratuitous ARP State	Enabled
Gratuitous ARP Time	60 seconds
DeJitter Buffer Depth	150 milliseconds
Network PID	8188
Insert Network PID reference in PAT	Enabled
Cho Dart CRC Alarm Set Threshold	10

Authentication

Authentication provides three operating modes: Disabled, Local, and Remote. The Disabled operating mode allows users read/write access to any GUI field without logging in. The Local and Remote operating modes require users to login. The difference between Local and Remote modes is the search order of the two user/password databases. In Local mode, the local database is searched first followed by the remote (RADIUS) database. In Remote mode, the remote database is searched first followed by the local database.

There are two levels of access for the Local and Remote mode, administrator and user. The administrator level allows read/write access of the GUI fields. The user level permits read access only. There can be only one administrator and up to five users logged in to the RF Gateway 1 at a time. The administrator login Id is "admin" and the local user login Ids are factory set to "rfgw1" through "rfgw5." The remote administrator login Ids are those with the service type attribute set to 6, or those with the sub-string "priv-lvl=15" anywhere within the cisco-av-pair attribute string.

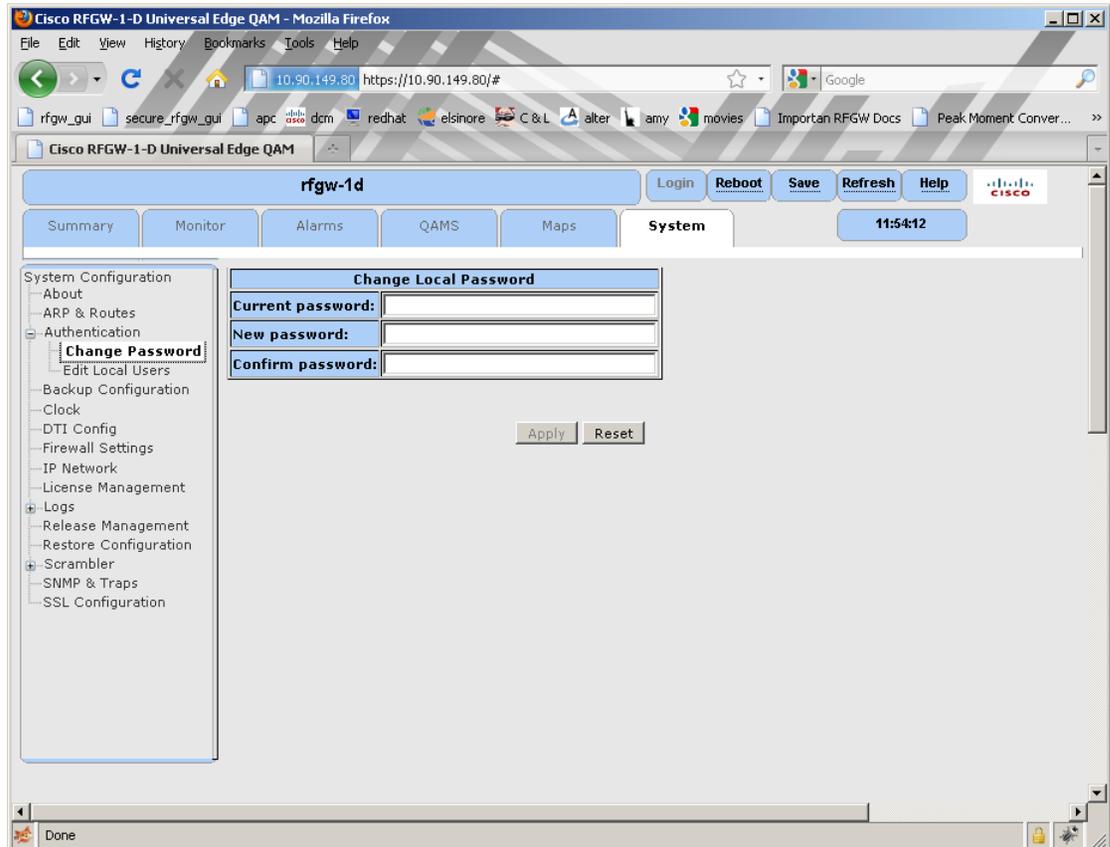
The default password is "0000" for the administrator and each of the five users. In the event that the administrator password is forgotten, it may be reset to "1111" using the front panel.

Administrator Password

Follow the instructions below to set the administrator password.

