

# Nokia Configuration Tool

Admin Guide

**NOKIA**



# Contents

<b>1. Nokia Configuration Tool Overview .....</b>	<b>3</b>	3.5. VoIP Service Settings .....	17
1.1. Why NCT .....	3	3.6. E-mail Accounts Configuration .....	18
1.2. Supported Phones .....	3	3.7. Mail for Exchange Configuration .....	20
1.3. Release Highlights .....	3	3.8. SCCP Configuration.....	22
1.4. About NCT User Guide.....	3	3.9. PKI and Certificate Configuration .....	23
1.5. Salient Features.....	3	3.10. NCC for Alcatel Lucent Configuration .....	24
<b>2. Working with Nokia Configuration Tool.....</b>	<b>4</b>	3.11. F-Secure Configuration.....	27
2.1. Initialising the Tool.....	4	3.12. Other Configurations .....	28
2.2. Main View of the Tool.....	4	3.12.1. Files and Applications.....	28
2.3. Workspace .....	5	3.12.2. Contacts.....	28
2.3.1. Creating a Workspace .....	5	3.12.3. Sync.....	29
2.3.2. Managing Workspaces.....	5	3.12.4. Device Manager.....	29
2.4. Profiles.....	5	3.12.5. IM Servers .....	30
2.4.1. Creating Profiles.....	5	3.12.6. MMS Settings .....	30
2.4.2. Managing Profiles.....	6	3.12.7. Voice Call Continuity .....	31
2.5. Device Management .....	7	3.12.8. Destinations.....	32
2.5.1. Edit Online.....	7	3.12.9. Device Encryption .....	32
2.5.2. Mail for Exchange Certificate Enrollment	7	3.13. Editing, Deleting, and Duplicating	
2.5.3. Configure .....	7	Profile Settings.....	32
2.5.4. Edit Device Info .....	8	3.14. Selecting Profile Settings to be	
2.5.5. Delete Device .....	8	Sent to the Phone.....	33
2.5.6. Support for other Devices –		3.15. Classification of User and General Settings....	33
Auto Detect and Support Feature .....	8		
2.5.7. Connecting Phone using Bluetooth® .....	8	<b>4. VPN Configuration .....</b>	<b>33</b>
<b>3. Configuring and Provisioning Profiles .....</b>	<b>9</b>	4.1 Small description on VPN settings.....	33
3.1. Access Points Configuration .....	9	4.1.1 Settings based on authentication methods ...	34
3.1.1. Configuring Packet Data Settings.....	9	<b>5. Troubleshooting.....</b>	<b>34</b>
3.1.2. Configuring WLAN Settings .....	10	5.1. Generic Issues .....	34
3.1.3. Configuring Global WLAN Settings .....	13	5.2. PKI Related Issues .....	35
3.2. VPN Configuration.....	14	5.3. VPN Related Issues.....	35
3.3. VoIP Configuration .....	15	5.4. VoIP Service Settings Related Issues .....	35
3.4. SIP Configuration .....	15	5.5. WLAN Related Issues.....	35
		5.6. Restrictions and Known Issues.....	35

# 1. Nokia Configuration Tool Overview

Nokia Configuration Tool (NCT) is a PC application that enables you to manage the settings of Nokia Symbian phones. Your PC and phone must be connected through a Universal Serial Bus (USB) cable or through Bluetooth.® With NCT, you can configure various settings like Wireless-Local Area Network (W-LAN), Email, Internet Access Points (IAP), and VPN on a single phone or several phones at the same time. Files, contact cards, and applications can also be transferred from the phone to the PC and vice-versa.

## 1.1. Why NCT

Nokia Configuration Tool 6.2 is a feature-packed tool that enables you to easily manage your phone's profile settings ranging from emails, VoIP, Internet telephony to VPN, PKIs, and F-secure. Its compatibility with many devices and ease of use makes it a preferred tool with users.

## 1.2. Supported Phones

Nokia Configuration Tool supports Nokia Symbian phones. The phones supported are listed below:

Nokia E51, Nokia E52 PR 2.0 and newer, Nokia E55 PR 2.0 and newer, Nokia E60, Nokia E61, Nokia E61i, Nokia E62, Nokia E65, Nokia E66, Nokia E70, Nokia E71, Nokia E72, Nokia E75 PR 2.1 and newer, Nokia E90 Communicator, Nokia N97, Nokia N97 mini, Nokia N8, Nokia E7, C7, C6, E5 phones.

NOTE: To use the Nokia Configuration Tool 6.2 with Nokia E52, Nokia E55, and Nokia E72 phones, install the appropriate phone service pack that is available at the Nokia website.



Also with unique auto-detect and support feature, add support for many other models such as Nokia X6, Nokia N86 8MP, Nokia 5530 XpressMusic, Nokia 6124 classic, Nokia N82, Nokia N95 8GB, Nokia N95-3 NAM, Nokia 5700 XpressMusic, Nokia 6110 Navigator, Nokia N95, Nokia 6790 slide, Nokia 5730 XpressMusic, Nokia 6650 fold, Nokia N96, Nokia 5233, and more.

## 1.3. Release Highlights

The enhancements in the 6.2 release are as follows:

- SCCP Improvements
- SNAP Improvements
- Support of new Nokia phones (C5, E6, X6, X7 and C7-Astound)
- Support of new mVPN Client Side Features (Soft Token, Silent Extended Authentication and Proxy)
- Provide feedback through Image icon on Main Screen / Help Menu
- UX Improvements
- NCT 6.1 Issue Fixes

## 1.4. About NCT User Guide

Nokia Configuration Tool User Guide is primarily aimed at system administrators who configure phone profiles for users within an organisation. However, this guide provides information and explanation for most of the features and sections to support other end users also.

## 1.5. Salient Features

The salient features of NCT User Guide are as follows:

### 1. Access Points

An Access Point (AP) is a point in the network where your phone connects to a network. You must define Internet Access Points on your phone to use any internet related features or services.

For information on configuring AP settings, refer to Access Points configuration.

### 2. Public Key Infrastructure

A public key infrastructure (PKI) enables users of an unsecure public network such as the internet to securely and privately exchange data through the use of a public and private cryptographic key pair that is obtained and shared through a trusted authority.

For information on configuring PKI settings, refer to **PKI and Certificate configuration**.

### 3. SCCP

Nokia Call Connect for Cisco application uses Cisco's SCCP protocol (Skinny Client Control Protocol) to connect to Cisco Unified Communications Manager. NCT can be used to deliver an SCCP profile and related parameters to the device.

For information on configuring SCCP settings, refer to **SCCP configuration** and Nokia Call Connect for Cisco User's Guide.

### 4. VoIP Service Settings

In VoIP Service Settings, the Internet is used as the transmission medium for telephone calls. Because of the bandwidth efficiency and low costs that VoIP technology can provide, more and more businesses and end users prefer Internet telephone over the traditional copper-wire telephone systems.

For information on configuring VoIP Service Settings, refer to **VoIP Service Settings**.

### 5. VPN

The Nokia Mobile VPN is an Internet protocol security (IPSec) virtual private network (VPN) application that allows you to access enterprise intranet services securely from mobile phones. VPN policies define how data is encrypted for transfer over unsecured networks. VPN access points pair VPN policies with Internet Access Points to create encrypted connections.

For information on configuring VPN settings, refer to **VPN configuration**.

### 6. F-Secure

Secure your phone, network, and the data transmitted over the Internet with F-Secure.

For information on configuring F-secure settings, refer to **F-Secure configuration**.

### 7. NCC for Alcatel-Lucent

Nokia Call Connect (NCC) for Alcatel-Lucent integrates Nokia phones with the fixed corporate telephony infrastructure of Alcatel-Lucent OmniPCX Enterprise and OmniPCX Office, using both the cellular network and WLAN with VoIP technologies. Significant cost savings, increased productivity, and easy access to corporate PBX services are the key benefits.

For information on configuring NCC for Alcatel-Lucent settings, refer to **NCC for Alcatel-Lucent configuration**.


## 2. Working with Nokia Configuration Tool

This chapter introduces the following topics:

- Initialising NCT
- Main view of NCT
- Workspaces
- Profiles

### 2.1. Initialising the Tool

To initialise the Nokia Configuration Tool, do one of the following:




- Click **Start > Programs > Nokia > Nokia Configuration Tool 6.2**.
- Click the NCT icon  on the desktop.

### 2.2. Main View of the Tool

The following is a screen capture of the main view of the tool.



Figure 1: Main Workspace

Sections	Description
Action icons	Allows you to manage profiles.
Profiles	Provides information on the profiles that are created on the tool. It also allows you to manage the profiles.
Devices	Provides the following information on the phones that have been connected to NCT. <ul style="list-style-type: none"> <li>• IMEI number of the phone</li> <li>• Phone type</li> </ul>
Device menu	A small drop-down menu that helps you to manage the phones. The options here are the same as the options in the Devices menu of the Menu bar.
Connection status	Displays the connection status and type. <ul style="list-style-type: none"> <li> – Phone is not connected</li> <li> – Phone is connected through Bluetooth®</li> <li> – Phone is connected through USB</li> </ul>
Navigation buttons	Allow you to select the previous or the next phone for which a profile was created or configured.

## 2.3. Workspace

A workspace is a directory that contains phone data files and configuration profiles. When the Nokia Configuration Tool is initialised for the first time, the tool prompts you to create a workspace. When you create a workspace, a folder with information about the phone and the profiles is created at a specified location. You can manage the workspaces by using the File menu.

- Open existing workspaces
- Create new workspaces
- Create a duplicate of the currently open workspace and its contents
- Delete an existing workspace

### 2.3.1. Creating a Workspace

Creating a workspace is the first activity you perform with the Nokia Configuration Tool.

Perform the following steps to create a workspace.

1. On the **Menu** bar, click **File > New workspace**.
2. In the **New Workspace** dialog box, select the desired location and type a name for the workspace in the **Workspace name** field.
3. Click OK.

**NOTE:** Click **Cancel**, to cancel the creation of the workspace.

### 2.3.2. Managing Workspaces

#### Opening a Workspace

Perform the following steps to open a workspace.

1. On the **Menu** bar, click **File > Open workspace**.
2. In the Open Workspace dialog box, navigate to the appropriate location, select the workspace to be opened, and click **OK**.


#### Duplicating a Workspace

Perform the following steps to duplicate a workspace.

1. Open the workspace which you intend to duplicate.
2. On the **Menu** bar, click **File > Duplicate workspace**.
3. In the Duplicate Workspace dialog box, navigate to the desired location, type a name for the duplicate Workspace in the **Workspace name** field, and click **OK**.

#### Deleting a Workspace

Perform the following steps to delete a workspace.

1. Open the workspace you want to delete.
2. On the Menu bar, click File > Delete workspace.
3. In the Confirm Delete Workspace dialog box, click  to confirm deletion.


**NOTE:** After deleting a workspace, the tool prompts you to open an existing workspace or create another workspace. Select the desired option to continue.

## 2.4. Profiles

A Profile is a collection of settings such as WLAN, Email, Internet Access Point, and VPN that you define or specify for a particular phone. It is stored as an XML file in the workspace. You can create separate profiles for different purposes and phones. When you transfer a profile to a phone, the settings defined in the profile are configured on the phone. You can use one of the following options in the tool to manage your profiles:


- **Profiles** option on the **Menu** bar
- Action icons in the main view

## 2.4.1. Creating Profiles

A profile can be created by using either the  button or the New profile option in the Profiles menu.

In the following procedure, the New profile option in the Profiles menu is used to create a profile.

**NOTE:** A phone need not be connected to the PC when creating a profile.

1. On the **Menu** bar, click **Profiles > New profile**.
2. Select the appropriate phone model and click .

**NOTE:** If a compatible phone is connected to the PC, it is automatically selected by NCT and displayed in the selected list.

3. In the **Configuration profile name** field, type a name for the configuration profile.

**NOTE:** The IMEI number of the phone with current date is displayed in the **Configuration profile name** field. Overwrite that to type a desired name.

4. If required, type any required or desired information about the profile in the **Info** field.
5. To save and close the **Profile configuration** dialog box, click the **Save and Close** icon. To save and continue configuring the profile settings, click the **Save** icon. To close the dialog box without saving the profile, click the **Close** icon.

Refer to **Configuring and Provisioning Profiles** for information to add other settings to the profile.

## 2.4.2. Managing Profiles


### Editing Profiles

To edit a profile and its settings,

1. On the **Menu** bar, click **Profiles > Edit** profile OR click the edit icon.
2. In the **Edit Configuration Profile** dialog box, make the necessary changes to the profile settings.
3. Click the **Save and Close/Save/Close** icons, as appropriate.

### Duplicating Profiles

To duplicate a profile,

1. Select the profile which you intend to duplicate.
2. On the **Menu** bar, click **Profiles > Duplicate profile**.
3. Select the appropriate phone model and click .
4. Perform steps 3 – 5 of the **Creating Profiles** procedure.

## Deleting Profiles



To delete a profile,

1. Select the profile to be deleted.
2. On the Menu bar, click **Profiles > Delete profile**.

**NOTE:** You can also select the profile to be deleted, right-click, and select **Delete profile**.

## Importing Profiles



To import a profile,

1. In the Action icons bar, click the  icon.
2. In the **Import Configuration Profile** dialog box, select the phone from which you want to import the profile and click .

**Result:** The **Import Configuration Profile** box displays the progress of the import process. Depending on the success or failure of the operation, appropriate messages are displayed.

## Exporting Profiles

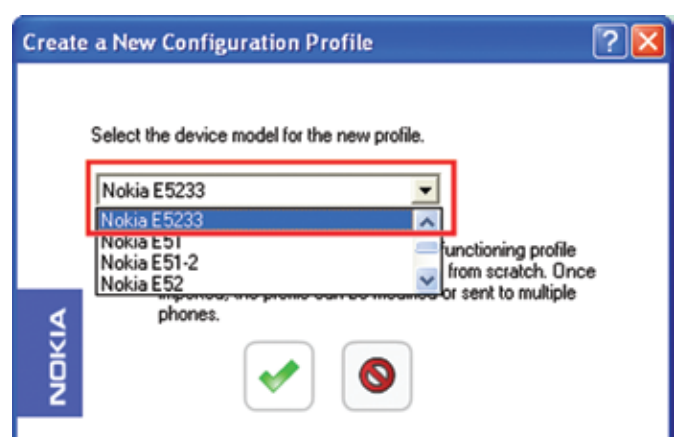
To export a profile,

1. Click the  icon.
2. In the **Send Configuration Profile** dialog box, select the profile that you want to export.
3. Select the phone to which you want to send the profile and click .

**Result:** The **Send Configuration Profile** box displays the progress of the export process. Depending on the success or failure of the operation, appropriate messages are displayed.

## Creating Generic Profiles

Using NCT, you can create generic profiles. Generic profiles can be configured on any phone that is compatible with the tool. To create a generic profile, select **Nokia Generic** in the **Create a New Configuration Profile** dialog box.



## 2.5. Device Management

The device management option in NCT allows you to manage settings and profiles on your phone.



