# USB eToken and USB Flash Features Support

**Q. What is USB eToken support?**

**A.** The USB eToken feature supports the eToken Pro key by Aladdin Knowledge Systems, providing primary secure means to store and deploy information separate from the router chassis, usually a bootstrap configuration or VPN credentials. This feature enable secure and portable loading of router credentials and configuration data supported by low-touch and enterprise level provisioning systems.

**Q. What is the USB Flash Module?**

**A.** The USB Flash Module is a hardware device sold by Cisco Systems® that provides a secondary Flash capability on Universal Serial Bus (USB) ports.

**Q. When will USB support be available?**

**A.** Support for USB interfaces will be available in Cisco IOS® release 12.3(14)T and later releases depending on the respective routing platforms.

Minimum Cisco IOS release for USB support:

- For Cisco 877, Cisco 1811, and Cisco 1812
- For Cisco 1800 Series (modular), Cisco 2800 series and Cisco 3800 series: 12.3(14)T
- For Cisco 7200 VXR series with NPE-G2: 12.4(4)XD, in the future: in 12.4T and 12.2SB

**Q. Which platforms support these two features?**

**A.** The features are supported on any Cisco router with native USB interfaces. This includes Cisco 871, 1811, 1812, 1841, 2800 Series, 3800 Series Integrated Services (ISRs), and 7200 VXR Series Services Aggregation routers.

**Q. Will this feature support USB 2.0?**

**A.** The feature is USB version-independent. Both the USB Flash and the eToken are USB 2.0 devices. The Cisco 7200 VXR series with NPE-G2 supports USB1.1 and 2.0. The Cisco 3800 Series, the Cisco 2800 Series and the Cisco 1800 Series (modular) Integrated Services Routers support only USB 1.1 interfaces. The Cisco 871, the Cisco 1811, and the Cisco 1812 Integrated Services Routers have USB 2.0 interfaces.

**Q. What are the part numbers?**

**A.** The table below shows USB Flash part numbers.

| Part Number | Description |
|---|---|
| **MEMUSB-64FT** | 64 MB USB Flash |
| **MEMUSB-64FT=** | 64 MB USB Flash (spare) |
| **MEMUSB-128FT** | 128 MB USB Flash |
| **MEMUSB-128FT=** | 128 MB USB Flash (spare) |
| **MEMUSB-256FT** | 256 MB USB Flash |
| **MEMUSB-256FT=** | 256 MB USB Flash (spare) |

**Q. Are other Flash sizes supported?**

**A.** No. Only the Cisco Flash devices listed above are supported.

**Q. Are any other USB devices supported?**

**A.** No. The USB Flash and USB eToken are the only USB devices supported at this time.

**Q. What is MAX-28/38-FLASH-BN?**

**A.** This Part Number provides the maximum for Cisco 2800/3800 with Compact Flash (256MB) and USB Flash (256MB).

## Applications

**Q. How does the Removable Credentials feature work?**

**A.** The Removable Credentials feature uses a third-party product, the eToken by Aladdin http://www.aladdin.com/etoken/cisco. The eToken uses smart card technology to protect a small area of memory and grants access via a PIN. When IP Security (IPSec) VPN credentials are stored on the eToken, they are safely external to the router. When the token is inserted in a USB port, the router can pass the PIN and unlock it, retrieving the credentials and copying them into running memory. When the token is removed, the router will erase the credentials from running memory, ensuring that they cannot be retrieved from the router itself.

**Q. What are the features supported by USB Flash?**

**A.** The USB Flash feature provides an optional, secondary storage capability. Images, configurations, or other files can be copied to or from the Cisco USB Flash stick with the same reliability as storing and retrieving files using the Compact Flash card. IOS images can also be booted from the USB flash.

**Q. What is the touchless or low-touch provisioning application?**

**A.** Combined with either the Cisco Configuration Engine or a Trivial File Transfer Protocol (TFTP) server, the USB ports can support a touchless or low-touch provisioning application. By using either the Flash for nonsecure provisioning or the eToken for a secure solution, routers can be deployed directly from the factory floor to the end user. Both USB options can hold a bootstrap configuration that allows the router to boot and establish baseline connectivity. Once connectivity is established, the router may contact an Configuration Engine or TFTP server to download its full configuration or a new Cisco IOS Software image. This capability eliminates the requirement to send a skilled technician to the customer premises for each installation.

