AN2698

针对 SAM L11 的安全 UART 自举程序

简介

许多现代化的嵌入式系统需要更新应用程序映像，以修复错误或支持新功能。知识产权保护在这一过程中起着关键作用。尽管单片机固件保护机制十分稳健，但是在从外部源传输数据时，固件容易被拦截。

要解决该问题，可以选择使用安全自举程序并且仅向公众分发固件的加密映像。本应用笔记介绍了 SAM L11 器件安全自举程序的设计、操作以及加密算法。

目录

1. 功能

安全 UART 自举程序具有以下特性：

- 安全
- 小尺寸（2 KB）
- 使用 UART RX 和 TX 引脚以及自举程序进入（Bootloader Entry）引脚
- 可自行更新
- 应用程序完整性验证
- 提供可按用户要求定制的源代码

2. 硬件配置

自举程序使用的 UART 引脚取决于器件型号，如下表所示。

表 2-1. 硬件配置

器件	UART Tx	UART Rx	进入引脚
SAM L11	PA16	PA17	PA19

自举程序进入引脚是一个低电平有效的引脚。在自举程序开始运行时，对引脚的值进行采样。虽然在对引脚进行采样之前会启用内部上拉电阻，但建议在外部上拉自举程序进入引脚以提高抗噪声能力。

安全自举程序的 UART 设置为 115200 8, N,1。

3. 进入方法

自举程序可通过多种方式调用：

1. 如果应用程序闪存区没有有效的应用程序，则自举程序会自动运行。如果应用程序映像中指定的字段大小小于器件的最大应用程序大小，且该字段大小是 256 字节减去 32 字节的倍数，则会将该应用程序视为有效应用程序。映像大小值必须位于应用程序映像起始偏移量的偏移 0x10 处。通常情况下，该值由保留的异常向量占用，因此不会干扰该应用程序代码。
   此外，可通过 SHA-256 哈希值验证映像完整性。哈希值必须位于该应用程序映像后的 32 个字节处。
2. 如果自举程序开始运行时，自举程序进入引脚的值较小，则自举程序按外部请求运行。

外部复位优先于任何其他进入方法。

4. 器件配置

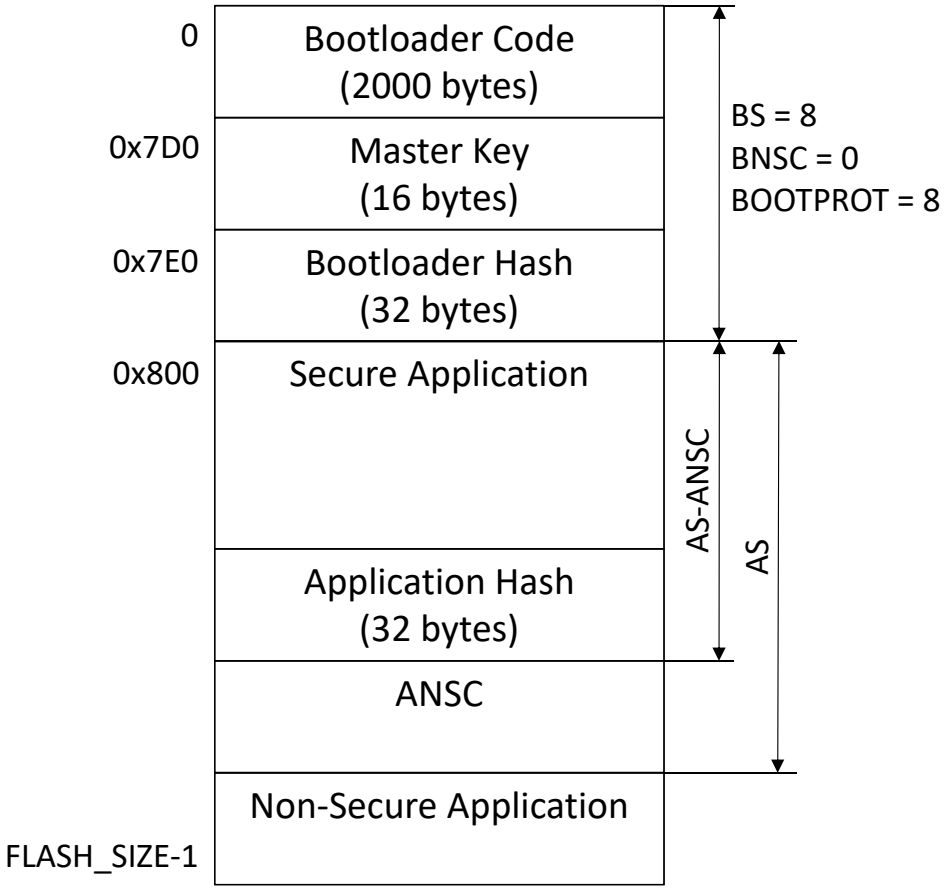
为确保全方位保护敏感信息，必须对 NVM 引导配置行（Boot Configuration Row，BOCOR）进行以下设置：