- 1 Navigate to the *System/Authentication/Change Password* page.

Result: The following screen is displayed.



The password character set is A-Z, a-z, 0-9, ~!@\$^*()_-.+.

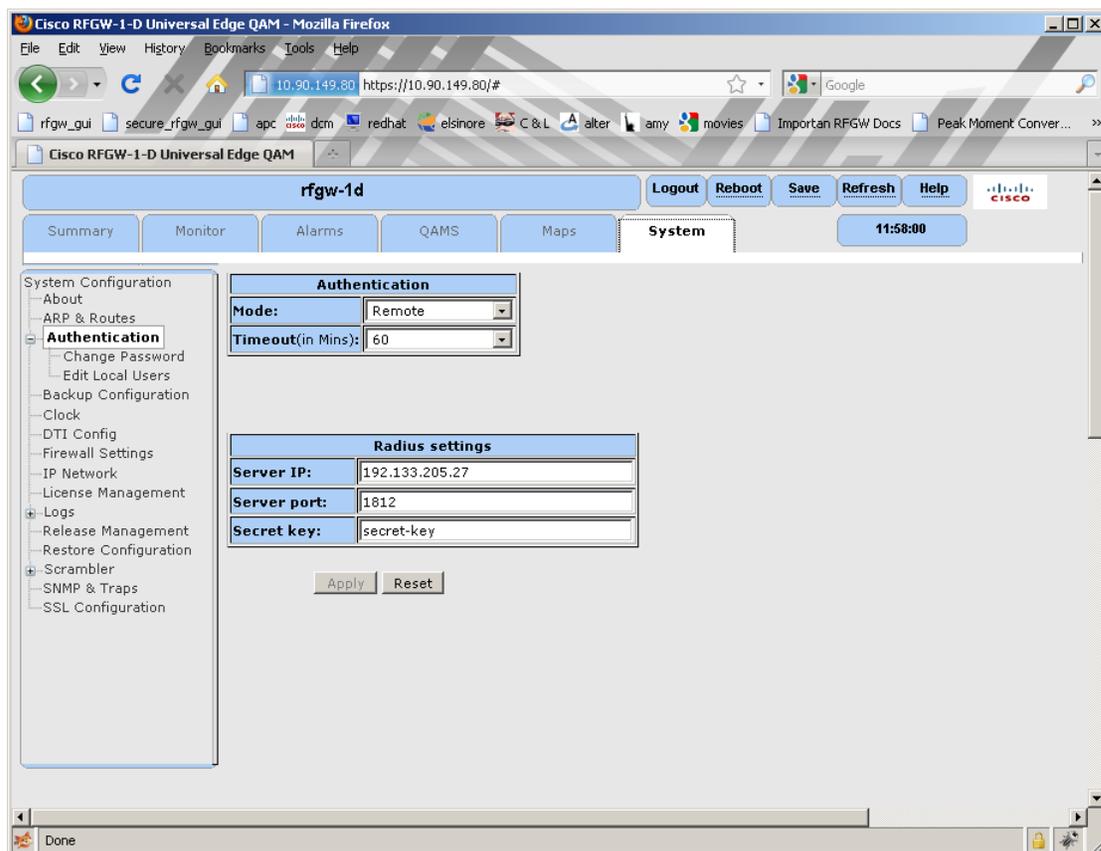
- 2 In the *Change Local Password* box, enter the current password, new password, and then confirm password.
- 3 Click **Apply** to save settings.

Authentication/Radius Settings

Follow the instructions below to set authentication/radius settings.

- 1 Navigate to the *System/Authentication* page.

Result: The following screen is displayed.



- 2 Enter settings for *Mode*, *Timeout*, *Server IP*, *Server port*, and *Secret key*.
- 3 Click **Apply** to save settings.

