

Using WLAN



Nokia E90 Communicator

NOKIA
Eseries

Nokia E90 Communicator Using WLAN

Legal Notice

Copyright © 2007 Nokia. All rights reserved.

Nokia, Nokia Connecting People, Eseries and E90 Communicator are trademarks or registered trademarks of Nokia Corporation. Other product and company names mentioned herein may be trademarks or tradenames of their respective owners.

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

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

To the maximum extent permitted by applicable law, under no circumstances shall Nokia or any of its licensors be responsible for any loss of data or income or any special, incidental, consequential or indirect damages howsoever caused.

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

The availability of particular products and applications and services for these products may vary by region. Please check with your Nokia dealer for details, and availability of language options.

Contents

Introduction.....	4
Using WLAN wizard	5
Defining WLAN connection settings.....	7
Creating a WLAN Internet Access Point for a WLAN access point.....	7
Modifying EAP settings.....	11
Creating a WLAN Internet Access Point for an ad hoc network	11
Defining other WLAN settings.....	14
Establishing a WLAN connection	15
Viewing the status of a WLAN connection	16
WLAN troubleshooting.....	17

Introduction

The purpose of this document is to guide you in using wireless LAN (WLAN) connections with your Nokia E90 Communicator. Typical situations in which you might use WLAN with Nokia E90 Communicator include, but are not limited to, downloading e-mail with attachments, browsing the web and downloading files, connecting to company network, connecting to a WLAN-capable laptop computer, sending a document to a WLAN-connected printer, and making Internet calls (VoIP calls). WLAN connections can be used both in public situations, such as when waiting at an airport or staying at a hotel, and in private wireless networks at your office or home.

Nokia E90 Communicator supports the following WLAN features:

- IEEE 802.11g and 802.11b WLAN standards
- Wi-Fi Protected Access 1.0 and 2 (WPA/WPA2)
- For interoperability with older WLAN networks, Nokia E90 Communicator also supports the legacy static WEP security and dynamic WEP security



Note: The typical transmission range of WLAN connections is limited from 30 meters in indoor spaces to 100 meters in open spaces. The range of wireless devices can be affected by metal surfaces, solid high-density materials and obstacles in the signal path.

Using WLAN wizard

The WLAN wizard helps you to connect to a wireless LAN, and shows the status of your wireless LAN connections and network searches in the active standby mode. To view the available options, scroll to the row showing the status, and press the scroll key. Depending on the status, you can start the web browser using a wireless LAN connection, disconnect from a wireless LAN, search for wireless LANs, or set network scanning on or off.

If wireless LAN scanning is off and you are not connected to any wireless LAN, *WLAN scanning off* is displayed in the active standby mode. To set scanning on and search for available wireless LANs, scroll to the status, and press the scroll key.

To start a search for available wireless LANs, scroll to a status, press the scroll key, and select *Search for WLAN*. To set wireless LAN scanning off, scroll to a status, press the scroll key, and select *Switch WLAN scan off*.

When you select *Start Web browsing*, the WLAN wizard automatically creates an internet access point (IAP) for the selected wireless LAN. The IAP can also be used with other applications requiring wireless LAN connection.

If you select a secured wireless LAN network, you are asked to enter the relevant passcodes. To connect to a hidden network, you must enter the correct hidden service set identifier (SSID).

You can also start the WLAN wizard separately to get more information on wireless LANs within range. Select  > *Connectivity* > *WLAN wiz.* Found networks are displayed.



Scroll to the desired network, select *Options*, and from the following:

- *Start Web browsing* or *Continue Web browsing* – Start or continue browsing the web using the IAP of the wireless LAN.
- *Disconnect WLAN* – Disconnect the active connection to the wireless LAN.
- *Refresh* – Update the list of available wireless LANs.
- *Details* – View the details of the wireless LAN.
- *Define access point* – Create an internet access point without starting the web browser.

Always enable one of the available encryption methods to increase the security of your wireless LAN connection. Using encryption reduces the risk of unauthorized access to your data.

Defining WLAN connection settings

This chapter discusses the WLAN settings in Nokia E90 Communicator. Special focus is on the selection of the WLAN security mode.

Different connectivity settings, including GPRS, WLAN and other technologies, are organised in so called Internet Access Points (IAPs) in your device. For WLAN access point usage, a WLAN IAP can be created. The advantage of using WLAN access point is that you have more control (particularly regarding security) over network traffic because it passes through the access point, and that you can use any resources in the wired network that the WLAN access point is connected to. The most important settings in the WLAN IAP include the network name (SSID), the WLAN security mode, and the security mode specific security settings.