- 引导闪存安全大小（BS）= 8
- 引导闪存非安全可调用大小（BNSC）= 0
- 引导保护大小（BOOTPROT）= 8
- 引导选项（BOOTOPT）= 1
- 引导配置 CRC（BOCORCRC）= 正确的 BOCOR CRC32 值
- 引导配置行哈希值（BOCORHASH）= 正确的 BOCOR SHA-256 值

必须正确计算 BOCORCRC 和 BOCORHASH 并对其进行编程，引导 ROM 才能确认该应用程序。有关更多详细信息，请参见 SAM L11 产品数据手册的“引导 ROM”章节。

存储器映射中指定的熔丝设置结果如下图所示：

图 4-1. SAM L11 闪存映射



此外，必须在执行自举程序之前清除用户行位 RXN（永不执行 RAM），因为自举程序从 SRAM 中运行以便自行更新。

5. 自举程序命令

所有自举程序命令都采用同一通用格式，如下表所示。

表 5-1. 自举程序命令

命令 ID	保护值	数据 0	...	数据 N
1 字节	4 字节	4 字节	...	4 字节

数据字的数量和含义因命令而异。所有数据字必须采用小尾数法（LSB 优先）格式发送。

保护值必须是 0x2b620bc3 常数值，以便对乱真命令提供额外保护。

命令帧中所有字节的发送间隔不能大于 100 ms。在 100 ms 的空闲时间之后，将丢弃不完整的命令，自举程序返回并等待接收新的命令 ID。如果存在同步丢失的问题，此行为允许主机重新进行同步。

自举程序可以识别以下命令：

1. `Unlock (0xA0)`
2. `Data (0xA1)`
3. `Verify (0xA2)`

`Unlock` 命令必须在第一个 `Data` 命令发出之前发出，包含以下有效载荷：

- 数据 0——起始偏移量
- 数据 1——映像大小
- 数据 2 至数据 5—— 杜撰数据

起始偏移量是指从闪存开始算起的偏移量。要升级自举程序，必须将该值设置为零。

应用程序的映像偏移与器件有关，有效值列在下表中。映像偏移必须与擦除单元大小的边界对齐，该边界也与器件有关。映像大小必须以擦除单元字节为增量。

表 5-2. 应用程序映像偏移的有效值

器件	应用程序偏移（字节）	擦除单元大小（字节）
SAM L11	2048	256

杜撰数据是一个任意的 16 字节值，给定密钥的值不能重复。该数字可以是计数器上的增量值、随机字节序列或两者组合的数字。如果使用随机数，请确保其熵源可靠。有关使用此数字进行加密和验证的详细信息，请参见附录 A。

`Data` 命令用于发送映像数据，并包含以下有效载荷：

- 数据 0——起始偏移量
- 数据 1 至数据 N—— 映像数据（擦除单元大小字节）
- 数据 N+1 至数据 N+17——映像 MAC（16 字节）

起始偏移量必须位于之前通过 `Unlock` 命令解锁的区域。任何尝试在解锁区域之外进行写入的请求都会产生错误，且会丢弃所提供的数据。

映像数据必须加密和验证。映像消息验证码（Message Authentication Code，MAC）可确保数据通过验证，并且在传输过程中不会损坏。MAC 还可确保数据处于当前存储单元和当前文件内。有关生成和使用此数字进行验证和加密的详细信息，请参见附录 A。

