..|...|.. cisco

Mobile Workforce Architecture: VPN Deployment Guide for Nokia, iPhone, and RIM with Cisco ISR G2



This deployment guide explains the configuration of the Cisco IOS VPN (Integrated Services Router Generation 2 [ISR G2]) head-end router for use with native VPN clients of Nokia, iPhone, and Blackberry devices. This guide assumes that the basic Cisco IOS[®] VPN head-end configuration is in place. The configurations discussed here include any network-related configurations, such as inside and outside interface assignments, IP address configuration, hostname, domain, and default routes. Configurations are shown using the Cisco[®] command-line interface (CLI).

This deployment guide has two main parts:

- Part 1 discusses the configurations required on Cisco IOS VPN head ends to support Nokia, iPhone, and RIM devices. Cisco IOS Software Release 151-3.T.bin was the version tested. Note that unlike Nokia and iPhone devices, which work over 3G and 4G and WiFi, RIM IPsec VPN works only over WiFi hotspots. Also note that RIM with public key infrastructure (PKI) works only when xAuth with PKI is enabled on the RIM device.
- Part 2 consists of Appendixes A, B, and C, which discuss manual installation of VPN settings on iPhone, Nokia, and RIM devices.

Part 1: Cisco IOS VPN Head-End Configuration

Following are the steps to configure the VPN gateway to work with iPhone, Nokia, and RIM devices. Authentication is based on PKI and certificates either from a Microsoft or Cisco IOS Software certificate authority (CA). This guide assumes a Microsoft CA. This guide also assumes that there is not a split tunnel and that profile matching is based on the OU or department field in the certificate.

Table 1 lists the high-level steps required to configure Cisco IOS Software to support Nokia, iPhone, and RIM devices.

| Step | Description |
|------|---|
| 1 | Define authentication, authorization, and accounting (AAA) settings. |
| 2 | Define the PKI trustpoint. |
| 3 | Authenticate and enroll with the CA. |
| 4 | Define the certificate map. |
| 5 | Define Internet Security Association and Key Management Protocol (ISAKMP) policy. |
| 6 | Define a pool from which the client is assigned an IP address. |
| 7 | Define mode configuration parameters. |
| 8 | Define the ISAKMP profile. |
| 9 | Define the transform set. |
| 10 | Define the IP Security (IPsec) profile. |
| 11 | Define the virtual template. |

 Table 1.
 Steps for Configuring Cisco IOS Software for Nokia, iPhone, and RIM Mobile Devices

Step 1: Define AAA Settings

This step defines the AAA settings. Here, local is used as the default method of authentication and authorization.

aaa new-model

aaa authentication login default local none

aaa authorization network default local none

Step 2: Define the PKI Trustpoint

This step defines the PKI trustpoint and the CA server to be used. Note that depending on the phone OS type— Nokia, RIM, or iPhone—some settings inside the trustpoint, such as fqdn/subjecname/ip-address, must exactly match the configuration shown here.

crypto pki trustpoint <trustpoint name>
enrollment mode ra
enrollment url http://<CA server url>
! e.g. http://ca.cisco.com:80/certsrv/mscep/mscep.dll
serial-number
fqdn <IP Address of WAN Interface>
ip-address <IP Address of WAN Interface>
subject-name CN=<IP Address of WAN Interface>

revocation-check none

authorization username subjectname commonname

Step 3: Authenticate and Enroll with the CA

This step helps ensure that the router uses the Simple Certificate Enrollment Protocol (SCEP) enrollment process, so you need a Microsoft CA with an SCEP client.

crypto pki authenticate <CA server name>

crypto pki enroll <CA server name>

Step 4: Define the Certificate Map

Define a certificate map for smartphones. Note that two certificate maps are created. RIM and Nokia use only the phonepki certificate map. iPhones use two certificate maps (phonepki and dummy) because of certain restrictions in Apple iOS.

crypto pki certificate map phonepki 10

subject-name co phonepki

crypto pki certificate map DUMMY 20

subject-name co dummy

Step 5: Define ISAKMP Policy

This step defines the ISAKMP policy and settings.

crypto isakmp policy 1 encryption 3des group 2 crypto isakmp keepalive 10 10 crypto isakmp nat keepalive 50

crypto isakmp xauth timeout 90

Step 6: Define a Pool from Which the Client Is Assigned an IP Address This step defines the pool used to assign an IP address to the client.

