Using eTokens with Cisco Virtual Office

Introduction

This white paper provides detailed design and implementation information for deploying eTokens with Cisco® Virtual Office. Please refer to the Cisco Virtual Office overview (found at http://www.cisco.com/go/cvo) for further information about the solution, its architecture, and all of its components.

What Is an eToken?

An eToken is a hardware device that provides password authentication, helping to identify a user. It looks similar to a pen drive and is inserted into the USB port of a router or computer. Once the eToken has been inserted and the user has provided a valid login, the user is given appropriate access to the system. eTokens are beneficial to corporations, organizations, libraries, banks, finance companies, educational institutions, and government and defense organizations. They are also useful wherever security is necessary, whether on a personal computer or in a cyber café. They are widely used in e-banking, e-commerce, stock trading, and online data and financial transactions.

How eTokens Work with Cisco Virtual Office

eTokens provide security in Cisco Virtual Office by allowing connectivity to the corporate servers when inserted and dropping the secure tunnels when removed. This guide describes the steps needed for an end user to connect a new router to a VPN using an eToken. It gives a detailed description of inserting and removing the eToken and managing eToken access. It also provides a step-by-step guide to securely provisioning a Cisco Virtual Office remote VPN router with an eToken.

Platforms and Images

When using eTokens with Cisco Virtual Office, many platforms are supported. Some examples are the Cisco 7300, 7200 or 7600 Series Routers for the hub and the Cisco 870, 880, 1800, 2800, and 3800 Series Integrated Services Routers for the spokes.

The recommended Cisco IOS® Software image for both hub and spokes is 12.4(15)T IOS or later. For the Cisco 880 Series routers, the recommended image is 12.4(20)T.

The Cisco Configuration Professional version used should be 1.0.

The Cisco Security Manager should be version 3.2 or higher and should be integrated with the Cisco Configuration Engine, 2.0 or the latest certified version.

The Secure Device Provisioning (SDP) and Cisco IOS public key infrastructure (PKI) certificate server run on Cisco IOS Software Release 12.4(15)T or later.

Using eTokens with Cisco Virtual Office

eTokens can be used with Cisco Virtual Office in three different ways:

- As a physical key, holding only RSA keys
- To bootstrap a remote router, holding RSA keys plus a small config file
- To hold the almost-complete spoke configuration

The first option is the most practical one and is described in detail in this guide. With this option, a new router and new eToken can be shipped directly to the end user or acquired off the shelf. Only the default factory configuration is needed in both devices. The entire Cisco Virtual Office configuration is pushed remotely.

The second option, the bootstrap technique, establishes the initial lines of configuration that are just the minimum to have a remote router establish a secure tunnel to a management server. It includes a PKI trust point and certificate, IP Security (IPsec) configuration, clock synchronization, and a Cisco CNS agent that makes the Cisco Configuration Engine react to events.

For cases in which the eToken is used to hold the bootstrap configuration, or for the third option, storing the full Cisco Virtual Office configuration, an extra step is necessary to copy the configuration file to the eToken. This step is not covered in this guide. It requires a tool to push a Cisco IOS Software configuration to an eToken. The Token Management System (TMS) application software from Aladdin can be used to save PKI certificates plus a Cisco IOS Software configuration file in an eToken. This could, however, also be done manually.

We recommend the first option because it is straightforward to implement and achieves the major goal: to be able to conveniently enable and disable a Cisco Virtual Office spoke with just an eToken. It also adds no extra overhead to managing the Cisco Virtual Office deployment, since the only thing needed is to add three extra lines of configuration.

For secure remote provisioning of new Cisco Virtual Office spokes, SDP is the best approach for getting the spokes connected. This is the case for medium and large enterprises or service providers—deployments in which a zero-touch secure deployment is achieved with the Cisco Security Manager, combined with the Cisco Configuration Engine as the provisioning tool and SDP for remotely pushing a PKI certificate, plus a bootstrap configuration template for new spokes joining the VPN.

In the guide, we focus on the steps that the end user will go though to connect a new Cisco ISR to a VPN while using an eToken to securely lock the router's access to the central site.

