CHAPTER 1

# An Overview of the Cisco Unified Wireless IP Phone 7921G

The Cisco Unified Wireless IP Phone 7921G provides wireless voice communication over an Internet Protocol (IP) network. Like traditional analog telephones, you can place and receive phone calls and access features such as hold, transfer, and speed dial. In addition, because the phone connects to your wireless LAN, you can place and receive phone calls from anywhere in your wireless environment.

This chapter includes the following topics:

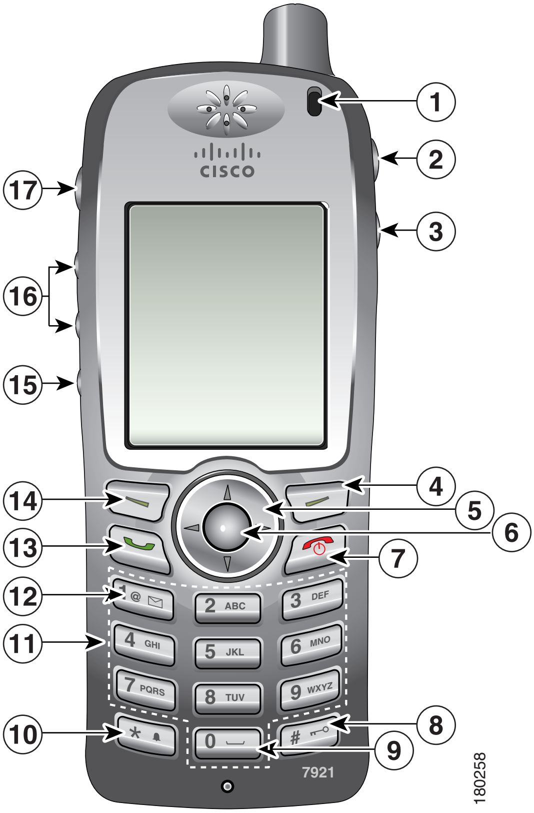
# Understanding the Cisco Unified Wireless IP Phone 7921G

The Cisco Unified Wireless IP Phone 7921G is an 802.11 dual band wireless device that provides comprehensive voice communications in conjunction with Cisco Unified Communications Manager and Cisco Aironet 802.11b/g and Cisco Aironet 802.11a Access Points (APs) in a private business communications network. This phone model supports G.711a, G.711u, G.729a, G.729ab, G.722/iLBC, and decodes all variants of G.711, G.722/iLBC, and G.729. The phone also supports wideband (16 bits, 16 kHz) audio.

You must configure and manage a wireless IP phone like other IP phones and wireless devices on your network. The wireless IP phone supports multiple lines and most of the IP phone features of other Cisco Unified IP Phones.

Figure 1-1 shows the Cisco Unified Wireless IP Phone 7921G. The table that follows describes the functions of the keys on the phone.

*Figure 1-1 Cisco Unified Wireless IP Phone 7921G Buttons and Keys*



| | | |
|---|---|---|
| **1** | Indicator light (LED) | Provides these indications:<br>• Solid red—Phone is connected to AC power source and battery is charging.<br>• Solid green—Phone is connected to AC power source and battery is fully charged.<br>• Fast blinking red—Incoming call. (Phone can be charging or fully charged.)<br>• Slow blinking red—Voice message. (When connected to AC power source, red light displays longer than when phone is using only the battery.)<br>• Slow blinking green—Phone is using only battery power. Phone is registered with the wireless network and is within service coverage area. |
| **2** | Headset port | Port for plugging in a headset or ear bud. |
| **3** | Speaker button | Toggles the speaker mode on or off for the phone. |
| **4** | Right softkey button | Activates the Options menu for access to the list of softkeys. Sometimes displays a softkey label. |
| **5** | Navigation button | Accesses these menus and lists from the main screen:<br>Directory △<br>Line View ▷<br>Settings ▽<br>Services ◁<br>Allows you to scroll up and down menus to highlight options and to move left and right through phone numbers and text entries. |