**Q. What are the differences between the USB Flash and the eToken?**

**A.** The Table below shows the differences between the USB Flash and USB eToken:

| Function | USB eToken | USB Flash |
|---|---|---|
| **Accessibility** | Used to securely store and transfer digital certificates and router configurations from the eToken to the router. | Used to store and deploy router configurations and images from the USB Flash to the router. |
| **Storage Size** | 32Kb | • 64MB<br>• 128MB<br>• 256MB |
| **File Types** | • Typically used to store bootstrap data, digital certificates and configurations for Firewalls and IPSec VPNs<br>• eTokens cannot store Cisco IOS images | Stores an file type that might be stored on a compact flash |
| **Security** | • Files can be encrypted and accessed only with a user PIN<br>• Files can also be stored in a non-secure format | Files can only be stored in a non-secure format. |
| **Boot Images and Configurations** | Secondary configuration can be booted from the eToken to the router. Secondary configuration allows users to load their IPSec configuration. | Boot Cisco IOS images on Cisco 1841, 2800 and 3800 |

## Removable Credentials

**Q. What is an eToken?**

**A.** An eToken is a brand name for a smart card on a USB token. The eToken brand name is owned by Aladdin Knowledge Systems, and the eToken PRO device is supported for this application. The eToken provides a small amount of Flash storage space, up to 32 KB, that is protected by the smart card. The smart card is unlocked with a PIN.

**Q. What is a smart card?**

**A.** A smart card is a credit-card-sized plastic card that contains a general-purpose microprocessor, typically an 8-bit microcontroller such as a Motorola 6805 or an Intel 8051. The microprocessor is underneath a gold contact pad located on one side of the card. In the case of an eToken, this has been ported to a USB form factor.

**Q. Where do I get the eTokens?**

**A.** The eToken is made and sold by Aladdin Knowledge Systems. They must be purchased through an Aladdin-certified partner. To find an Aladdin partner in your area or for more information about Aladdin Knowledge Systems and their products, visit: http://www.aladdin.com/cisco

**Q. How does the eToken get a PIN?**

**A.** The eToken actually uses two PINs-an administrator PIN and a user PIN. The user PIN has a default value; the administrator PIN does not. The administrator PIN is required to set or change the user PIN. The user PIN is used to unlock the token and gain access to the protected memory areThe PINs can be set and changed from the router command-line interface (CLI) or using Aladdin's Token Management System (TMS). For more information on TMS, visit http://www.aladdin.com.

**Q. How do I put files on the eToken?**

**A.** There are two ways to place files onto the eTokens. The first is to transfer a file directly from the router using the "copy" command. The second is using the TMS software application from Aladdin Knowledge Systems. For more information on TMS, visit http://www.aladdin.com.

**Q. What kind of files can I put on the eToken?**

**A.** Any file that will fit on the eToken can be put there. Primarily, binary X.509 digital certificates and configuration files are placed there for secure storage. The configuration file can also contain preshared keys. Except for the configuration files, all files must be copied from the CLI.

**Q. How do I check for files on the eToken?**

**A.** You can look at the contents of the eToken by using the show <token_name> or dir <token_name> command. The available token names can be seen using show file systems.

**Q. Is there a way to delay the removal of credentials after the eToken is removed?**

**A.** Yes. By using the removal timeout command, you can set the amount of time the credentials will remain after removal of the eToken. The default period is until the next Internet Key Exchange (IKE) session authentication period, when the keys will need to be accessed again. Any period less than the default must be configured.

**Q. Can I copy the credentials from the eToken to the router and store them there?**

**A.** Yes. You can copy the credentials and store them directly on the router, but this eliminates the value of removable credentials.

**Q. Can the eToken generate the keys for VPN tunnels?**

**A.** At this point, the eToken can only be used for secure storage. The router must generate the keys.

**Q. Can I boot an image from the eToken?**

**A.** No. The eToken only has 32 KB of storage, which is not sufficient to hold a Cisco IOS Software image.

**Q. Does the eToken have a nonsecured storage area?**

**A.** Yes. The eToken can secure files on a per-file basis, so files can be stored in a nonsecure or secure manner.

**Q. Can I boot a configuration from the eToken?**

**A.** Yes, you can use the boot config command to specify a location to find the boot configuration. You can also use the crypto pki token <token_name> secondary config <file> command to load a secondary configuration file and merge it into the running configuration rather than overwriting it. The secondary config allows you to not only boot a config from an eToken, but to also load your IPSec configuration only when the token is installed, providing more security.