### 2.5.1. Edit Online

The Edit Online option allows you to edit the current profiles and settings on your phone by importing them to the PC. The edited information can be transferred back to the phone.

**NOTE:** NCT does not store the edited settings to a profile in a workspace.

Settings already present in the phone cannot be deleted through NCT. They can only be edited.

Perform the following steps to edit the settings of a phone using the **Edit online** option.

1. On the **Menu** bar, click **Devices > Edit online**.
2. In the **Edit Configuration Profile Online** dialog box, select the phone, the settings of which you want to edit online and click . NCT reads the phone data.
3. Select the required profile setting to be updated and click .

**Result:** The **Send Configuration Profile** box displays the progress of the process. Depending on the success or failure of the operation, appropriate messages are displayed.

### 2.5.2. Mail for Exchange Certificate Enrollment

Mail for Exchange Certificate Enrollment option allows you to easily and quickly configure Mail for Exchange.

Perform the following steps to configure Mail for Exchange using the Mail for Exchange Certificate Enrollment.

1. On the **Menu** bar, click **Devices > Mail for Exchange Certificate Enrollment**.
2. In the **Mail for Exchange Certificate Enrollment** dialog box, provision the following fields:
  - **Exchange server** – Name of the exchange server.
  - **Email address** – Email address of the user.
  - **Use default port** – Select this check box to use the default port. If the default port number is selected, then the system uses the exchange server default port number – 443.
  - **Port number** – To use a different port enter appropriate value in the Port number field.
  - **Domain** – Type the name of the exchange server domain.

- **Authentication** – Select the required authentication type from this drop-down menu.
- **Username** – Username for this Email account.
- **Password** – Type a password for the username.
- **Certificate** – If **Certificate** option is selected as the authentication type, then click the **Load Certificate** button, browse to the appropriate location, select the required certificate file and click **OK**.

**NOTE:** The certificate file types that can be loaded are .pfx, .p12, .cer, .der, and .crt.

3. Click Done.

**Result:** The Mail for Exchange settings are sent to the connected phone.

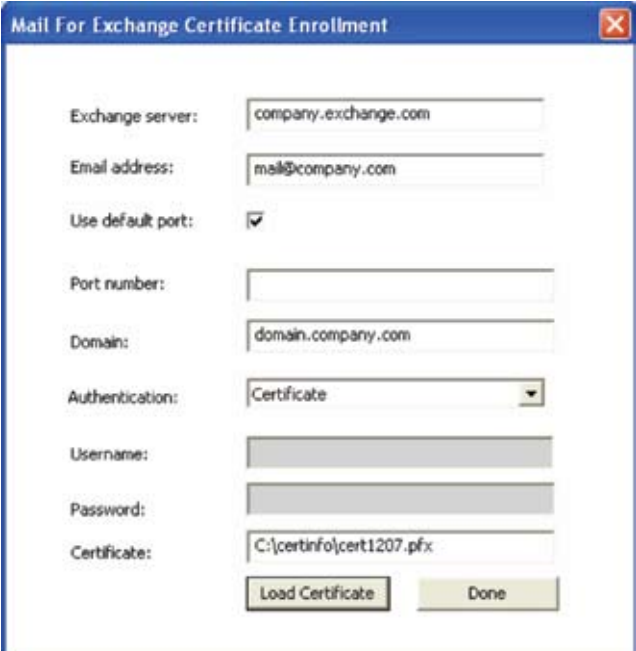


Figure 2: Mail For Exchange Certificate Wizard

### 2.5.3. Configure

The Configure option allows you to send selected profiles to selected phones. This option is similar to the Exporting Profiles option.


Perform the following steps to send selected profiles from PC to a phone.

1. On the **Menu** bar, click **Devices > Configure**.
2. In the **Configure Device** dialog box, select the profile you want to transfer to the phone.

**Result:** The **Send Configuration Profile** box displays the progress. Depending on the success or failure of the operation, appropriate messages are displayed.


## 2.5.4. Edit Device Info

The **Edit Device Info** option allows you to enter a name for the phone and other information which can be used to identify the phone. Perform the following steps to edit the phone information.

1. On the **Menu** bar, click **Devices > Edit Device info**.
2. In the **Edit Device Information** dialog box, make the necessary changes and click .

## 2.5.5. Delete Device

Some information about the phone like the IMEI number, the phone name, and profile name is stored in the **Devices** folder of the workspaces. If you do not want to continue using a particular phone or retain information about the phone to be used or seen by other users, perform the following steps to delete the phone information using the **Delete Device** option.

1. On the **Menu** bar, click **Devices > Delete Device**. The **Confirm Delete Devices** dialog box prompts you to confirm deletion.
2. Click  to confirm deletion.

## 2.5.6. Support for other Devices – Auto Detect and Support Feature

NCT facilitates auto detection and generation of support files for phones other than the ones listed in the supported phones section.

To enable support for such phones:

1. Start NCT and while tool is running, connect the required phone through the USB cable.

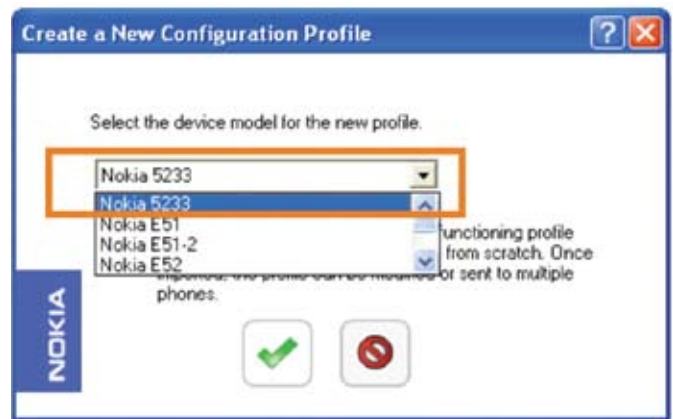


2. If the application is capable of supporting the connected phone, it displays a message to that effect and processes the phone for support.

A new device connection has been detected, would you like NCT to configure support for this device? The application may need to be re-started after the configuration.

3. The application may restart to complete the process.
4. The phone support is added permanently to your edition of NCT and you can see the phone added in the supported phones list.

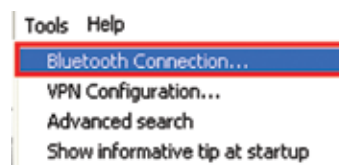
For example, support can be added for Nokia 5233.



**NOTE:** Availability of features and other settings for unlisted phones are not pre-tested. Therefore, there is no liability on NCT for the same.


## 2.5.7. Connecting Phone using Bluetooth®

Before you can use Bluetooth® to transfer settings to the phone, a one-time pairing of the phone may be required – to do this please use the menu item **Tools > Bluetooth Connection**



The application will search and list all Bluetooth® enabled phones, select the phone you wish to pair and complete the process by providing the same pass code on application and phone prompt.



Once the pairing is successful the  image is displayed to indicate the connection type.

## 3. Configuring and Provisioning Profiles

### 3.1. Access Points Configuration




Access points are required to connect to the Internet through your phone. Access Points (APs) are specially configured nodes on wireless local area networks (WLANs). The following connection types can be configured using NCT:

- Packet Data
- Wireless LAN

**IMPORTANT:** You have to ask your service provider for the relevant and appropriate setting information.

#### 3.1.1. Configuring Packet Data Settings

A packet data connection is a data connection over the mobile network. Perform the following steps to add a packet data access point group to a profile.

1. Select the profile for which you intend to add a packet data access point and click .
2. In the left pane of the **Edit Configuration Profile** dialog box, click the **Access points** folder.
3. In the **Access points** section, click .
4. In the **Choose Group Type** dialog box, select **Packet data** from the drop-down and click .
5. Provision the following fields for the group:
  - **Connection name** – Type a descriptive name for the packet data group.
  - **Access point name** – Type a name for the access point. This information is provided by the service provider.
  - **Username** – Enter a user name.
  - **Password** – Enter a password.

If you define a username and password, then you will need them while connecting to the internet through your phone. These are not mandatory fields. However, some service providers may insist on having a username and password. Depending on the service provider's settings, both or at least the password will be case sensitive.

6. Click the **IP configuration** folder on the left pane.
7. Provision the following field for IP configuration:
  - **Network type** – Select the network type: **IPv4** or **IPv6**.

**NOTE:** If you select **IPv4**, then only the **Auto retrieve IP** and **Auto retrieve DNS** check boxes are enabled. If you select the **IPv6**, then only the **DNS Address** field is enabled.

- **Auto retrieve IP** – Select the check box to automatically obtain the IP address from the **Dynamic Host Configuration Protocol (DHCP)** server or Wi-Fi router. This setting is sometimes also called dynamic IP address.
  - **Phone IP address** – If you do not select the **Auto retrieve IP** check box, this field is enabled. Enter the IP address of the phone.
  - **Auto retrieve DNS** – Select the check box to automatically obtain Domain Name Server (DNS) settings.
  - **Primary DNS address** and **Secondary DNS address** – If you do not select the Auto retrieve DNS check box, these fields are enabled. Enter a primary and secondary DNS address in the respective fields.
  - **DNS Address** – Select one of the following options:
    - **Automatic** – to automatically retrieve IPv6 DNS settings.
    - **Well known** – to use standard addresses.
    - **User defined** – to use user defined settings.
  - **IPv6 Primary DNS address** and **IPv6 Secondary DNS address** – If you have selected the **User defined** option for DNS address, then enter appropriate IPv6 Primary and Secondary DNS addresses.
8. Click the **Proxy** folder on the left pane.




**NOTE:** Continue to configure the settings in the Proxy folder only if you intend to use **proxy** settings.

- **Send proxy settings** – Select this check box to send proxy settings to the phone.
- **Proxy name** – Type an appropriate name for the proxy server.
- **Logical proxy ID** – Type a logical proxy ID.
- **Proxy server address** – Type the IP address or domain name of the proxy server. This is a mandatory field for the proxy settings.
- **Proxy port number** – Type the port number associated with the proxy server.
- **Addresses that are not using proxy** – Type the IP address or domain name of sites that are not using the proxy setting.
- **Network AP connected to proxy** – Type the name of the network AP which is connected to the proxy server.
- **Homepage** – Type the IP address or domain name of the homepage.

- **Proxy user ID** – Type a user name for the proxy setting.
  - **Proxy user password** – Type a password for the proxy setting user name.
9. Click the **Save and Close/Save/Close** icons, as appropriate.

### 3.1.2. Configuring WLAN Settings

Mobile Wireless LAN (WLAN) systems provide users with access to real-time information anywhere in their organisation. This mobility enables productivity and service opportunities that are not possible with a wired network. Perform the following steps to add a WLAN access point group to a profile.

1. Select the profile for which you intend to add a packet data access point and click .
2. In the left pane of the **Edit Configuration Profile** dialog box, click the **Access points** folder.
3. In the **Access points** section, click .
4. In the **Choose Group Type** dialog box, select **Wireless LAN** from the drop-down and click .
5. Provision the following fields for the group:

- **Connection name** – Type a descriptive name for the WLAN group.
- **WLAN network mode** – Select one of the following network modes:
  - **Infrastructure** – Infrastructure mode joins a wireless network to a wired Ethernet network. It also supports central connection points for WLAN clients.
  - **Ad hoc** – Ad-hoc mode facilitates phones within range to discover and communicate with each other in a peer-to-peer fashion without involving a central access point, such as a router.
- **WLAN network name** – Enter the WLAN network name. It is also called the Service Set Identifier (SSID). This name is used to identify a particular WLAN. It is provided by the system administrator of the network that you are connecting to. In the Ad-hoc mode, the users name the WLAN. SSIDs are case sensitive alphanumeric text strings with a maximum length of 32 characters.
- **WLAN primary network name** – Type the primary network name.
- **WLAN security mode** – The security mode depends on the configuration of your router. Select one of the following security modes:

- **Open network** – No encryption is used in the open network mode.
- **WEP** – This security mode is supported for compatibility with Wired Equivalent Privacy (WEP) networks. Pre-configured static WEP keys are required for this mode. The WEP mode provides a lower level of security than the Wi-Fi Protected Access (WPA) mode. If you use the WEP mode, you should change the key regularly.
- **802.1x** – This security mode is provided to support the legacy Dynamic WEP system, and also to support networks that are migrating from Dynamic WEP to Wi-Fi Protected Access (WPA/WPA2). In this mode, a Nokia phone is able to join both dynamic WEP and WPA networks.
- **WPA/WPA2** – The Wi-Fi Protected Access (WPA/WPA2) security mode provides the highest level of security among the WLAN security modes.
- **WPA2 only** – WPA2 has replaced WPA. WPA2 provides more security than WPA.
- **WPA/WPA2 mode** – If you selected 802.1x, WPA/WPA2, or WPA2 only options for network security mode, then you have to select one of the following options:
  - **EAP** – Select EAP if you want to use the Extensible Authentication Protocol (EAP) module. The advantage of this module is that you need not configure the key on individual phones.
  - **Pre-shared key** – In PSK method, keys are automatically changed and authenticated between phones after a specified time, or after a specified number of packets are transmitted.
- **Pre-shared key** – If you selected the Pre-shared key option, type the password (also called a master key) in the field. The format of key depends on the network which uses it. It can be alphanumeric or a paraphrase.
- **Network status** – Select one of the following options depending on the network type you are connecting to:
  - **Public** – Select public if the network is a public network.
  - **Hidden** – Select hidden if the network is hidden.

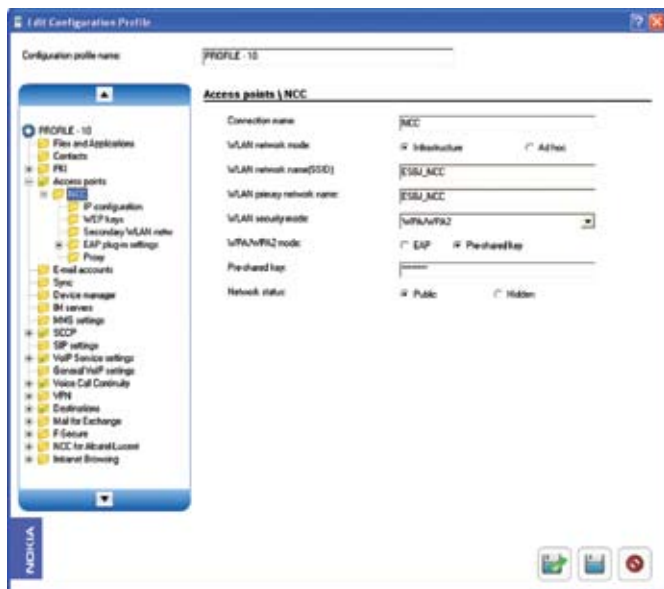


Figure 3: Access Point settings editor for Nokia Call Connect

- Click the **IP configuration folder** under the newly created WLAN AP and provision the following fields. These fields are the same as the fields in the **IP configuration** section of packet data group configuration. Refer to **Step 7** of the **Configuring Packet Data** settings procedure for the description of these fields.