| | | |
|---|---|---|
| **6** | Select button | Activates the Help menu from the main screen.<br>Allows you to select a menu item, a softkey, a call, or an action. |
| **7** | Power/End button (red) | Turns the phone on or off, silences a ringing call, or ends a connected call.<br>When using menus, acts as a shortcut to return to the main screen. |
| **8** | Pound (#) key | Toggles between locking and unlocking the keypad.<br>Allows you to enter these special characters when you are entering text: **# ? ( ) [ ] { }** |
| **9** | Zero (0) key | Enters “0” when dialing a number. Allows you to enter a **space** or these special characters when you are entering text: **, . ‘ “ \| _ ~ ’** |
| **10** | Asterisk (*) key | Toggles between Ring and Vibrate mode.<br>Allows you to enter these special characters when you are entering text: *** + - / = \ : ;** |
| **11** | Keypad | Allows you to dial numbers, enter letters, and choose menu items by number.<br>Press and hold key 1 to access your voice messaging system. |
| **12** | One (1) key | Enters “1” when dialing a number. Allows you to access the voice messaging system.<br>Allows you to enter these special characters when you are entering text: **! @ < > $ % ^ &** |
| **13** | Answer/Send button (green) | Allows you to answer a ringing call or, after dialing a number, to place the call. |
| **14** | Left softkey button | Activates the softkey option displayed on the screen. When customized by the phone administrator or user, allows direct access to the Phone Book or voice messages. |

| | | |
|---|---|---|
| **15** | Mute button | Toggles the mute feature on or off. |
| **16** | Volume button | When the phone is idle, allows you to control the ring volume, turn on the vibrate option, or turn off the ring.<br>When an incoming call is ringing, allows you to press this button once to silence the ring for the call.<br>During a call, allows you to control the speaker volume for the handset, headset, and speaker mode. |
| **17** | Applications button | Configurable button that is used with XML applications, such as Push to Talk or Directory services. See "Setting Up Services" section on page 7-26. |

For more information about phone features and how they operate, refer to the *Cisco Unified Wireless IP Phone 7921G Guide*.

**Related Topics**

- Features Supported on the Cisco Unified Wireless IP Phone 7921G, page 1-6
- Overview of Configuring and Installing the Cisco Unified Wireless IP Phone 7921G, page 1-17

# Features Supported on the Cisco Unified Wireless IP Phone 7921G

The Cisco Unified Wireless IP Phone 7921G functions much like traditional IP phones allowing you to place and receive telephone calls while connected to the wireless LAN. In addition to traditional phone features, the Cisco Unified Wireless IP Phone includes features that enable you to administer and monitor the phone as a network device.

⚠ **Caution** This product is not a medical device and may use an unlicensed frequency band that is susceptible to interference from other devices or equipment.

This section provides information about these topics:

- Feature Overview, page 1-7
- Configuring Telephony Features, page 1-7
- Configuring Security for the Phone, page 1-8
- Configuring Network Access for the Phone, page 1-9
- Providing Users with Feature Information, page 1-9

## Feature Overview

The Cisco Unified Wireless IP Phone 7921G provides traditional telephony functionality, such as call forwarding and transferring, call pickup, redialing, speed dialing, conference calling, and voice messaging system access, as well as these features:

- Wireless access to your phone number and the corporate directory.
- Access to network data, XML applications, and web-based services.
- Online customizing of phone features and services from your User Options web pages.
- An online help system that displays information on the phone screen.

### Related Topics

- Configuring Network Profiles, page 4-10
- Configuring Features, Templates, Services, and Users, page 7-1

## Configuring Telephony Features

You can modify certain settings for the Cisco Unified IP Phone from the Cisco Unified Communications Manager Administration application. Use this web-based application to set up phone registration criteria and calling search spaces, to configure corporate directories and services, and to modify phone button templates, among other tasks. See the "Telephony Features Available for the Phone" section on page 7-2 and *Cisco Unified Communications Manager Administration Guide* for additional information.

For more information about the Cisco Unified Communications Manager Administration application, refer to Cisco Unified Communications Manager documentation, including *Cisco Unified Communications Manager System Guide*. You can also use the context-sensitive help available within the application for guidance.

