ATWINC15x0

Transport Layer Security (TLS) User's Guide

Introduction

This user's guide describes the ATWINC1500 Wi-Fi Network Controller to build state-of-the-art Internet of Things (IoT) applications.

The following topics will be covered:

- How examples are organized
- Target board information
- Instructions for each example
- TLS 1.2 supported cipher suites
- Certificate Installation on ATWINC1500
- ATECC508 crypto device support

Prerequisites

- Hardware Prerequisites:
  - SAM D21 Xplained Pro Evaluation Kit
  - ATWINC1500 extension
  - Micro-USB Cable (Micro-A/Micro-B)
- Software Prerequisites:
  - Atmel Studio 7.0
  - Wi-Fi® TLS TCP Server application

Figure 1. SAM D21 XSTK Board Demo Setup

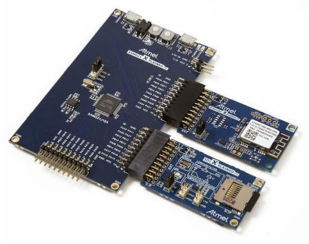


Table of Contents

1. Overview

The ATWINC1500 features an embedded low-memory footprint TLS protocol stack bundled within the ATWINC1500 firmware.

The following features are supported:

- TLS versions TLS1.0, TLS1.1 and TLS1.2
- TLS client operation with TLS client authentication
- TLS server mode

The TLS stack has a simple application interface. TLS functionality is abstracted by the socket interface of the ATWINC1500, thereby hiding the implementation complexity from the application developer and minimizing the porting effort of plain TCP code to TLS.

1.1 TLS Supported Ciphers

ATWINC1500 supports the following cipher suites (for both Client and Server modes):

1. TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
2. TLS_RSA_WITH_AES_128_GCM_SHA256
3. TLS_DHE_RSA_WITH_AES_128_CBC_SHA
4. TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
5. TLS_RSA_WITH_AES_128_CBC_SHA
6. TLS_RSA_WITH_AES_128_CBC_SHA256

Optionally supports ECC cipher suites:

1. TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
2. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
3. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
4. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
5. TLS_ECDHE_ ECDSA _WITH_AES_128_CBC_SHA256

1.2 TLS Certificate Store on ATWINC1500 Stacked Flash

For proper operation of both the TLS server and TLS client authentication, the ATWINC1500 device must have a certificate/private key pair assigned to it.

An 8KB flash area is reserved for storing the TLS certificates starting from offset 20KB in the ATWINC1500 stacked flash.

1.3 TLS Certificate Constraints

For TLS server and TLS client authentication, ATWINC1500 accepts the following certificate types:

- RSA certificates with a key size no greater than 2048 bits
- ECDSA certificates for NIST P256 EC Curve (secp256r1) only (conditionally supported)

2. TLS Certificate Installation

TLS certificate data is installed on the ATWINC1500 stacked flash by using either the `image_builder.exe` tool or the dedicated tool `tls_cert_flash_tool.exe`.

The following subsections describe both approaches.

Note: The `tls_cert_flash_tool` is invoked from `download_all.bat` after the firmware image is downloaded to the flash (like the `root_certificate_downloader` tool). So, the `download_all.bat` may be edited to change this behavior or change the file paths.

2.1 Certificate Installation (`tls_cert_flash_tool` Write)

The `tls_cert_flash_tool` writes the certificate data on the ATWINC1500 stacked flash directly (similar to the `root_certificate_downloader` tool). It patches an existing ATWINC1500 binary firmware image file.

By default, the tool writes to the flash. If a firmware image file is specified, the tool will patch the provided image file.