- **Auto retrieve IP**
- **Auto retrieve DNS**
- **Primary name server (same as the Primary DNS address field)**
- **Secondary name server (same as the Secondary DNS address field)**
- **DNS address**
- **IPv6 Primary name server**
- **IPv6 Secondary name server**

If you have not selected the **Auto retrieve IP** option, then provision the following fields:

- **Phone IP address**
- **Subnet mask**
- **Default gateway**

- If you have selected WEP security mode, then click the WEP keys folder in the newly created WLAN folder tree and provision the following fields:

- **Authentication type** – Depending on the type of authentication, select **Open** or **Shared**.
- **WEP key in use** – Select the WEP key that you will be using between #1 - #4.

**NOTE:** Depending on the number of WEP keys

you want to configure, configure the relevant fields for keys from #1 - #4.

- **WEP key encryption** – Select the desired WEP encryption key length. Supported options are 64 and 128 bits. More bits in the key means a higher level of security.
- **WEP key format** – Select whether you want to enter the WEP key data in Hexadecimal format or in text format (ASCII).

**NOTE:** The WEP encryption method encrypts data before it is transmitted. Access to the network is denied to users who do not have the required WEP keys. If your phone receives a data packet that is not encrypted with the WEP key when WEP security mode is configured to be used on your phone, the data packet is discarded. In an Ad-hoc network, all phones must use the same WEP key.

- If you want to configure **secondary WLAN** settings, click the Secondary WLAN networks folder and type appropriate values in the **WLAN network name** and **WLAN primary network name** fields.
- If you have selected EAP module for WPA/WPA2 mode, then click the **EAP plug-in settings** folder and define values for the following fields:
  - **Enabled EAP plug-ins** – Select appropriate EAP plug-ins that can be used by the phone. You can change the EAP plug-ins priority by selecting **Raise priority** or **Lower priority**. The plug in options are as follows:
    - **EAP-SIM** – Mechanism for authentication and session key distribution using the Global System for Mobile Communications (GSM) Subscriber Identity Module (SIM).
    - **EAP-AKA** – Mechanism for authentication and session key distribution using the Universal Mobile Telecommunications System (UMTS) Subscriber Identity Module (USIM).
    - **EAP-TLS** – An IETF-standardised authentication method based on the protocol used for secure Web traffic via the Secure Sockets Layer (SSL) protocol. EAP-Transport Layer Security (TLS) is a preferred option if you want mutual authentication.
    - **EAP-FAST** – Flexible Authentication via Secure Tunneling (FAST) is a protocol proposal by Cisco Systems as a replacement for Lightweight Extensible Authentication Protocol (LEAP). It is usable in the same environments as LEAP, however FAST is resistant to dictionary attacks.
    - **EAP-PEAP** – Protected Extensible Authentication Protocol (PEAP) is an extension

of the EAP-TLS mode. EAP-PEAP and EAP-TTLS are preferred options for enterprise users who want the security of TLS, but have legacy authentication methods or token-based authentication methods.

- **EAP-LEAP** – Lightweight Extensible Authentication Protocol (LEAP), also known as Cisco-EAP uses the username/password pair to authenticate both the client and the authentication server.
- **EAP-TTLS** – Tunneled Transport Layer Security (EAP-TTLS).
- **EAP-SIM** and **EAP-AKA** folders – Provision the following fields in the respective folders:
  - **Username** – Specifies the user's identity. If a username is not specified then the EAP method sends an auto generated user identity. The maximum length is 255 characters.
  - **Realm** – Specifies the override realm that is sent.
- **EAP-TLS folder** – Provision the following fields in the folder:
  - **Username** – Specifies the user's identity. If a username is not specified then the EAP method sends an auto generated user identity. The maximum length is 255 characters.
  - **Realm** – Specifies the override realm that is sent.
  - **Check realm of the certificate** – Specifies whether the realm of the server's certificate should be verified.
- **Certificates folder** – Expand the Certificates folder under the EAP-TLS folder, create a certificate with required options and set appropriate values.
 

**NOTE:** Two options, User certificate and CA certificate, are available under the Certificates folder. Certificates must have been added in the PKI-Certificate folder to configure them in the EAP-TLS folder.
- **EAP-FAST folder** – Provision the following fields in this folder:
  - **Username** – Specifies the user's identity. If a username is not specified then the EAP method sends an auto generated user identity. The maximum length is 255 characters.
  - **Realm** – Specifies the override realm that is sent.
  - **Allow Authenticated Provision Mode** – Specifies if EAP-FAST type's authenticated provision mode usage is allowed.
  - **Allow ADHP** – Specifies if EAP-FAST type's

Authenticated Diffie-Hellman Provisioning (ADHP) mode usage is allowed.

- **Certificates folder** – Expand the Certificates folder under the EAP-FAST folder, create a certificate with required options and set appropriate values.
 

**NOTE:** Two options, User certificate and CA certificate, are available under the Certificates folder. To configure certificates in the EAP-FAST folder, you must first add them in the PKI-Certificate folder.
- **EAP-PEAP folder** – Provision the following fields in this folder: Username – Specifies the user's identity. If a username is not specified then the EAP method sends an auto generated user identity. The maximum length is 255 characters.
  - **Realm** – Specifies the override realm that is sent.
  - **Allow PEAPv0** – Defines whether PEAP version 0 is allowed to run.
  - **Allow PEAPv1** – Defines whether PEAP version 1 is allowed to run.
  - **Allow PEAPv2** – Defines whether PEAP version 2 is allowed to run.
  - **Check realm of the certificate** – Defines whether the realm of the server's certificate should be verified.
  - **Authentication session validity time** – Specifies (in minutes) how long the authentication session is valid. During this time EAP-TLS, EAP-TTLS, and EAP-PEAP authentication can do faster session resumes instead of full authentication. If this is omitted or false, full authentication is executed.
- **Certificates folder** – Expand the Certificates folder under the EAP-PEAP folder, create a certificate with required options and set appropriate values.
 

**NOTE:** Two options, User certificate and CA certificate, are available under the Certificates folder. To configure certificates in the EAP-PEAP folder, you must first add them in the PKI-Certificate folder.
- **Cipher suites folder** – Defines a list of cipher suites in use in EAP methods that utilise TLS authentication. The list is in priority order. You can change the cipher suite priority by selecting **Raise priority** or **Lower priority**.
- **EAPs folder** – Click **EAPs > EAP-MSCHAPv2** and provision the following fields:
  - **Username** – Specifies the user's identity. If a username is not specified then the EAP

method sends an auto generated user identity. The maximum length is 255 characters.


- **Password** – Desired password for the username. It is used for user authentication. Maximum length is 255 characters.
10. Click the Proxy folder on the left pane if you intend to use proxy settings.

**NOTE:** The **proxy** settings are the same as the proxy settings in Step 9 of the **Configuring Packet Data settings** procedure.

11. Click the **Save and Close/Save/Close** icons, as appropriate.

### 3.1.3. Configuring Global WLAN Settings

Perform the following steps to add Global WLAN configuration settings to a profile.

1. Select the profile for which you intend to add Global WLAN configuration and click .
2. In the **Edit Configuration Profile** dialog box, click the Global WLAN folder in the left pane.
3. In the **Global WLAN** section, provision the following fields:

- **Send Global WLAN Settings** – Select the check box to send Global WLAN settings to your phone.
- **Internet Connectivity Test** – Select one of the following options:
  - **Run Automatically** – Specifies automatic Internet connectivity test.
  - **Ask Permission** – Specifies permission based Internet connectivity test.
  - **Never Run** – Specifies never to run the Internet connectivity test.
- **Use Default Settings** – Select the check box to use default settings on your phone.
- **RTS Threshold** – Type the minimal packet size where CTS/RTS handshake has been used.
- **TX Power Level** – Select the transmission power level from 4, 10, or 100mW.
- **Power Saving** – Select the check box to make power saving methods on your phone.
- **Background Scan Interval** – Type the background scan interval in seconds, which determines WLAN icon on your phone.
- **Scan Rate** – Select the scan rate for probing request from the following options:
  - **ENoRate**

- **E1Mbps**
- **E2Mbps**
- **E5\_5Mbps**
- **E11Mbps**
- **E22Mbps**
- **EBASIC\_1Mbps**
- **EBASIC\_2Mbps**
- **EBASIC\_5\_5Mbps**
- **EBASIC\_11Mbps**
- **EBASIC\_22Mbps**
- **RCPITrigger** – Type a default value for RCPI trigger.
- **RCPIDifference** – Type the difference in current and best connections.
- **MaxTriesToFindNw** – Type the number of times the network is scanned before giving up.
- **DelayBetweenFindNw** – Type the delay in time, in microseconds, while trying to find a network.
- **AllowRadiosMeasurements** – Select the check box to allow CCX radio measurements on your phone.
- **QosNullFrameInterval** – Type the interval to send a QoS NULL data frame.
- **MTU** – Type the maximum transfer unit for WLAN.

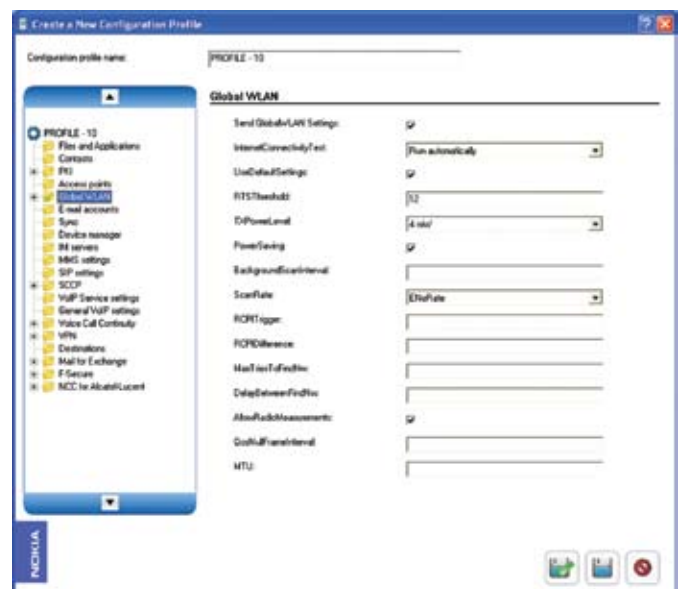


Figure 4: Global Wireless LAN settings editor

4. Click the **WLAN Advanced Settings** folder and type appropriate information in the following fields:
  - **MinActiveChannelTime** – Minimum time the channel is active.

- **MaxActiveChannelTime** – Maximum time the channel is active.
  - **MaxTxMSDULifeTime** – Life time for maximum transmission of MSDU.
  - **ScanExpiration Timer** – Timer for the scan expiry.
  - **UnloadDriver Timer** – The timer to unload the driver.
  - **Roam Timer** – The timer for roaming.
  - **ConnRegain Timer** – The timer to regain the connection.
  - **MinPassiveChannelTime** – The minimum time the channel is passive.
  - **MaxPassiveChannelTime** – The maximum time the channel is passive.
  - **QosNullFrameTimeout** – The timeout for the Qos Null Frame.
  - **LongRetryLimit** – The limit for long retry.
  - **ShortRetryLimit** – The limit for short retry.
  - **MaxApFailureCount** – The maximum failure count of the application.
  - **LongBeaconFindCount** – The find count for the long beacon.
5. Click the **Save and Close/Save/Close** icons, as appropriate.

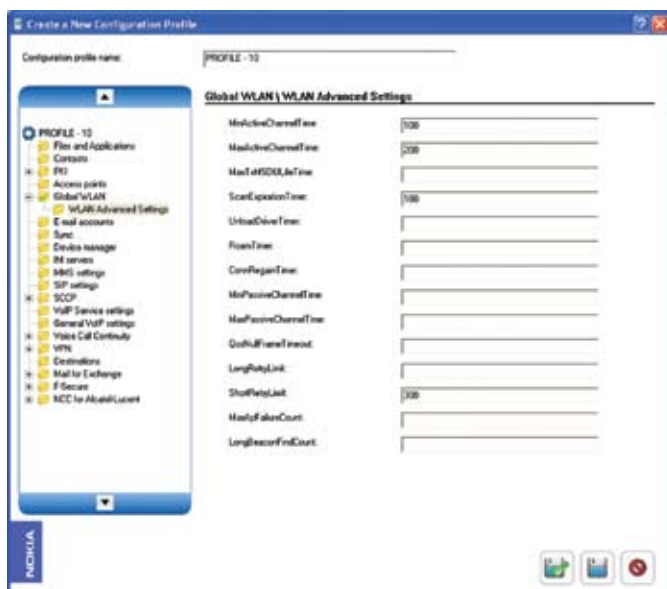





Figure 5: Advanced Global Wireless LAN settings editor

### 3.2. VPN Configuration

Perform the following steps to add VPN configuration settings to a profile.

1. Select the profile for which you intend to add VPN configuration and click .
2. In the Edit Configuration Profile dialog box, click the VPN folder in the left pane.
3. In the **VPN** section, provision the following fields:
  - **Client version** – Type the version of the Nokia Mobile VPN Client software present in the phone.
  - **Event log** – Provides event log activities related to VPN connection.
  - **Policies folder** – Click the Policies folder and click  in the VPN section. Policies can be configured either by loading from a file or by specifying the details in the VPN section.
    - **Loading from file** – Click the Load from file button to load a policy file. Supported file types are .pol and .pin.
    - **To manually load VPN settings, provision the following fields:**
      - \* **Name** – Enter a descriptive name for the VPN policy.
      - \* **Version** – The version of the policy. Note that this is different from the policy format version that is specified inside the policy content.
      - \* **Issuer** – Enter the name of the VPN policy issuer.
      - \* **Description** – Description of the policy.
      - \* **Contact** – Specify contact information for the policy.
      - \* **Content** – The actual VPN policy content. Content can include references and policies.
4. Click the **Access points** folder and click .
5. In the **VPN\Access points** section, provision the following fields:
  - **Name** – Enter a descriptive name for the VPN access point.
  - **VPN policy** – Select the VPN policy to be used with this access point.
  - **Default access point** – Select default internet access point to be used with this VPN access point. The default access point is used to connect to the internet through which the VPN connection is tunneled.
6. Click the **Save and Close/Save/Close** icons, as appropriate.