ip local pool easyvpn-pool <first_ip_addr last_ip_addr>

Step 7: Define the Mode Configuration Parameters

This step defines the parameters that an Easy VPN client receives from the server. The dummy profile is used only for iPhone devices.

crypto isakmp client configuration group phonepki dns <*dns server IP>* domain <*domain name*> pool easyvpn-pool save-password ----→ forces the client to save the password crypto isakmp client configuration group dummy

dns <**dns server IP**>

domain <**domain name**>

pool easyvpn-pool

Step 8: Define the ISAKMP Profile This step defines an ISAKMP profile that links the CA server, maps, AAA settings, and mode configuration parameters defined here in a single profile.

crypto isakmp profile phonepki ca trust-point <trustpoint name> match identity group phonepki match identity user-fqdn domain cisco.com client authentication list local !! needed only if doing xauth isakmp authorization list local client configuration address respond virtual-template 6 crypto isakmp profile dummy - need a dummy profile for iPhone self-identity address match identity group dummy client authentication list local isakmp authorization list local client configuration address respond virtual-template 6 Step 9: Define the Transform Set This step defines the IPsec settings. crypto ipsec transform-set t1 esp-3des esp-sha-hmac crypto ipsec transform-set t3 esp-aes 256 esp-sha-hmac mode transport require crypto ipsec transform-set t4 esp-3des esp-sha-hmac mode transport require Step 10: Define the IPsec Profile This profile links all transform sets under a single profile. crypto ipsec profile stealth set transform-set t3 t4 t1

Step 11: Define the Virtual Template

This step associates the physical interface with the virtual interface and applies the IPsec profile to the virtual interface.

```
interface Virtual-Template6 type tunnel
ip unnumbered <WAN interface>
ip mtu 1400
ip tcp adjust-mss 1200
tunnel mode ipsec ipv4
tunnel path-mtu-discovery
tunnel protection ipsec profile stealth shared
interface FastEthernet4
no ip dhcp client request tftp-server-address
ip address dhcp
load-interval 30
duplex auto
speed auto
!
```

Note

• If you are using Loopback 1 as the WAN interface, the configuration would be: interface Loopback1

```
ip address <routable WAN IP> <subnet mask>
```

• For RIM, you need to define a username and password along with the certificates: username xyz password xyz

Part 2: Appendix

This section describes the step-by-step installation and management of VPN settings on mobile phones, including VPN policy, VPN settings, and VPN connectivity.

Appendix A: Nokia E Series Manual Step-by-Step VPN Configuration with Certificates This section provides step-by-step instructions on the installation and management of VPN settings on the Nokia E Series devices.

The Nokia E Series phone needs to be activated and associated with a phone number, and Internet access must be operational.

- 1. From nokia.com, install Nokia PC Suite on your PC.
- 2. Use Nokia PC Suite to upgrade the Nokia firmware, connecting USB or Bluetooth or infrared.



 Open a browser on your computer and request a certificate for the phone from the CA server at http://<IP of CA server>/certsrv.

| Nicrosoft Certi | lisate Services - Nicrosoft Internet Explaner | |
|---|---|------------------|
| Elle Edit Veni | Fyrates look 1910 | * |
| (ant . () | · 🖪 🔹 🟠 🔎 Savdi 👷 Farottal 🥝 🔗 - 🖓 🧛 • 🖃 • 🔜 Ol • 💭 | |
| the lite | ta calentary/tortrana.ep | 💌 🛃 Ge 🛛 Line ** |
| Advanced Ce | rtificate Request | 0 |
| Identifying Infer | mation: | |
| Name | Mobile E71 Certificate | |
| E-Mail | phakore@cisco.com | |
| Company | Cisco Systems Inc | |
| Department | phoneki | |
| C8- | Cha long | |
| State | Ca | |
| Country/Region | US | |
| Type of Certifica | te Nooded: | |
| | Client Authentication Certificate | |
| and star | | |
| Key Options: | | |
| 050 | Create new key set O Des existing key set | |
| Kay Heave | Officience Officiency Officiency Officiency | |
| Key Size | 1024 Miles 304 (seminaria legitaria dal 2020 2020 2020 2020 2020 2020 2020 20 | |
| | Automatic key container name O User specified key container name | |
| | Mark keys as suportable Europt keys to file | |
| | Enable strong priode key protection | |
| | These earlies is the local computer conditions take Stores after certain a local computer action invested of in the user's conditione action. Does not invested the local Conditioner Stores and any in the facual administrations of the certainer or user a key in the facual matchine action. | |
| Additional Optio | ns: | |
| Request Format | @CMC OPKCS10 | |
| Hosh Algorithm | SH4.1 City used to sign miquest. | |
| | Save request to a file | |
| Attehates | 10 | |
| love | | |
| Add and the second s | | Chock Providence |

Note that the department field is the same as that defined in the configuration of the Cisco IOS VPN head end (for example, phonepki).