We assume that PKI is used across the VPN deployment; otherwise, eTokens would not make sense for a Cisco Virtual Office deployment.

Again, for more detailed information about Cisco Virtual Office, please visit http://www.cisco.com/go/cvo.

Using an eToken to Store Only RSA Keys

This section describes how to deploy an eToken that is used to store only RSA keys with Cisco Virtual Office. The eToken works as a physical lock mechanism: when inserted, it allows connectivity to the corporate servers to be established; when removed, it automatically drops the secure tunnels.

The configuration is nearly the same as for a regular Cisco Virtual Office deployment; only one extra command is needed:

```
crypto pki token eToken removal timeout 1
```

This command forces the router to clear the active running memory of whatever is defined as stored in the eToken. In other words, if we save RSA keys in the eToken, removing it from the router will force tunnels to be dropped after one second as the keys are deleted from memory.

The following are a few other commands that can be used with eTokens:

```
CVO-spoke1-vpn#crypto pki token eToken ?
  admin       access to administrative functions
  change-pin  new PIN to access token
  label       new label for token
  lock        log out and lock the token
  login       PIN to access token
  logout      log out of the token
  unlock      decrypt token pin and log in the token
```

Inserting the eToken

Inserting the eToken displays the following information in the console. The USB eToken is now ready to use for crypto, after we log in with the correct PIN:

```
27847769: Apr 24 17:05:36.740 PDT: %USB_HOST_STACK-6-
USB_DEVICE_CONNECTED: A Low speed USB device has been inserted in port
0.
27847770: Apr 24 17:05:38.204 PDT: %USB_TOKEN_FILESYS-6-
USB_TOKEN_INSERTED: USB Token device inserted: usbtoken0.
27847771: Apr 24 17:05:38.208 PDT: %USB_TOKEN_FILESYS-6-
REGISTERING_WITH_IFS: Registering USB Token File System usbtoken0:
might take a while...
27847772: Apr 24 17:05:38.556 PDT: %CRYPTO-6-TOKENINSERTED:
Cryptographic token eToken inserted in usbtoken0
```

The eToken’s PIN can be entered at the console using an exec command:

```
CVO-spoke1-vpn#crypto pki token eToken login 1234567890
Token eToken is usbtoken0
Token login to usbtoken0(eToken) successful
```

It can also be entered into a browser window, from a PC connected to the router. Assuming that we still have the factory default LAN configured—10.10.10.0/24—the URL would be as follows: http://10.10.10.1/level/15/exec/crypto/pki/token/eToken/login

The default login credentials for the router are: cisco/cisco

We can now generate RSA keys that will be saved in the eToken:

```
CVO-spoke1-vpn(config)#crypto key generate rsa general-keys label
etoken-keys modulus 1024 storage eToken
The name for the keys will be: etoken-keys
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
CVO-spoke1-vpn(config)#end

CVO-spoke1-vpn#show crypto key mypubkey rsa
% Key pair was generated at: 17:17:35 PDT Apr 24 2006
Key name: etoken-keys
 Storage Device: usbtoken0 (label=eToken)
 Usage: General Purpose Key
 Key is not exportable.
 Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181
00C2A22F
  73014BCD 5318A955 83114823 639C2927 1BB15330 A259E6A4 97FC94BA
8077FAE4
  62CCB475 F42E9852 2C4D5B2A AAF7EB53 C535CA0E 61314F4D EFB3A744
F8D53E3F
  FABF0D8D 070F2500 FF3C282C A2D09C4F FDABBF1F AD88034A 3F068ED5
FDFFE38C
  4517D856 C6D2CE7D F463C5AB A67EE665 D006E3DB 9DD3C314 6BADF021
67020301 0001
% Key pair was generated at: 17:17:36 PDT Apr 24 2006
Key name: etokens-keys.server
Temporary key
 Usage: Encryption Key
 Key is not exportable.
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00BB46B7
0EB4C59B
  F4D10B05 3438704B 6C72A086 E39F14BC FE77C84A C652B280 F602882B
6B5BA009
  EC7F0E56 910237EA 07D58490 2E5D1DE1 7AB8FB3C FDE8B479 5078335A
01333799
3EE4D5A4 996BA4D3 442CF53C AE81D375 4EADC86D F6554491 99020301 0001
```