You can access the complete Cisco Unified Communications Manager documentation suite at this location:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

### Related Topic

- Telephony Features Available for the Phone, page 7-2

## Configuring Security for the Phone

Implementing security in the wireless network (WLAN) protects against data tampering threats and identity theft of phones. To alleviate these threats, the Cisco wireless LAN provides many options for user authentication with servers and for encrypting communications streams between phones and network devices.

For information about supported security options for the Cisco Unified Wireless IP Phone 7921G, see the "Authentication Mechanisms in the Wireless Network" section on page 2-19.

For information about security features supported by Cisco Unified Communications Manager and Cisco Unified IP Phones, see the "Understanding Security Features for Cisco Unified IP Phones" section on page 1-10.

### Related Topics

- Security for Voice Communications, page 2-6
- Choosing Authentication and Encryption Methods, page 2-22
- Understanding Security Features for Cisco Unified IP Phones, page 1-10

# Configuring Network Access for the Phone

Like other network devices, you must configure IP phones to access Cisco Unified Communications Manager and the rest of the IP network using the wireless LAN. There are two methods for configuring network settings such as DHCP, TFTP, and for wireless settings for the phone.

- Cisco Unified Wireless IP Phone 7921G web pages
- Network Profiles menu on the Cisco Unified Wireless IP Phone 7921G

You can access the configuration web pages by using a browser from your PC. For more information, see Using the Cisco Unified Wireless IP Phone 7921G Web Pages, page 4-1.

You can also configure network settings on the phone itself. For more information about configuring features from the phone, see Chapter 5, "Configuring Settings on the Cisco Unified Wireless IP Phone."

Because the Cisco Unified Wireless IP Phone is a network device, you can obtain detailed status information about it. This information can assist you in troubleshooting problems that users might encounter when using their IP phones. See Chapter 9, "Monitoring the Cisco Unified Wireless IP Phone Remotely," for tips on using this information.

### Related Topics

- Using the Cisco Unified Wireless IP Phone 7921G Web Pages, page 4-1
- Configuring Settings on the Cisco Unified Wireless IP Phone, page 5-1
- Monitoring the Cisco Unified Wireless IP Phone Remotely, page 9-1

# Providing Users with Feature Information

If you are a system administrator, you are the primary source of information for Cisco Unified Wireless IP Phone users in your network or company. To ensure that you distribute the most current feature and procedural information, familiarize yourself with Cisco Unified Wireless IP Phone 7921G documentation. Make sure to visit the Cisco Unified IP Phone web site:

http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_maintain_and_operate.html

From this site, you can view additional phone documentation.

In addition to providing documentation, it is important to inform users about available Cisco Unified IP Phone features—including features specific to your company or network—and about how to access and customize those features, if appropriate.

For a summary of the key information that you can provide to phone users, see Appendix A, "Providing Information to Users By Using a Website."

**Note** The radio frequency (RF) for the Cisco Unified Wireless IP Phone 7921G is configured for a specific regulatory domain. If users attempt to use this phone outside of the regulatory domain, the phone will not function properly and they might violate local regulations.

### Related Topic

Providing Information to Users By Using a Website, page A-1

# Understanding Security Features for Cisco Unified IP Phones

Implementing security in the Cisco Unified Communications Manager system prevents identity theft of the phone and Cisco Unified Communications Manager server, and also prevents data, call signaling, and media stream tampering.

To alleviate these threats, the Cisco IP telephony network establishes and maintains authenticated and encrypted communication streams between a phone and the server, digitally signs files before they are transferred to a phone, and encrypts media streams and call signaling between Cisco Unified IP phones.

Table 1-1 shows where you can find additional information about security in this and other documents.