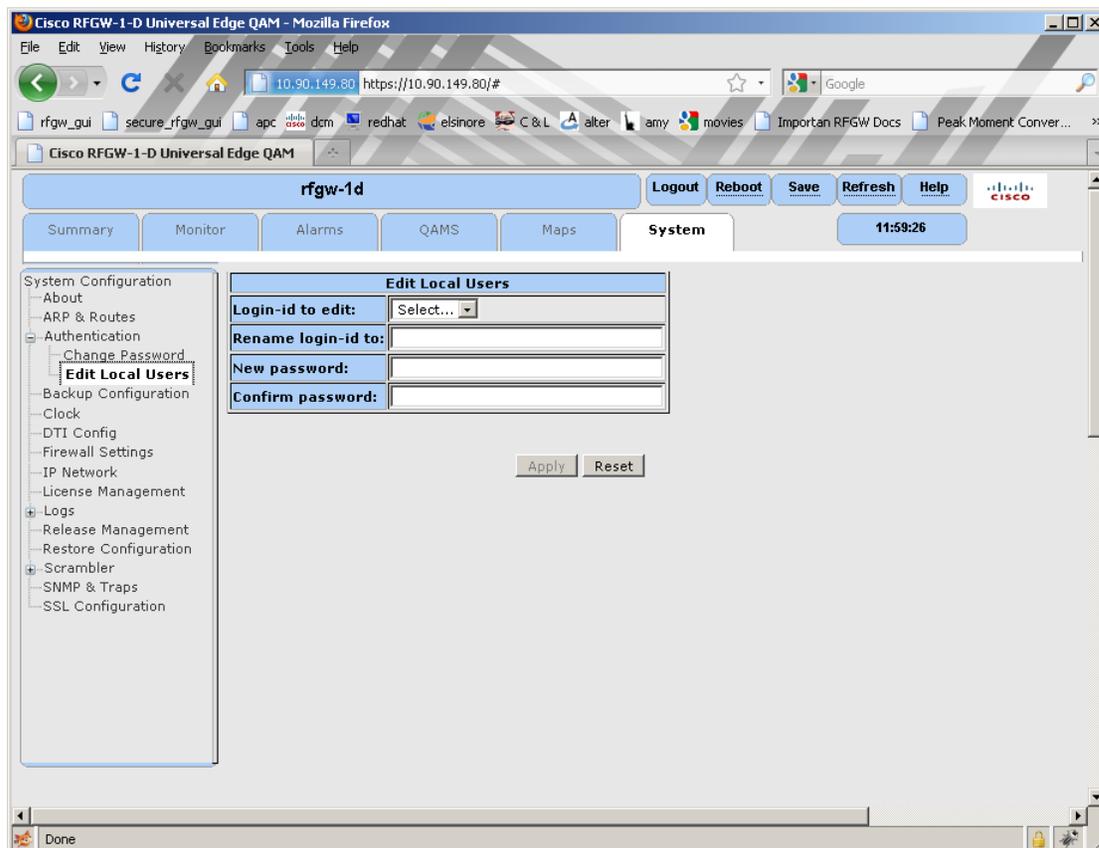
Edit Local Users

Follow the instructions below to change the user login Id and passwords.

Note: This screen is disabled if the operating mode is set to Disabled.

- 1 Navigate to the *System/Authentication/Edit Local Users* page.

Result: The following screen is displayed.



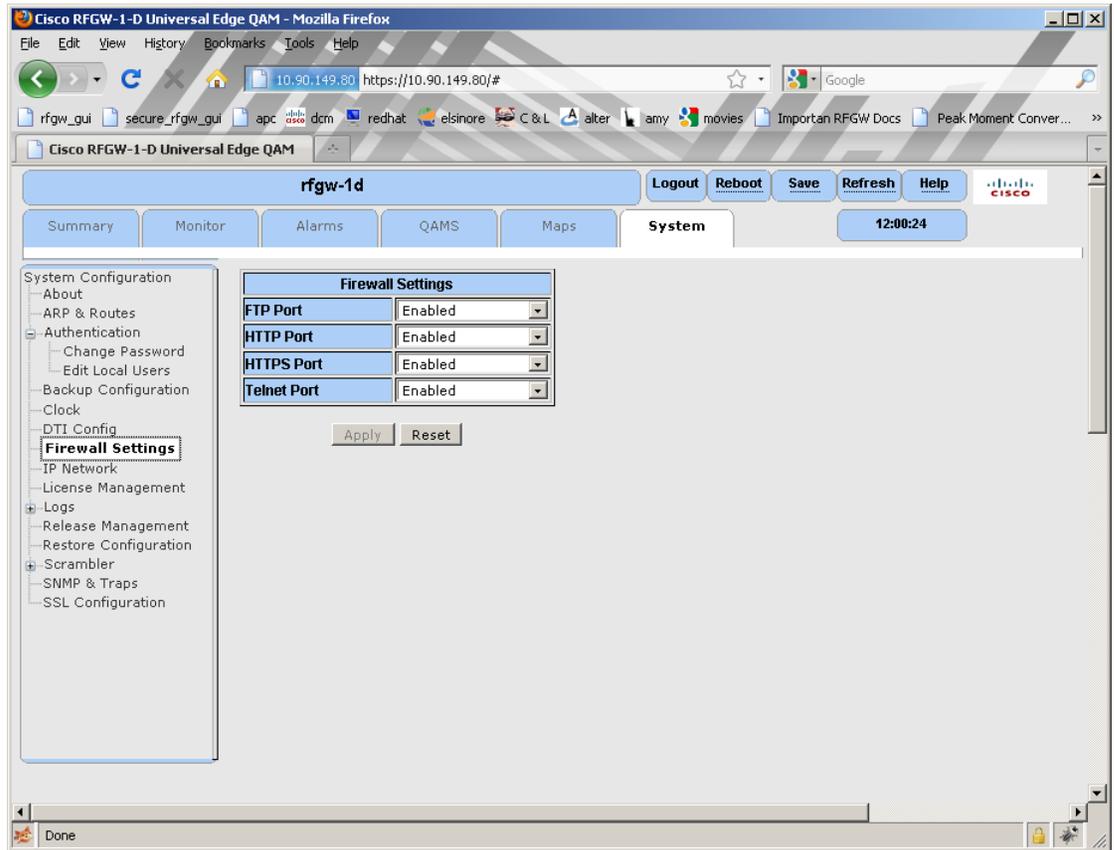
- 2 From the drop-down menu, select the login Id to be changed.
- 3 Enter the the login-id new name.
- 4 Enter new password.
- 5 Confirm new password.
- 6 Click **Apply** to save settings.