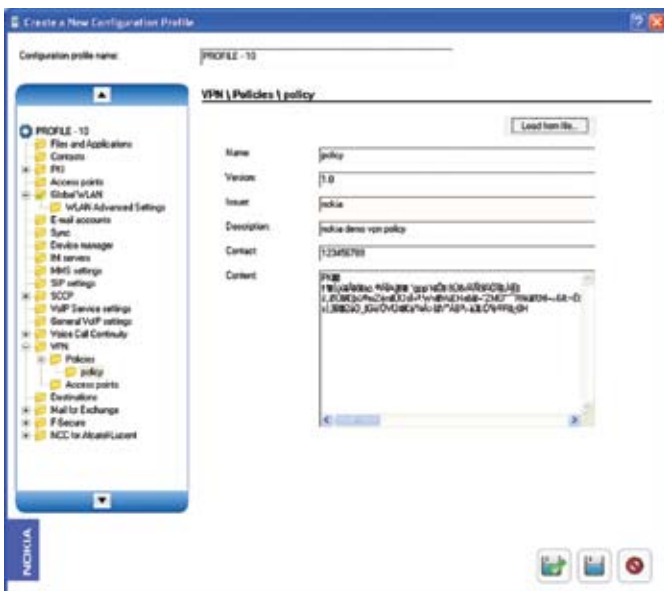
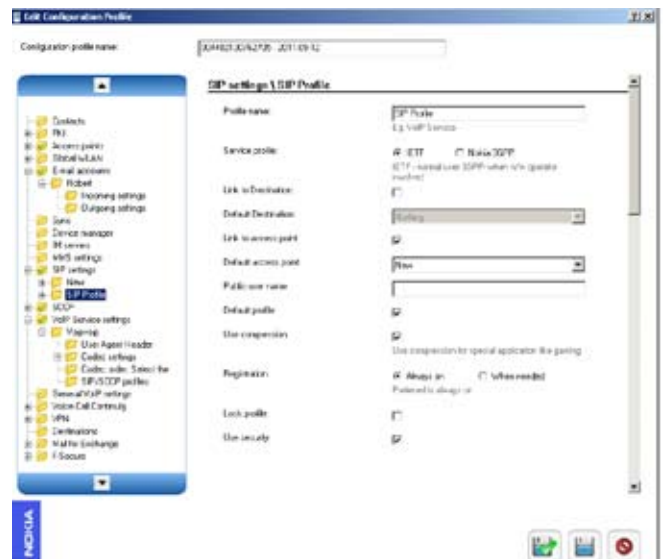


Figure 6: Mobile VPN Policy loader

- **Allow anonymous calls** – Defines whether anonymous callers are allowed to call this phone.
- **Hysteresis** – Defines when to make a handover to a new access point.
- **Handover attenuation** – Defines the strength of the signal that is required for making a handover to a new access point.
- **Preferred mode** – Allows the user to choose preferred telephony mode.
- **Do not disturb** – Defines whether the Do Not



Disturb feature is enabled or disabled.

- **PS call waiting** – Call waiting can be disabled, in which case the called party is not informed about the incoming call and the caller receives a busy tone or message. If waiting is enabled the called party receives a caller waiting indication and the caller receives waiting indication and/or the phone continues ringing.
- **VoIP Profile ID** – Select the required VoIP profile ID.

4. Click the **Save and Close/Save/Close** icons, as appropriate.

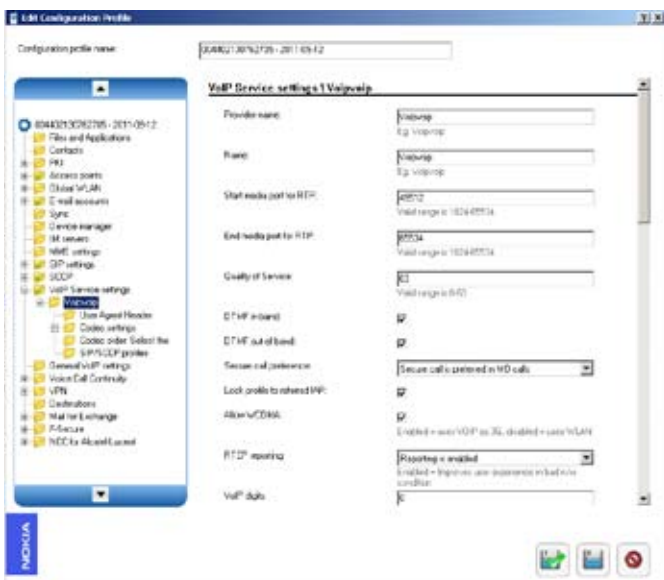
### 3.4. SIP Configuration

Session Initiation Protocol (SIP) is a signaling protocol for internet telephony and you need to define a SIP profile before configuring internet call settings.


Perform the following steps to provision SIP settings for a profile:

1. Select the profile for which you intend to add SIP settings and click .
2. In the **Edit Configuration Profile** dialog box, click

## 3.3. VoIP Configuration



Perform the following steps to configure VoIP settings for a profile.

1. Select the profile for which you intend to add VoIP configuration and click .
2. In the **Edit Configuration Profile** dialog box, click the **General VoIP settings** folder in the left pane.
3. In the **General VoIP settings** section provision the following fields:
  - **Send settings** – Select this check box to send the settings to the phone.
  - **CLIR/CLIP** – Select CLIP or CLIR. With CLIP enabled, the caller ID is sent, but with CLIR the caller ID is not sent.

the **SIP settings** folder in the left pane.

3. In the **SIP settings** section, provision the following fields:

- **Profile name** – Type a name for the SIP profile.
- **Service profile** – Select one of the following options to specify the SIP profile type. The default is IETF.
  - **IETF** – Select IETF if you want to use private WLAN.
  - **Nokia 3GPP** – Select Nokia 3GPP if you want to use a 3G service provider access point.
- **Link to Destination** – Select the check box to send the settings to the phone.
- **Default Destination** – If you select the Link to Destination option, all the destinations created for this profile are listed in the Default Destination drop-down list. Select the required destination.
- **Link to access point** – Select the check box to send the settings to the phone.
- **Default access point** – If you select the Link to access point option, all the access points created for this profile are listed in the Default access point drop-down list. Select the required access point.
- **Public user name** – Type the user name received from your service provider. The name must be given in the username@domain format.
 

**NOTE:** Domain name must be included in Public user name.
- **Default profile** – If you want this SIP profile to be used as a default profile, select this check box.
- **Use compression** – Select Yes or No as specified by your service provider. The default is No.
- **Registration** – Select one of the following registration types:
  - **When needed** – Select this option for manual registration.
  - **Always on** – Select this option for automatic registration.
- **Lock profile** – Select this check box to disable editing of this profile from the phone.
- **Use security** – Select this check box to enhance the security of the SIP profile.

4. Click the Proxy server folder under the newly created SIP profile and provision the

following fields.

- **Proxy server address** – Type the IP address or domain name for the proxy server.
- **Realm** – Type the proxy server realm.
- **Username** – Type a username.
- **Password** – Type a password for the username.
- **Transport type** – Select from one of the following options for sending data over the network.
  - **Auto** – The available or supported protocol is used.
  - **UDP** – User Datagram Protocol is used.
  - **TCP** – Transmission Control Protocol is used.
- **Port** – Type the port number of the proxy server.
 

**NOTE:** The port number relates to the protocol.
- **Allow loose routing** – Select Yes or No as specified by your service provider. The default is Yes.

5. Click the Registrar server and provision the following fields:

- **Registrar server address** – Type the IP address or domain name for the registrar server.
- **Realm** – Type the registrar server realm.
- **User name** – This field is enabled only if you have selected IETF for the SIP profile type.
- **Private user identity** – This field is enabled only if you have selected Nokia 3GPP for the SIP profile type.
- **Password** – Type a password for the username or the private user identity.
- **Transport type** – Select from one of the following options for sending data over the network.
  - **Auto** – The available or supported protocol is used.
  - **UDP** – User Datagram Protocol is used.
  - **TCP** – Transmission Control Protocol is used.
- **Port** – Type the port number of the registrar server.


6. Click the **Save and Close/Save/Close** icons, as appropriate.

### 3.5. VoIP Service Settings


Perform the following steps to provision VoIP Service Settings for a profile:

1. Select the profile for which you intend to add VoIP

Service Settings and click .

2. In the left pane of the **Edit Configuration Profile** dialog box, click the **VoIP Service Settings** folder.
3. In the **VoIP Service Settings** section, click .
4. In the **VoIP Service Settings/New** section provision the following fields:
  - **Provider name** – Type the name of your VoIP service provider.
  - **Name** – Type a name for the VoIP profile.
  - **Start media port for RTP** – The media port values for this field are auto-generated. To change the values, type the appropriate media port number for Real-Time Transport Protocol (RTP).
  - **End media port for RTP** – The media port values for this field are auto-generated. To change the values, type the appropriate media port number for RTP.
  - **Quality of Service** – The value in this field allows your phone calls to be given higher priority in the network. Type an appropriate value. It must be between 0 and 63.
  - **DTMF in-band** – Define whether to generate DTMF (Dual Tone Multi-Frequency) digits in-band. If the in-band option is selected, DTMF tones are sent as compressed audio and they are part of the actual VoIP call audio stream.
  - **DTMF out-of-band** – Define whether to generate DTMF (Dial Tone Multi-Frequency) digits out-of-band. If the out-band option is selected, DTMF tones are sent as RTP payload. Both the in-band and out-band options can be enabled.
  - **Secure call preference** – Select which of the following options you want to use:
    - **Non-secure call is preferred**
    - **Secure call is preferred in MO calls**
    - **Secure call is mandatory in MO calls**
  - **Lock profile to referred IAP** – Select this check box if you want to use the VoIP profile from a pre-defined IAP only. If this setting is enabled, the Internet telephone application shows only the pre-defined IAPs of the VoIP service.
  - **Allow WCDMA** – If this setting is enabled, the Internet telephone application shows the available Wideband Code Division Multiple Access (WCDMA) access points.
  - **RTCP reporting** – Select from one of the



following options to enable or disable Real-time Transport Control Protocol (RTCP) reporting. RTCP gathers statistics about media connection. It is used to increase the Quality of Service.

- **RTCP reporting is enabled**
  - **RTCP reporting is disabled**
  - **VoIP digits** – Specify appropriate VoIP caller ID characters for caller identification. The value must be 0 or between 3 and 20. If the value is 0, all digits are meaningful.
  - **Ignore URI domain** – Select from one of the following options to ignore the domain part of an address (URI) for Internet calls.
    - **Never**
    - **Only if E.164 numbers are used**
    - **Always**
  - 5. In the left pane, under the newly created internet telephone settings folder, click the User Agent Header folder and configure appropriately. User Agent Header (UAH) settings are used to identify the user and phone (acting as a client).
    - **Terminal type** – Select whether the terminal type is written or not written to the UAH.
      - **Not written to UAH**
      - **Written to UAH**
    - **WLAN MAC address** – Select whether the MAC address is written or not written to the UAH.
      - **Not written to UAH**
      - **Written to UAH**
    - **UAH free string** – Type the text to be written in the SIP VoIP UAH.
  - 6. Click the **Codec settings** folder and click .
- Folders are created in a predefined order for the following speech codecs:
- **AMR-WB** – Adaptive Multi-Rate – Wideband Speech Codec (AMR-WB) is a audio-data compression scheme used in GSM and UMTS technologies. It is a sub-type of AMR.
  - **AMR** – Adaptive Multi-Rate is also used in GSM and UMTS technologies.
  - **PCMU**
  - **PCMA**
  - **iLBC**
  - **G729** – Is mostly used in VoIP applications where bandwidth must be conserved.
  - **CN**

**NOTE:** A different order can also be defined, or some of the codecs can be entirely disabled, but this is not recommended due to possible problem scenarios.

7. Click the **AMR-WB** folder and provision the following fields:
  - Jitter buffer size – A default value is populated in this field. Change the value if required. A jitter buffer is used to store arriving packets in order to minimise delay variations. Unit is Milliseconds.
  - Use octet-align – Select whether octet-align is used. If not selected, bandwidth-efficient operation is employed.
  - Packet media length – This field specifies the length of time in milliseconds represented by the media in a packet.
  - Maximum packet time – This field specifies the maximum amount of media which can be encapsulated in each packet, expressed as time in milliseconds.
  - Enable VAD – Select this check box to enable Voice Activity Detection (VAD).
  - Mode change period – This field specifies the number of frame-blocks – that is, the frame-block period at which codec mode changes are allowed for the sender.
  - Mode-change-neighbour – Select this check box to allow mode changes to be made only with neighboring modes in the active codec mode set. Otherwise changes between any two modes in the active codec mode set are allowed.
  - Max-red – Select the maximum duration (in milliseconds) that elapses between the primary (first) transmission of a frame and any redundant transmission that the sender will use. You can also select not to use redundancy.
8. Click the Mode set folder under the AMR-WB folder and set appropriate bit rates.
 


NOTE: Settings for other codecs are similar to the AMR-WB settings. Click appropriate codec folders and configure accordingly.

The G729 codec has one extra field to enable AnnexB. Select the check box to enable enhancement according to annexure-b of IETF RFC 3555.
9. Click the codec order folder and click .
10. Click the codec order folder and set appropriate values.
11. Click the SIP/SCCP profiles folder and click .
12. Select the Enable SIP Profile in VoIP check box.

13. Select the preferred SIP profile from the drop-down list.
14. Click the Save and Close/Save/Close icons, as appropriate.

### 3.6. Email Accounts Configuration

Mobile email configuration enables you to get your work and home email on your phone. The main advantage of mobile email configuration is that it helps you to quickly respond to urgent issues. You can configure multiple email accounts on your phone. Perform the following steps:

1. Select the profile for which you intend to add email settings and click .
2. In the left pane of the **Edit Configuration Profile** dialog box, click the **Email account settings** folder.
3. In the **Choose Group Type** dialog box, select the email protocol that your remote mailbox service provider recommends:
  - **IMAP4** – is a version of the Internet Message Access Protocol (IMAP). It is a standard protocol for accessing email on a remote server. With IMAP4, you can manage your mails by searching, sorting, creating, editing, and deleting message folders.
  - **POP3** – is a version of the Post Office Protocol (POP). It is a standard protocol for accessing email on a remote server. With POP3, you can check your remote mailbox and download emails.
4. If you have selected IMAP4, provision the following fields:
  - **Mailbox name** – Type a descriptive name for the mailbox settings.
  - **My name** – Type your name
  - **My email address** – Type the email address provided by your service provider. Replies to your messages are sent to this address. The address must be a valid email address.
  - **IMAP4 folder path** – Type the IMAP4 folder path.
  - **SMTP authentication** – Select this check box to enable SMTP authentication.

**NOTE:** Fields for configuring POP3 protocol are similar to IMAP4 protocol fields. The only difference is the APOP secure login check box. Select the check box to use the Authenticated Post Office Protocol (APOP) to encrypt your passwords when they are transmitted.
5. Click the **Incoming settings** folder under the newly created IMAP4/POP3 account and provision the following fields:

- **IMAP4 user name** or **POP3 user name** – Enter the user name to the incoming email server.
- **IMAP4 password** or **POP3 password** – Enter the password to the incoming email server. If you leave the password field blank, you are prompted for a password when you try to connect to your remote mailbox.
- **Link to access point** – Select the check box to Link to access point setting to the email server.
- **IMAP4 access point in use** or **POP3 access point in use** – From the drop-down list, select the internet access point that you want to use. For more information on configuring access points, refer to **Access Points configuration**.
- **IMAP4 mail server** or **POP3 mail server** – Type the IP address or host name of the server that receives your email.
- **IMAP4 port** or **POP3 port** – Type the server port address. The server port is a logical port number of a server. Common values for SMTP servers begin with 25 and common values for web servers begin with 80.
- **Security (ports)** – To use a secure connection and encryption, select one of the following options:
  - **StartTLS** – Selecting this option upgrades a plain text connection to an encrypted connection instead of using a separate port for encrypted communication.
  - **SSL/TLS** – Either Secure Socket Layer (SSL) or Transport Layer Security (TLS) options are used for encryption.