It is also possible for WLAN devices to communicate directly with each other without any WLAN access points. This is done via ad hoc networks, which are established by a single user and others can then join in. Ad hoc connections are easy to set up, but they are limited to devices within the wireless transmission range. You can use ad hoc WLAN connections to print a document in your device to a compatible printer, for example.

Creating a WLAN Internet Access Point for a WLAN access point

- 1 Select  > *Tools* > *Settings* > *Connection* > *Access points*.
- 2 The list of existing access points is shown. Press *Options* > *New access point* to create a new Internet access point.
To use an existing access point as a basis for the new one, select *Options* > *Duplicate access point*.
- 3 Define the following settings:
 - *Connection name* – Type a descriptive name for the Internet access point, such as **My WLAN Internet**.
 - *Data bearer* – Select *Wireless LAN*.
 - *WLAN network name* – To enter the service set identifier (SSID), that is, the name that identifies the specific wireless LAN, select *Enter manually*. The name must be exactly the same as in your Wi-Fi router. If you do not enter the SSID here, you are not able to connect to networks that use a hidden SSID. To select the network from the wireless LANs in range, select *Search for networks*.
 - *Network status* – Select *Hidden* if the network you are connecting to is hidden, or *Public* if it is not hidden.

- **WLAN network mode** – Select *Infrastructure*. In this mode, devices can communicate with each other and with wired LAN devices through a wireless LAN access point.
- **WLAN security mode** – You must select the same security mode that is used in the wireless LAN access point. If you select *WEP* (wired equivalent privacy), *802.1x*, or *WPA/WPA2* (Wi-Fi protected access), you must also configure the relevant additional settings as described in step 4. The available modes are:
 - **Open network** – This security mode is commonly used with HTTP based logon. User authentication is performed at a higher layer using a HTML login page.
 - **WEP** – This security mode is supported for compatibility with IEEE 802.11 Wired Equivalent Privacy (WEP) networks. Pre-configured static WEP keys are required for this mode. There are two notations in use in the WLAN industry for the WEP key length representation, which sometimes makes things a bit confusing. The reason is that WEP key has a 24 bit common part and some vendors count this as being part of the key length, while some vendors do not. Both notations are equivalent at WLAN protocol level and fully interoperable.



Note: 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. In the WEP mode, the secure connection icon is not displayed.

- **802.1x** – This security mode is provided in order to support the legacy Dynamic WEP system, and to support networks that are migrating from Dynamic WEP to Wi-Fi Protected Access (WPA/WPA2). In this mode, Nokia E90 Communicator is able to join both dynamic WEP and WPA networks. Dynamic WEP refers to the fact that WEP keys are not static or pre-configured, but they are dynamically generated as part of the Extensible Authentication Protocol (EAP) authentication procedure. If WLAN access points support WPA, then it is recommended to use the WPA/WPA2 security mode instead of this mode.
- **WPA/WPA2** – The Wi-Fi Protected Access (WPA/WPA2) security mode provides the highest level of security among the WLAN security modes of Nokia E90 Communicator.
- **Homepage** – Enter the Web address of the page you want to display as a home page when you use this access point.



Note: The settings available for editing may vary.

- 4 If you selected *WEP* as the *WLAN security mode*, define the following in *WLAN security settings*:
- *WEP key in use* – Select which WEP key is used (#1–#4).
 - *Authentication type* – Select *Open* or *Shared*. Use the *Open* authentication when no authentication is required. The *Shared* authentication verifies that an authenticating wireless client has the same WEP key as your WLAN access point.



- *WEP key settings* – The remaining settings are defined here:
 - *WEP encryption* – Select the desired WEP encryption key length. Supported options are 64 and 128 bits. The more bits there are in the key, the higher the level of security. WEP keys consist of a secret key and a 24-bit initialisation vector. For example, some manufacturers refer to the 104-bit key as a 128-bit key (104+24). Both keys offer the same level of encryption and are therefore interoperable.

WEP key format – Select whether you want to enter the WEP key data in *Hexadecimal* format or in text format (*ASCII*). It is important that the same notation is used both in the access point and the Nokia E90 Communicator.

WEP key – Enter the WEP key data. The number of characters you can enter depends on the key length you have chosen.