Firewall Settings

The FTP, HTTP, HTTPS, and Telnet ports may be enabled or disabled using the Firewall Settings menu. Logic prevents disabling both HTTP and HTTPS simultaneously but it's not a recommended setting in any case. Logic also prevents disabling HTTP if the web server did not detect a valid key and certificate upon startup.

Follow the instructions below to set Firewall settings.

- 1 Navigate to the *System/Authentication/Firewall* Settings page.



- 2 Click the drop-down box and select *Disabled*.
- 3 Click **Apply** to save settings.

SNMP Trap Destination Port

The trap receiver UDP port can be configured using the SNMP & Traps menu item.

- 1 Navigate to the *System/Scrambler/SNMP & Traps* page.

Result: The following screen is displayed.

The screenshot shows the Cisco RFGW-1-D Universal Edge QAM configuration interface in Mozilla Firefox. The browser address bar shows the URL `https://10.90.149.80/#`. The interface includes a navigation menu on the left with the following items: System Configuration, About, ARP & Routes, Authentication, Backup Configuration, Clock, DTI Config, Firewall Settings, IP Network, License Management, Logs, Release Management, Restore Configuration, Scrambler, **SNMP & Traps**, and SSL Configuration. The main content area is titled "Trap Receiver Configuration" and contains a table with the following data:

Row	IP Address	State	Trap Community string	UDP port
1	64.100.109.3	Disabled	*****	162
2	0.0.0.0	Disabled	*****	162
3	0.0.0.0	Disabled	*****	162
4	0.0.0.0	Disabled	*****	162
5	0.0.0.0	Disabled	*****	162

Below the table are buttons for "Apply" and "Reset". Below that is a "Community String Configuration" section with input fields for "Read" and "Write", and an "Apply" button.

- 2 In the *Trap Receiver Configuration* box, enter the UDP port setting.

Enabling HTTPS on the RF Gateway 1

The RF Gateway 1 web server is shipped from the factory with HTTPS disabled. To enable HTTPS, you will need an FTP server, Open Source toolkit for SSL, and a version of RF Gateway software that contains SSL kernel support such as 02.05.XX.

It is recommended that you inform your IT and security departments before installing keys and certificates on live RF Gateway units.

Important: Key files contain a private key and must be handled in strict accordance with your company's security policy, especially the unprotected key known as `server.pem`.

Steps for Enabling HTTPS

The following steps for enabling HTTPS are explained in detail in the following sections.

- Create a CA
- Create a unique key and CSR for each RF Gateway 1 unit required to support HTTPS
- Sign each CSR with the CA
- Download each key and certificate from the FTP server to each RF Gateway 1 unit
- Import the CA certificate into each browser that you plan to use with your RF Gateway 1 unit

In the following steps, the command prompt is shown in italics, the user input is shown in bold, and the computer response is shown in normal typeface.