6. Click the **Outgoing** settings folder under the newly created IMAP4/POP3 account and provision the following fields:
  - **SMTP user name** – Type the user name for SMTP authentication.
  - **SMTP password** – Type a password for SMTP authentication.
  - **Link to access point** – Select this check box to send the access point settings to the phone.
  - **SMTP access point in use** – If you selected the Link to access point check box, then the access points configured for your profile are populated in this drop-down menu. Select the required access point.
  - **SMTP mail server** – Type the hostname or IP address of the server which sends your emails.
  - **SMTP server port** – Type the server port address.
  - **Security (ports)** – To use a secure connection and encryption, select one of the following options:
    - **StartTLS** – Selecting this option upgrades a plain text connection to an encrypted connection instead of using a separate port for encrypted communication.
    - **SSL/TLS** – Either Secure Socket Layer (SSL) or Transport Layer Security (TLS) options are used for encryption.

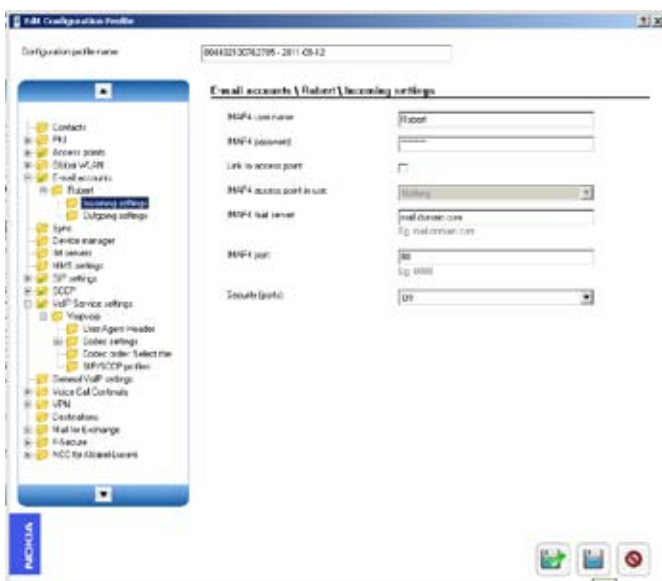


Figure 7: Incoming email account settings editor

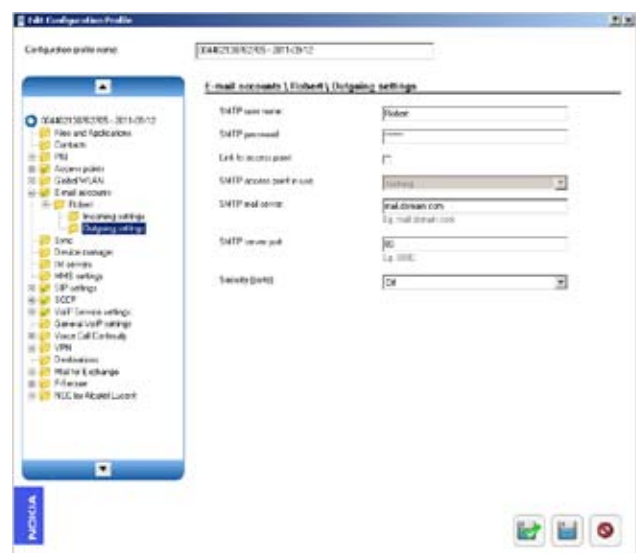



Figure 8: Outgoing email account settings editor

7. Click the **Save and Close/Save/Close** icons, as appropriate.

### 3.7. Mail for Exchange configuration

Mail for Exchange configuration synchronises the organisation's Microsoft Exchange accounts or Lotus Notes with your phone mail box enabling you to use respective inboxes, calendar, and contacts on your Nokia phone.

Perform the following steps to configure Mail for Exchange settings for a profile:

1. Select the profile for which you intend to add Mail for Exchange settings and click .
2. In the left pane of the **Edit Configuration Profile** dialog box, click the Mail for Exchange folder.
3. In the **Mail for Exchange** section, provision the following fields:
  - **Send settings** – Select this option to send settings to the phone.
  - **Exchange server** – Type the exchange server name.
  - **Secure connection** – Select this check box to use an SSL connection to the server.
  - **Link to Destination** – Select the check box to send the settings to the phone.
  - **Default Destination** – If you select the Link to Destination option, all the destinations created for this profile are listed in the Default Destination drop-down list. Select the required destination.
  - **Link to access point setting** – Select this option to send access point settings to the phone.
  - **Access point** – If you have selected the Link to access point setting check box, all the access points configured for the profile are listed in the drop-down. Select the required access point. Your mobile will use this access point to connect to the Exchange server.
  - **Sync while roaming** – If you want your phone to synchronise data while roaming, select from one of the following options:
    - **Yes, always** – This is the default setting. Synchronisation occurs according to the sync schedule even while roaming.
    - **Yes, on peak only** – Synchronisation occurs only during the peak hours specified in the profile.
    - **No** – Disables synchronisation while roaming
  - **Use default port** – Select this check box to use the default port.
  - **Port number** – If you have selected the **Use default port** option, the system populates the default port number – 80. If you want to use a different port, do not select the User default

port option and enter appropriate value in the Port number field.

- **Domain** – Type the exchange server domain name.
- **User Settings**
  - **Authentication** – Select one of the following options:
    - \* **Credentials** – If this option is selected, then a username and password has to be provided for authentication.
    - \* **Certificate** – If this option is selected, an appropriate authenticating certificate must be loaded on NCT. When this option is selected, click the **Load Certificate** button, browse to the appropriate location, select the required certificate file and click **OK**.

NOTE: The selected certificate is saved in the phone store under the Certificates section. The certificate file types that can be loaded are .pfx, .p12, .cer, .der, and .crt.

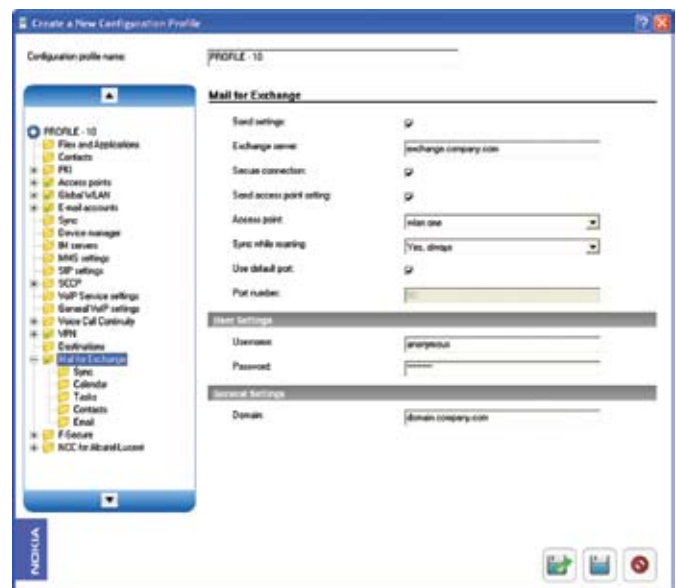


Figure 9: Mail for Exchange configuration settings editor

4. Click the **Sync** folder and provision the following fields:
  - **In case of conflict** – If a file has been modified on both the phone and the server, you can select from one of the following options to specify the information/file that will be used:
    - **Server wins**
    - **Phone wins**
  - **Peak sync schedule** – Select synchronisation intervals during peak intervals from the available options.

- **Manual** – synchronisation occurs only when you select to synchronise.
- **Always on** – Synchronisation is always on.
- **Every 15 minutes**
- **Every 30 minutes**
- **Every 1 hour**
- **Every 4 hours**
- **Every 12 hours**
- **Off-peak sync schedule** – Select one of the following options:
  - **Manual** – synchronisation occurs only when you select to synchronise.
  - **Always on** – Synchronisation is always on.
  - **Every 15 minutes**
  - **Every 30 minutes**
  - **Every 1 hour**
  - **Every 4 hours**
  - **Every 12 hours**
- **Peak start time** – Start time for peak hours in a day.
- **Peak end time** – End time for peak hours in a day.
- **Peak days** – Specify the days in a week which have peak hours.
- **Heartbeat interval** – Specify the ping interval posted to the server for Always-on jobs. Default is 5.

5. To synchronise the calendar, click the **Calendar** folder and provision the following fields:
  - **Synchronise calendar** – Select the check box if you want to synchronise the calendar on your phone and Exchange server.
  - **Sync calendar back** – Specifies how far back in time calendar entries are synchronised.

**NOTE:** All the future calendar entries are synchronised.

  - **Initial sync** – Specify if you want to retain or delete items on the phone with one of the following options:
    - **Keep items on phone** – All existing calendar entries on your phone are synchronised to the Exchange server and vice-versa.
    - **Delete items on phone** – All existing calendar entries on your phone are deleted before synchronising with the Exchange server.
6. To synchronise the tasks, click the Tasks folder and provision the following fields:
  - **Synchronise tasks** – Select this check box if you want to synchronise tasks.
  - **Sync completed tasks** – Select Yes or No to specify whether you want to synchronise completed tasks or not.
  - **Initial Sync** – Specify if you want to retain or delete items on the phone with one of the following options:
    - **Keep items on phone** – All existing tasks on your phone are synchronised to the Exchange server and vice-versa.
    - **Delete items on phone** – All existing tasks on your phone are deleted before synchronising with the Exchange server.

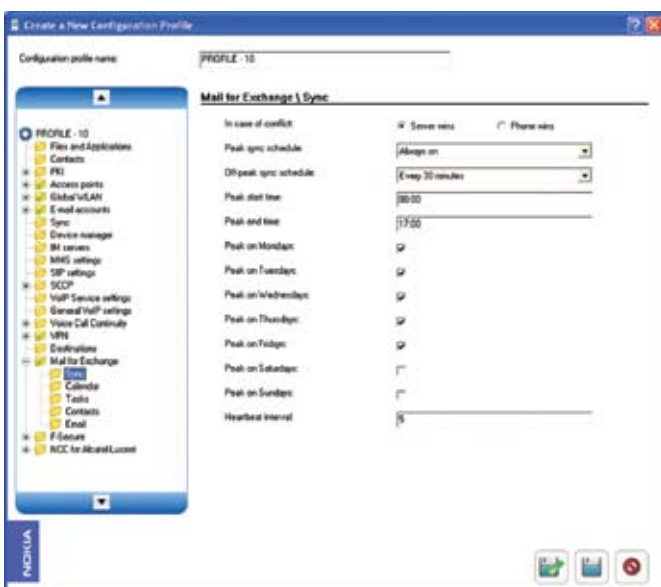


Figure 10: Mail for Exchange Sync settings editor

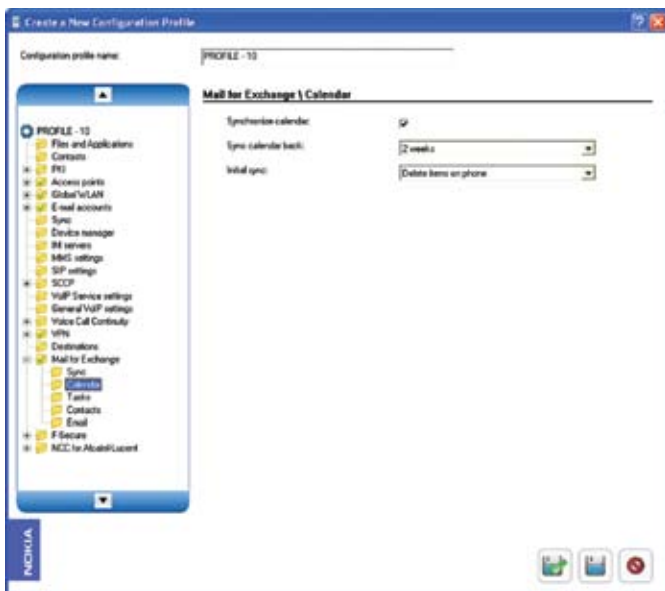


Figure 11: Mail for Exchange Calendar settings editor

- To synchronise contacts, click the **Contacts** folder and provision the following fields:

- **Synchronise contacts** – Select this check box if you want to synchronise contacts.
- **Initial Sync** – Specify if you want to retain or delete items on the phone with one of the following options:
  - **Keep items on phone** – All existing contacts on your phone are synchronised to the Exchange server and vice-versa.
  - **Delete items on phone** – All existing contacts on your phone are deleted before synchronising with the Exchange server.

- To synchronise emails, click the **Email** folder and provision the following fields:

- **Synchronise email** – Select this check box if you want to synchronise emails.
- **Email address** – Type your Microsoft Exchange email address.
- **Show new mail pop-up** – Select this check box if you want a pop-up to notify about a new email.
- **Use signature** – Select this check box if you want to use a signature. The signature will be appended to all mails.
- **Signature** – Type the signature text.
- **When sending mail** – Select from one of the following options to specify the sending of your mail:
  - **Send immediately**
  - **Send at next sync only**

- **Sync messages back** – Select appropriate options to specify which of your email messages should be synchronised. You can synchronise all messages, or synchronise only the most recently received messages.

**NOTE:** Large numbers of email messages affect the phone's performance.

- Click the **Save and Close/Save/Close** icons, as appropriate.

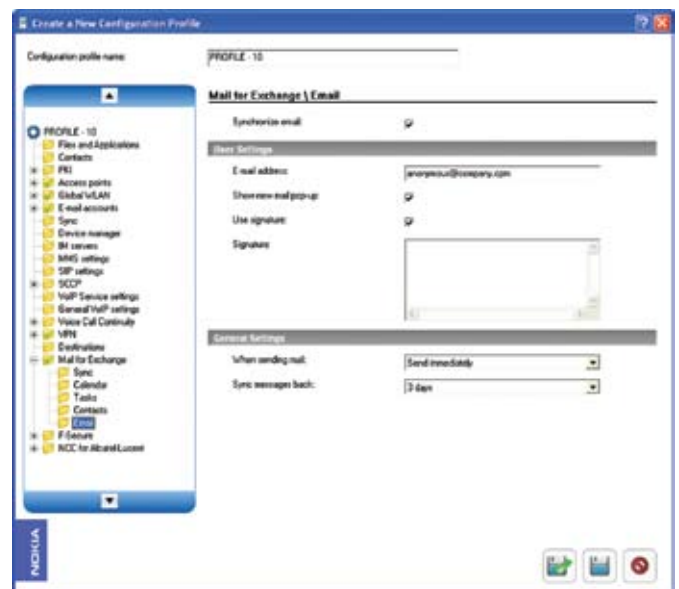






Figure 12: Mail for Exchange Email settings editor

### 3.8. SCCP Configuration

Perform the following steps to configure SCCP settings for the profile. Please, note that Nokia Call Connect for Cisco application needs to be installed to device before configuring it.