Note: Wired equivalent privacy (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. When WEP security mode is in use, if your device receives a data packet not encrypted with the WEP keys, the data is discarded. In an Ad-hoc network, all devices must use the same WEP key.

If you selected *802.1x* as the *WLAN security mode*, define the following in *WLAN security settings*:

- *WPA/WPA2* – Select *EAP* if you want to use an EAP module for authentication. If you select *Pre-shared key*, type the password (also called a master key) in the field. Note that the same key must be entered in the wireless LAN access point.



- *EAP plug-in settings* – If you selected *EAP*, you must also define these settings. See "Modifying EAP settings" for more information.



Note: 802.1x authenticates and authorises devices to access a wireless network, and prevents access if the authorisation process fails.

If you selected *WPA/WPA2* as the *WLAN security mode*, define the following in *WLAN security settings*:

- *WPA/WPA2* – Select *EAP* if you want to use an EAP module for authentication. If you select *Pre-shared key*, type the password (also called a master key) in

the field. Note that the same key must be entered in the wireless LAN access point.

- *EAP plug-in settings* – If you selected *EAP*, you must also define these settings. See "Modifying EAP settings" for more details.
 - *WPA2 only mode* – Select *Off* to enable both WPA and WPA2 modes. If you select *On*, the access point must support WPA2 mode.
- 5 After setting up a basic Internet access point for *Wireless LAN*, select *Back* to save the settings of your WLAN IAP and exit, or *Options* > *Advanced settings* to define the following advanced settings:

- *IPv4 settings* – Enter the device IP and name server addresses for IPv4 Internet protocol.
- *IPv6 settings* – Select or enter the name server addresses for IPv6 Internet protocol.
- *Proxy server address* – Enter the proxy server address.
- *Proxy port number* – Enter the proxy server port number. Proxy servers are intermediate servers between a browsing service and its users, which are used by some service providers. These servers may provide additional security and speed up access to the service.

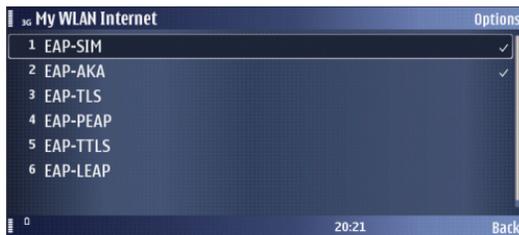


Note: The settings available for editing may vary. Contact your service provider for more information.

Modifying EAP settings

The extensible authentication protocol (EAP) plug-ins are used in wireless networks to authenticate wireless devices and authentication servers, and the different EAP plug-ins make possible the use of various EAP methods (network service).

To use an EAP plug-in when you connect to a WLAN using the access point, select the desired plug-in via [WLAN security settings](#) > [EAP plug-in settings](#) and [Options](#) > [Enable](#). The EAP plug-ins enabled for use with this access point have a check mark next to them. To not use a plug-in, select [Options](#) > [Disable](#).



To edit the EAP plug-in settings, select [Options](#) > [Edit](#).

To change the priority of the EAP plug-in settings, select [Options](#) > [Raise priority](#) to attempt to use the plug-in before other plug-ins when connecting to the network with the access point, or [Options](#) > [Lower priority](#) to use this plug-in for network authentication after attempting to use other plug-ins.

The available options may vary. Check the EAP plug-in values from your WLAN administrator.

Creating a WLAN Internet Access Point for an ad hoc network

- 1 Select [Tools](#) > [Settings](#) > [Connection](#) > [Access points](#).
- 2 The list of existing access points is shown. Press [Options](#) > [New access point](#) to create a new Internet access point.
To use an existing access point as a basis for the new one, select [Options](#) > [Duplicate access point](#).
- 3 Define the following settings:
 - [Connection name](#) – Type a descriptive name for the Internet access point, such as **Office ad hoc connection**.
 - [Data bearer](#) – Select [Wireless LAN](#).
 - [WLAN network name](#) – To enter the service set identifier (SSID), that is, the name that identifies the specific wireless LAN, select [Enter manually](#). Use the same name as in your Wi-Fi router. If you do not enter the SSID here, you are not able to connect to networks that use a hidden SSID. To select the network from the wireless LANs in range, select [Search for networks](#).
 - [Network status](#) – Select [Hidden](#) if the network you are connecting to is hidden, or [Public](#) if it is not hidden.