Note: The PKI trust point should contain the name of this generated RSA key pair, so that if the eToken is removed and the router regenerates RSA keys on its own, due to the auto-renewal timers expiring, it will keep using the eToken RSA keys for the VPN tunnels. In the example just given, the trust point would be:

```
crypto ca trustpoint bootstrap-cert
 enrollment url http://bootstrap-cert:80
 serial-number
 subject-name CN=CVO-spoke1-vpn
 revocation-check none
 rsakeypair etoken-keys 1024
```

Removing the eToken

Removing the eToken will bring down any active tunnel that uses the PKI trust point associated with these RSA keys. This is what is seen in the console:

```
27847838: Apr 24 17:29:15.922 PDT: %SYS-5-CONFIG_I: Configured from
console by admin on console
27847839: Apr 24 17:29:18.890 PDT: %USB_HOST_STACK-6-
USB_DEVICE_DISCONNECTED: A USB device has been removed from port 0.
27847840: Apr 24 17:29:18.994 PDT: %LINEPROTO-5-UPDOWN: Line protocol
on Interface FastEthernet0/1, changed state to down
27847841: Apr 24 17:29:18.998 PDT: %USB_TOKEN_FILESYS-6-
USB_TOKEN_REMOVED: USB Token device removed: usbtoken0.
27847842: Apr 24 17:29:18.998 PDT: %CRYPTO-6-TOKENREMOVED:
Cryptographic token eToken removed from usbtoken0
27847843: Apr 24 17:29:18.998 PDT: %CRYPTO-4-TOKENKEYTIMEOUT: RSA
keypairs for token eToken and associated IPSEC sessions will be
deactivated in 1 seconds
27847844: Apr 24 17:29:19.998 PDT: %CRYPTO-4-TOKENKEYSDEACTIVATED: RSA
keypairs from token eToken and associated IPSEC sessions being
deactivated now
27847845: Apr 24 17:29:20.002 PDT: %SSH-5-DISABLED: SSH 1.99 has been
disabled
27847846: Apr 24 17:29:29.909 PDT: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 7:
Neighbor 10.7.12.2 (Tunnel13) is down: holding time expired
27847847: Apr 24 17:29:29.917 PDT: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 7:
Neighbor 10.7.12.1 (Tunnel13) is down: holding time expired
```

The system log messages shown above are for a router in which Dynamic Multipoint Virtual Private Network (DMVPN) internal network is 10.7.12.0/20.

As IPsec tunnels go down, the routing protocol also goes down.

Managing the eToken Access

The PIN for the eToken can be changed by the administrator or the end user, given the proper privileges. The Aladdin eToken, for example, comes with the factory default PIN of 1234567890. This is a number, but it can also be a string.

To change this PIN, you can use the command-line interface (CLI):

```
CVO-spoke1-vpn#crypto pki token eToken change-pin my_new_secret
Token eToken is usbtoken0
Token PIN change on usbtoken0(eToken) successful
```

However, for a VPN remote Cisco Virtual Office router, we recommend that the end user be instructed to use a browser to change the PIN. To enable this, you need to give the CLI exec privilege level 1: the capability to change the PIN. This involves adding the following line to the Cisco Virtual Office spoke configuration:

```
CVO-spoke1-vpn(config)#privilege exec level 1 crypto pki token eToken
change-pin
```

Now the end user can change the PIN in the browser by going to this URL: http://10.32.247.105/level/01/exec/crypto/pki/token/eToken/change-pin

This example assumes that the remote Cisco Virtual Office site has configured the 10.32.247.105 protected LAN side router IP address. Note that we use privilege level 1 here, as we do not want the end user to have full access to the Cisco Virtual Office spoke router.

The Cisco Virtual Office administrator does not need to keep track of the PIN that the end user defines.