2.1.1 Syntax

The following figure describes the usage of the <`Write`> command.

```
Write X.509 Certificate chain on WINC Device Flash or a given WINC firmware
image file
 [Usage]: tls_cert_flash_tool.exe write [options]
 where options are:
 -key file      Private key in PEM format (RSA Keys only). It MUST NOT be
                encrypted.
 -nokey         The private key is not present. This is meaningful if a the
                private key is hidden into a secure hardware. This is the
                typical case of using ECC508 for ECC secure key storage
 -cert file     X.509 Certificate file in PEM or DER format. The certificate
                SHALL contain the public key associated with the given
                private key (If the private key is given).
 -cadir path    [Optional] Path to a folder containing the intermediate CAs
                and the Root CA of the given certificate.
 -fwimg path    [Optional] Path to the firmware binary image file.
                If this option is not given, the keys shall be written
                directly on the WINC Device Flash
 -erase         Erase the certificate store before writing. If this option is
                not given, the new certificate data is appended to the
                certificate store

  Examples
    tls_cert_flash_tool.exe Write -key rsa.key -cert rsa.cer -erase
    tls_cert_flash_tool.exe Write -nokey -cert ecdsa.cer -cadir CADir
    tls_cert_flash_tool.exe Write -key rsa.key -cert rsa.cer -cadir CADir
    tls_cert_flash_tool.exe Write -key rsa.key -cert rsa.cer -fwimg
m2m_aio_3a0.bin
```

2.1.2 Command Line Parameters

Option	Type	M/C/O	Description
-erase	—	O	Clear the TLS certificate section before writing the supplied data. If this option is not specified, the TLS Certificate section will be updated (the new certificate data is appended to the section).
-key <file>	File in PEM format	C	Private key file for the device. The tool can parse only RSA private keys. This is a conditional option (it MUST exist for an RSA certificate chain).
-nokey	—	C	No private key file is supplied to the tool. This is the useful when using a secure storage for private keys (the case of ATECC508).
-cert <file>	File in PEM or DER format	M	An X.509 end user certificate issued for the ATWINC1500 device. It must be associated with the given private key file (the certificate binds the public key that corresponds to the given private key).
-cadir <dir>	Folder	O	A directory (or folder) containing intermediate CA certificates and/or the Root CA certificate of the ATWINC1500 certificate chain(s).
-fwimg <file>	FW Bin IMG	O	Specifies a ATWINC1500 firmware All-in-One (AIO) image file (m2m_aio_3a0.bin) to patch. If this option is not specified, the tool will attempt to write on the ATWINC1500 stacked flash.

Note: For certificate chains with a depth larger than 1 (the End User Certificate is signed with an intermediate CA certificate rather than the Root Certificate directly), the -cadir option must be given with the directory containing the valid Intermediate CA certificate file(s). If this is not done, the connection may be refused by the server when TLS client authentication is used.

2.1.3 Typical Usage Scenarios

The `tls_cert_flash_tool` is not designed as a general purpose certificate conversion tool. It is intended to support the following use cases:

1. RSA authentication only (i.e., an RSA certificate with its private key is installed)
2. ECDSA authentication only (i.e., an ECDSA certificate is installed)
3. Both RSA and ECDSA are supported on the device, and therefore both certificates are installed

The following subsections illustrate using the tool in the three cases.

2.1.3.1 RSA Authentication Only

Install an RSA Certificate along with its private key (write directly on the ATWINC1500 stacked flash).

```
tls_cert_flash_tool.exe WRITE -key rsa.key -cert rsa.cer –cadir CA –erase
```

Install an RSA Certificate along with its private key (patch an existing ATWINC1500 device firmware image file).

```
tls_cert_flash_tool.exe write -key rsa.key -cert rsa.cer –erase –fwimg
m2m_aio_3a0.bin
```

2.1.3.2 ECDSA Authentication Only

Install an ECDSA certificate with no private key supplied (write directly on the ATWINC1500 stacked flash).

```
tls_cert_flash_tool.exe write -nokey -cert ecdsa.cer –cadir CA –erase
```

Install an ECDSA certificate (patch an existing ATWINC1500 device firmware image file).

```
tls_cert_flash_tool.exe -nokey -cert ecdsa.cer –cadir CA –erase –fwimg
m2m_aio_3a0.bin
```

2.1.3.3 Both ECDSA and RSA Authentication

```
tls_cert_flash_tool.exe write -key rsa.key -cert rsa.cer –cadir CA –erase
```

```
tls_cert_flash_tool.exe write -nokey -cert ecdsa.cer –cadir CA
```