- **WLAN network mode** – Select *Ad-hoc*. In this mode, devices can send and receive data directly with each other, and no wireless LAN access point is needed.
- **WLAN security mode** – You must select the same security mode that is used in the wireless LAN access point. If you select *WEP* (wired equivalent privacy), you must also configure the relevant additional settings as described in step 4. The available modes are:
 - **Open network** – This security mode is commonly used with HTTP based logon. User authentication is performed at a higher layer using a HTML login page.
 - **WEP** – This security mode is supported for compatibility with IEEE 802.11 Wired Equivalent Privacy (WEP) networks. Pre-configured static WEP keys are required for this mode. There are two notations in use in the WLAN industry for the WEP key length representation, which sometimes makes things a bit confusing. The reason is that WEP key has a 24 bit common part and some vendors count this as being part of the key length, while some vendors do not. Both notations are equivalent at WLAN protocol level and fully interoperable.



Note: 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. In the WEP mode, the secure connection icon is not displayed

- **Homepage** – Enter the Web address of the page you want to display as a home page when you use this access point.



Note: The settings available for editing may vary.

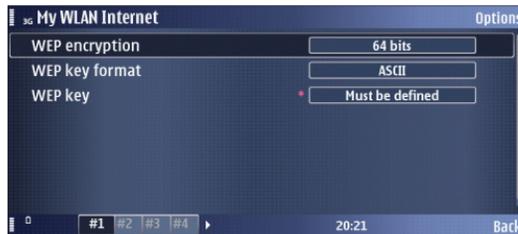
- 4 If you selected *WEP* as the **WLAN security mode**, define the following in **WLAN security settings**:
 - **WEP key in use** – Select which WEP key is used (#1–#4).
 - **Authentication type** – Select *Open* or *Shared*. Use the *Open* authentication when no authentication is required. The *Shared* authentication verifies that an

authenticating wireless client has the same WEP key as your WLAN access point.



- **WEP key settings** – The remaining settings are defined here:
 - WEP encryption** – Select the desired WEP encryption key length. Supported options are 64 and 128 bits. The more bits there are in the key, the higher the level of security. WEP keys consist of a secret key and a 24-bit initialisation vector. For example, some manufacturers refer to the 104-bit key as a 128-bit key (104+24). Both keys offer the same level of encryption and are therefore interoperable.
 - WEP key format** – Select whether you want to enter the WEP key data in *Hexadecimal* format or in text format (*ASCII*). It is important that the same notation is used both in the access point and the Nokia E90 Communicator.

WEP key – Enter the WEP key data. The number of characters you can enter depends on the key length you have chosen.



Note: Wired equivalent privacy (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. When WEP security mode is in use, if your device receives a data packet not encrypted with the WEP keys, the data is discarded. In an Ad-hoc network, all devices must use the same WEP key.

- 5 After setting up a basic Internet access point for *Wireless LAN*, select *Back* to save the settings of your ad hoc IAP and exit, or *Options* > *Advanced settings* to define the following advanced settings:
 - **IPv4 settings** – Enter the device IP and name server addresses for IPv4 Internet protocol.

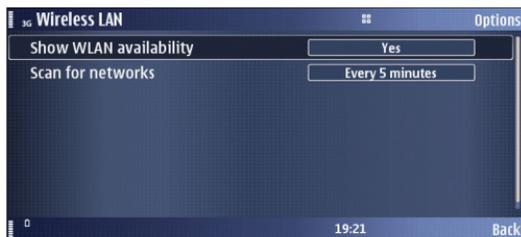
- *IPv6 settings* – Select or enter the name server addresses for IPv6 Internet protocol.
- *Ad-hoc channel* – Select *User defined* to manually enter a channel number (1–11).
- *Proxy server address* – Enter the proxy server address.
- *Proxy port number* – Enter the proxy server port number. Proxy servers are intermediate servers between a browsing service and its users, which are used by some service providers. These servers may provide additional security and speed up access to the service.



Note: The settings available for editing may vary. Contact your service provider for more information.

Defining other WLAN settings

To access the other WLAN settings, select  > *Tools* > *Settings* > *Connection* > *Wireless LAN*.



- 1 In *Show WLAN availability*, select whether the device should show WLAN availability (*Yes* or *Never*). If background scanning is enabled (*Yes*), the device will detect the availability of WLAN automatically. Various applications can use this information to know when a WLAN network is available. The availability of a WLAN network will be indicated in the user interface with an icon in the top right corner of the screen. If background scanning is disabled (*Never*), then WLAN networks will only be scanned for when an application is establishing a connection to the Internet.
- 2 If *Show WLAN availability* is set to *Yes*, set *Scan for networks* to the desired value (*Every minute*, *Every 2 minutes*, *Every 5 minutes*, *Every 10 minutes*).
- 3 Press *Back* to save the settings.



