USB 闪存模块和 USB eToken 支持

概述

问：什么是 USB eToken 支持？

答：USB eToken 特性支持 Aladdin Knowledge Systems 开发的 eToken Pro 密钥，能够安全地与机箱分开保存和部署信息，一般包括启动配置或 VPN 证书。这个特性能够方便地以安全方式加载低接触和企业级配置系统支持的路由器证书和配置数据。

问：什么是 USB 闪存模块？

答：USB 闪存模块是由思科系统®公司销售的硬件设备，能够在通用串行总线（USB）端口上提供备用闪存功能。

问：USB 支持将从什么时候开始提供？

答：对 USB 接口的支持将从 IOS 12.3（14）T 开始提供。

问：哪些平台支持这两个特性？

答：配有本机 USB 接口的所有思科路由器都支持这两个特性，包括 Cisco 871、1811、1812、1841、2800 系列和 3800 系列集成多业务路由器。

问：这个特性是否支持 USB 2.0？

答：这个特性与 USB 版本无关。USB 闪存和 eToken 都属于 USB 2.0 设备。Cisco 1841、Cisco 2800 系列和 Cisco 3800 系列集成多业务路由器只支持 USB 1.1 接口。Cisco 871、1811 和 1812 集成多业务路由器配有 USB 2.0 接口。

问：产品编号是什么？

答：USB 闪存的产品编号如下表所示。

产品编号	说明
MEMUSB-64FT	64 MB USB 闪存
MEMUSB-64FT=	64 MB USB 闪存（备件）
MEMUSB-128FT	128 MB USB 闪存
MEMUSB-128FT=	128 MB USB 闪存（备件）
MEMUSB-256FT	256 MB USB 闪存
MEMUSB-256FT=	256 MB USB 闪存（备件）

问：是否支持其它闪存规格？

答：不支持。只支持表中列出的思科闪存设备。

USB 闪存模块和 USB eToken 支持

问：是否支持其它 USB 设备？

答：不支持。此次支持的 USB 设备只包括 USB 闪存和 USB eToken。

应用

问：可拆卸证书特性的工作原理是什么？

答：可拆卸证书特性使用的是第三方产品，即 Aladiin（www.aladdin.com/cisco）开发的 eToken。eToken 使用智能卡技术保护小存储区域，并通过 PIN 决定是否允许访问。如果将 IP Security（IPSec）VPN 证书保存在 eToken 上，可以安全地存在于路由器外部。如果将令牌插入到 USB 端口中，路由器可以验证 PIN 通过，解锁并获取证书，然后将其复制到当前内存中。拆卸令牌后，路由器将从当前内存中擦除证书，以保证任何人不能从路由器本身获取证书。

问：USB 闪存支持哪些特性？

答：USB 闪存特性提供了可选的备用存储功能。镜像、配置或其它文件可以复制到思科 USB 闪存条上，也可以从思科 USB 闪存条复制，而且可靠性与利用 Compact 闪存保存和恢复文件的可靠性相当。

问：什么是无接触或低接触配置应用？

答：如果与 Cisco CSN 2100 系列智能引擎或普通文件传输协议（TFTP）服务器结合在一起，USB 端口可以支持无接触或低接触配置应用。如果利用闪存提供非安全配置，或者利用 eToken 建立安全解决方案，将能够直接把路由器从工厂部署到最终用户。两种 USB 方式都保存启动配置，以便路由器启动和建立基线连接。建立连接之后，路由器可以与智能引擎或 TFTP 服务器联络，下载完整配置或新的 Cisco IOS Software 镜像。有了这个功能之后，企业不再需要每次安装时都向客户地点派遣技术人员。

问：USB 闪存与 eToken 之间有什么区别？

答：USB 闪存与 USB eToken 之间的区别如下表所示：

功能	USB eToken	USB 闪存
可访问性	用于安全地保存数字证书和路由器配置，并将这些配置从 eToken 传输到路由器。	用于保存和部署路由器配置和镜像，并将这些配置和镜像从 USB 闪存部署到路由器。
存储大小	32Kb	• 64MB • 128MB • 256MB
文件类型	• 一般用于存储启动数据、数字证书以及防火墙和 IPSec VPN 的配置 • eToken 不能存储 Cisco IOS 镜像	保存 Compact Flash 也可以存储的文件类型
安全性	• 文件只能通过用户 PIN 加密和访问 • 文件也可以用非安全格式存储	文件只能用非安全格式存储
启动镜像和配置	• 配置可以从 eToken 导入到路由器中 • 备用配置可以从 eToken 导入到路由器中。利用备用配置，用户可以加载 IPSec 配置	• 配置文件自动从 USB 闪存传输到路由器