4. Install the certificate on your computer.

| Akonet Gerlikzte lerium - Akonet Tolenet Tolenet | |
|--|---------------------------|
| No Ed. Jan Justice Talk Jup | |
| Otal + O - E E C Part Strate O O- S E - E E S | |
| Altina 👸 192 (1) 7.1.16.302/orden/det/fun.488 | - Da ini |
| Manual and an Annual - 01/1400000 | |
| | 1885 |
| Certificate Issued | |
| The cettificate you requested was issued to you | |
| Instal this certificate | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| Paterital Sciping Videlini | 20 |
| The Website is addrog are an acceleration to the computer. Allowing an anticular dividual to galaxy scarcer finates is a society res. The Web also addro fixed, which not if alway respectively you bond that to say in this response to your rely. | ntal collision you it not |
| Do you want the proportion address configurations of Odd the Fyron rout the Web atte. Otherwise, do: No. | |
| > > | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| 0 | 🔮 bienst |
| Anter BREOSARS Con-Bei Bri Gen Bei Bri Bei Bei Bei Bei Bei Bei Bit | NO. 6 4 8 30 9 8 St 2 R. |

- 5. Export the certificate.
 - a. For Export the Private Keys, click Yes.
 - b. Select Include All the Certificates in the Certification Path If Possible.
 - c. Type a password.
 - d. Provide a name for the certificate, such as Mobile E72 Certificate.p12Complete the export. The certificate is exported to the desktop.

| d Cetilicate Services - RACASERVER | | | |
|---|--|---|--|
| cate installed | | | |
| w certificate has been successfully installed. | | | |
| et Options 2 est General Private Option Content Conservation 2 Private 2 Private | | | |
| averi Adva | | | |
| Rubrigs help you control the internet content that can be reveal on the computer | | | |
| Enatia. Lating | | | |
| Use confliction to problemly identity proceed, confliction | Centrate 2 | 3 | |
| Des 55, State Cellicater. Publisher. | bindelarges: db | | |
| insonal elementor. | Personal Other Regile Internediate Continuation Authorities Trusted Face Continuation | E | |
| AddCorplete stores previous entries AutoCorplete | based to based by Expendent Peerdy Same | | |
| T and suggests matches for you | Pier Cert RA-CA-SERVER SECTION dames Bittable Cert for Alam 114-CA-SERVER (62)(0001 diames | Centrificate Lopert Witeard | |
| Moscolt Pelle Austrat itors you My Polle | Bindule CT Cert RA-CA-XXXIX (\$25,000) dianes Bindule CT Certificate RA-CA-XXXIX (\$20,000) dianes | file to Laport Specify the name of the file you want to export | |
| | | | |
| | | Tienane TECHNIKETARE Bown | |
| U. Like set | L | | |
| | Bust. Epst. Reve Advand. | 1 | |
| | Cartificate estanded purposes | | |
| | Cert Automician, Soure End, Entryping He System | | |
| | | | |
| | Core | | |
| | | Clad. Net> Ceol | |
| | | | |
| | | | |
| | | | |
| | | | |

6. Create a VPN policy using the Nokia Mobile VPN Client Policy Tool. Refer to the sample screen shot here to create the .vpn file.

| General Information | | | Certificate A | uthority | |
|-----------------------|--|---|---------------|---------------------------------|--------|
| Policy name | Paragi/PN | | Format | BIN | |
| VPN gateway address | <pre><vpn-gatewayipaddress></vpn-gatewayipaddress></pre> | | Data | C:\Program Files\Nokia\Nokia Mo | bile V |
| IKE | | | User Certific | ate | |
| IKE mode | IKEv1 main | ~ | Certificate | user-1.cer | |
| Authentication method | RSA_SIGNATURES | | Private key | user-1.key | |
| Identity type | RFC822_NAME | ~ | Subje | ect DN suffix | |
| Identity value | pthakore@cisco.com | | RFC822NA | ME (FQDN) | |
| Remote ID type | ~ | | | Keylength 1024 💌 | |
| Remote ID | | | PKCS#12 | | |
| EAP realm prefix | | | PKCS file | C:\Program Files\Nokia\Nokia Mo | bile V |
| Silent CRACK | | | VPC file | | |
| Usemane | | | | | |
| Password | | 1 | | | |
| Preshared Key | | | | | |
| Format | STRING_FORMAT | ~ | | | |
| Key | | | | | |