该自举程序支持闪存同时写入和接收下一个数据块。一旦第一个状态码返回，就会发送下一个数据块。

由于会出现此行为，因此将最后一个数据块写入闪存之前，需要发送最后一个数据块的状态码。若要确保写入此数据块，主机必须发送另一个命令并等待响应。因此，必须在最后一个数据块之后发送 `Verify` 或 `Reset` 命令。

`Verify` 命令用于验证映像数据且不包含有效负载。通过 MAC 确保数据传输期间的映像完整性，自举程序可以读回写入闪存的数据。在映像上传期间，随时都可以发出 `Verify` 命令，因为将返回验证状态的当前值。

`Reset` 命令用于退出自举程序并运行应用程序，除了使用自举程序进入引脚进入自举程序的情况。在特定情况下，完成进入引脚编程后，必须将进入引脚值设置为高电平，且必须进行硬件复位才能运行该应用程序。

`Reset` 命令包含以下有效载荷：

- 数据 0 — 任意值 0
- 数据 1 — 任意值 1
- 数据 2 — 任意值 2
- 数据 3 — 任意值 3

提供的任意值将传递到 SRAM 前四个存储单元处的应用程序。

6. 响应代码

自举程序会发送单字符响应代码以响应每个命令。在收到上一个命令的响应代码之后或者若超过 100 ms 未响应，可发送顺序命令。

以下是可能采用的响应代码：

- OK (0x50) — 已成功接收和处理命令
- Error (0x51) — 处理命令期间出错
- Invalid (0x52) — 收到无效命令
- CRC OK (0x53) — CRC 校验成功
- CRC Fail (0x54) — CRC 校验失败

7. 编程算法

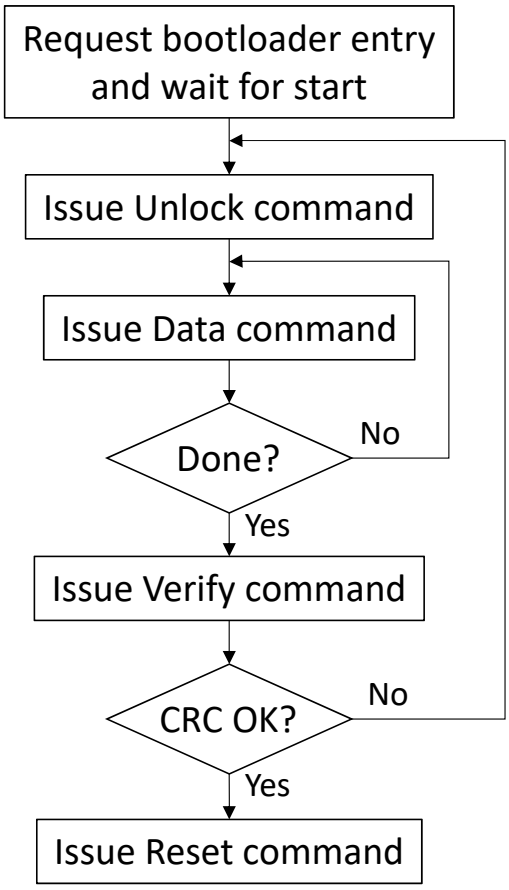
发出每个命令后，主机至少等待 100 ms 才能收到响应代码。如果在此期间没有收到响应代码，则该命令可视为丢失并且可以重复执行该命令。

主机控制器必须执行以下操作才能更新固件：

1. 请求自举程序进入。
2. 等待至少 50 ms 以启动自举程序。
3. 使用所需的映像参数发出 `Unlock` 命令。
4. 使用应用程序数据发送 `Data` 命令。
5. 重复第 4 项，直到传输完整个映像。
6. 发出 `Verify` 命令，并检查响应代码。
7. 如果响应代码为 CRC Fail，则从第 3 项开始进行重复更新。
8. 发出 `Reset` 命令。

下图中对该算法进行了说明：

图 7-1. 编程算法



8. 附录 A：安全步骤

本节基于主机角度介绍安全步骤。自举程序执行步骤与此类似，但顺序相反。

该自举程序使用基于 AES-128 的 CBC-MAC 发出命令并进行数据验证，使用输出反馈（Output Feedback，OFB）模式下的 AES-128 对传输的数据进行加密。