Steps for Securely Provisioning a Cisco Virtual Office Remote VPN Router with an eToken, from the Remote Site Perspective

Assuming that Cisco Security Manager plus the Cisco Configuration Engine are used to generate and push the Cisco Virtual Office configuration to the remote router with the help of the SDP feature, and that the eToken will only hold the RSA keys, the steps for provisioning a remote VPN router with an eToken are as follows:

Step 1. User requests a new service from the Cisco Virtual Office administrator, who will use Cisco Security Manager to create a new device and define the security and IP policies that the new spoke will run. The end user needs to tell the administrator how the new spoke will have access to the Internet (ISP details). Then the administrator deploys the router’s configuration; this involves staging a config file in the Cisco Configuration Engine containing the final configuration, plus issuing an enroll command to get the new routers trusted by the corporate PKI certificate server.

Step 2. In the meantime, a new Cisco ISR and eToken are shipped to the end user/remote site, containing only the factory default configuration.

Step 3. To provision the router, the end user follows the instructions given in the “Cisco Virtual Office Provisioning Steps” document received from the administrator via email (or mail). These quick steps will trigger the full provisioning of the new VPN spoke router.

Please read the management guides at http://www.cisco.com/go/cvo for detailed information on how to configure all of the Cisco Virtual Office management servers, respective routers, and tools.

Steps for Provisioning Cisco Virtual Office

This section contains an example of a document that can be sent to the end user containing steps for deploying a new spoke.

In this example a Cisco 881 Integrated Services Router is used, and it is assumed that the ISP provides a Dynamic Host Configuration Protocol (DHCP) service from a modem, or when the end user has a NAT box to access the Internet.

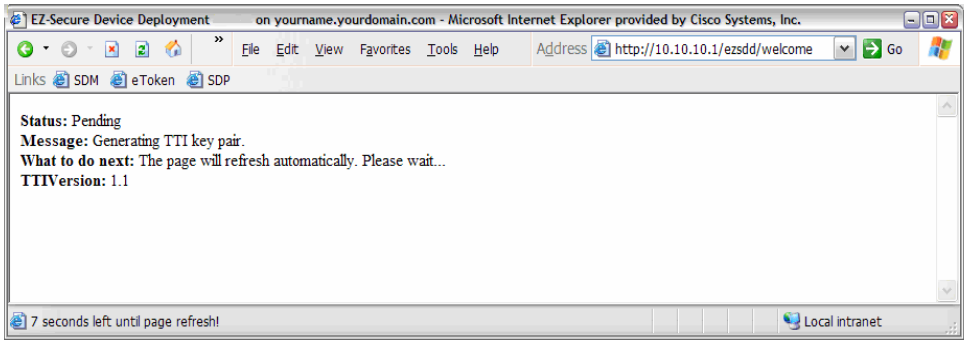
WELCOME TO OUR COMPANY SITE-TO-SITE VPN.

The following instructions will let you provision the new Cisco 881 router that will allow you to connect to our central office

The full process will take a few minutes. Please follow these steps carefully.

1. Connecting the router to the Internet
    - Connect the 881-FastEthernet4-WAN interface to the modem provided by your internet service provider, or to a NAT router if you use one.
    - Connect a PC to the 881 (LAN side), for example, to FastEthernet0.
    - If you have a DHCP connection, your PC should already be able to access the Internet at this point. Make sure that your PC is physically connected to the Cisco Virtual Office router.
    - If your IP address assignment type is anything other than DHCP, you must run the Cisco Configuration Professional tool and follow the steps to get the router connected to the Internet before you can proceed. For more information about Cisco Configuration Professional, please refer to Cisco Configuration Professional Quick Start Guide. It can be downloaded from here http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=281795035.
2. Unlocking the eToken after it is inserted in the Cisco 881 router
    - Insert the eToken in the Cisco 881 router (this step is absolutely necessary to guarantee that security RSA keys are stored in the eToken). The eToken should blink in red once inserted.
    - Open a browser window in the PC connected to the 881 router.
    - Enter this URL: http://10.10.10.1/level/15/exec/crypto/pki/token/eToken/login.
    - Use the username/password setup in the first step to go into enable mode (in the example above it is admin/bingo123).
    - Type the eToken unlock security PIN; the factory default for the Aladdin eToken is 1234567890.
3. Invoking the Secure Device Provisioning (SDP) to fully configure the router
    - Open a browser window in the PC connected to the Cisco 881 router.
    - Type http://10.10.10.1/ezsdd/welcome to execute the SDP software