 You can also choose View > Advanced Wizard and generate ISAKMP and IPsec policies as configured on the Cisco IOS VPN head end. Following are the settings in the Advanced Wizard view for both ISAKMP and IPsec.

| Nokia Mobile VPN Clie | nt Policy Tool | |
|--|--|-------|
| e View Help | | NOKIA |
| Information □ IPsec □ SAs □ vpn6_1 □ Selectors □ remote - self defined □ self defined □ self defined | Policy Information Name Parag VPN Version 1.0 Description | |
| Certificates | Issuer name | |
| | | |
| | | |
| Generate VPN Policy | | |

| e View Help | | | NOKIA |
|---|---|---|-------|
| Information IPsec SAs Selectors remote self defined IKE Certificates | IPsec SA Parameters Name Encryption algorithm Hash algorithm Remote identity Perfect Forward Secrecy Hard lifetime add time Soft lifetime use time Soft lifetime use time Replay window length | Vph6_1 3DES SHA1 0.0.0.00 N © DFF 3600 seconds 9 seconds 9 | |

| e View Help | | NOKIA |
|------------------------|---------------------------|-------|
| Information | IPsec Selector Parameters | |
| G SAs | Type remote 🗸 |] |
| Selectors | Selector | |
| remote self defined | Address 0.0.0 | |
| - self defined | Netmask 0.0.0 |] |
| IKE Certificates | IPsec SA vpn6_1 | |
| | | |
| | | |

| : View Help | | | NOKIA |
|----------------------|---------------------------|---|-------|
| Information | IPsec Selector Parameters | | |
| ⊟ SAs | Type self defined | ~ | |
| vpn6_1 Selectors | Selector inbound = { } | | |
| - remote | Address | | |
| self defined | Netmask | | |
| E IKE | IPsec SA | | |
| 20 OCI (1100100 | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| : View Help | | | NOKIA |
|-----------------------|----------------------------|------------|-------|
| Information | -IPsec Selector Parameters | - | |
| ⊟ SAs | Type self d | lefined 🔽 | |
| vpn6_1 ⊟ Selectors | Selector outbo | ound = { } | |
| - remote | Address | | |
| self defined | Netmask. | | |
| IKE | IPsec SA | | |
| | Constrained of | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| View Help | | NOKIA |
|---------------------------------|---|-------|
| Information IPsec | General IKEv1 IKEv2 PSK CRACK | |
| 🖻 SAs | General IKE Parameters | |
| vpn6_1 ⊡-Selectors remote | IKE mode IKE v1 main | |
| | Authentication method RSA_SIGNATURES | |
| self defined | VPN gateway address <vpn-gatewayipaddress></vpn-gatewayipaddress> | |
| IKE Proposals | Identity type RFC822_NAME | ~ |
| E Certificates | Identity value pthakore@cisco.com | |
| | DNS server IP address | |
| | Send notification TRUE | - |
| | Perfect forward secrecy | |
| | Initial contact TRUE | |
| | Use internal addressing FALSE | |
| | DPD heartbeat 20 🗢 seconds | |
| | NAT keepalive 20 😂 seconds | |
| | Bekeving threshold 90 😂 % | |
| | ESP UDP port | |
| | | |
| | DEVICE V | |
| | | |

| e View Help | | NOKIA |
|--|---|-------|
| Information IPsec SAs vpn6_1 Selectors remote self defined IKE Proposals Certificates | General IKEVI IKEV2 PSK CRACK IKEVI Parameters Responder lifetime TRUE Send certificate TRUE IPsec expire TRUE Replay status FALSE Use mode config TRUE Use NAT probe FALSE Use commit bit FALSE Use XAUTH FALSE | |



8. Use Nokia PC Suite to connect the phone to the PC with USB or Bluetooth.

a. Copy the TEST11.vpn policy to any of the folders of the Nokia E72. Copy the new VPN client mVPN_S60_v3_1_080826.sisx to the same directory.