数据的安全性和验证以存储在自举程序最后 16 个字节中的主密钥为基础。如果对自举程序映像进行初始化编程后，需要更新密钥，则必须替换整个自举程序。这是必要步骤，因为密钥值包含在自举程序的 SHA-256 哈希值中。自举程序的更新方式与常规应用程序相同，因此需要进行完整的安全处理。这意味着旧密钥必须用于新密钥的加密和验证。如果旧密钥丢失，则无法使用此自举程序恢复器件。

默认加密密钥为 `00:01:02:03:04:05:06:07:08:09:0a:0b:0c:0d:0e:0f`。

恰当的安全做法是永远不要直接使用主密钥。相反，要从主密钥和特定于给定会话或应用程序映像的其他信息派生会话密钥。

采用以下步骤获取会话密钥：

```
GenerateSessionKey(StartingOffset, ImageSize, MasterKey)
    Temp = (StartingOffset || ImageSize || 0x00000000 || 0x00000000)
    SessionKey = AES(AES(Nonce, MasterKey) ^ Temp, MasterKey)
```

其中，“||”是串联运算符，0x00000000 是 32 位补零值，而 AES（密钥，数据）是使用该密钥在 16 字节数据上进行的 AES-128 操作。起始偏移量和映像大小必须与通过 Unlock 命令传递的对应值匹配。

生成的会话密钥对于闪存中的特定映像和存储单元是唯一的。杜撰数据用于消除可能重复的会话密钥，因为典型的应用程序映像的偏移量位置相同，且其大小大致相同。

会话密钥长度为 16 个字节，用于加密和验证操作。

加密和验证程序对在擦除块大小边界处对齐的数据块进行操作。该程序使用命令头（块偏移）确保已验证的数据无法写入其他位置。加密算法将数据拆分为 16 字节块，然后使用 AES-128 算法加密。数据块加密后，需要验证，因为加密处理易受密码文本修改的影响，而在解密阶段无法检测密码文本修改。

```
EncryptAndAuthenticateBlock(SessionKey, BlockOffset, Data)
    Result = GuardValue || BlockOffset
    EncIV  = (offset || 0x00000000 || 0x00000000 || 0x00000000)
    MacTemp = (offset || 0x00000000 || 0x00000000 || 0x00000000)
    MAC = AES(MacTemp, SessionKey)
    for Block in Data:
        EncTemp = AES(EncIV, SessionKey)
        EncBlock = Block ^ EncTemp
        EncIV = EncTemp
        MAC = AES(MAC ^ EncBlock,  SessionKey)
        Result = Result || EncBlock
    return Result || MAC
```

此 Python 脚本以上述安全步骤为基础，用于生成加密映像并对其进行编程。关于更多详细信息，请参见附录 B。

9. 附录 B：与自举程序搭配使用的 PC 实用程序（加密映像）

自举程序具有多个评估实用程序。流程可分为准备通过开放渠道自由分发的加密映像和实际更新。

encrypt.py 是一个加密实用程序。其语法如下：

选项：

```
-h, --help              show this help message and exit
-f FILE, --file=FILE    input file
-k KEY, --key=KEY encryption key (16 bytes separated with ':')
-o OFFS, --offset=OFFS destination offset (default 0x800)
```

示例调用（单行）：

```
python encrypt.py -k 00:01:02:03:04:05:06:07:08:09:0a:0b:0c:0d:0e:0f -f test_app_l11.bin
```

encrypt.py 会将后缀.enc 添加到输入文件名中，以获取输出文件名。

每次调用都会产生不同的文件内容，因为每次调用都会生成一个随机杜撰数据。

boot.py 是一个更新实用程序，用于获取加密映像并通过串行端口上传。其语法如下：

选项：

```
-h, --help                  show this help message and exit
-v, --verbose               enable verbose output
-i PATH, --interface=PATH   communication interface
-f FILE, --file=FILE        binary file to program
--boot                      enable write to the bootloader area
```

