

Using CertAgent™ for Strong User Authentication in Check Point VPN-1

Copyright© 2002 Information Security Corporation.
All rights reserved.

This document describes how to set up strong authentication between a SecuRemote client and a Check Point firewall using CertAgent as the certificate issuing software.¹

To create a certificate request using Check Point VPN-1 SecuRemote:

1. In the SecuRemote's main window select **Certificates->Offline Registration Utility...**
2. Select **Create a digital certificate**.
3. Enter the requested information (first name, last name, *etc.*) and click **Next**.
4. Click **Save to a file (to later send via e-mail)**.
5. Click **Browse...** and in the **Choose a PKCS#10 file** dialog that appears specify a file in which to store the certificate request. Click **Save** to return to the wizard, then click **Next**.
6. Important: Record the reference number and authentication code that are displayed for later reference.
7. Send the.p10 file you created to your CA (i.e., to the CertAgent "issuer" responsible for issuing your certificate).

To issue an end-user certificate using CertAgent:

1. Move the user's .p10 file into the directory where CertAgent normally looks for certificate requests (*i.e.*, into your 'crq.in' folder or the directory specified in the **Additional Source of Requests** field in the Options settings for your profile.)
2. Start CertAgent if it is not already running.
3. Select **Profiles** in the **File** menu, or click **Profiles** in the button bar, and make sure your profile is selected in the **Active Issuer** list. (If you haven't already established an issuer profile, do so now using the **New** or **Wizard** buttons.)
4. Select **Requests->Pending** from the **File** menu (or click **Requests** in the button bar and then select "**pending certificate requests**" in the **View** drop down list, if that view is not already active). The user's certificate request should appear in the list. (If it doesn't, make sure you performed step 1 correctly.)
5. In the **Output** settings tab below the list of pending certificate requests, specify an output **Directory** and set the **Format** field to ".p7b certificate chain" (the last item in the **Format** menu).
6. (optional) Change or set any desired attributes on the **Validity Period**, **RDNs**, and **Extensions** tabs. (Hint: You can also use the **LDIFs** tab to facilitate the later entry of certificates into an LDAP directory.)
7. Click the certificate request to select it, then click **Issue**, enter your password, and click **OK** to create the certificate.

¹ CertAgent certificates have been tested with Check Point 4.1 and SecuRemote Version 4.1 SP-5 3DES (Build: 4199), instructions and results for different versions of SecuRemote may vary.

8. (optional) To make things easier for the end user, locate the output '.p7b' file in Windows Explorer – it will be in the output directory you specified in step 5 – and change the file extension to '.p7c'.
9. Now send the new '.p7c' (or '.p7b') file along with your signing certificate (and any other certificates in the chain) to the end user *as separate files*. (Note: it will be easier for the SecuRemote end-user if you send all certificates as separate '.p7c' files. You may even want to convert the CA certificate to a '.p7c' file.)
10. Install the new certificate on the firewall for user authentication. (Let us know if you need more detailed instructions for this step.)

To install the certificate in the SecuRemote client:

1. In the SecuRemote main window, choose **Certificates->Offline Registration Utility...**
2. Select **Import a digital certificate** and click **Next**.
3. Select the reference number you were given earlier and enter the corresponding authentication code. Click **Next**.
4. Select **Import from a file** and click **Browse....** In the **Choose a PKCS#7 File** dialog, locate your '.p7c' file, select it, and click **Open**.
5. Click **Next** to view the information in the certificate. Review it (to make sure it's yours!) and then click **Next**.
6. You will be asked to provide the CA's certificate. Select **Import from a file**, then click **Browse....**
7. In the **Choose a PKCS#7 File** dialog, select the CA's certificate file – if your CA sent you a '.p7b' file rather than a '.p7c' file, you'll first need to change the file filter to '*.*' from '*.p7c' in order to see it – and click **Open**.
8. Click **Next**. SecuRemote will show you the info in the CA certificate. Review it and then click **Next**.
9. In the next dialog, you will be asked where you want to save your Entrust Profile. Enter a filename and location, then click **Next**.
10. Now set your password and confirm it by entering it again. Click **Finish**.
11. When you see a dialog confirming that your profile was created record the validation string for later reference.
12. In the **VPN-1 SecuRemote Authentication** dialog you can now select **Use Certificate**, select the applicable '.epf' file, enter your password, and connect to the firewall.