- 9. Disconnect the phone from USB.
- 10. Choose E72 > Menu > Office > File Manager and find the new VPN client. Install the VPN client.
- 11. Choose Menu > Office > File Manager and find the new VPN policy. Click and install it. Provide the P12 password (used in Step 5) and then a phone store password (the new password must contain no fewer than six characters).
- 12. Choose Menu > Tools > Settings > General > Security > Certificate Management > Authority Certificates and make sure that the RA-CA-SERVER certificate is installed.
- Choose Menu > Tools > Settings > General > Security > Certificate Management > Phone Certificate and make sure that Mobile E72 Certificate.p12 is installed.

- 14. Choose Menu > Tools > Settings > Connectivity > Destinations > Internet and make sure that your services provider 3G or 4G network is listed. Add an access point if you are using a public hotspot.
- 15. Choose Menu > Tools > Settings > Connectivity > Destinations > Intranent > VPN > Edit VPN and make sure that VPN internally is using the Internet destination group. Choose Automatically Connect in the VPN settings.
- 16. Launch a browser and use the intranet access point configured earlierand make sure that you can access corporate resources. You can also choose Applications > Office > Intranet and manually connect to the intranet.

Appendix B: iPhone Manual Step-by-Step VPN Configuration with Certificates

The iPhone must be activated and associated with a phone number, and Internet access must be operational.

- 1. Install the iPhone Configuration Utility and iTunes from www.apple.com. The iPhone Configuration Utility Version 3.2.0.267 was used for testing.
- 2. Connect your iPhone to the PC using the USB cable provided.
- 3. Upgrade your iPhone software, if needed, using iTunes.
- 4. Open the iPhone Configuration Utility.
- Request a certificate for the phone from RA-CA-SERVER at <u>http://<IP</u> of CA server>/certsrv. Note that the department field should be the same as that defined in the configuration of the Cisco IOS VPN gateway: for example, phonepki.
- 6. Install the certificate on your local computer.

- 7. Export the certificate.
 - a. For Export the Private Keys, click Yes.
 - b. Select Include All the Certificates in the Certification Path If Possible.
 - c. Type a password.
 - d. Provide a name for the certificate: for example, iPhone.p12.
 - e. Complete the export. The certificate is exported to the desktop.

| r Lectocité Sambes - RA-CA-SERVER | | | | |
|--|---|--|---|-----------|
| w ontificate has been successfully installed. 1 Optime 2 successfully installed 2 Social (Covertions) Pagens (Advancement) Weit Advancement) | N. N | | | |
| Ratego hely you conful the Internet content that can be viewed on the conpute | Certificates | 22 | 3 | |
| Dear SS, State Cetificates. Publichers. and information Add/Complete tones previous entries and roggetit middlen in you. Add/Complete. | Entended purpose: (AD) Fersonal Other People Intermediate Certification Authoriti Immed To Immed To Immed To Immed To Texture T | es Trusted Root Certificator * * reto | Certificate Expert Witzerő | × |
| Mosoch Polisk kristet store your My hole. personal information. DK Cancel App | Phote 17 Certificate 44-CA-20108 NO. | (2009 dares | Specify the name of the file you want to report File name. | Bowe |
| | Import Export Renove Conflicter Handed surgeons Cleret Aufhentication, Secore Brook, Energystrig He System | Advanced | | |
| | | Que | (bb) | Net> Ceol |
| | | | | |

- 8. Use the iPhone Configuration Utility to create a VPN policy according to the Cisco IOS Software configurations shown earlier. Note that the following steps are presented as samples only.
 - a. Define the General Settings: You can name your profile whatever you want and define a corresponding identifier.

| B General Mandatory | Identity | |
|--|----------|--|
| Passcode | | Name Display name of the profile (shown on the device) |
| | | vontori |
| Restrictions Not Configured | | Identifier Unique identifier for the profile (e.g. com.company.profile) |
| 🔿 Wi-Fi | | com.ciscoin.profile |
| Not Configured | | Organization Name of the organization for the profile |
| 1 Payload Configured | | cisco sys inc |
| Email Not Configured | | Description Brief explanation of the contents or purpose of the profile |
| Exchange ActiveSync Not Configured | | Profile description. |
| DAP Not Configured | | |
| CalDAV Not Configured | | Security Control when the profile can be removed. |
| Subscribed Calendars Not Configured | | Lenth A |
| Web Clips Not Configured | | |
| Credentials 1 Payload Configured | | |
| SCEP 1 Payload Configured | | |
| Advanced Not Configured | | |
| | | |

b. Define the PKSC 12 certificate. Choose Credentials and click Configure. The screens will automatically guide you to select the certificate you want to use for VPN connectivity.

