



**Nokia Mobile VPN
Web-based
configuration for
Symbian devices**

NOKIA

Nokia for Business

Table of Contents

Introduction.....	3
References.....	3
Abbreviations and definitions	3
Overview	4
Environment configuration	5
Service installation.....	6
Service configuration.....	7
Mobile device configuration	8
Pre-requisites for the mobile device.....	8
Configuration.....	8

Work together. Smarter.

Nokia Inc. 102 Corporate Park Drive, White Plains, NY 10604 USA

Americas Tel: 1 877 997 9199 • Email: usa@nokiaforbusiness.com

Asia Pacific Tel: +65 6588 33 64 • Email: asia@nokiaforbusiness.com

Europe France +33 170 708 166 • UK +44 161 601 8908 • Email: europe@nokiaforbusiness.com

Middle East and Africa Dubai +971 4 3697600 • Email: mea@nokiaforbusiness.com

www.nokiaforbusiness.com



Nokia for Business

Introduction

This document explains how to configure a web-based provision service for Symbian mobile VPN clients when using Microsoft Windows Server 2008 R2 [3] as Secure Gateway.

References

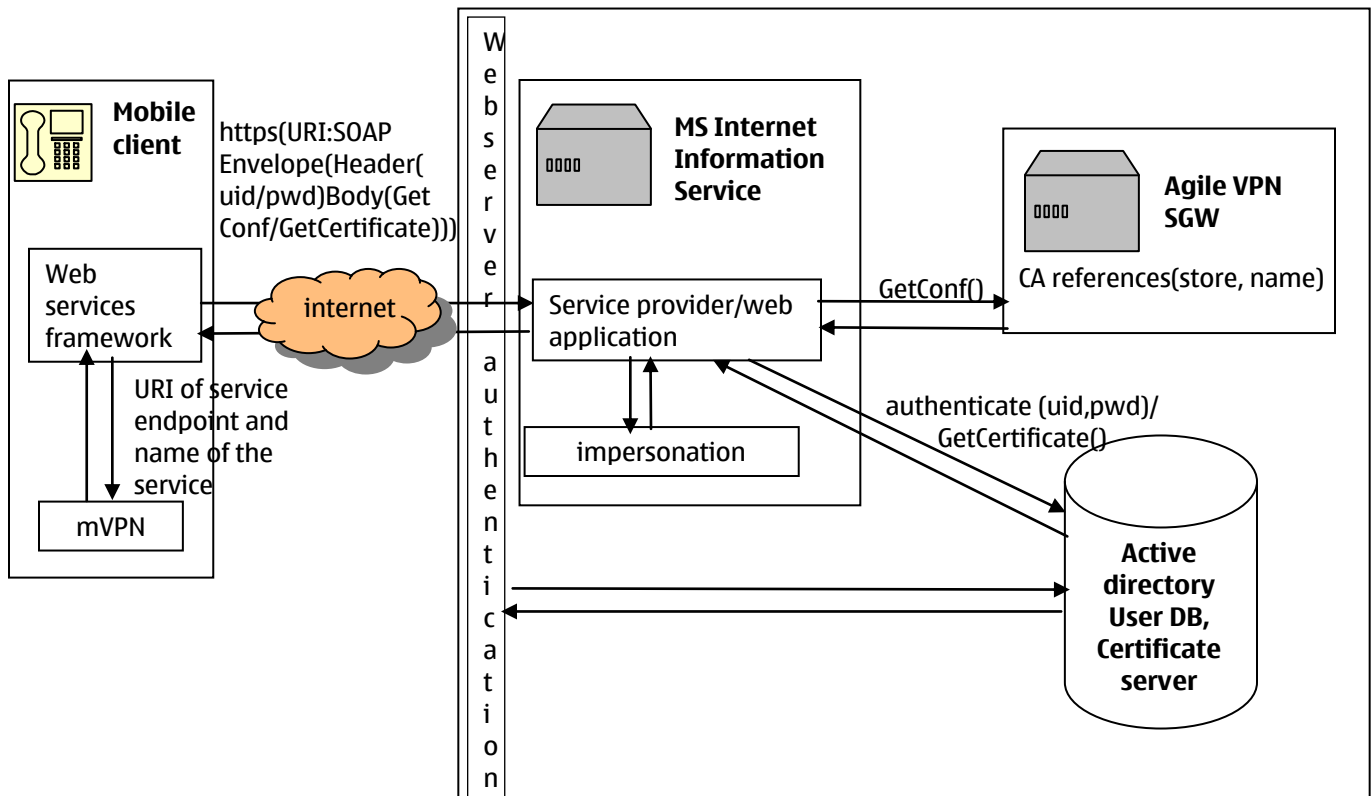
[1] Step-by-Step Guide: Deploy remote access with VPN Reconnect	http://www.microsoft.com/downloads/en/details.aspx?FamilyID=7e973087-3d2d-4cac-abdf-cc7bde298847&displaylang=en
[2] Nokia_Mobile_VPN_Policy_Specification.doc	
[3] Windows Server 2008 R2	http://www.microsoft.com/windowsserver2008/en/us/product-documentation.aspx
[4] Internet Information Server	http://technet.microsoft.com/en-us/library/cc753433(WS.10).aspx