USB 闪存模块和 USB eToken 支持

可拆卸证书

问：什么是 eToken？

答：eToken 是 USB 令牌上智能卡的商标名称。eToken 商标名称由 Aladdin Knowledge Systems 所有。为实现这种应用，还支持 eToken PRO 设备。eToken 提供了少量的闪存存储空间，最高 32KB，并受智能卡保护。智能卡用 PIN 解锁。

问：什么是智能卡？

答：智能卡是一种信用卡大小的塑料卡，其中包含一个通用微处理器，一般是 8 位微控制器，例如 Motorola 6805 或 Intel 8051。微处理器放置在卡一端的金色接触垫的下面。eToken 的智能卡已经做成 USB 形状。

问：在哪儿能买到 eToken？

答：eToken 由 Aladdin Knowledge Systems 制造并销售，产品编号为<产品编号>，但必须通过经 Aladdin 验证的合作伙伴购买。如果想查找本地的 Aladdin 合作伙伴，请访**问：**www.aladdin.com/cisco。如果想详细了解 Aladdin Knowledge Systems 及其产品，请访**问：**www.aladdin.com/cisco。

问：eToken 怎样才能获得 PIN？

答：实际上，eToken 共使用两个 PIN：管理员 PIN 和用户 PIN。用户 PIN 有默认值，而管理员 PIN 没有默认值。只有拥有了管理员 PIN，才能设置或修改用户 PIN。用户 PIN 用于执行令牌解锁，并访问受保护的内存区。PIN 可以从路由器命令行界面（CLI）设置和修改，也可以利用 Aladdins 的令牌管理系统（TMS）设置和修改。如果想详细了解 TMS，请访**问：**www.aladdin.com。

问：怎样在 eToken 上放置文件？

答：在 eToken 上放置文件的方式有两种。第一种是利用“复制”命令直接从路由器传输文件，第二种是使用 Aladdin Knowledge Systems 开发的 TMS 软件应用。如果想详细了解 TMS，请访**问：**www.aladdin.com。

问：哪类文件可以放置在 eToken 上？

答：适合 eToken 的所有文件都能放置其上。为实现安全存储，一般将二进制 X.509 数字证书和配置文件存储在 eToken 上。配置文件还可以包含预共享密钥。除配置文件外，其它所有文件都必须从 CLI 复制。

问：怎样检查 eToken 上的文件？

答：可以使用show <token_name> 或dir <token_name> 命令查看eToken的内容。如果想查看可用令牌名称，可以使用show file systems命令。

问：拆卸eToken后是否可以延期从内存中删除证书？

答：可以。利用removal timeout命令，可以设置eToken拆卸之后内存中的证书有效期。默认期限是下一互联网密钥交换（IKE）操作验证期到来，即需要再次访问密钥之前。管理员可以设置短于默认期的各种期限。

问：是否可以将证书从eToken复制并存储到路由器上？

答：可以。可以将证书复制并直接存储在路由器上，但这样就失去了可拆卸证书的价值。

USB 闪存模块和 USB eToken 支持

问：eToken是否能为VPN通道产生密钥？

答：目前，eToken还只能用于安全存储。路由器必须产生密钥。

问：是否可以从eToken启动镜像？

答：不能。eToken的存储量只有32KB，不足以支持Cisco IOS Software镜像。

问：eToken是否有非安全存储区？

答：是的。eToken能够以文件为单位保护文件，因此，文件能够以非安全或安全方式存储。

问：是否可以从eToken启动配置？

答：可以，可以使用boot config命令规定查找启动配置的位置，也可以使用crypto pki token <token_name> secondary config <file>命令加载备用配置文件，并将其合并到当前配置中，而不是覆盖当前配置。利用备用配置，不但能从eToken启动配置，还能只在安装令牌时加载IPSec配置，提高安全性。

USB 闪存

问：USB 闪存条提供哪些规格？

答：USB 闪存条包括64MB、128MB和256MB规格，不支持其它容量。

问：是否可以为该应用使用任何USB闪存条？

答：不是，只能使用思科USB闪存条。多数第三方闪存条都需要安装基于Windows的API和动态插入驱动程序。Cisco IOS Software不支持Windows应用。思科测试表明，如果没有API，许多内存棒都无法正常运行。所有第三方闪存条都需要符合思科第三方内存策略要求，欲知详情，请访**问：**http://www.cisco.com/en/US/products/prod_warranties_item09186a00800b5594.html。