Creating a CA

Create a CA named `ca.key`:

```
OpenSSL> genrsa -des3 -out ca.key 4096
```

```
Loading 'screen' into random state - done
```

```
Generating RSA private key, 4096 bit long modulus
```

```
.....  
.....  
.....++  
.....++
```

```
e is 65537 (0x10001)
Enter pass phrase for ca.key:
Verifying - Enter pass phrase for ca.key:
OpenSSL>
```

Creating a CA Certificate

Create a CA certificate named *ca.crt*:

```
OpenSSL> req -new -x509 -days 365 -key ca.key -out ca.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]:**Kentucky**

Locality Name (eg, city) []:**LaRue**

Organization Name (eg, company) [Internet Widgits Pty Ltd]:**Sinking Spring Farm**

Organizational Unit Name (eg, section) []:**Log Cabin**

Common Name (eg, YOUR name) []:**Abraham**

Email Address []:**honest@abe.com**

```
OpenSSL>
```

Creating a Server Key

Create a server.key and an unprotected server key name server.pem.

Server.pem, which you'll create below, is not password protected. Guard it well because it contains your private RSA key in the clear for all to see.

```
OpenSSL> genrsa -des3 -out server.key 4096
Loading 'screen' into random state - done
Generating RSA private key, 4096 bit long modulus
.....
.....
.....++
.....++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
OpenSSL> rsa -in server.key -out server.pem
Enter pass phrase for server.key:
writing RSA key
OpenSSL>
```

Creating a CSR

Create a Certificate Signing Request named server.csr:

Recall that when using HTTPS, your browser requires that the site name match the Common Name on the certificate. Therefore you must use the IP Address of the RFGW-1 as the certificate Common Name below.

```
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]:**Indiana**

Locality Name (eg, city) []:**West Lafayette**

Organization Name (eg, company) [Internet Widgits Pty Ltd]:**Purdue University**

Organizational Unit Name (eg, section) []:**Delta Chi Fraternity**

Common Name (eg, YOUR name) []:**10.90.149.80**

Email Address []:**amelia@purdue.edu**

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

An optional company name []:**Boilermakers Inc.**

OpenSSL>

Sign the CSR

Sign the Certificate Signing Request with the self-created CA made earlier and name it public.crt: Browsers such as Firefox are very picky about serial numbers and check for duplicates. Serial numbers must be unique for each signing.

```
OpenSSL> x509 -req -days 365 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01
-out public.crt
```

Loading 'screen' into random state - done

Signature ok

subject=/C=US/ST=Indiana/L=West Lafayette/O=Purdue University/OU=Delta
Chi Frate

raternity/CN=10.90.149.80/emailAddress=amelia@purdue.edu

Getting CA Private Key

Enter pass phrase for ca.key:

OpenSSL>

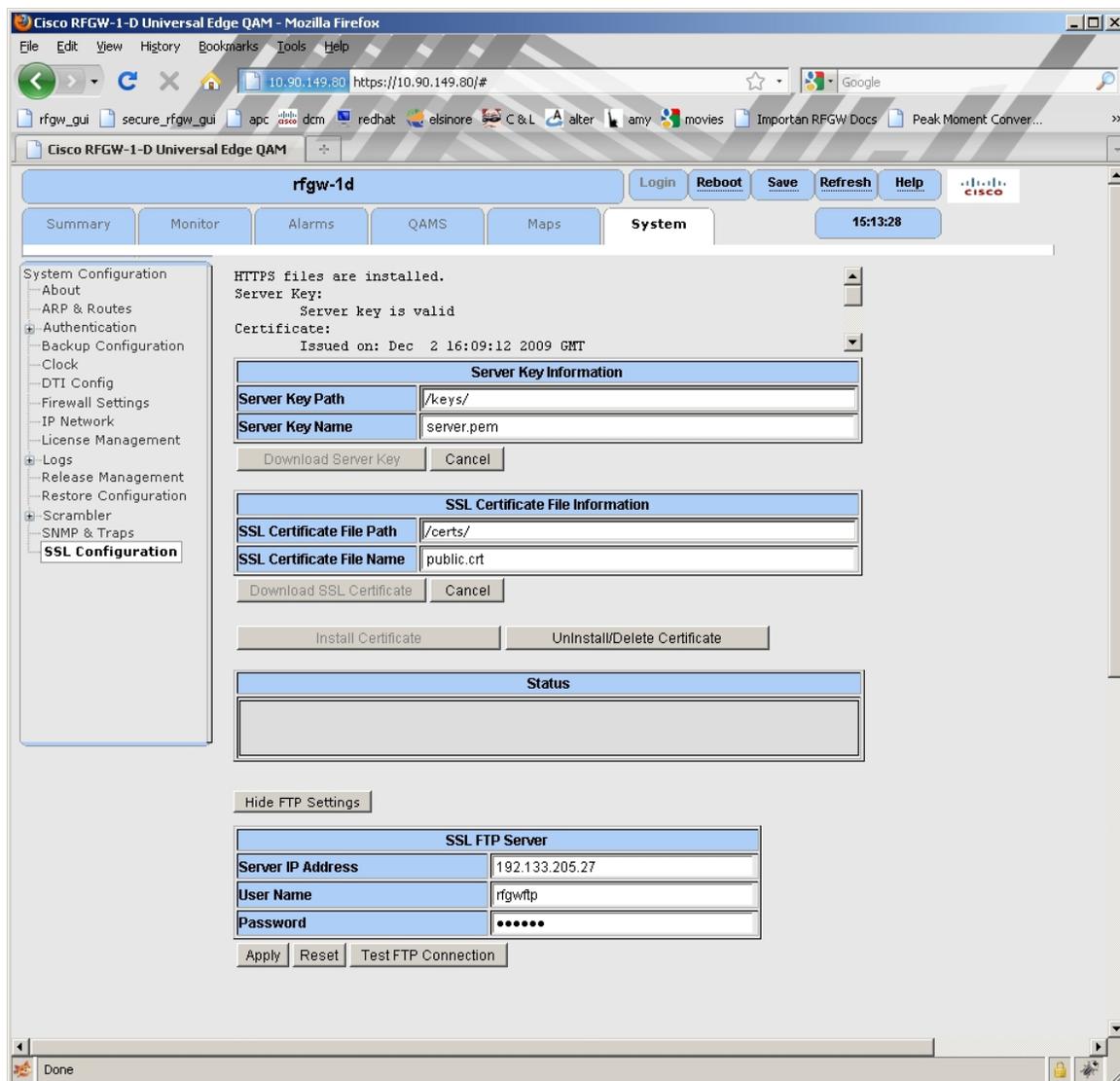
Downloading Key and Certificate files to the RF Gateway 1

The SSL Configuration menu is used to set the FTP server IP address, user name, and password. It is also used to set the path to the key and certificate file and the key and certificate filename. The Server Key name (server.pem) must not be password protected.

Follow the instructions below to configure the SSL settings.

- 1 Navigate to the *System/Scrambler/SSL Configuration* page.

Result: The following screen is displayed.



- 2 In the *Server Key Information* box, enter the *Server Key Path* and *Server Key Name*.

Note: It is recommended that the Server Key be named "server.pem".

- 3 In the *SSL Certificate File Information* box, enter *SSL Certificate File Path* and the *SSL Certificate File Name*.

Note: It is recommended that the file be named "public.crt".

- 4 Click **Download Server Key** followed by **Download SSL Certificate**.

Result: The status window indicates whether the files are valid or invalid.

- 5 Once the files are validated, click **Install Certificate** to restart the server.

Result: After a few seconds, firewall permitting, the server responds to both HTTP and HTTPS requests.

Note: Invalid files are automatically deleted.

- 6 Click **UnInstall/Delete Certificate** to disable HTTPS.

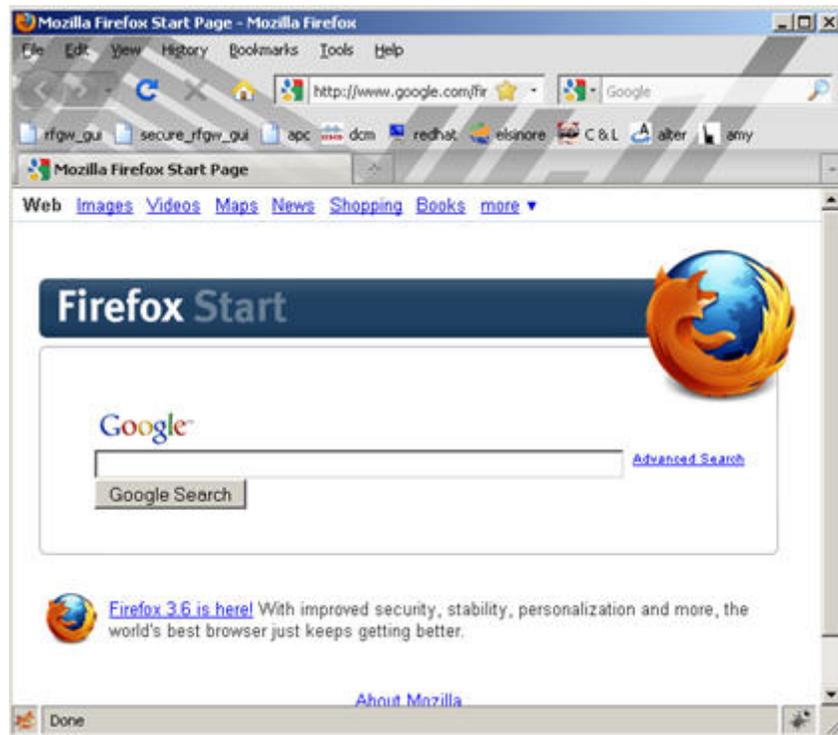
Result: The key and certificate files are deleted and the web server restarts.