Note: Selecting *Never* for *Show WLAN availability* reduces battery consumption.

Establishing a WLAN connection

This chapter describes how you can establish a WLAN connection. It uses a Web browser connection as an example, but other kinds of WLAN connections, such as an ad hoc connection to your printer, work the same way.

To establish a WLAN connection:

- 1 Make sure you have a valid user name and password for the network and that you have created a WLAN IAP as described in "Creating a WLAN Internet Access Point for a WLAN access point".
- 2 Switch on your Nokia E90 Communicator.
- 3 Select  > *Web*.
- 4 Enter the URL of the Web page that you want to visit, and press *Go to*.
- 5 If necessary, select the IAP you created previously, or select *Search for WLAN* to select from all available WLANs.
- 6 When your browser is redirected to the authentication page, enter your user name and password.
You can now use the connection just like any other connection. If you experience problems with the WLAN connection, make sure that you are within the range of the access point.
- 7 When you are finished, press *Options* > *Exit* to close the connection and the browser.
To close the connection, but leave the browser open, *Options* > *Advanced options* > *Disconnect*.

Viewing the status of a WLAN connection

To view the status of your active WLAN connection, select

 > *Connectivity* > *Conn. mgr.* > *Active data connections.*



- 1 Select the network from the list and then select *Options* > *Details* to see the connection status, network name, signal strength, network mode, connection security, TX power, amount of sent and received data, and the duration and speed of the selected active connection.

Press *OK* to close the *Details* view and *Back* to return to *Conn. mgr.*

- 2 Select *Available WLAN networks* to view all WLAN networks that can be accessed and their signal strength. You can select *Options* > *Details* to view their details as described above.
Select *Options* > *Reload* to refresh the list.



Tip: You can use the Log application to find out information about past connections. Select

 > *Log* to start it.

WLAN troubleshooting

Some common problems that may occur when using WLAN are discussed in this section.

- **Wrong proxy settings:** if you cannot browse the Web even though the WLAN connection is working and the IP settings seem to be correct, check that the HTTP/HTTPS proxy settings are defined correctly in the advanced settings of your WLAN access point.
- **Problems with the WEP security mode:** if you encounter these, check that the WEP keys have been entered in the correct format (ASCII vs. HEX) and have the right number of characters. ASCII WEP keys are also case sensitive; check that you have not confused any upper or lower case letters in the key. Incorrect WEP keys may cause a situation where Nokia E90 Communicator is able to associate with a WLAN network but no data can be transferred. Also remember to check that the WEP authentication mode is correct. In the access point it may be called, for example, "WEP authentication", "shared-key authentication" or "Wi-Fi security mode".
- **Poor signal quality:** to check the signal quality of your WLAN connection, select  > [Connectivity](#) > [Conn. mgr.](#) > [Active data connections](#) > [Options](#) > [Details](#). If the signal quality is weak or even moderate, you may encounter connection problems. Try again nearer the access point.
- **Wrong security mode:** it is possible that you have configured the security mode correctly, but it may not be the right mode. To check the security mode that the network uses, select  > [Connectivity](#) > [Conn. mgr.](#) > [Active data connections](#) > [Options](#) > [Details](#).
- **Problems with the WPA/WPA2 or 802.1x security mode:** if you encounter these, check the following:
 - 1 Check that the WPA mode is the right one (pre-shared key or EAP).
 - 2 Check the pre-shared key.
 - 3 Check that all EAP types that are not needed are disabled.
 - 4 Check that EAP type settings are correct (passwords, user names, certificates, etc.).
- **Problems with access point configuration:** if you encounter these, check the following:
 - 1 Many WLAN access points contain proprietary "Turbo" mode's claiming to enhance data rates. These functionalities should be disabled from the IAP if there is any reason to believe that they are causing problems to legacy WLAN terminals.
 - 2 Many interoperability problems are solved by updating the IAP firmware to the latest version.
- **Not all channels are available:** if you use the device in the offline mode or in the USA, only channels 1–11 are available. Channels 1–13 are available in Europe.

- **Finally...:** remember that all Wi-Fi certified devices are unfortunately not compatible, even if they are supposed to be.