示例调用（单行）：

```
python boot.py -v -i COM12 -t -f test_app_l11.bin.enc
```

如果加密映像的偏移量小于自举程序大小，则--boot 是必选项。这是为了避免自举程序意外重写而提供的额外保护。

key_update.py 是一个用于设置或更新自举程序映像中加密密钥的实用程序。该实用程序还可以计算并附加自举程序映像的 SHA-256 哈希值。该文件可就地更新，其语法如下：

选项：

```
-h, --help              show this help message and exit
-f FILE, --file=FILE    output file name
-k KEY, --key=KEY       encryption key (16 bytes separated with ':')
```

示例调用（单行）：

```
key_update.py -k 0:1:2:3:4:5:6:7:8:9:0:1:2:3:4:5 -f bootloader_l11.bin
```

注： 除 Python 软件外，还需要 pySerial 模块才能访问串行端口。

Microchip 网站

Microchip 网站 http://www.microchip.com/为客户提供在线支持。客户可通过该网站方便地获取文件和信息。只要使用常用的互联网浏览器即可访问，网站提供以下信息：

- **产品支持**——数据手册和勘误表、应用笔记和示例程序、设计资源、用户指南以及硬件支持文档、最新的软件版本以及归档软件
- **一般技术支持**——常见问题（FAQ）、技术支持请求、在线讨论组以及 Microchip 顾问计划成员名单
- **Microchip 业务**——产品选型和订购指南、最新 Microchip 新闻稿、研讨会和活动安排表、Microchip 销售办事处、代理商以及工厂代表列表

变更通知客户服务

Microchip 的变更通知客户服务有助于客户了解 Microchip 产品的最新信息。注册客户可在他们感兴趣的某个产品系列或开发工具发生变更、更新、发布新版本或勘误表时，收到电子邮件通知。

欲注册，请登录 Microchip 网站 http://www.microchip.com/。在“支持”（Support）下，点击“变更通知客户”（Customer Change Notification）服务后按照注册说明完成注册。

客户支持

Microchip 产品的用户可通过以下渠道获得帮助：

- 代理商或代表
- 当地销售办事处
- 应用工程师（FAE）
- 技术支持

客户应联系其代理商、代表或应用工程师（FAE）寻求支持。当地销售办事处也可为客户提供帮助。本文档后附有销售办事处的联系方式。

也可通过以下网站获得技术支持： http://www.microchip.com/support

Microchip 器件代码保护功能

请注意以下有关 Microchip 器件代码保护功能的要点：

- Microchip 的产品均达到 Microchip 数据手册中所述的技术指标。
- Microchip 确信：在正常使用的情况下，Microchip 系列产品是当今市场上同类产品中最安全的产品之一。
- 目前，仍存在着恶意、甚至是非法破坏代码保护功能的行为。就我们所知，所有这些行为都不是以 Microchip 数据手册中规定的操作规范来使用 Microchip 产品的。这样做的人极可能侵犯了知识产权。
- Microchip 愿意与关心代码完整性的客户合作。
- Microchip 或任何其他半导体厂商均无法保证其代码的安全性。代码保护并不意味着我们保证产品是“牢不可破”的。

代码保护功能处于持续发展中。Microchip 承诺将不断改进产品的代码保护功能。任何试图破坏 Microchip 代码保护功能的行为均可视为违反了《数字器件千年版权法案（Digital Millennium Copyright Act）》。如

果这种行为导致他人在未经授权的情况下，能访问您的软件或其他受版权保护的成果，您有权依据该法案提起诉讼，从而制止这种行为。

法律声明

本出版物中所述的器件应用信息及其他类似内容仅为您提供便利，它们可能由更新之信息所替代。确保应用符合技术规范，是您自身应负的责任。Microchip 对这些信息不作任何明示或暗示、书面或口头、法定或其他形式的声明或担保，包括但不限于针对其使用情况、质量、性能、适销性或特定用途的适用性的声明或担保。Microchip 对因这些信息及使用这些信息而引起的后果不承担任何责任。如果将 Microchip 器件用于生命维持和/或生命安全应用，一切风险由买方自负。买方同意在由此引发任何一切伤害、索赔、诉讼或费用时，会维护和保障 Microchip 免于承担法律责任，并加以赔偿。除非另外声明，否则在 Microchip 知识产权保护下，不得暗中或以其他方式转让任何许可证。