问：USB 闪存支持哪类文件？

答：可以在路由器Compact 闪存上存储的所有文件都可以在USB 闪存上存储，包括Cisco IOS Software镜像和配置文件。

问：是否可以直接从USB 闪存模块启动镜像？

答：不可以。USB驱动程序只在Cisco IOS Software上提供。只有启动了Cisco IOS镜像才能加载驱动程序，只有加载了驱动程序才能将文件复制到USB 闪存模块，或者从USB 闪存模块复制文件。

问：是否可以从USB 闪存模块启动配置文件？

答：可以。安装USB 闪存模块之后，路由器将自动接收，并给予支持。

问：是否可以在路由器上对USB 闪存模块执行格式化？

答：可以，可以在路由器或PC上对模块执行格式化。执行PC格式化过程中，必须将文件系统规定为“FAT16文件系统”。

无接触或低接触配置

问：什么是无接触或低接触配置？

答：无接触配置指直接从工厂向客户地点供货，然后远程执行软件配置和设置，整个过程中不需要

USB 闪存模块和 USB eToken 支持

高技术人员接触路由器。利用无接触配置，可以通过自动流程执行配置。低接触配置是无接触配置的改版，指需要高技能人员或系统工程师花费少量时间与路由器实时交互。

问：USB 闪存和USB eToken特性怎样支持该应用？

答：利用USB 闪存特性，最终用户可以将配置文件和/或Cisco IOS Software镜像存储在USB 闪存模块上。如果启动之前就将该模块插入路由器，而且当前启动配置包含“boot config <usb闪存:filename>”或“boot system 闪存 <usb闪存:image_name>”命令，路由器将用命名文件启动。USB闪存模块上的启动配置文件将把路由器与智能引擎或TFTP服务器连接，或者与可以完整配置路由器的完全配置连接。用保存在USB 闪存模块上的镜像文件启动路由器时，要求启动帮助镜像能够读取USB 闪存设备。另外，程序文件还可以更新路由器上的Cisco IOS Software镜像，部署新的特性集。

eToken模块能够将启动配置存储在无保护内存空间里。路由器也可以从这种配置启动，然后与Cisco CNS 2100系列智能引擎或TFTP服务器联络，获得完整的最终配置。当智能引擎把安全Cisco IOS特性集推广到路由器上时，这种情况可以得到扩展。一旦路由器配置中具备了安全特性集和正确的PIN，将能够解除包含数字证书或VPN证书的eToken模块保护区的锁定，对IPSec通道进行验证。

一般问题

问：使用这些特性时需要哪些Cisco IOS特性集？

答：支持USB接口的第一个Cisco IOS Software版本是IOS 12.3（14）T。USB 闪存模块可以与任何Cisco IOS特性集、IP Base或以上的特性集配合使用。但是，无论怎样使用eToken模块，都要求高级安全特性集或以上的特性集。

问：思科管理工具是否将负责管理令牌、PIN和可拆卸证书？

答：思科路由器以及Security Device Manager（SDM）和CiscoWokrs Resource Manager Essentials（VMS）都计划支持这些特性。CiscoWokrs VMS还计划在未来版本中与TMS集成在一起。

问：两种USB设备能否同时使用？

答：在Cisco 2811、2821、2851和3845路由器上，可以同时使用两种USB设备。设备使用与接口无关，因为它们是在插入时自动编号的。Cisco IOS Software将把设备识别为USB 0和USB 1。任何USB端口都可以使用支持设备的任意组合。

问：能否使用USB扩展电缆？

答：USB扩展电缆已通过测试，可以使用。选择电缆时，应使用两端都有完整绝缘层的电缆，以保证连接时没有金属线露在外面，否则会出现电磁放电或静电脉冲现象。

问：能否使用一个USB集线器添加更多设备？

答：目前还不支持USB集线器。所有USB设备都必须直接与主板上的USB接口相连。

思科系统（中国）网络技术有限公司

北京
北京市东城区东长安街 1 号东方广场东方经贸城东一办公楼 19-21 层
邮政编码：100738
电话：(8610) 85155000
传真：(8610) 85181881

上海
上海市淮海中路 222 号力宝广场 32-33 层
邮政编码：200021
电话：(8621) 33104777
传真：(8621) 53966750

广州
广州市天河北路 233 号中信广场 43 楼
邮政编码：510620
电话：(8620) 85193000
传真：(8620) 38770077

成都
成都市顺城大街 308 号冠城广场 23 层
邮政编码：610017
电话：(8628) 86961000
传真：(8628) 86528999

如需了解思科公司的更多信息，请浏览 http://www.cisco.com /cn

2005 年 5 月翻译