Importing the CA Certificate

Follow the instructions below to import the CA certificate into Firefox.

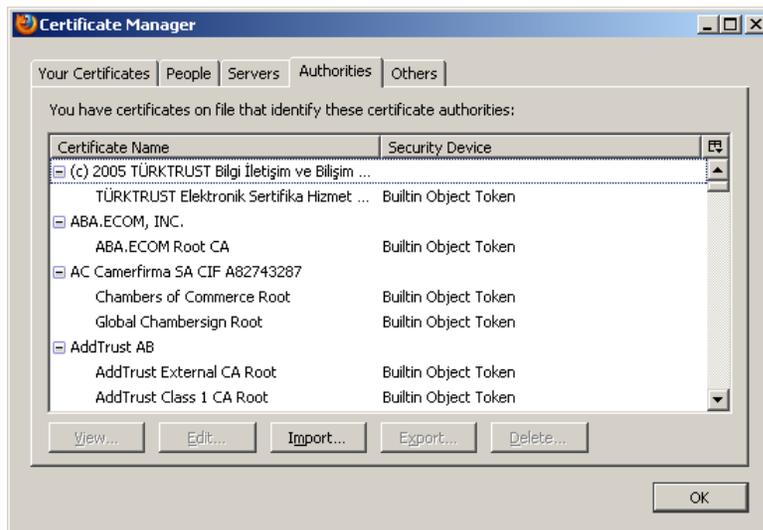
- 1 Launch Firefox.

Result: The following screen is displayed.



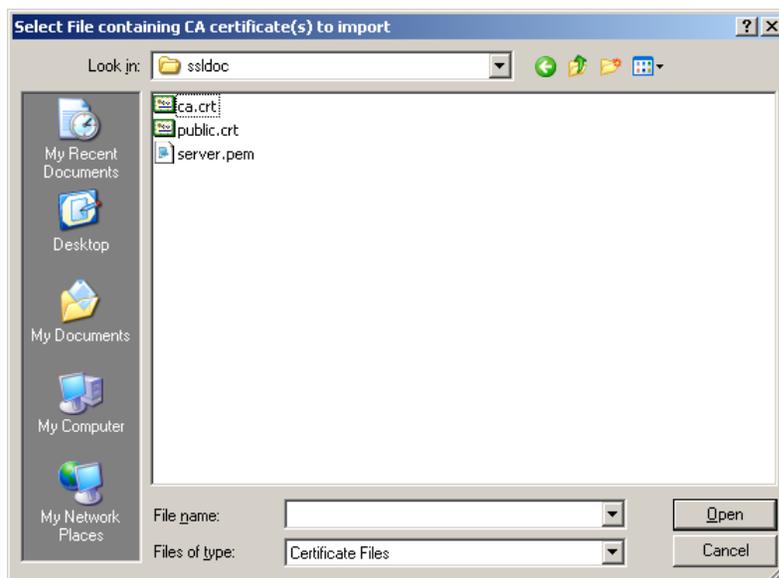
- 2 Click **Tools - Options - Advanced - Encryption - View Certificates - Authorities**.

Result: The following screen is displayed.



3 Click **Import**.

Result: The following screen is displayed.