商标

Microchip 的名称和徽标组合、Microchip 徽标、AnyRate、AVR、AVR 徽标、AVR Freaks、BitCloud、chipKIT、chipKIT 徽标、CryptoMemory、CryptoRF、dsPIC、FlashFlex、flexPWR、Heldo、JukeBlox、KeeLoq、Kleer、LANCheck、LINK MD、maXStylus、maXTouch、MediaLB、megaAVR、MOST、MOST 徽标、MPLAB、OptoLyzer、PIC、picoPower、PICSTART、PIC32 徽标、Prochip Designer、QTouch、SAM-BA、SpyNIC、SST、SST 徽标、SuperFlash、tinyAVR、UNI/O 和 XMEGA 是 Microchip Technology Incorporated 在美国和其他国家或地区的注册商标。

ClockWorks、The Embedded Control Solutions Company、EtherSynch、Hyper Speed Control、HyperLight Load、IntelliMOS、mTouch、Precision Edge 和 Quiet-Wire 为 Microchip Technology Incorporated 在美国的注册商标。

Adjacent Key Suppression、AKS、Analog-for-the-Digital Age、Any Capacitor、AnyIn、AnyOut、BodyCom、CodeGuard、CryptoAuthentication、CryptoAutomotive、CryptoCompanion、CryptoController、dsPICDEM、dsPICDEM.net、Dynamic Average Matching、DAM、ECAN、EtherGREEN、In-Circuit Serial Programming、ICSP、INICnet、Inter-Chip Connectivity、JitterBlocker、KleerNet、KleerNet 徽标、memBrain、Mindi、MiWi、motorBench、MPASM、MPF、MPLAB Certified 徽标、MPLIB、MPLINK、MultiTRAK、NetDetach、Omniscient Code Generation、PICDEM、PICDEM.net、PICkit、PICtail、PowerSmart、PureSilicon、QMatrix、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 和 ZENA 为 Microchip Technology Incorporated 在美国和其他国家或地区的商标。

SQTP 为 Microchip Technology Inc.在美国的服务标记。

Silicon Storage Technology 为 Microchip Technology Inc.在除美国外的国家或地区的注册商标。

GestIC 是 Microchip Technology Inc.的子公司 Microchip Technology Germany II GmbH & Co. KG 在除美国外的国家或地区的注册商标。

在此提及的所有其他商标均为各持有公司所有。

ISBN： 978-1-5224-3901-1

DNV 认证的质量管理体系

ISO/TS 16949

Microchip 位于美国亚利桑那州 Chandler 和 Tempe 与位于俄勒冈州 Gresham 的全球总部、设计和晶圆生产厂及位于美国加利福尼亚州和印度的设计中心均通过了 ISO/TS-16949:2009 认证。Microchip 的 PIC® MCU 和 dsPIC® DSC、KEELOQ®跳码器件、串行 EEPROM、单片机外设、非易失性存储器及模拟产品严格遵守公司的质量体系流程。此外，Microchip 在开发系统的设计和生产方面的质量体系也已通过了 ISO 9001:2000 认证。