***Table 1-1 Cisco Unified IP Phone and Cisco Unified Communications Manager Security Topics***

| Topic | Reference |
|---|---|
| Detailed explanation of security, including set up, configuration, and troubleshooting information for Cisco Unified Communications Manager and Cisco Unified IP Phones | Refer to *Cisco Unified Communications Manager Security Guide* |
| Security features supported on the Cisco Unified IP Phone | See the "Overview of Supported Security Features" section on page 1-12 |
| Restrictions regarding security features | See the "Security Restrictions" section on page 1-17 |
| Viewing a security profile name when running Cisco Unified Communications Manager 5.0 or later | See the "Understanding Security Profiles" section on page 1-15 |
| Identifying phone calls for which security is implemented | See the "Identifying Encrypted and Authenticated Phone Calls" section on page 1-16 |
| Transport Layer Security (TLS) connection | See the "Networking Protocols Used with Cisco Unified Wireless IP Phones" section on page 2-8<br>See the "Phone Configuration Files and Profile Files" section on page 2-25 |
| Security and the phone startup process | See the "Understanding the Phone Startup Process" section on page 3-27 |
| Security and phone configuration files | See the "Phone Configuration Files and Profile Files" section on page 2-25 |
| Changing the TFTP Server 1 or TFTP Server 2 option on the phone when security is implemented | See the "Configuring Network Profiles" section on page 4-10 |
| Items on the Security Configuration menu on the phone | See the "Viewing Security Information" section on page 8-2 |
| Unlocking the CTL file | See the "Accessing the CTL File Screen" section on page 8-4 |
| Disabling access to a phone's web pages | See the "Specific Configuration Options for the Cisco Unified Wireless IP Phone 7921G" section on page 7-22 |

*Table 1-1 Cisco Unified IP Phone and Cisco Unified Communications Manager Security Topics*

| Topic | Reference |
|---|---|
| Troubleshooting | See the "General Troubleshooting Information" section on page 10-21<br>Refer to *Cisco Unified Communications Manager Security Guide,* Troubleshooting chapter |
| Resetting or restoring the phone | See the "Erasing the Local Configuration" section on page 10-28 |

## Overview of Supported Security Features

Table 1-2 provides an overview of the security features that the Cisco Unified Wireless IP Phone 7921G supports. For more information about these features and about Cisco Unified Communications Manager and Cisco Unified IP Phone security, refer to *Cisco Unified Communications Manager Security Guide*.

For information about current security settings on a phone, choose **Settings > System Configuration > Security Configuration**. For more information, see the "Viewing Security Information" section on page 8-2.

**Note** Most security features are available only if a certificate trust list (CTL) is installed on the phone. For more information about the CTL, refer to "Configuring the Cisco CTL Client" chapter in the *Cisco Unified Communications Manager Security Guide*.

*Table 1-2 Overview of Security Features*

| Feature | Description |
|---|---|
| Image authentication | Signed binary files (with the extension .sbn) prevent tampering with the firmware image before it is loaded on a phone. Tampering with the image causes a phone to fail the authentication process and reject the new image. |
| Customer-site certificate installation | Each Cisco Unified IP Phone requires a unique certificate for device authentication. Phones include a manufacturing installed certificate (MIC), but for additional security, you can specify in Cisco Unified Communications Manager Administration that a certificate be installed by using the Certificate Authority Proxy Function (CAPF). Alternatively, you can install an LSC (locally significant certificate) from the Security Configuration menu on the phone. See the "Configuring the Security Certificate on the Phone" section on page 5-17 for more information. |
| Device authentication | Occurs between the Cisco Unified Communications Manager server and the phone when each entity accepts the certificate of the other entity. Determines whether a secure connection between the phone and a Cisco Unified Communications Manager should occur, and, if necessary, creates a secure signaling path between the entities using TLS protocol. Cisco Unified Communications Manager will not register phones unless they can be authenticated by the Cisco Unified Communications Manager. |
| File authentication | Validates digitally-signed files that the phone downloads. The phone validates the signature to make sure that file tampering did not occur after the file creation. Files that fail authentication are not written to Flash memory on the phone. The phone rejects such files without further processing. |
| Signaling Authentication | Uses the TLS protocol to validate that no tampering has occurred to signaling packets during transmission. |
| Manufacturing installed certificate | Each Cisco Unified IP Phone contains a unique manufacturing installed certificate (MIC), which is used for device authentication. The MIC is a permanent unique proof of identity for the phone, and allows Cisco Unified Communications Manager to authenticate the phone. |