2.2 Certificate Read (`tls_cert_flash_tool` Read)

```
Read X.509 Certificate chain from WINC Device Flash or a given WINC firmware
image file

 [Usage]: tls_cert_flash_tool.exe read [options]
 where options are:
 -rsa           Print WINC Device RSA certificate (if any)
 -ecdsa         Print WINC Device ECDSA certificate (if any)
 -dir           List all files in the WINC TLS Certificate Store associated
                with the selected authentication (rsa or ecdsa or both)
 -fwimg path    [Optional] Path to the firmware binary image file.
                If this option is not given, the certificates shall be read
                directly from the WINC Device Flash
 -out path      A path to a directory where the certificates will be saved.
This
                option forces the certificates to be written in files. If
this option
                is not specified, the certificates shall be printed on
standard out.
 -all           Dump all certificates in the WINC certificate chain
provisioned on WINC
                (if any) in addition to the WINC Device certificate.
 -privkey       Print the RSA private key (if -rsa option is given) to the
standard out.
                The RSA private dumping is off by default.

  Examples
    tls_cert_flash_tool.exe read -rsa -privkey -dir
    tls_cert_flash_tool.exe read -rsa -all
    tls_cert_flash_tool.exe read -rsa -out C:/Certs/
    tls_cert_flash_tool.exe read -rsa -ecdsa -dir-fwimg m2m_aio_3a0.bin
```

Option	Type	M/C/O	Description
-rsa	—	O	Print the ATWINC1500 device RSA certificate
-ecdsa	—	O	Print the ATWINC1500 device ECDSA certificate
-dir	—	O	List all files in the ATWINC1500 TLS certificate store associated with the selected authentication (RSA or ECDSA or both)
-out <dir>	Path to a folder	O	A directory (or folder) in which the tool will write the certificate files
-all	—	O	A directory (or folder) containing intermediate CA certificates and/or the Root CA certificate of the ATWINC1500 certificate chain(s)

-fwimg <file>	FW Bin IMG	O	Specifies a ATWINC1500 firmware All-in-One (AIO) image file (m2m_aio_3a0.bin) to patch. If this option is not specified, the tool will attempt to write on the ATWINC1500 stacked flash
-privkey	—	O	Force private key printing. If not specified, the private key will not be printed

2.3 Using image_builder Tool to Install Certificates

The `image_builder` tool can compile the TLS certificate data into the ATWINC1500 firmware image file when it builds the All-in-One image (*m2m_aio_3a0.bin*).