- Select the profile for which you intend to add SCCP settings and click .
- In the left pane of the Edit Configuration Profile dialog box, click the SCCP folder.
- Provision the following fields:
  - **Send SCCP settings** – Select this check box to send the SCCP license settings to the phone.
  - **WLAN Mac Address** – is a read only property
  - **PrefixEnabled** – The PrefixEnabled leaf defines if prefix is Enabled/Disabled for PSTN calls.
  - **ForNumbersLonger** – The dialing prefix is applied if phone number is longer than value of this node.
  - **Value** – The Value leaf defines the prefix value for PSTN calls.

- **TwoStageDialingEnabled** – The TwoStageDialingEnabled leaf defines if TwoStageDialing is Enabled/Disabled.
  - **TwoStageDialingNbr** – The TwoStageDialingNbr leaf defines PBX's two-stage dialing phone number.
  - **TwoStageDialingPincode** – The TwoStageDialingPincode leaf defines PBX's two-stage dialing pincode.
4. Click the SCCPAcc folder under the SCCP folder.
  5. Click .
  6. Provision the following fields:
    - **Profile Name** – Type a name for the SCCP profile.
    - **Use automatic registration** – Select this check box to automatically register turn on scanning for the WLAN network.
    - **Use DHCP** – Select this check box to enable the Dynamic Host Configuration Protocol (DHCP) to direct your phone to the Trivial File Transfer Protocol (TFTP) server.
    - **TFTP Server Address** – If you have not selected the Use DHCP check box, type the TFTP server address.
    - **Phone number for call forwarding** – Type the phone number for call forwarding.
    - **Voice mail box number** – Type the number of the voice mail box.
    - **Prefix for international calls** – Type the appropriate international call prefix.
    - **Online service URL** – Type the URL address of the online service server.
    - **Switch to GSM number** – Type the GSM number to which the internet call can be switched over. This is valid only for S60 3.1 devices. For S60 3.2 and newer devices WLAN<->GSM handover is defined in Voice Call Continuity settings.
    - **Link to access point setting** – Select the check box to send access point settings to the phone
    - **Default access point** – If you select the Link to access point setting check box, the access points for the particular profile is populated in this drop-down list. Select the desired access point to be the default access point.
  7. Click the **Save and Close/Save/Close** icons, as appropriate.
1. Select the profile for which you intend to add PKI and Certificate settings and click .
  2. In the left pane of the Edit Configuration Profile dialog box, click the PKI folder.
  3. In the PKI section, provision the following fields:
    - **Send store type** – Select the check box to send the settings to your phone.
    - **Store type** – Select a store type from the following options:
      - **Device key and certificate stores**
      - **User key and certificate stores**
  4. Click the Certificates folder and click .
  5. In the Certificates section, provision the following fields:
    - **Name** – Type the name which can be used to refer to the certificate from the VPN policy.
    - **Issuer name** – Type the name of the certificate issuer.
    - **Subject name** – Type the name of the certificate subject.
    - **Type** – Select one of the following options:
      - **Client (user) certificate**
      - **CA certificate**
      - **Peer (phone) certificate**
    - **Format** – This field displays the certificate format.
    - **Fingerprint algorithm** – Select one of the following options to specify the algorithm that is used.
      - **MD5**
      - **SHA-1**
    - **Fingerprint value** – Specify the fingerprint value.
    - **Serial number** – Type the serial number of the certificate.
    - **Validity begin** – Type the date starting when the certificate is valid.
    - **Validity end** – Type the date when the certificate becomes invalid.
    - **Deletable** – Select this check box to specify if the certificate can be deleted from the phone.
    - **Trusted** – Select this check box to specify if the certificate can be trusted or not.
    - **Send applicability** – Select this check box to

### 3.9. PKI and Certificate Configuration

Perform the following steps to add PKI and Certificate configuration settings to a profile.

specify if applicability is sent or not. This setting means that you authorise the certificate to verify web pages, email servers, software packages, and other data. Only trusted certificates can be used to verify services and software.

- Applicability – Specify the applicability.

6. Click the **Save and Close/Save/Close** icons, as appropriate.

### 3.10. NCC for Alcatel-Lucent Configuration

Perform the following steps to configure Nokia Call Connect (NCC) for Alcatel-Lucent settings to a profile.

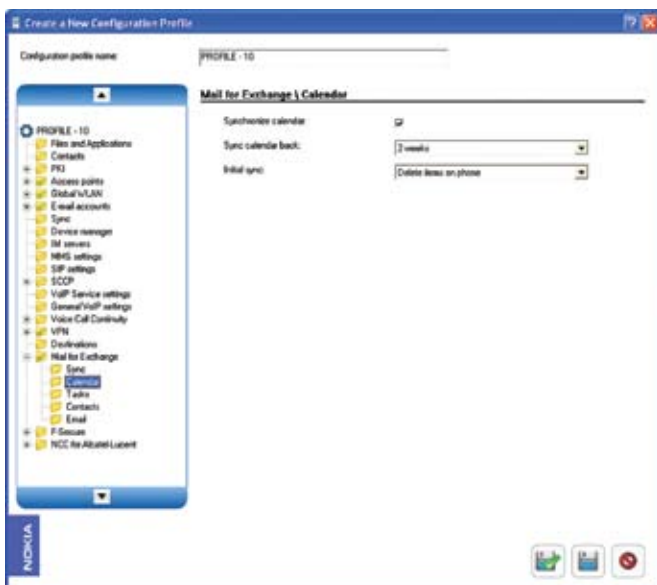


Figure 13: Nokia Call Connect for Alcatel Lucent settings editor

2. In the left pane of the Edit Configuration Profile dialog box, click the NCC for Alcatel-Lucent folder.
3. In the **NCC for Alcatel-Lucent** section, provision the following fields:
  - **Send NCC for Alcatel-Lucent settings** – Select this check box if you want to send the NCC settings to the phone.
  - **Alcatel-Lucent OmniPCX type** – Select the appropriate type from the following options:
    - **Alcatel-Lucent OmniPCX Enterprise**
    - **Alcatel-Lucent OmniPCX Office**
  - **Bus. voice mail number** – Type the business voice mail number.
4. Click the PBX Alcatel Omni PCX folder and provision the following fields:

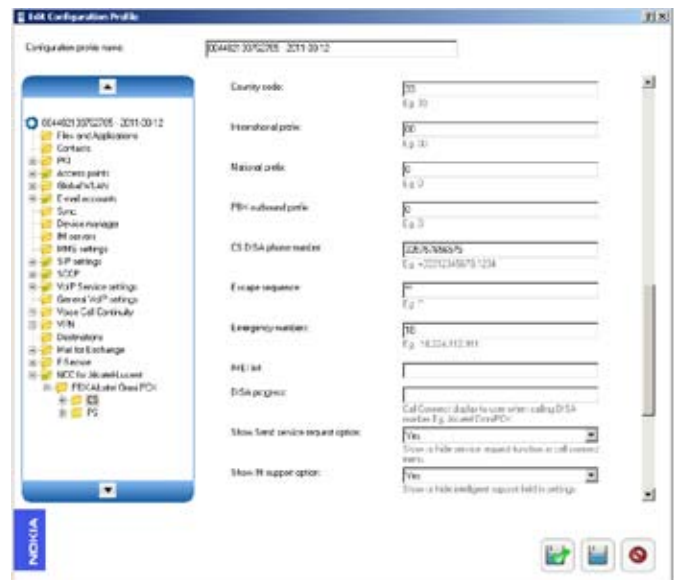


Figure 14: Nokia Call Connect settings editor for Alcatel Lucent Omni PCX CS

- **Private plan size** – Type the number of digits in the PBX numbering plan. This plan defines the length of the extension numbers.
- **Dialling prefix** – Type the two character dialling prefix used to force GSM and Direct Inward System Access (DISA) calls. The first is the dialling prefix character used to force a GSM call and second is the dialling prefix character used to force a DISA call.
- **Country code** – Type the country code.
- **International prefix** – Type the international prefix number.
- **National prefix** – Type the national prefix number.
- **PBX outbound prefix** – Type the PBX outbound prefix number.
- **CS DISA phone number** – Type the circuit switched (CS) DISA phone number.
- **Escape sequence** – Type the escape sequence which is used to send DTMF sequences to the PBX.
- **Emergency numbers** – Type comma-separated list of emergency numbers. These numbers are called using GSM.
- **IMEI list** – Type a comma-separated list of International Mobile Equipment Identity (IMEI) numbers.
- **DISA progress** – Specify the text string that Nokia Intellisync Call Connect uses when calling the DISA number. The value is stored in **Contacts** on the phone. The call log displays this string when a DISA call is made.
- **Show Send service request option** – Select from one of the following options:

- **Yes** – Shows the send service request option in Nokia Intellisync Call Connect.
  - **No** – Does not show the send service request option.
- **Show IN support option** – Select from one of the following options:
    - **Yes** – Shows the Intelligent network (IN) support settings in Nokia Intellisync Call Connect.
    - **No** – Does not show the Intelligent network (IN) support settings.
  - **Enable Intelligent network support** – Select Yes or No, to enable or disable intelligent network support on the phone while roaming in networks that do not support IN.
6. Click the Feature codes folder under the CS folder and then click the In-call folder.
7. Provision the following fields:
- **Answer waiting call** – DTMF sequence to answer waiting calls.
  - **Second call** – DTMF sequence to start a second call. When Nokia Intellisync Call Connect sends the DTMF sequence to start a second call, the PBX puts the active call on hold and generates a hold tone on the line. Then the PBX makes the second call.
  - **Swap calls** – DTMF sequence to swap between an active call and a call on hold.
  - **Transfer calls** – DTMF sequence to transfer an active call to another number.
  - **Start conference** – DTMF sequence to create a three-party conference call.
  - **End conference** – DTMF sequence to end a conference call.
  - **Call attendant (in-call)** – DTMF sequence to call the telephone exchange attendant during an active call.
  - **Request callback** – DTMF sequence to request callback when the line is busy.
  - **Park calls** – DTMF sequence to park a call. If users do not pick up the parked call before a timer goes off, external calls are rerouted either to the attendant or to the number that parked the call.
  - **Leave message** – DTMF sequence to leave messages in voice mailboxes.
  - **Reverse call** – DTMF sequence to reverse the charges of a call to the PBX.
  - **End call** – DTMF sequence to end a second call.
8. Click the Non-call folder and provision the following fields:
- **Call attendant (non-call)** – DTMF sequence to call the telephone exchange attendant.
  - **Forward calls on no answer** – DTMF sequence to forward calls when no one answers.
  - **Forward calls on busy** – DTMF sequence to forward calls when the line is busy.
  - **Forward all calls** – DTMF sequence to update call forwarding settings to forward all calls.
  - **Forward on no answer or busy** – DTMF sequence to forward calls when the line is busy or when no one answers.
  - **Cancel call forwarding** – DTMF sequence to cancel call forwarding.
  - **Do not disturb** – DTMF sequence to set availability status to Do Not Disturb.
  - **Available** – DTMF sequence to set availability status to Available.
  - **Pick up parked calls** – DTMF sequence to pick up parked calls.
  - **Nomadic mode** – DTMF sequence to activate nomadic mode.
  - **Cancel nomadic mode** – DTMF sequence to cancel nomadic mode.
  - **Forward to personal assistant** – DTMF sequence to forward calls to the personal assistant.
  - **Forward to voice mail** – DTMF sequence to forward calls to voice mail.
  - **Call forwarding status** – DTMF sequence to check the call forwarding status of the user.
9. Click the User-specific folder and provision the following fields:
- **Directory number** – Type the extension number assigned to the internal cellular client.
  - **PIN** – Type the Private identifier number (PIN) which users enter in the DISA Password field in business settings in Nokia Intellisync Call Connect.
  - **Secret code** – Personal identification code (password) is a text string of four characters. Users can change their secret code from their desk extension.
  - **Trunk group number** – This field is reserved for future use.
  - **Extension** – Type the extension number within

the telephone exchange.

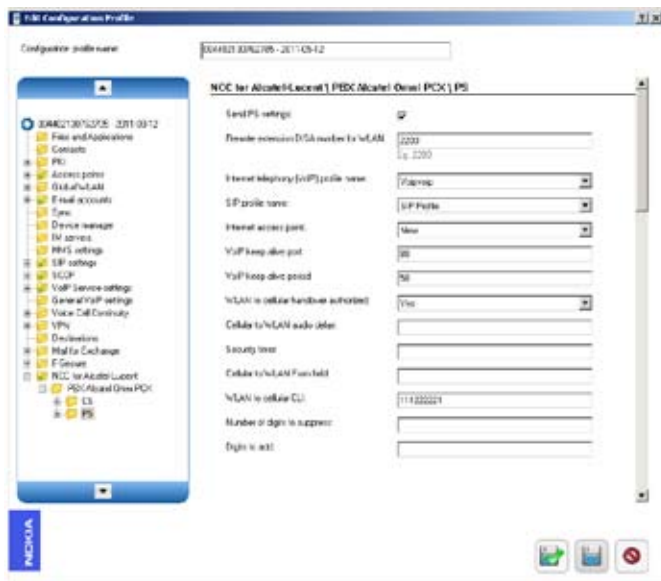
10. Click the PS folder and provision the following fields:

- **Send PS settings** – Select this check box to send Packet Switched (PS) settings to the phone.
- **Remote extension DISA number for WLAN** – Use the OmniPCX Enterprise Configuration application to view the remote extension DISA number in the Remote Extension DISA field in the prefix plan. In business WLAN mode, Nokia Intellisync Call Connect makes VoIP calls to this number to register to Alcatel-Lucent Cellular Extension and to issue commands to the PBX.
- **Internet telephony (VoIP) profile name** – Type the Internet telephony profile name that can be used by Nokia Intellisync Call Connect to make calls in business WLAN mode.

**NOTE:** The Internet telephony profile name specified here must be specified in the phone also.

- **SIP profile name** – Type the SIP profile name that can be used by Nokia Intellisync Call Connect to make calls in business WLAN mode.

**NOTE:** The SIP profile name specified here must be specified in the phone also.



**Figure 15:** Nokia Call Connect settings editor for Alcatel Lucent Omni PCX PS

- **Internet access point** – Type the access point that can be used by Nokia Intellisync Call Connect to make calls in business WLAN mode.

**NOTE:** The Internet access point name specified here must be specified in the phone also.

- **VoIP keep alive port** – Type the port number of the keep alive server.

- **VoIP keep alive period** – Type the VoIP keep alive period (in seconds). This period is used to inform the server if the phone is still connected to the server. Set to 0 to disable keep alive.
- **WLAN to cellular handover authorised** – Select Yes to authorise handover from WLAN to cellular networks.
- **Cellular to WLAN audio delay** – Specify the handover delay. During handover from cellular networks to WLAN the client delays switching off the cellular audio based on this value. It is mandatory if handover is authorised.
- **Security timer** – Specify the time to accept the SIP invite initiated by the phone. If the invitation is not acknowledged before the security timer expires, the phone tries to use the cellular network to make a call. This field is mandatory if handover is authorised.
- **Cellular to WLAN From field** – During handover, the server makes an SIP call with a specific From field to identify the call. The phone detects the specific From field and, therefore, it does not present the call to the user. The phone switches the audio from cellular to WLAN.
- **WLAN to cellular CLI** – Specify the Calling Line Identifier (CLI) which is used to indicate an incoming cellular call when switching from WLAN to cellular networks.
- **Number of digits to suppress** – Specify the number of digits to suppress from the beginning of a non-canonical number in SIP URI. For business WLAN mode only.
- **Digits to add** – Specify the number of digits to add at the beginning of a non-canonical number in SIP URI after the suppressed digits have been removed. For business WLAN mode only.