*Table 1-2 Overview of Security Features (continued)*

| Feature | Description |
|---|---|
| Secure SRST reference | After you configure a SRST reference for security and then reset the dependent devices in Cisco Unified Communications Manager Administration, the TFTP server adds the SRST certificate to the phone cnf.xml file and sends the file to the phone. A secure phone then uses a TLS connection to interact with the SRST-enabled router. |
| Media encryption | Uses SRTP to ensure that the media streams between supported devices proves secure and that only the intended device receives and reads the data. Includes creating a media master key pair for the devices, delivering the keys to the devices, and securing the delivery of the keys while the keys are in transport. |
| Signaling encryption | Ensures that all SCCP signaling messages that are sent between the device and the Cisco Unified Communications Manager server are encrypted. |
| CAPF (Certificate Authority Proxy Function) | Implements parts of the certificate generation procedure that are too processing-intensive for the phone, and it interacts with the phone for key generation and certificate installation. The CAPF can be configured to request certificates from customer-specified certificate authorities on behalf of the phone, or it can be configured to generate certificates locally. |
| Security profiles | Defines whether the phone is non-secure, authenticated, or encrypted. See the "Understanding Security Profiles" section on page 1-15 for more information. |
| Encrypted configuration files | Lets you ensure the privacy of phone configuration files. |

*Table 1-2 Overview of Security Features (continued)*

| Feature | Description |
|---|---|
| Optional disabling of the web server functionality for a phone | You can prevent access to a phone's web page, which displays a variety of operational statistics for the phone. |
| Phone hardening | Additional security options, which you control from Cisco Unified Communications Manager Administration:<br>• Disabling Gratuitous ARP (GARP)<br>• Disabling access to the Setting menus<br>• Disabling access to web pages for a phone<br>**Note** You can view current settings for the GARP Enabled, and Web Access options by looking at the phone's Device Information menu. For more information, see the "Viewing Security Information" section on page 8-2. |

**Related Topics**

- Understanding Security Profiles, page 1-15
- Identifying Encrypted and Authenticated Phone Calls, page 1-16
- Viewing Device Information, page 8-6
- Security Restrictions, page 1-17

# Understanding Security Profiles

A security profile, which defines whether the phone is non-secure, authenticated, or encrypted, is associated with every Cisco Unified IP Phone that is supported in Cisco Unified Communications Manager 5.0 and later. For information about configuring the security profile and applying the profile to the phone, refer to *Cisco Unified Communications Manager Security Guide*.

**Note** For Cisco Unified IP Phones using Cisco Unified CallManager 4.1 and later, security is configured on each phone. For more information about configuring security, refer to *Cisco Unified CallManager Security Guide, Release 4.1 (2)* or a later release document.

To view the security mode that is set for the phone, from the phone screen, choose **Settings > Device Information > Security > Security Mode**. For more information, see the "Viewing Security Information" section on page 8-2.

### Related Topics

- Identifying Encrypted and Authenticated Phone Calls, page 1-16
- Viewing Device Information, page 8-6
- Security Restrictions, page 1-17

## Identifying Encrypted and Authenticated Phone Calls

When security is implemented for a phone, you can identify authenticated or encrypted phone calls by icons on the screen on the phone.

In an authenticated call, all devices participating in the establishment of the call are authenticated by the Cisco Unified Communications Manager. When a call in progress is authenticated, the call progress icon to the right of the call duration timer in the phone screen changes to this icon: 🛡

In an encrypted call, all devices participating in the establishment of the call are authenticated by the Cisco Unified Communications Manager. In addition, call signaling and media streams are encrypted. An encrypted call offers the highest level of security, providing integrity and privacy to the call. When a call in progress is being encrypted, the call progress icon to the right of the call duration timer in the phone screen changes to this icon: 🔒

**Note** If the call is routed through non-IP call legs, such as the PSTN, the call might be non-secure even though it is encrypted within the IP network and has a lock icon associated with it.

### Related Topics

- Understanding Security Features for Cisco Unified IP Phones, page 1-10
- Understanding Security Profiles, page 1-15
- Security Restrictions, page 1-17

## Security Restrictions

When using a phone that is not configured for encryption, the user cannot barge into an encrypted call. When barge fails in this case, a reorder tone (fast busy tone) plays on the barge initiator's phone.