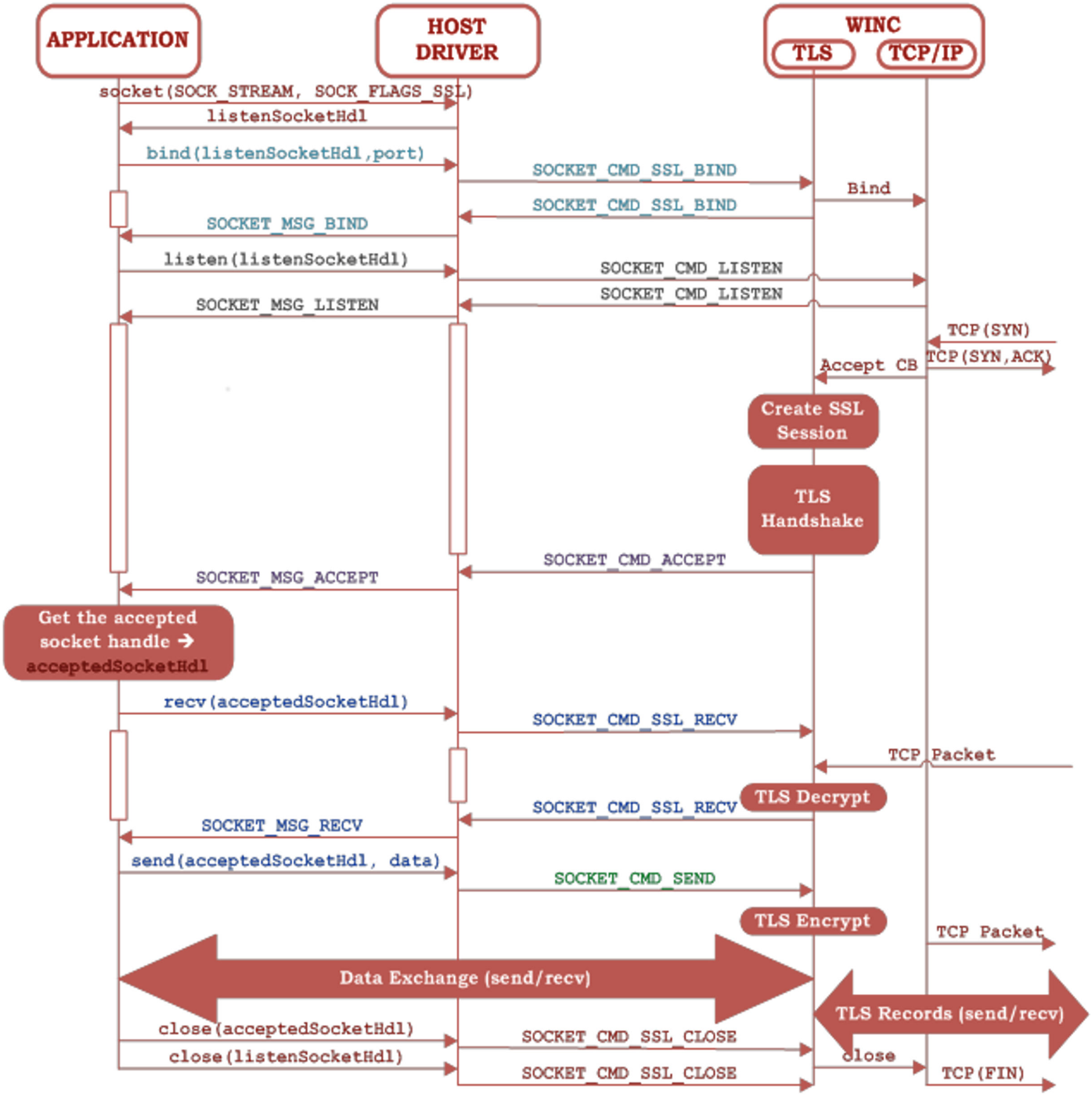
ATWINC1500 sample certificates are available in ASF under the “WINC1500_FIRMWARE_UPDATE_PROJECT\src\firmware\tls_cert_store” for demo purposes.

3. TLS Server APIs

From the application's point of view, the TLS functionality is wrapped behind the socket APIs. This hides the complexity of TLS from the application, which can use the TLS in the same fashion as that of the TCP (non-TLS) server. The main difference between TLS sockets and regular TCP sockets is that the application sets the `SOCKET_FLAGS_SSL` while creating the TLS server listening socket. The detailed sequence of the TLS connection establishment is described in the figure below.

For proper TLS server operation, ensure that both the `SOCKET_FLAGS_SSL` flag and the correct port number are set in the TLS server application. For instance, an HTTP server application cannot use flags while calling the socket API function and bind to port 80. The same application source code becomes an HTTPS server application if you use the flag `SOCKET_FLAGS_SSL` and change the port number to bind to port 443.

Figure 3-1. TLS Server Connection Flow



4. Document Version History

Revision A (April 2017)

- Initial release.

The Microchip Web Site

Microchip provides online support via our web site at http://www.microchip.com/. This web site is used as a means to make files and information easily available to customers. Accessible by using your favorite Internet browser, the web site contains the following information:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user’s guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQ), technical support requests, online discussion groups, Microchip consultant program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

Customer Change Notification Service

Microchip’s customer notification service helps keep customers current on Microchip products. Subscribers will receive e-mail notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, access the Microchip web site at http://www.microchip.com/. Under “Support”, click on “Customer Change Notification” and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Field Application Engineer (FAE)
- Technical Support

Customers should contact their distributor, representative or Field Application Engineer (FAE) for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in the back of this document.

Technical support is available through the web site at: http://www.microchip.com/support

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip’s Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.

- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as “unbreakable.”