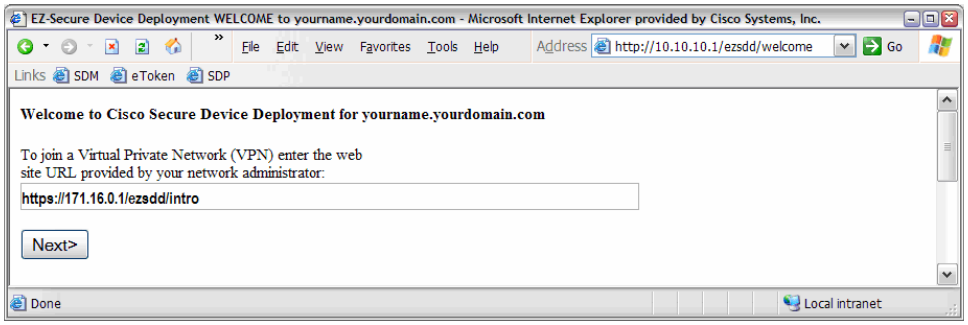
Figure 1. Start of the SDP provisioning


EZ-Secure Device Deployment on yourname.yourdomain.com - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Address http://10.10.10.1/ezsdd/welcome
Go
Links SDM eToken SDP
7 seconds left until page refresh!
Local intranet

Status: Pending
Message: Generating TTI key pair.
What to do next: The page will refresh automatically. Please wait...
TTIVersion: 1.1

- After the router has auto-generated security RSA keys, type in the respective box this URL for joining our VPN: https://172.16.0.1/ezsdd/intro

Figure 2. Entering the SDP Registrar URL


EZ-Secure Device Deployment WELCOME to yourname.yourdomain.com - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Address http://10.10.10.1/ezsdd/welcome
Go
Links SDM eToken SDP
Done
Local intranet

Welcome to Cisco Secure Device Deployment for yourname.yourdomain.com

To join a Virtual Private Network (VPN) enter the web
site URL provided by your network administrator:

https://171.16.0.1/ezsdd/intro

Next>

- Click Next.
- Accept the proposed SSL certificate.
- Enter your Cisco Virtual Office VPN username/password (provided by your administrator).
- Click Next to have the bootstrap template downloaded to your router.

At this point, SDP applies a predefined configuration template (which is retrieved from the Cisco Security Manager) plus a PKI certificate signed by the SDP registrar itself and trusted by the Cisco Virtual Office management gateway.

This will bootstrap the Cisco 881 router and allow it to establish an IPsec tunnel to the management gateway and thus have access to the Cisco Configuration Engine / Cisco Security Manager. Now the full configuration file, pre-generated by the Cisco Security Manager and staged in the Cisco Configuration Engine, will be pushed to the router.

No user intervention is needed during this stage.

All these steps take about one minute to execute, the time needed for the spoke to enroll with the SDP registrar, get a PKI certificate, and load a small bootstrap template, followed by the management tunnel coming up and the full configuration file being retrieved from the Cisco Configuration Engine.

Reinserting the eToken at a Later Time

The full Cisco Virtual Office configuration should include the login credentials for the eToken user who will enter his or her PIN every time it is inserted. This user can have privilege level 1, and the crypto pki login command should be set to allow a privilege level 1 user to execute it.

The following commands are an example:

```
username etoken privilege 1 secret 0 eToken
privilege exec level 1 crypto pki
```

This example is for a Cisco Virtual Office spoke configured with the 10.32.247.104/28 protected network.

The end user document continues now. Please note that we set up the username etoken and password eToken with privilege level 1 for this purpose.

