How to Connect with SSL Network Extender using a Certificate
Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Documentation
The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=12512
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>29 August 2011</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on How to Connect with SSL Network Extender using a Certificate ).
How to Connect with SSL Network Extender using a Certificate

Objective
This document shows how to connect with SSL Network Extender using a third party user certificate.

Supported OS
- Windows 7 32-bit and 64-bit
- Windows XP

Supported Versions
- Security Gateway R70 and higher

Before You Start

Related Documentation and Assumed Knowledge
- VPN Admin Guide
- sk37782 (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk37782&js_peid=P-114a7bc3b09-10006&partition=Advanced&product=Security) SNX users fail to authenticate using certificates
- sk33319 SNX access with CA authentication fails
- How-to-configure-3-level-CA-on-Win2k8.doc

Certificate Authority structure overview:
Microsoft Active Directory: mycorp.cp
Root CA: RootCA
Subordinate CA: policyCA
Connecting with SSL Network Extender using a Certificate

Get Root Certificate

1. In the Active Directory Certificate Services - policyca Welcome window, under Select a task, select Download a CA certificate, certificate chain, or URL.

   ![Server Manager (DC2008R2)](image)

   Microsoft Active Directory Certificate Services - policyca

   Welcome

   Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to perform other security tasks.

   You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the

   For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

   Select a task:
   - Request a certificate
   - View the status of a pending certificate request
   - Download a CA certificate, certificate chain, or CRL

2. In the Active Directory Certificate Services - RootCA Download a CA Certificate, Certificate Chain, or CRL window, under Encoding method, select Download CA certificate.

   ![Certificate Transparency](image)

   Download a CA Certificate, Certificate Chain, or CRL

   To trust certificates issued from this certification authority, install this CA certificate.

   To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

   CA certificate:

   ![Certificate Transparency](image)

   Encoding method:

   - DER
   - Base 64
   - Install CA certificate
   - Trusted CA certificate
   - Download latest CA CRL
   - Download latest CRL
Get First Subordinate CA Certificate

1. In Active Directory Services - policyca Welcome window, under Select a task, select Download a CA certificate, certificate chain, or CRL.

2. In Active Directory Certificate Services - policyca Download a CA Certificate, Certificate Chain, or CRL window, under Encoding method, select Download CA certificate chain.

3. Get a second subordinate CA certificate as in step 2.

Add CA to SmartCenter

1. Open SmartDashboard.

2. In Servers and OPSEC applications, expand Trusted CAs, right-click Trusted CAs > New CA > Trusted.
3. In the **Certificate Authority Properties - RootCA** window, in the **OPSEC PKI** tab, under **Certificate**, click **GET** and under **Retrieve CRL From**, select **HTTP Server(s)**.

4. Select the root certificate that was created earlier.

5. Create another Trusted CA object and import a certificate from the first subordinate CA.

6. Create another Trusted CA object and import a certificate from the second subordinate CA.
Generate a Gateway Certificate

1. Open the gateway/gateway cluster object.
2. In IPSec VPN, click Add. In the Certificate Properties window that opens, select the last subordinate CA.
3. Click Generate.

4. In the Generate Certificate Request window, enter the DN.

5. In the gateway, click View.
6. In the **Certificate Request View** window, click **Copy to Clipboard**.

![Certificate Request View](image)

7. In the **Active Directory Certificate Services - issuer** **Welcome** window, under **Select a task**, select **Request a Certificate**.

![Active Directory Certificate Services](image)

**Welcome**

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL).

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

**Select a task:**
- Request a certificate
- View the status of a pending certificate request
- Download a CA certificate, certificate chain, or CRL

8. In the **Request a Certificate** window, select **advanced certificate request**.

![Request a Certificate](image)

**Request a Certificate**

Select the certificate type:
- User Certificate

Or, submit an **advanced certificate request**

9. In the **Submit a certificate Request** window, in the **Saved Request** field, paste the data from the **Certificate Request View**, which you copied to clipboard and click **Submit**.

![Submit a Certificate Request](image)

**Submit a Certificate Request or Renewal Request**

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate:

![Saved Request](image)

**Certificate Template:**
- [Web Server](#)

**Additional Attributes:**

- Attributes:

  ![Submit button](image)
10. In the Active Directory Certificate Services - MSCA-ROOT-CA Certificate Issued window, select Download certificate chain.

11. In the gateway/gateway cluster IPSec VPN, import the p7b certificate to the gateway/gateway cluster, select it and click Complete.

12. In VPN clients, make sure SSL Network Extender is selected.

13. Make sure Office Mode is configured according to VPN Admin Guide.

**Issue User Certificate**

2. In the Active Certificate Services - issuer Welcome window, select Request a certificate.

4. In the **User Certificate - Identifying Information** window, click **Submit**.

5. In the **Certificate Issued** window, click **Install this certificate**.
6. In Windows **Certificates** window, **Personal** folder, **Certificates** sub folder, select the certificate.

![Certificate Window](image)

7. In the **General** tab, make sure it states **You have a private key that corresponds to this certificate**.

![Certificate Information](image)
8. In the **Certification Path** tab, view the certificate and make sure the status is **This certificate is OK**.
9. Connect to SSL Network Extender. Select the certificate when prompted and click **OK**.
Index

B
Before You Start • 5

C
Connecting with SSL Network Extender using a Certificate • 6

H
How to Connect with SSL Network Extender using a Certificate • 5

I
Important Information • 3

O
Objective • 5

R
Related Documentation and Assumed Knowledge • 5

S
Supported OS • 5
Supported Versions • 5