4 Search for and select your ca.crt file.

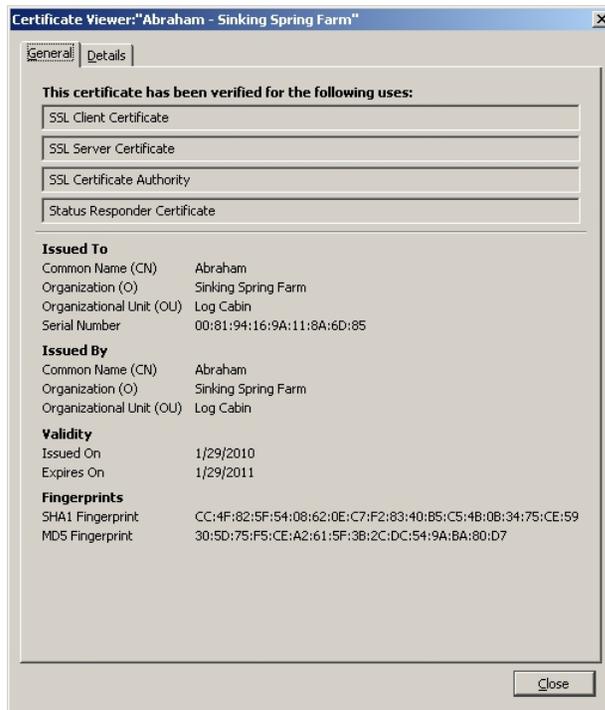
5 Click **Open**.

Result: The following screen is displayed.



- 6 Check the **Trust this CA to identify web sites** box.
- 7 Click **View** to examine your CA certificate.

Result: The following screen is displayed.



3

Customer Support Information

If You Have Questions

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

Access your company's extranet site to view or order additional technical publications. For accessing instructions, contact the representative who handles your account. Check your extranet site often as the information is updated frequently.

Glossary

CA

Certificate Authority.

CSR

Certificate Signing Request.

FTP

file transfer protocol. Allows users to transfer text and binary files to and from a personal computer, list directories on the foreign host, delete and rename files on the foreign host, and perform wildcard transfers between hosts.

GUI

graphical user interface. A program interface that takes advantage of a computer graphics capabilities to make the program visually easier to use.

HTML

hypertext markup language.

HTTP

hypertext transfer protocol.

HTTPS

hypertext transfer protocol secure.

IP

Internet protocol. A standard that was originally developed by the United States Department of Defense to support the internetworking of dissimilar computers across a network. IP is perhaps the most important of the protocols on which the Internet is based. It is the standard that describes software that keeps track of the internetwork addresses for different nodes, routes, and outgoing/incoming messages on a network. Some examples of IP applications include email, chat, and Web browsers.

Glossary

IP address

Internet protocol address. A 32-bit sequence of numbers used for routing IP data. Each IP address identifies a specific component on a specific network. The address contains a network address identifier and a host identifier.

ISO

International Organization for Standardization. An international body that defines global standards for electronic and other industries.

PC

personal computer.

RADIUS

Remote authentication dial in service. A networking protocol that provides centralized Authentication, Authorization and Accounting (AAA) management for computers to connect and use a network service.

RMA

return material authorization. A form used to return products.

SCG

Scrambling Control Group.

SNMP

Simple Network Management Protocol.

SSL

Secure Sockets Layer.

UDP

Index

A

Authentication • 6

C

CA • 21

Creating a CA • 12

Creating a CA Certificate • 13

Creating a CSR • 14

Creating a Server Key • 13

CSR • 21

customer support information • 20

Customer Support Information • 20

D

Downloading Key and Certificate files to the RF Gateway 1 • 15

E

Enabling HTTPS on the RF Gateway 1 • 12

F

Firewall Settings • 9

FTP • 21

G

GUI • 21

H

HTML • 21

HTTP • 21

HTTPS • 21

I

Importing the CA Certificate • 17

Introduction • 1

IP • 21

IP address • 22

ISO • 22

N

New Menu Items • 5

P

PC • 22

R

RADIUS • 22

RMA • 22

S

SCG • 22

Sign the CSR • 15

SNMP • 22

SNMP Trap Destination Port • 11

Software Enhancements • 4

Software Version 2.5.x Security Features • 3

SSL • 22

U

UDP • 22



Cisco Systems, Inc.
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

678 277-1120
800 722-2009
www.cisco.com

This document includes various trademarks of Cisco Systems, Inc. Please see the Notices section of this document for a list of the Cisco Systems, Inc. trademarks used in this document.

Product and service availability are subject to change without notice.

© 2010, 2012 Cisco and/or its affiliates. All rights reserved. September 2012 Printed in USA	Part Number 78-4037508-01 Rev B
--	---------------------------------