- **Wait 1 minute** to allow the full VPN configuration to be downloaded.
- Now renew your PC IP address. To do this do (assuming that you're using Microsoft Windows):
  - Click Start -> Run
  - Type "cmd" (or "command," depending on the Windows version).
  - Type "ipconfig /release" followed by "ipconfig /renew" (if the end machine runs another OS, the procedure for bouncing the interface is needed here).
- After a new IP address is shown, open a browser and test your connectivity to the internal corporate site.

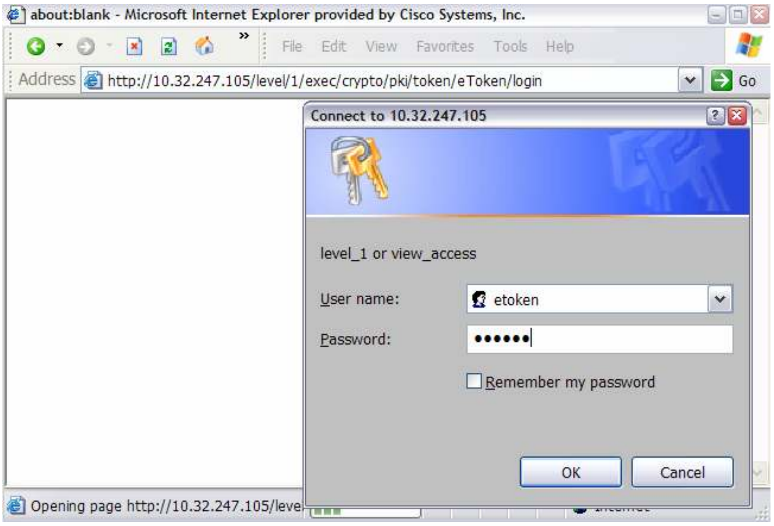
Reinserting the eToken at a Later Time

You will have to unlock the eToken private security keys every time the eToken is inserted or the router is power-cycled.

To activate the security keys stored in the eToken, follow these steps. Please note that your router local home IP address is now **10.32.247.105**.

- Open a browser window in a PC connected to the Cisco 881 router
- Enter this URL: http://10.32.247.105/level/1/exec/crypto/pki/token/eToken/login
- Use the **etoken/eToken** username/password to allow you to go into exec mode. You should change these default credentials, for your own security. See below for instructions on how to do this.
- Enter the eToken unlock PIN. The factory default is 1234567890.

Figure 3. Log in with privilege level 1 to unlock the eToken



about:blank - Microsoft Internet Explorer provided by Cisco Systems, Inc.

Address: http://10.32.247.105/level/1/exec/crypto/pki/token/eToken/login

Connect to 10.32.247.105

level_1 or view_access

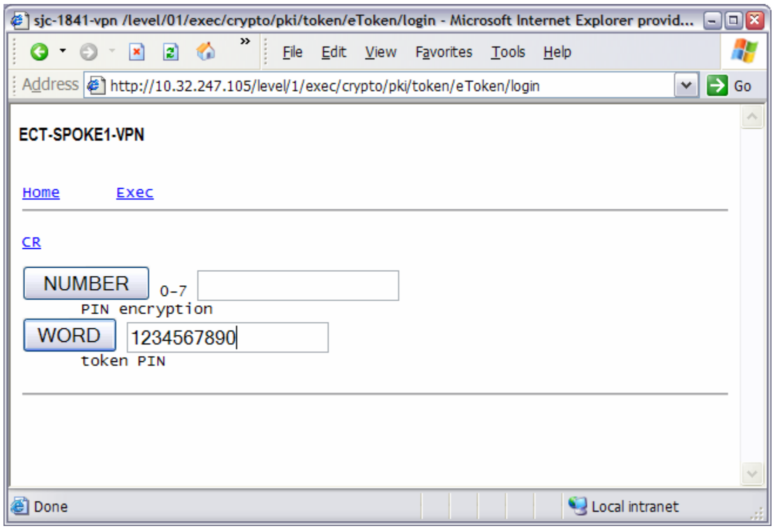
User name: etoken

Password: ••••••

☐ Remember my password

Opening page http://10.32.247.105/leve

Figure 4. Enter the PIN for the eToken



sjc-1841-vpn /level/01/exec/crypto/pki/token/eToken/login - Microsoft Internet Explorer provid...