11. Click the Feature Codecs folder under the PS folder and provision the following fields:

- **Handover type** – Select one of the following options:
  - **Assisted** – User initiates handover.
  - **EMS** – EMS initiates handover automatically.
- **WLAN to cellular handover** – DTMF code to hand over calls from WLAN to cellular networks. Must be set if handover is authorised.
- **Cellular to WLAN handover** – DTMF code to hand over calls from cellular networks to WLAN. Must be set if handover is authorised.
- **Cellular off** – DTMF code to send the cellular off signal before switching off the cellular interface during a handover operation.

12. Click the Save and Close/Save/Close icons, as appropriate.

### 3.11. F-Secure Configuration

Perform the following steps to configure F-Secure settings for a profile.

1. Select the profile for which you intend to add F-Secure settings and click .
2. In the left pane of the Edit Configuration Profile dialog box, click the F-Secure folder.
3. Provision the following fields:
  - **Send settings** – Select this check box to send the F-Secure settings to the phone.
  - **Subscription code** – Type the F-Secure Mobile Security subscription code.
  - **Send the access point settings** – Select this check box to send the default access point settings to the phone.
  - **Default access point** – Select the default access point.
  - **License file** – The license file content is given in XML-format. The file is used when F-Secure Mobile Security client is activated.
  - **Application update policy** – Select one of the following options for application updates:
    - **Download automatically**
    - **Ask before downloading**
  - **Start automatically on device boot** – Select one of the following options for starting the F-Secure Mobile Security client:
    - **Yes**
    - **No**
  - **Enable forced updates** – Select the check box to enable forced updates.
  - **Force update interval** – If you have selected to enable forced updates, specify the force update interval.
  - **Unique client code** – Type the unique client code. It is provided by your service provider and cannot be changed.
4. Click the Real-time folder under the F-Secure folder and provision the following fields:
  - **Scanning mode** – Select one of the following options:
    - **Real-time** – Files are scanned when they are accessed.
    - **Manual** – Files are scanned when you choose to scan them.
  - **Enable scanning mode selection** – Select Yes or No to enable scanning mode selection.
5. Click the Automatic update folder and provision the following fields:
  - **Enable automatic update** – Select the check box to enable automatic update.
  - **Automatic update interval** – Specify how often F-Secure can check for updates. Time entered is in minutes.
  - **Enable automatic update selection** – Select Yes or No to enable automatic update selection from the phone.
6. Click the Firewall folder and provision the following fields:
  - **Firewall protection** – Select one of the following options to specify firewall protection level:
    - **Allow all**
    - **Normal**
    - **High**
    - **Deny all**
    - **Custom**
  - **Enable firewall protection selection** – Select Yes or No to enable/disable firewall protection from the phone.
  - **Custom rule set** – If you have selected firewall protection level to custom, specify the custom rule set.
7. Click the Infected file handling folder and provision the following fields:
  - **Delete infected file**
  - **Quarantine infected file**
  - **Release infected file**
  - **Disinfect infected file**
  - **Emphasised infected-file handling option** – Select one of the available options to emphasise your selection.
8. Click the **Save and Close/Save/Close** icons, as appropriate.


### 3.12. Other Configurations

#### 3.12.1. Files and Applications


The Files and Applications option in the NCT allows you to add files and installable applications like SISX, SIS and JAD/JAR to a profile and transfer them to a phone. Files can also be deleted or arranged in specified folders in the phone.

Perform the following procedures to add, delete, and arrange files and applications on your phone using the NCT.



### Adding

1. Click the **Files and Applications** folder in the left pane. The **Files** section opens on the right side.
2. Click .
3. In the resulting Add File dialog box, browse to the appropriate location, select the file to be added to the profile and click OK.
4. Click the **Save and Close/Save/Close** icons, as appropriate.

### Deleting

1. Click the **Files and Applications** folder in the left pane.
2. In the Files section, select the files to be deleted.
3. Click .
4. Click the **Save and Close/Save/Close** icons, as appropriate.

### Arranging

1. Click the **Files and Applications** folder in the left pane.
2. Select the files to be arranged – moved up or down.
3. Click  or .
4. Click the **Save and Close/Save/Close** icons, as appropriate.

### Specifying folders




1. Click the **Files and Applications** folder in the left pane.
2. Select the files to be moved to a specific folder.
3. Click the change target icon.
4. The path in the **Target folder** column becomes editable.
5. Make necessary changes and click the **Save and Close/Save/Close** icons, as appropriate.

## 3.12.2. Contacts



Using the NCT, you can create contact cards and add them to a profile and later transfer them to your phone. The supported file formats are vCard and CSV. Contacts can also be removed from the profile.

Perform the following steps to create, add, and remove contacts:

### Creating a contact card

1. Click the **Contacts** folder in the left pane. The **Contacts** section opens on the right side.
2. Click .
3. In the resulting Select Contact dialog box, select Create new and click .
4. In the Create Contact dialog box, type appropriate information in the fields and click .
5. In the Save Contact dialog box, browse to the required location and click OK to save the contact card.
6. Click the **Save and Close/Save/Close** icons, as appropriate.

### Adding contacts


1. Click the Contacts folder on the left pane.
2. Click .
3. In the resulting Select Contact dialog box, choose Select from existing option and click .
4. In the Add contact dialog box, browse to appropriate location, select the required contact cards, and click **OK**.

**NOTE:** To select more than one contact card use the CTRL key.

5. Click the **Save and Close/Save/Close** icons, as appropriate.

**NOTE:** The number of contacts added to the profile is displayed in the Contacts section, below the list of contacts.


### Deleting contacts




1. Click the **Contacts** folder in the left pane.
2. In the Contacts section, select the contacts to be deleted.
3. Click .
4. Click the **Save and Close/Save/Close** icons, as appropriate.

## 3.12.3. Sync

The Sync feature allows you to synchronise all the required files on your phone and a PC/specified server.



Perform the following steps to add Sync settings to a profile.

1. Select the profile for which you intend to add Sync settings and click .
2. In the left pane of the Edit Configuration Profile dialog box, click the Sync folder.

3. Click  in the Sync section.
4. In the Sync section, provision the following fields:
  - **Sync Profile name** – Type a name for the sync profile.
  - **Server ID** – Type the Server ID with which the phone will communicate for syncing the data.
  - **Data bearer** – Select the media used to communicate with the server:  
Bluetooth® – Preferred option if you are syncing data with a PC.  
Internet – Preferred option if you are syncing data with a server on the internet.
  - **Access point** – If you select Internet as the Data bearer type, then specify the access point to be used.
  - **Host address** – Type the URL address of the synchronisation server.
  - **Port** – Type the port number for the server.
  - **Username** – Type a username to access the synchronisation server.
  - **Password** – Type a password for the username.
5. Click the **Applications** folder under the newly created Sync setting folder and click .
6. In the Choose Group Type dialog box, select the required application and click . The available applications are Bookmarks, Calendar, Contacts, Email, MMS, Notes, and SMS.
7. Type the Remote database URL for the selected application.
8. Click the **Save and Close/Save/Close** icons, as appropriate.

### 3.12.4. Device Manager



Perform the following steps to configure Device Manager (DM) settings for a profile.

1. Select the profile for which you intend to add device manager settings and click .
2. In the left pane of the Edit Configuration Profile dialog box, click the **Device manager** folder.
3. Click  in the Device manager section.
4. Provision the following fields:
  - **DM Server name** – Type a name for the DM server.
  - **Server ID** – Type the Server ID.
  - **Authentication Type** – Select from one of the following options:

- **Basic**
  - **Md5**
  - **Host address** – Type the URL address of the DM server.
  - **Port** – Type the Port number of the DM server.
  - **Username** – Type a username to access the Sync server.
  - **Password** – Type a password for the username.
  - **Network Authentication** – Select the check box to enable network authentication.  
**NOTE:** If you select the Network Authentication check box, the Network Username and Network password are enabled.
  - **Network username** – Type a username for network authentication.
  - **Network password** – Type a password for the username.
  - **Session mode** – Select the media used to communicate with the server:
    - **Bluetooth®** – Preferred option if you are syncing data with a PC.
    - **Internet** – Preferred option if you are syncing data with a server on the Internet.
  - **Access point** – If you select Internet as the session mode type, then specify the access point to be used.
5. Click the **Save and Close/Save/Close** icons, as appropriate.

### 3.12.5. IM Servers

Perform the following steps to configure IM server settings for a profile.

1. Select the profile for which you intend to add IM server settings and click .
2. In the left pane of the **Edit Configuration Profile** dialog box, click the IM servers folder.
3. Click  in the IM servers section.
4. Provision the following fields:
  - **Server name** – Type the name for the chat server
  - **Send access point** – Select the check box if you want to use a specific access point.
  - **Access point in use** – Select the access point to be used to connect to the server.
  - **Web address** – Type the URL address of the IM server.

- **User ID** – Type a user ID for the IM server.
  - **Password** – Type a password for the user ID.
5. Click the Save and Close/Save/Close icons, as appropriate.

### 3.12.6. MMS Settings

With the NCT, you can edit the Multimedia (MMS) settings of your phone. These settings affect the way MMS messages are sent and received. Perform the following steps to configure MMS settings for a profile.

1. Click the MMS settings folder in the left pane.
2. In the MMS Settings section, provision the following fields:

- **Send MMS settings** – Select the check box to send MMS settings to your phone.
- **Image size** – Select the image size you want to use when sending MMS messages. The available options are Small, Medium, and Large.
- **MMS creation mode** – Select the MMS messages creation mode from one of the following options:
  - **Free** – Allows all attachment types.
  - **Restricted** – Prevents you from creating MMS messages that are not supported by the network or receiving phone.
  - **Guided** – Warns you if you are creating MMS messages that are not supported by the network or receiving phone.

- **Access point in use** – Select the access point to be used.

**NOTE:** All access points configured for the profile are listed in the drop-down menu.

- **Multimedia retrieval** – Select the MMS message reception mode from the following options:
  - **Always automatic** – The phone receives MMS messages automatically.
  - **Automatic in home network** – MMS messages are automatically received only when the subscriber is in home network.
  - **Manual** – With this option MMS messages are downloaded to the phone only after your confirmation or you have to login to the message center to download the MMS messages.
  - **Off** – MMS message reception is disabled.
- **Allow anonymous messages** – Select this option to receive MMS messages from

anonymous senders.

- **Receive adverts** – Select this option to receive advertisements.
  - **Deny report sending** – Select this option if you do not want to send delivery reports.
  - **Receive report** – Select this option if you want to receive a delivery report.
  - **Message validity** – Specify the message validity period. Messages are stored in the message center for the specified period.
3. Click the Save and Close/Save/Close icons, as appropriate.

### 3.12.7. Voice Call Continuity

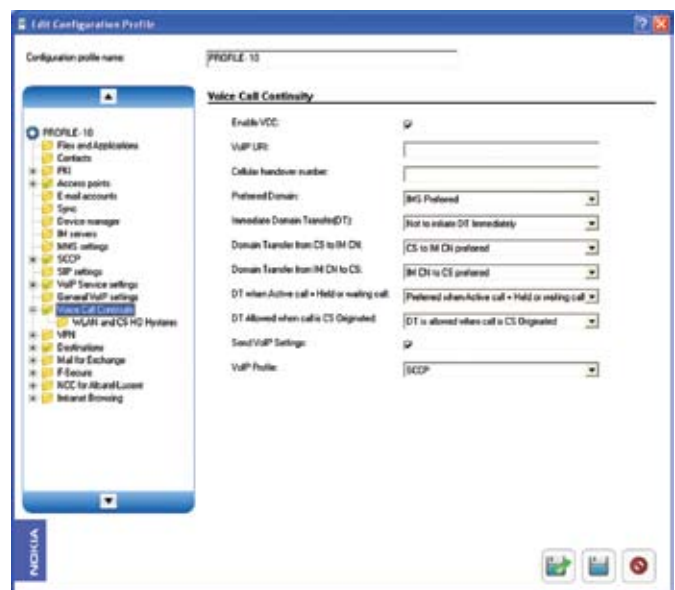



Figure 16: Voice Call Continuity settings editor

1. Select the profile for which you intend to add destination settings and click .
2. In the left pane of the Edit Configuration Profile dialog box, click the Voice Call Continuity folder.
3. In the VCC section, provision the following fields:
  - **Enable VCC** – Select this check box to enable VCC.
  - **VoIP URI** – Type the VCC Domain Transfer URI that is included in SIP INVITE requests that are used to initiate domain transfer.
  - **Cellular handover number** – Type the VCC Domain Transfer Number that the user includes in the setup of a circuit switched (CS) call to initiate domain transfer.
  - **Preferred Domain** – Select one of the following options for your phone originated calls and sessions:



- **IMS Preferred**
  - **CS Preferred**
  - **Immediate Domain Transfer (DT)** – Select one of the following options to specify the Immediate Domain Transfer to specify whether to initiate a VCC domain transfer (DT) immediately to the operator's preferred domain when that domain becomes available. This operator policy affects only active sessions.
    - **Not to initiate DT immediately**
    - **Initiate DT immediately**
  - **Domain Transfer from CS to IM CN** – Select one of the following options to specify whether a VCC domain transfer from the CS domain to IMS domain is preferred or not.
    - **CS to IM CN preferred**
    - **CS to IM CN not preferred**
  - **Domain Transfer from IM CN to CS** – Select one of the following options to specify whether a VCC domain transfer from IMS domain to CS domain is preferred or not.
    - **IM CN to CS preferred**
    - **IM CN to CS not preferred**
  - **DT when Active call + Held or waiting call** – Select one of the following options to specify whether the network operator prefers the domain transfer to occur when the VCC phone is engaged in an active, held, or waiting call or session in the transferring-out domain or not.
    - **Preferred when Active call + Held or waiting call**
    - **Not preferred when Active call + Held or waiting call**
  - **DT Allowed when call is CS Originated** – Select one of the following options to specify whether DT is allowed when a call is CS originated:
    - **DT is allowed when call is CS originated**
    - **DT is not allowed when call is CS originated**
  - **Send VoIP Settings** – Select this check box to send the VoIP settings to the phone.
  - **VoIP Profile** – Select the preferred VoIP profile.
4. Click the WLAN and CS HO Hysteresis folder and provision the following fields:
- **WLAN HO Threshold**
  - **WLAN HO Hysteresis**

- **WLAN Hysteresis Timer Low**
- **WLAN Hysteresis Timer High**
- **CS HO Threshold**
- **CS HO Hysteresis**
- **CS Hysteresis Timer Low**
- **CS Hysteresis Timer High**

5. Click the Save and Close/Save/Close icons, as appropriate.

### 3.12.8. Destinations


Perform the following steps to add destinations to a profile.