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip’s code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Legal Notice

Information contained in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION, INCLUDING BUT NOT LIMITED TO ITS CONDITION, QUALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR PURPOSE. Microchip disclaims all liability arising from this information and its use. Use of Microchip devices in life support and/or safety applications is entirely at the buyer’s risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

Trademarks

The Microchip name and logo, the Microchip logo, AnyRate, AVR, AVR logo, AVR Freaks, BeaconThings, BitCloud, CryptoMemory, CryptoRF, dsPIC, FlashFlex, flexPWR, Heldo, JukeBlox, KeeLoq, KeeLoq logo, Kleer, LANCheck, LINK MD, maXStylus, maXTouch, MediaLB, megaAVR, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, Prochip Designer, QTouch, RightTouch, SAM-BA, SpyNIC, SST, SST Logo, SuperFlash, tinyAVR, UNI/O, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

ClockWorks, The Embedded Control Solutions Company, EtherSynch, Hyper Speed Control, HyperLight Load, IntelliMOS, mTouch, Precision Edge, and Quiet-Wire are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Adjacent Key Suppression, AKS, Analog-for-the-Digital Age, Any Capacitor, AnyIn, AnyOut, BodyCom, chipKIT, chipKIT logo, CodeGuard, CryptoAuthentication, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, EtherGREEN, In-Circuit Serial Programming, ICSP, Inter-Chip Connectivity, JitterBlocker, KleerNet, KleerNet logo, Mindi, MiWi, motorBench, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, Omniscient Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, PureSilicon, QMatrix, RightTouch logo, REAL ICE, Ripple Blocker, SAM-ICE, Serial Quad I/O, SMART-I.S., SQI, SuperSwitcher, SuperSwitcher II, Total Endurance, TSHARC, USBCheck, VariSense, ViewSpan, WiperLock, Wireless DNA, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

Silicon Storage Technology is a registered trademark of Microchip Technology Inc. in other countries.

GestIC is a registered trademark of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

All other trademarks mentioned herein are property of their respective companies.

ISBN: 978-1-5224-1671-5

Quality Management System Certified by DNV

ISO/TS 16949

Microchip received ISO/TS-16949:2009 certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona; Gresham, Oregon and design centers in California and India. The Company's quality system processes and procedures are for its PIC® MCUs and dsPIC® DSCs, KEELOQ® code hopping devices, Serial EEPROMs, microperipherals, nonvolatile memory and analog products. In addition, Microchip's quality system for the design and manufacture of development systems is ISO 9001:2000 certified.

Worldwide Sales and Service

AMERICAS

Corporate Office
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-792-7200
Fax: 480-792-7277
Technical Support:
http://www.microchip.com/
support
Web Address:
www.microchip.com

Atlanta
Duluth, GA
Tel: 678-957-9614
Fax: 678-957-1455

Austin, TX
Tel: 512-257-3370

Boston
Westborough, MA
Tel: 774-760-0087
Fax: 774-760-0088

Chicago
Itasca, IL
Tel: 630-285-0071
Fax: 630-285-0075

Dallas
Addison, TX
Tel: 972-818-7423
Fax: 972-818-2924

Detroit
Novi, MI
Tel: 248-848-4000

Houston, TX
Tel: 281-894-5983

Indianapolis
Noblesville, IN
Tel: 317-773-8323
Fax: 317-773-5453
Tel: 317-536-2380

Los Angeles
Mission Viejo, CA
Tel: 949-462-9523
Fax: 949-462-9608
Tel: 951-273-7800

Raleigh, NC
Tel: 919-844-7510

New York, NY
Tel: 631-435-6000

San Jose, CA
Tel: 408-735-9110
Tel: 408-436-4270

Canada - Toronto
Tel: 905-695-1980
Fax: 905-695-2078

ASIA/PACIFIC

Asia Pacific Office
Suites 3707-14, 37th Floor
Tower 6, The Gateway
Harbour City, Kowloon