Address: http://10.32.247.105/level/1/exec/crypto/pki/token/eToken/login

ECT-SPOKE1-VPN

NUMBER 0-7
PIN encryption

WORD 1234567890
token PIN

Done

Local intranet

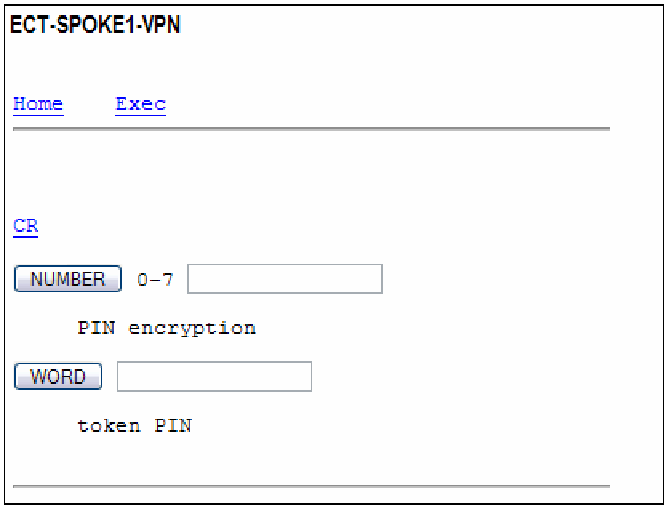
Changing the eToken PIN

You need to change your eToken PIN from time to time. Please change it right after you make sure your router is working properly.

To change the eToken PIN, follow these steps:

- Open a browser window in a PC connected to the spoke router.
- Enter this URL: http://10.32.247.105/level/1/exec/crypto/pki/token/eToken/login
- Log in to the router using the token/eToken username/password.
- Enter the current eToken unlock PIN. The factory default is 1234567890.
- Change the pin by entering this URL: http://10.32.247.105/level/1/exec/crypto/pki/token/eToken/change-pin
- Enter the new PIN. It can be numeric, or a word.

Figure 5. Change the eToken PIN



Important Information about the eToken PIN

The end user must enter the PIN every time the eToken is reinserted or the router is power-cycled. After the PIN has been changed, the administrator can reset the login failure count to zero (via the “crypto pki token max-retries” command). The maximum number of allowable login failures is set by default to 15; after that the eToken is permanently locked and can be recovered only with the admin-PIN.

If you want to change the admin-PIN on the token, you must be logged into the eToken as admin, via the “crypto pki token admin login” command. For example,

```
crypto pki token usbtoken0 admin login 5678
```

Please contact your eToken provider for more information about the admin-PIN.

The scenario just described is for situations in which we want to be extra careful and have the end user always unlock the eToken by entering the PIN. However, if you just want to use the eToken as a physical key for on/off operation, without the need to type a PIN, you can set auto-login in the router configuration. This command allows the router to log the eToken in automatically when it is inserted into port USB0. It can be saved to NVRAM as well.

```
crypto pki token usbtoken0:login 1234567890
```

Now the end user can safely insert/remove the eToken and does not need to worry about the PIN, while still having an easy way to lock the router’s VPN access to the central office.

References

- Cisco Virtual Office solution guides and information: http://www.cisco.com/go/cvo
- USB eToken and USB Flash Features Support: http://www.cisco.com/en/US/products/ps6247/products_data_sheet0900aecd80232473.html
- Detailed USB storage use: http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a0080420500.html#wp1090554
- Using eToken with Cisco IOS Software Release 12.3(14)T: http://www.cisco.com/en/US/products/ps6247/products_white_paper0900aecd80275112.shtml
- Cisco Security Manager: http://www.cisco.com/en/US/partner/products/ps6498/index.html
- Cisco Configuration Professional: http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=281795035

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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 C11-492748-00 08/08