1. Select the profile for which you intend to add destination settings and click .
  2. In the left pane of the Edit Configuration Profile dialog box, click the Destinations folder.
  3. Click  in the Destinations section.
  4. Provision the following fields:
    - **Name** – Type a name for the destination.
    - **Properties and Purposes** – Select the appropriate option to specify the property (highlighted or hidden) and purpose (for example, internet) of the destination.
    - **Protection** – Select one of the following protection options:
      - **No Protection**
      - **No Addition/Modification of SNAP and APs**
      - **SNAP Name Protected**
    - **Hide** – Select this check box to hide the destination.
    - **APPriority List** – All APs configured for the profile are listed here. Select the preferred AP. Use the Raise priority and Lower priority buttons to change the priority of the APs.
    - **Send Embedded Destination** – Select this check box to send the embedded destination to the phone.
    - **Embedded SNAP** – Select the preferred SNAP to be embedded in the destination.
5. Click the Save and Close/Save/Close icons, as appropriate.

### 3.12.9. Device Encryption

The Device Encryption option allows you to protect the data that is stored on the phone memory and the memory card.

Perform the following steps to encrypt the phone memory or the memory card or both.

1. On the Menu bar, click Devices > Edit online.
2. In the Edit Configuration Profile Online dialog box, select the phone for which you intend to encrypt the phone memory and the memory card and click .




Result: NCT reads the phone data and the available phone settings are displayed in the Edit Configuration Profile Online dialog box.

3. In the Edit Configuration Profile Online dialog box, click the Device Encryption folder and select one of the following options from the Enable drop-down menu as required:
  - **Phone and card memory enabled** – Both phone and memory card encryption is enabled.
  - **Memory card disabled** – Memory card encryption is disabled.
  - **Phone memory disabled** – Phone memory encryption is disabled.
  - **Both disabled** – Both phone and memory card encryption is disabled.
4. Depending on the option you selected, expand the Device Encryption folder and perform one of the following:
  - For phone memory, click the Phone Memory folder and select Encrypt or Decrypt from the Phone memory drop-down.
  - For memory card, click the Memory Card folder and select one of the following options:
    - **Decrypt** – The memory card is decrypted.
    - **Encrypt** – The key is generated in the phone and stored in write-only memory. Restoring factory settings makes the card unreadable.
    - **Backup encrypt** – The key is generated in the phone and stored in write-only memory, but a copy of the key remains in the device manager and the administrator can retrieve the key. This option allows restoring the key after a factory reset or making the card readable in other phones.
    - **Restore encrypt** – The key is not generated in the phone, but sent to the phone from the device manager. The key is stored in the phone in write-only memory. This operation can be used to restore a key that was saved



using the backup encryption option.

5. Click the Save and Close/Save/Close icons, as appropriate.

### 3.13. Editing, Deleting, and Duplicating Profile Settings

- To edit any of the profile settings, navigate to the appropriate folder, select the profile setting and click .
- To delete any profile settings, navigate to the appropriate folder, select the profile setting and click .
- To duplicate any profile settings, navigate to the appropriate folder, select the profile setting and click .


### 3.14. Selecting Profile Settings to be Sent to the Phone

- To select a setting that you wish to send to the phone, select the setting and click the folder icon; selection will be indicated by .
- To de-select a setting, select the setting and click the checked folder icon. A de-selected folder is indicated by .
- Settings that do not have valid data are de-selected and are not sent to the phone.
- Some settings like Contacts, Sync, and Phone manager are always selected.

### 3.15. Classification of User and General Settings

Certain settings are classified as General and User Specific. This classification helps to differentiate between the settings that an Administrator has to enter or specify (General) while configuring certain features on the NCT and the settings that a user of the mobile can specify (User Specific) while using the phone.

## 4. VPN Configuration

Nokia Configuration Tool allows you to create and alter Virtual Private Network (VPN) policy files. VPN configuration utility can be invoked from the Tools menu or directly from the  button in the main screen.

The default window displays the basic settings that are required to create a VPN policy file.


On entering these details the VPN file can be generated and saved to the local storage for later use or can be directly sent to the phone.

You can also configure several advanced settings by using the Advanced button from this default window.

To open a VPN file you can also drag and drop it to the default VPN window. The following steps will help you to configure VPN:



Figure 17 – Nokia Mobile VPN Policy settings editor





1. In main window, click  button. VPN configuration window appears as shown in the figure below.

2. Enter the required fields.

For example:

Enter the policy name and VPN gateway address. Select an authentication method, say PRE-SHARED, from the drop-down box.

This enables the corresponding tab, in this case the Preshared Key tab.

3. Select any option, say FQDN, from Identity type drop-down option.
4. Enter an Identity value, select the Preshared Key tab and choose a suitable format and enter the key.
5. You are now ready to generate the policy.
6. Click  button to save policy file to your local storage device (e.g. hard disk).
7. Click  button to send the policy directly to connected phone. This button is greyed out if phone is not connected.
8. Click  button to load an existing policy file.
9. Click  button to configure advanced settings.

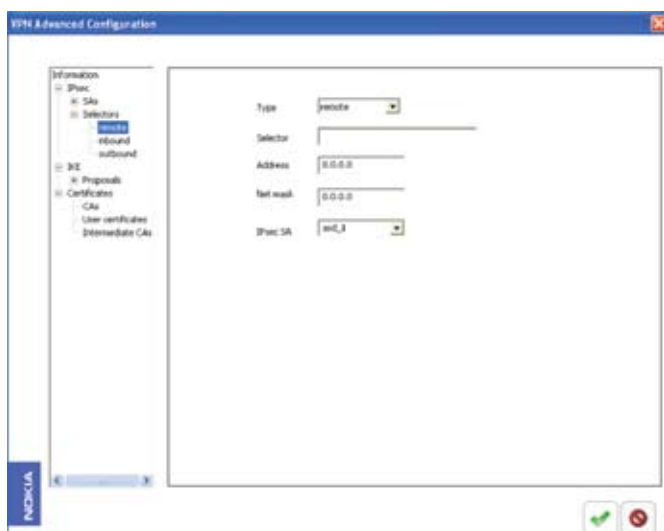


Figure 18 – Nokia Mobile VPN Advanced Configuration settings editor

## 4.1 Small description on vpn settings

All of the following values depend on how network is maintained. In real case scenario these values are provided by system administrator.

Selection of IKE mode depends on how network is supporting VPN access (this is depends on the type of mode supported by system administrator).

### 4.1.1 Settings based on authentication methods:

#### IKE-CRACK:

IKE tab: "Identity type" is used from certificate authority for following identity types. "FQDN", "RFC822\_NAME", "certificate owner". This uses certificate that is present under "certificate authority" tab.

For all remaining Identity types, need to edit "Identity value". E.g. For IPv4 - 10.120.24.35 (user IP address). This is applicable to all authentication methods.

Remote ID type: It is used only with IKEv2. Remote Id is secure gateway identity type for gateway identification that authenticates also gateway (mutual authentication) from gateway's certificate using chosen identity type.

Silent CRACK, certificate authority tabs:  
Enter username, password

#### Preshared Key:

IKE tab: refer "IKE tab" under "IKE-CRACK"

"Preshared key" tab: Enter preshared key

#### RSA\_SIGNATURES / DSS\_SIGNATURES:

For these both authentications either use Method1 or Method2 described below.

Method1:

IKE tab: refer "IKE tab" under "IKE-CRACK" PKCS#12:  
PKCS#12 is a bundle or package which contains all needed certs and keys

Method2:

IKE tab: refer "IKE tab" under "IKE-CRACK"

Certificate authority tab:

Enter certificates (.pem,cer,.der) provided by system administrator

User Certificate tab:

Enter certificates (.pem,cer,.der) provided by system administrator

Enter private key (.key) provided by system administrator

Enter "subject DNS suffix" e.g. domain.com

## 5. Troubleshooting

### 5.1. Generic Issues



**Question:** Nokia PC Suite detects my phone but Nokia Configuration Tool does not. What is the problem?

**Answer:** Make sure Nokia Configuration Tool supports your phone. If it does not, you cannot configure your phone with Nokia Configuration Tool. The supported phones are listed in the Supported Phones section. Check the contents of the Phone type combo box. A connection problem between the phone and the PC may also cause the detection to fail. Restart your computer and the Nokia Configuration Tool.

**Question:** Neither Nokia PC Suite nor Nokia Configuration Tool detects my phone. What is the problem?

**Answer:** Make sure that Nokia PC Suite and Nokia Configuration Tool support your phone. If they do, then restart your computer.

**Question:** I imported all the data from my phone to Nokia Configuration Tool and then made some modifications. After that, I sent the profile back to my phone. Now I have duplicate settings on my phone. Why does my phone have duplicate settings, although I sent the original phone settings back to the phone?

**Answer:** If you want to modify the settings that already exist on your phone, you have to use the Edit Online option. If you import the settings and then send the edited profile back to the phone, the existing settings are not replaced by the modified settings. Instead, duplicate settings are stored.

**Question:** The calendar and contact contents of a SyncML (DS) group are not transferred to my phone. What is the problem?

**Answer:** When editing the profile settings online, changing the settings of the Easy WLAN group, default SyncML (DS) groups, and default SyncML (DM) group is not possible because these are default settings and changing these settings may cause problems.

After importing a profile from a phone, it is recommended to delete the Easy WLAN access point, the default SyncML (DS) groups, and the default SyncML (DM) group from the configuration profile.

**Question:** The WLAN WEP key ID, encryption and data values are not imported from my phone. What is the problem?

**Answer:** For security reasons, those values are not imported from Nokia Communicator phones.

**Question:** Why does the Contact transfer fail?

**Answer:** If you transfer only one contact into a phone and then delete it from the phone, the subsequent contact transfers fail.

**Question:** Why does an import fail?

**Answer:** With some computer configurations, importing may fail. In an error situation, restart the computer and Nokia Configuration Tool. If that does not help, install Nokia Configuration Tool on a different computer.

The screenshot shows a web form for configuring a mailbox. It includes the following fields and sections:

- Mailbox name:** Nokia mailbox
- User Settings** (Section Header)
- My name:** Nokia User
- My e-mail address:** user@nokia.com
- General Settings** (Section Header)
- IMAP4 folder path:** (Empty text box)
- SMTP authentication:**

### 5.2. PKI Related Issues

**Question:** I cannot see any PKI groups although my phone shows them. I also tried to send a new certificate file to the phone but it is not possible due to many errors during sending. What is wrong?

**Answer:** Your phone doesn't have mVPN client software as a default. You have to install mVPN client software to your phone before it is possible to send or import PKI groups and settings.

**Question:** I am not able to add a new certificate file to a profile. What is the problem?

**Answer:** NCT allows certificate files to be added only in Edit online. Thus, if you navigate to the PKI group in Edit online, there is also an Import button from which a new certificate file can be added to a profile.

**Question:** I have added a new certificate file and there are three editable settings. One of them is Applicability setting and this list has such applications that are not intended to be used with my certificate file. How is it possible?

**Answer:** NCT shows all applications of the phone that are available for certificates. So, you would need to know yourself convenient applications to which you want to authorise your certificate file.

**Question:** I have made an import from my phone and I have tried to send the same setting to another phone. However there were many errors concerning certificates.

**Answer:** NCT does not support sending of certificates between two phones. That means that your imported certificates do not have all data that would be needed in the other phone. It is better to remove certificates from the imported profile so that you can avoid these kinds of errors.

**Question:** Why can't I see any services/applications in the Applicability list after importing a new certificate to a profile in Edit online?

**Answer:** Applicability list only shows the services/applications

if you have not pressed the update button previously in the same session. However, you can send the certificate to the phone and change the services/application settings in the phone. The second alternative is that you repeat the online edit and change these values then.

### 5.3. VPN Related Issues

**Question:** I tried to create a new VPN access point, but I was not able to see it at all. The access point group has only 'Packet data' and 'Wireless LAN' types. Where is VPN access point?

**Answer:** VPN access points are added under the VPN group. The VPN group contains a group, 'Access points', where it is possible to create new VPN access points to be sent to the phone.

**Question:** I cannot send VPN access point group to my phone, NCT only returns errors. What is wrong?

**Answer:** Your phone doesn't have VPN client software as a default, it has to be installed. After installation of VPN, all errors will disappear.

**Question:** I created a VPN access point in Edit online, but I am not able to use it as an access point in any of the other setting groups. Where can I find it?

**Answer:** You need to close the Edit Configuration Dialog and re-import settings from the phone by using Edit Online. After reopening edit online the VPN access point is also shown among the general access points; this enables the VPN access point to be used in other setting groups.

### 5.4. VoIP Service Settings Related Issues

**Question:** I configured SIP and VoIP service settings in my phone and then pressed the Import button that retrieved the phone's settings to NCT. But now, I have an invalid profile that has a few empty and invalid settings. How can I correct that?

**Answer:** Some phone models might cause problems in this case. You can change the profile settings manually so that the profile is valid. Also updating your phone's software may help.

### 5.5. WLAN Related Issues

**Question:** I tried to update Allow PEAPv0 value but it does not seem to take effect. What is wrong?

**Answer:** Some phone models do not allow changing PEAPv0, PEAPv1 and PEAPv3 values by using NCT. You need to change these settings in your phone.

**Question:** I configured a WLAN access point with EAP-PEAP/EAP-TLS in the phone and imported it into NCT. Why is the CA certificate setting blank?

**Answer:** Some certificates are not imported from some phone models and NCT can therefore not show the certificate reference if the certificate is not imported.

### 5.6. Restrictions and Known Issues

All settings – Avoid the € character for all settings.

**Email** – Make sure that a phone includes no more than five (5) mailboxes before a send operation. Otherwise, problems may occur during the sending or importing operation.

WLAN –

- A WLAN access point called Easy WLAN is shown in Nokia Configuration Tool. It is not possible to modify this settings group.
- Importing a WPA pre-shared key from a phone may fail.
- Importing WEP key settings from a phone having Hexadecimal 128 bit encryption may result in profile showing the format as ASCII, selecting Hexadecimal option will allow viewing of the appropriate key values.

**SIP Settings** – Sending to a phone may fail in some combinations and it is not recommended to send more than one SIP profile at a time.

**Phone Manager** – If you configure more than one phone manager setting at a time, the port numbers may cause problems.

**Sync** – The host address may show incorrect information after Nokia Configuration Tool sending operation. The address concatenated with :80 may be shown as the host address in the phone Host address field.

**Visit:** [www.nokia.com](http://www.nokia.com) for more information

### Revision History

NCT Release	Date of Release	Remarks
Nokia Configuration Tool 6.0	June 2010	Initial release for NCT 6.0
Nokia Configuration Tool 6.2	December 2010	Updated for NCT 6.2

Copyright © 2006-2011 Nokia. All rights reserved.

©Nokia Corporation 2011. All rights reserved. Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.