## USB Flash

**Q. What sizes of USB Flash sticks are supported?**

**A.** USB Flash sticks are supported in 64, 128, and 256 MB sizes. No other sizes are supported.

**Q. Can I use any USB memory stick for this application?**

**A.** No. Only Cisco USB memory sticks are supported. Most third-party memory sticks require the installation of Windows-based APIs and dynamic drivers upon insertion. Cisco IOS Software does not support Windows applications. Cisco testing has shown that many of these memory sticks do not function properly without their APIs. All third-party memory sticks are subject to Cisco's Third-Party Memory Policy, available at http://www.cisco.com/en/US/prod/prod_warranty09186a00800b5594.html.

**Q. What kind of files can the USB Flash support?**

**A.** Any file that you would normally store on a router's Compact Flash can also be stored on USB Flash. This includes Cisco IOS Software images, configuration files, Router and Security Device Manager files, Intrusion Prevention System files, and more....

**Q. Can I boot an image directly from the USB Flash module?**

**A.** Yes. USB drivers have been added to rommon, starting with version 12.4(13r).

**Q. Can I boot a configuration file from the USB Flash module?**

**A.** No. This is not supported yet.

**Q. Can I format the USB Flash module on the router?**

**A.** Yes. You can format the module on either a router or a PC. You must specify "FAT16 file system" as the file system for the PC format process to use.

**Q. Can I order Cisco IOS images on USB Flash?**

**A.** Yes, USB Flash, when ordered as spare (MEMUSB-64MBFT=, MEMUSB-64MBFT=, MEMUSB-64MBFT=) are configurable products. You can order them preloaded with IOS images.

## Touchless or Low-Touch Provisioning

**Q. What is touchless or low-touch provisioning?**

**A.** Touchless provisioning is the ability to ship a router platform directly from the factory to a customer site, and provide the software configuration and provisioning remotely, without a skilled person touching the router. With touchless provisioning, configuration is done through an automated process. Low-touch provisioning is a variation that requires some time spent by a skilled technician or systems engineer to interact in real time with the router.

**Q. How do the USB Flash and USB eToken features support this application?**

**A.** The USB Flash feature allows the end user to store a configuration file and/or a Cisco IOS Software image on the USB Flash module. If the module is inserted into the router prior to booting and if the current startup configuration contains a "boot config <usbflash:filename>" or "boot system flash <usbflash:image_name>" command, the router will boot with the named file. A bootstrap configuration file from the USB Flash module can link the router to an Configuration Engine or a TFTP server, or a full configuration that completely configures the router.

The eToken module can store a bootstrap configuration in unprotected space in its memory. The router can boot from this configuration as well, and can then contact a Configuration Engine or TFTP server for full, final configuration. This scenario can be expanded when the Configuration Engine pushes a security Cisco IOS feature set to the router. Once the router has a security feature set and the correct PIN in its configuration, it can unlock the protected area of the eToken module that contains a digital certificate or VPN credentials to authenticate an IPSec tunnel.

## General

**Q. What Cisco IOS feature sets are required to use these features?**

**A.** The first Cisco IOS Software release to support USB interfaces IOS release 12.3(14)T. The USB Flash module can be used with any Cisco IOS feature set, IP Base and above. Any use of the eToken module requires an Advanced Security feature set or above.

**Q. Will Cisco management tools manage tokens, PINs, and removable credentials?**

**A.** Cisco Router and Security Device Manager (SDM) supports these features.

**Q. Can I use two USB devices at the same time?**

**A.** On the Cisco 2811, 2821, 2851, 3825, 3845, and 7200 VXR (with NPE-G2) routers, you can use two USB devices at the same time. Use of the devices is interface-independent, as they are automatically numbered upon insertion. Devices will be identified in Cisco IOS Software as USB 0 and USB 1. Any combination of supported devices may be used in any USB port.

**Q. Can I use a USB extension cable?**

**A.** USB extension cables have been tested and are supported. When selecting a cable to use, make sure to use one with complete insulation coverage for both ends of the cable, such that no metal is exposed when the cable is properly connected. Exposed metal on some cables can make the solution susceptible to electromagnetic discharge or static electricity pulses.

**Q. Can I use a USB hub to add more devices?**

**A.** USB hubs are not supported at this time. All USB devices must be directly connected to the onboard USB interfaces.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**



Printed in USA C67-386278-00 12/06

 