| File Edit View Window Help | | Phone Configuration | Utility | wiciw. |
|--|---|---|--|--------|
| 😤 🙆 🛄 | | | | Q. Q. |
| Lincar Com Com Constructions Configuration | None support anytest | Monther mechanic profe- cencies under | Control 4:000000 00:00000 0:000000 0:00000 0:00000 0:00000 0:00000 0:000000 | |
| | Image: A starting in the index in the i | | Influence Constraints Constraints in service in straints on the COSS and ACCESS constraints in service in straints on the Cost and access in the Cost and access and access in the Cost and access i | |



c. Define the VPN settings. For the connection type, use iPsec. If you intend to use l2tp/ipsec as shown here, specify the connection type as l2tp. Also use the identity certificate configured in Step b.

| e Edit View Window Help | | sPhone Configuration | Usinty | |
|--|--|--|---|--------------------|
| 2 📧 🚺 | | | | () Q: |
| e Shert Export | 11-11-11-11-11-11-11-11-11-11-11-11-11- | Disk's | WARMAN AND A REAL PROPERTY OF A | ride Detail Search |
| Janer Denken Japiezanna Pronzeciej Politik Kontegeri den konte | Rumo angelad angelad | Identifier cons.conte.profile cons.conte.profile | Central 9120206 102-01 PM 7/21/2009 302-01 PM | |
| | 6 General | VPN | | |
| | Image: Second and a control of the | | Control basic Control basic <td< td=""><td></td></td<> | |

- 9. Install this profile on the phone. Then choose Settings > VPN on your iPhone.
- 10. Select the VPN profile as shown here.

| 11:16 AM | |
|-----------------|---|
| VPN | |
| | OFF |
| Configuration | |
| | ٥ |
| | ۲ |
| n | ۲ |
| Ρ | ٥ |
| onfiguration | ٥ |
| N Configuration | |
| | VPN Configuration P onfiguration |

| iPod 🗢 | 11:10 AM | - | | | |
|-------------------------------|------------|------------------|--|--|--|
| Cancel Add Configuration Save | | | | | |
| | ********** | | | | |
| L2TP | PPTP | IPSec | | | |
| cisco | | | | | |
| Description | Test Vpn | | | | |
| Server | 128.107.15 | 1.94 | | | |
| Account | admin | | | | |
| Password | ••••• | | | | |
| Use Certificate ON | | | | | |
| Certificate | | sheetal > | | | |
| | | Merenner de la C | | | |

11. Manually select the certificate on the phone for the VPN profile.

12. Turn on VPN connectivity, and you will be connected.



Appendix C: RIM Manual Step-by-Step VPN Configuration with Certificates

- 1. Download the certificate to your computer as described in Appendix A or B.
- 2. Synchronize the certificates on your computer with your RIM device using the Blackberry Desktop Manager Certificate Synchronization tool. Version 5.0.1 was used here.

In Version 6.0, you need a custom installation to get this option:

http://docs.blackberry.com/tr-tr/admin/deliverables/14334/Users cant find cert synch tool 602750 11.jsp

 Choose Options > Security > Advanced Security Options > VPN > Add a New VPN Profile. Change or define the parameters as shown here.

Name: <define any name> Gateway Typ: Cisco IOS With Easy VPN Server Concentrator address: 128.x.x.x. Group name:phonepki Group Password: User Name:cisco User Password: cisco Save Password: Select This option Client Certificate <Select certificate> CA Certificate <Select certificate> Select button "Dynamically Determine DNS> IP Address: Subnet Mask: Primary DNS: Secondary DNS: Domain Name: IKE DH Group: <Select Group> IKE Cipher: Select 3DES (168-bit Key) IKE Hash : Select HMAC SHA1 (160 bitys) Select button <Perfect Forward Secrecy> IPSec Crypto and has suite : Select 3DES-SHA1 NAT timeout (in minutes):1 Unselect <use hard token> Software token Serial Number <None Availble> Select <Disable VPN banner> Note: RIM VPN works only with WiFi. Make sure to select the VPN profile under the RIM WiFi settings.



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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Printed in USA