If the phone is configured for encryption, the user can barge into an authenticated or non-secure call from the encrypted phone. After the barge occurs, Cisco Unified Communications Manager classifies the call as non-secure.

If the phone is configured for encryption, the user can barge into an encrypted call, and the phone indicates that the call is encrypted.

A user can barge into an authenticated call, even if the phone that is used to barge is non-secure. The authentication icon continues to display on the authenticated phones in the call, even if the initiator's phone does not support security.

# Overview of Configuring and Installing the Cisco Unified Wireless IP Phone 7921G

When deploying a new IP telephony system, system administrators and network administrators must complete several initial configuration tasks to prepare the network for IP telephony service. For information and a checklist for setting up and configuring a complete Cisco IP telephony network, refer to the "System Configuration Overview" chapter in the *Cisco Unified Communications Manager System Guide*.

To add wireless IP phones to the IP network, system administrators also must perform a site survey to determine where to place and install access points (APs) for wireless voice coverage. For detailed information about a voice over WLAN deployment, refer to the *Cisco Enterprise Mobility 3.0 Design Guide*.

After you have set up the IP telephony system and configured system-wide features in Cisco Unified Communications Manager, you can add IP phones to the system.

The following topics provide an overview of procedures for adding Cisco Unified IP Phones to your network:

- Configuring the Cisco Unified Wireless IP Phone 7921G in Cisco Unified Communications Manager, page 1-18

- Installing the Cisco Unified Wireless IP Phone 7921G, page 1-19

## Configuring the Cisco Unified Wireless IP Phone 7921G in Cisco Unified Communications Manager

To add phones to the Cisco Unified Communications Manager database, you can use:

- Auto-registration
- Cisco Unified Communications Manager Administration
- Bulk Administration Tool (BAT)
- BAT and the Tool for Auto-Registered Phones Support (TAPS)

For more information about these choices, see the "Methods for Adding Phones to Cisco Unified Communications Manager" section on page 3-3.

For general information about configuring phones in Cisco Unified Communications Manager, refer to the "Cisco Unified IP Phone" chapter in the *Cisco Unified Communications Manager System Guide*.

For a checklist of tasks for configuring the phone in Cisco Unified Communications Manager, see the "Configuring the Cisco Unified Wireless IP Phone 7921G in Cisco Unified Communications Manager" section on page D-6.

### Related Topics

- Installing the Cisco Unified Wireless IP Phone 7921G, page 1-19
- Configuring Features, Templates, Services, and Users, page 7-1
- Configuring the Cisco Unified Wireless IP Phone 7921G in Cisco Unified Communications Manager, page D-6

# Installing the Cisco Unified Wireless IP Phone 7921G

After you have added the phones to the Cisco Unified Communications Manager database, you can complete the phone installation. You (or the phone users) can install the phone at the users's location. The Cisco Unified Wireless IP Phone Installation Guide that ships in the box with each phone provides directions for assembling the phone and accessories and charging the battery.

Prior to using the phone to connect to the wireless LAN, you need to configure a network profile for the phone. You can use the Cisco Unified Wireless IP  Phone 7921G web pages to set up the network profile and other phone settings, or you can configure the network profile using phone menus.

If you use auto-registration with Cisco Unified Communications Manager, you need to update the specific configuration information for the phone such as associating the phone with a user, changing the softkey template, or directory number.

**Note** Before you install a phone, even if it is new, upgrade the phone to the current firmware image. For information about upgrading, refer to the Readme file for your phone which is located at:
http://www.cisco.com/cgi-bin/tablebuild.pl/ip-7900ser-crypto

For a checklist of tasks for installing the phone, see the "Installing the Cisco Unified Wireless IP Phone 7921G" section on page D-10.

### Related Topics

- Understanding the Cisco Unified Wireless IP Phone 7921G, page 1-2
- Configuring the Cisco Unified Wireless IP Phone 7921G in Cisco Unified Communications Manager, page 1-18
- Installing the Cisco Unified Wireless IP Phone 7921G, page D-10
- Troubleshooting the Cisco Unified Wireless IP Phone 7921G, page 10-1

# Notices

The following notices pertain to this software license.

## OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

### License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

**OpenSSL License:**

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

### Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the

SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].