Abbreviations and definitions

IIS	Microsoft Internet information service
CA	Certificate authority
SGW	Secure Gateway
SOA	Service Oriented Architecture
URI	Uniform Resource Identifier

Overview

The web-based mobile VPN is a distributed, SOA-based application. When a Symbian device requests for the *AWS/AgileVPNProvisionService* internet service installed on a corporate site, the service provider responds by sending the policy, CA, and user certificate over the internet.



Picture 1. Web-based provision system for Symbian mobile VPN client

Environment configuration

For instructions on setting up the infrastructure, see document [1]. The main components are shown in picture 1. You need two servers: *Web server [4]* and *Certificate server*. You can use a standalone Windows server, or an active directory based on a more sophisticated infrastructure model, where services are distributed across an organisation. The system works in any domain model. You do not need to modify the current domain setup.

Service installation

1. Extract the service package content to the website under the *AWS* application.
2. Configure the web server to require SSL and basic authentication.
3. Configure impersonation to give the impersonated user the rights to read and issue certificates. The easiest way is to create a new user to a domain, and grant membership to the *Domain Admins* group. See [4] for instructions.

Service configuration

You need to configure two files in the *App_Data* directory:

- *AgileVPN.pol* policy file template. You can modify it as described in [2], or use it with the default value. The service logic updates the gateway address and certificate-related parameters automatically.
- *Config.xml* configuration file. Enter all the needed domain server addresses as follows:
 - If SGW is not on the same computer with the web server, the *sgw* key must have the *dns name* and *address* of SGW as attributes.
 - If the certificate server is not on the same computer with SGW, enter the *dns name* of the computer where the certificate service is running as the key *certificateServer*. It is preferred that the certificate service and SGW are on the same computer.
 - If the name of the server authentication certificate is different from the *dns name* of the *sgw*, enter the name of the certificate as the name of the *serverAuthCertificate* key. It is preferred that the server authentication certificate has the same name as the SGW computer dns [1].

The *Config.xml* file example is shown below:

```
<?xml version="1.0"?>
<configuration>
  <sgw name="sgw_name.domain.com" address="1.1.1.0"/>
  <certificateServer name=""/>
  <serverAuthCertificate name=""/>
</configuration>Client configuration
```

The example presents this computer hierarchy:

- The web server is running on a different computer than SGW.
- SGW is running on a computer *sgw_name.domain.com*, the IP address of which is 1.1.1.0.
- The certificate service is on the same computer as SGW, and the authentication certificate for SGW has the same name as the computer dns.

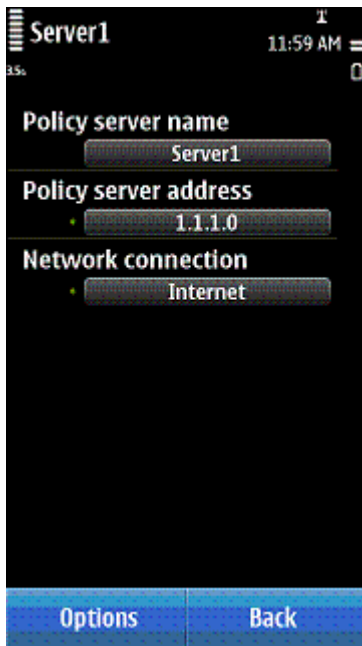
Mobile device configuration

Pre-requisites for the mobile device

- Symbian ^3 operating system
- Mobile VPN application
- Internet connectivity

Configuration

1. Open the VPN Management application.
2. Set the public address of the web server where the associated service is deployed.
3. Set the destination for the network connection.



Picture 2. Configuring mobile VPN policy server settings

Legal Notice

Reproduction, transfer, distribution or storage of part or all of the contents in this document in any form without the prior written permission of Nokia is prohibited.

Nokia and Nokia Connecting People are trademarks or registered trademarks of Nokia Corporation. Other product and company names mentioned herein may be trademarks or tradenames of their respective owners.

Nokia operates a policy of continuous development. Nokia reserves the right to make changes and improvements to any of the products described in this document without prior notice.

Under no circumstances shall Nokia be responsible for any loss of data or income or any special, incidental, consequential or indirect damages howsoever caused.

The contents of this document are provided "as is". Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, are made in relation to the accuracy, reliability or contents of this document. Nokia reserves the right to revise this document or withdraw it at any time without prior notice.