全球销售及服务网点

美洲	亚太地区	亚太地区	欧洲
公司总部 2355 West Chandler Blvd. Chandler, AZ 85224-6199 电话：1-480-792-7200 传真：1-480-792-7277 技术支持： http://www.microchip.com/support 网址： www.microchip.com **亚特兰大** 德卢斯，乔治亚州 电话：1-678-957-9614 传真：1-678-957-1455 **奥斯汀，德克萨斯州** 电话：1-512-257-3370 **波士顿** 韦斯特伯鲁，马萨诸塞州 电话：1-774-760-0087 传真：1-774-760-0088 **芝加哥** 艾塔斯卡，伊利诺伊州 电话：1-630-285-0071 传真：1-630-285-0075 **达拉斯** 艾迪生，德克萨斯州 电话：1-972-818-7423 传真：1-972-818-2924 **底特律** 诺维，密歇根州 电话：1-248-848-4000 **休斯敦，德克萨斯州** 电话：1-281-894-5983 **印第安纳波利斯** 诺布尔斯维尔，印第安纳州 电话：1-317-773-8323 传真：1-317-773-5453 电话：1-317-536-2380 **洛杉矶** 米申维耶霍，加利福尼亚州 电话：1-949-462-9523 传真：1-949-462-9608 电话：1-951-273-7800 **罗利，北卡罗来纳州** 电话：1-919-844-7510 **纽约，纽约州** 电话：1-631-435-6000 **圣何塞，加利福尼亚州** 电话：1-408-735-9110 电话：1-408-436-4270 **加拿大 - 多伦多** 电话：1-905-695-1980 传真：1-905-695-2078	**中国 - 北京** 电话：86-10-8569-7000 **中国 - 成都** 电话：86-28-8665-5511 **中国 - 重庆** 电话：86-23-8980-9588 **中国 - 东莞** 电话：86-769-8702-9880 **中国 - 广州** 电话：86-20-8755-8029 **中国 - 杭州** 电话：86-571-8792-8115 **中国 - 南京** 电话：86-25-8473-2460 **中国 - 青岛** 电话：86-532-8502-7355 **中国 - 上海** 电话：86-21-3326-8000 **中国 - 沈阳** 电话：86-24-2334-2829 **中国 - 深圳** 电话：86-755-8864-2200 **中国 - 苏州** 电话：86-186-6233-1526 **中国 - 武汉** 电话：86-27-5980-5300 **中国 - 西安** 电话：86-29-8833-7252 **中国 - 厦门** 电话：86-592-2388138 **中国 - 香港特别行政区** 电话：852-2943-5100 **中国 - 珠海** 电话：86-756-3210040 **台湾地区 - 高雄** 电话：886-7-213-7830 **台湾地区 - 台北** 电话：886-2-2508-8600 **台湾地区 - 新竹** 电话：886-3-577-8366	**澳大利亚 - 悉尼** 电话：61-2-9868-6733 **印度 - 班加罗尔** 电话：91-80-3090-4444 **印度 - 新德里** 电话：91-11-4160-8631 **印度 - 浦那** 电话：91-20-4121-0141 **日本 - 大阪** 电话：81-6-6152-7160 **日本 - 东京** 电话：81-3-6880- 3770 **韩国 - 大邱** 电话：82-53-744-4301 **韩国 - 首尔** 电话：82-2-554-7200 **马来西亚 - 吉隆坡** 电话：60-3-7651-7906 **马来西亚 - 槟榔屿** 电话：60-4-227-8870 **菲律宾 - 马尼拉** 电话：63-2-634-9065 **新加坡** 电话：65-6334-8870 **泰国 - 曼谷** 电话：66-2-694-1351 **越南 - 胡志明市** 电话：84-28-5448-2100	**奥地利 - 韦尔斯** 电话：43-7242-2244-39 传真：43-7242-2244-393 **丹麦 - 哥本哈根** 电话：45-4450-2828 传真：45-4485-2829 **芬兰 - 埃斯波** 电话：358-9-4520-820 **法国 - 巴黎** 电话：33-1-69-53-63-20 传真：33-1-69-30-90-79 **德国 - 加兴** 电话：49-8931-9700 **德国 - 哈恩** 电话：49-2129-3766400 **德国 - 海尔布隆** 电话：49-7131-67-3636 **德国 - 卡尔斯鲁厄** 电话：49-721-625370 **德国 - 慕尼黑** 电话：49-89-627-144-0 传真：49-89-627-144-44 **德国 - 罗森海姆** 电话：49-8031-354-560 **以色列 - 赖阿南纳** 电话：972-9-744-7705 **意大利 - 米兰** 电话：39-0331-742611 传真：39-0331-466781 **意大利 - 帕多瓦** 电话：39-049-7625286 **荷兰 - 德卢内市** 电话：31-416-690399 传真：31-416-690340 **挪威 - 特隆赫姆** 电话：47-7288-4388 **波兰 - 华沙** 电话：48-22-3325737 **罗马尼亚 - 布加勒斯特** 电话：40-21-407-87-50 **西班牙 - 马德里** 电话：34-91-708-08-90 传真：34-91-708-08-91 **瑞典 - 哥德堡** 电话：46-31-704-60-40 **瑞典 - 斯德哥尔摩** 电话：46-8-5090-4654 **英国 - 沃金厄姆** 电话：44-118-921-5800 传真：44-118-921-5820