Hong Kong
Tel: 852-2943-5100
Fax: 852-2401-3431

Australia - Sydney
Tel: 61-2-9868-6733
Fax: 61-2-9868-6755

China - Beijing
Tel: 86-10-8569-7000
Fax: 86-10-8528-2104

China - Chengdu
Tel: 86-28-8665-5511
Fax: 86-28-8665-7889

China - Chongqing
Tel: 86-23-8980-9588
Fax: 86-23-8980-9500

China - Dongguan
Tel: 86-769-8702-9880

China - Guangzhou
Tel: 86-20-8755-8029

China - Hangzhou
Tel: 86-571-8792-8115
Fax: 86-571-8792-8116

China - Hong Kong SAR
Tel: 852-2943-5100
Fax: 852-2401-3431

China - Nanjing
Tel: 86-25-8473-2460
Fax: 86-25-8473-2470

China - Qingdao
Tel: 86-532-8502-7355
Fax: 86-532-8502-7205

China - Shanghai
Tel: 86-21-3326-8000
Fax: 86-21-3326-8021

China - Shenyang
Tel: 86-24-2334-2829
Fax: 86-24-2334-2393

China - Shenzhen
Tel: 86-755-8864-2200
Fax: 86-755-8203-1760

China - Wuhan
Tel: 86-27-5980-5300
Fax: 86-27-5980-5118

China - Xian
Tel: 86-29-8833-7252
Fax: 86-29-8833-7256

ASIA/PACIFIC

China - Xiamen
Tel: 86-592-2388138
Fax: 86-592-2388130

China - Zhuhai
Tel: 86-756-3210040
Fax: 86-756-3210049

India - Bangalore
Tel: 91-80-3090-4444
Fax: 91-80-3090-4123

India - New Delhi
Tel: 91-11-4160-8631
Fax: 91-11-4160-8632

India - Pune
Tel: 91-20-3019-1500

Japan - Osaka
Tel: 81-6-6152-7160
Fax: 81-6-6152-9310

Japan - Tokyo
Tel: 81-3-6880- 3770
Fax: 81-3-6880-3771

Korea - Daegu
Tel: 82-53-744-4301
Fax: 82-53-744-4302

Korea - Seoul
Tel: 82-2-554-7200
Fax: 82-2-558-5932 or
82-2-558-5934

Malaysia - Kuala Lumpur
Tel: 60-3-6201-9857
Fax: 60-3-6201-9859

Malaysia - Penang
Tel: 60-4-227-8870
Fax: 60-4-227-4068

Philippines - Manila
Tel: 63-2-634-9065
Fax: 63-2-634-9069

Singapore
Tel: 65-6334-8870
Fax: 65-6334-8850

Taiwan - Hsin Chu
Tel: 886-3-5778-366
Fax: 886-3-5770-955

Taiwan - Kaohsiung
Tel: 886-7-213-7830

Taiwan - Taipei
Tel: 886-2-2508-8600
Fax: 886-2-2508-0102

Thailand - Bangkok
Tel: 66-2-694-1351
Fax: 66-2-694-1350

EUROPE

Austria - Wels
Tel: 43-7242-2244-39
Fax: 43-7242-2244-393

Denmark - Copenhagen
Tel: 45-4450-2828
Fax: 45-4485-2829

Finland - Espoo
Tel: 358-9-4520-820

France - Paris
Tel: 33-1-69-53-63-20
Fax: 33-1-69-30-90-79

France - Saint Cloud
Tel: 33-1-30-60-70-00

Germany - Garching
Tel: 49-8931-9700

Germany - Haan
Tel: 49-2129-3766400

Germany - Heilbronn
Tel: 49-7131-67-3636

Germany - Karlsruhe
Tel: 49-721-625370

Germany - Munich
Tel: 49-89-627-144-0
Fax: 49-89-627-144-44

Germany - Rosenheim
Tel: 49-8031-354-560

Israel - Ra'anana
Tel: 972-9-744-7705

Italy - Milan
Tel: 39-0331-742611
Fax: 39-0331-466781

Italy - Padova
Tel: 39-049-7625286

Netherlands - Drunen
Tel: 31-416-690399
Fax: 31-416-690340

Norway - Trondheim
Tel: 47-7289-7561

Poland - Warsaw
Tel: 48-22-3325737

Romania - Bucharest
Tel: 40-21-407-87-50

Spain - Madrid
Tel: 34-91-708-08-90
Fax: 34-91-708-08-91

Sweden - Gothenberg
Tel: 46-31-704-60-40

Sweden - Stockholm
Tel: 46-8-5090-4654

UK - Wokingham
Tel: 44-118-921-5800
Fax: 44-118-921-5820