

Honeywell WLAN Secure Wireless Client (SWC)

Для следующих терминалов:

Dolphin™ 6000 с ОС Windows® Mobile 6.5

Dolphin™ 6100/6500 с ОС Windows® CE 5.0

Dolphin™ 6100/6500 с ОС Windows® Embedded
Handheld 6.5

Dolphin™ 7600 с ОС Windows® CE 5.0

Dolphin™ 7600 с ОС Windows Mobile® 6

Dolphin™ 7850 с ОС Windows Mobile® 5.0

Dolphin™ 9700 с ОС Windows Mobile® 6.5

Dolphin™ 9900 с ОС Windows Mobile® 6.1

Dolphin™ 99EX с ОС Windows® Embedded
Handheld 6.5

Руководство пользователя

Отказ от ответственности

Корпорация Honeywell International (далее – «НИ») оставляет за собой право на внесение изменений в характеристики и другую информацию, содержащуюся в данном документе, без предварительного уведомления. Чтобы узнать о внесении таких изменений необходимо во всех случаях обращаться с соответствующим запросом в НИ. Информация, содержащаяся в данной публикации, не выражает каких-либо обязательств со стороны НИ.

НИ не несет ответственности за технические и редакторские ошибки в настоящем документе, а также за любые случайные или воследовавшие убытки, связанные с содержанием, описанными характеристиками или использованием данного материала.

Этот документ содержит информацию, защищенную авторским правом. Все права защищены. Запрещено копирование, воспроизведение или перевод на другой язык любой части этого документа без предварительного письменного согласия со стороны НИ.

Интернет: www.honeywellaidc.com

Товарные знаки

Dolphin, Dolphin RF, HomeBase, Mobile Base и QuadCharger являются товарными знаками или зарегистрированными товарными знаками корпорации Hand Held Products или корпорации Honeywell International.

Microsoft, Windows, Windows Mobile, Windows CE, Windows NT, Windows 2000, Windows ME, Windows XP, ActiveSync, Outlook и логотип Windows являются товарными знаками или зарегистрированными товарными знаками корпорации Microsoft.

Другие названия продуктов, упомянутые в настоящем документе, могут являться товарными знаками или зарегистрированными товарными знаками соответствующих компаний и являются собственностью соответствующих владельцев.

Патенты

Информация о патентах приведена по адресу www.honeywellaidc.com/patents.

© Honeywell International, 2007–2011 гг. Все права защищены.

Содержание

Глава 1. Настройка подключения к беспроводной локальной сети

Введение.....	1-1
Доступ к WLAN SWC	1-1
Цвета значка на панели команд.....	1-2
Индикатор состояния соединения	1-2
Включение драйвера радиосистемы WLAN.....	1-3
Установление соединения.....	1-3
Вкладка «Config» (Конфигурация)	1-6
Активация конфигурации.....	1-6
Вкладка «Config» (Конфигурация)	1-6
Использование функции поиска.....	1-7
Окно «Network» (Сеть).....	1-8
Режимы привязки	1-9
Общие конфигурации.....	1-13
WEP	1-13
PEAPv1-MSCHAPV2.....	1-14
WPA-PSK.....	1-14
Статический IP-адрес.....	1-15
Вкладка «Status» (Состояние).....	1-16

Глава 2. Работа в режиме прямого подключения

Введение.....	2-1
Требования	2-1
Выполнение прямого подключения	2-1

Глава 3. Настройка приложения WLAN SWC с помощью файла DeviceConfig

Обзор.....	3-1
Редактирование файла DeviceConfig.exm	3-1
Настройка терминала	3-2
Выбор профиля	3-2
Изменение режима энергосбережения	3-3

Глава 4. Инструменты для администрирования

Обзор.....	4-1
Вкладка «IP»	4-1

Вкладка «Advanced» (Дополнительно)	4-2
STATUS (Состояние)	4-3
STATUS_VERBOSE (Состояние подробно).....	4-3
SCAN (Поиск)	4-3
SCAN_RESULTS (Результаты поиска).....	4-3
LIST_NETWORKS (Список сетей).....	4-4
SELECT_NETWORK (Выбор сети)	4-4
ENABLE_NETWORK (Включить сеть)	4-4
REMOVE_NETWORK (Удалить сеть)	4-4
SAVE_CONFIG (Сохранить конфигурацию)	4-4
DISCONNECT (Разъединить).....	4-4
REASSOCIATE (Повторить привязку)	4-4
DHCP release (Освободить адрес DHCP)	4-4
DHCP renew (Обновить адрес DHCP)	4-4
DEBUG on (Включить режим отладки)	4-4
DEBUG off (Отключить режим отладки)	4-4
Техническая поддержка	5-1
Техническая поддержка через Интернет	5-1

Настройка подключения к беспроводной локальной сети

Введение

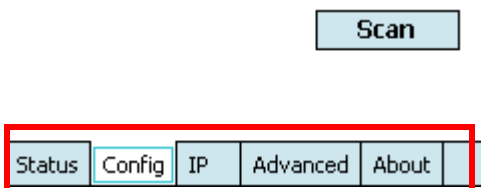
Примечание. Копии экранов и значки, приведенные в данном руководстве пользователя, могут отличаться от изображений на экране устройства.

Приложение WLAN Secure Wireless Client (SWC) настраивает беспроводное подключение радиосистемы 802.11b/g для различных терминалов Dolphin.

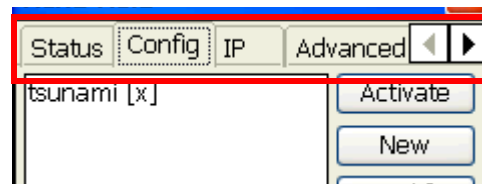
OC Windows Mobile 6.5	OC Windows Mobile 6	OC Windows Mobile 5.0	OC Windows CE 5.0	OC Windows Embedded Handheld 6.5
Dolphin 9700	Dolphin 7600	Dolphin 7850	Dolphin 7600	Dolphin 99EX
Dolphin 6000	Dolphin 9900		Dolphin 6100	Dolphin 6100
			Dolphin 6500	Dolphin 6500

В различных операционных системах окна приложения SWC выглядят по-разному. Например, на терминалах, работающих под управлением OC Windows CE, вкладки отображаются в верхней части окна, а на терминалах, работающих под управлением OC Windows Mobile — в нижней части окна.

Windows Mobile



Windows CE




Независимо от внешнего оформления содержимое окон одинаково на обоих терминалах.

IP-адреса, назначаемые сервером

Следует учитывать, что для всех назначаемых сервером IP-адресов используется протокол динамической настройки конфигурации узлов (DHCP).

Доступ к WLAN SWC

На панели команд экрана «Today» (Сегодня) нажмите значок .







Этот значок может менять цвет в зависимости от состояния радиосистемы (см. [Цвета значка на панели команд](#) на стр. 1-2.).

При запуске SWC на экране отображается вкладка «Status» (Состояние); до настройки подключения эта вкладка остается пустой. После подключения к точке доступа и если сеть настроена и активна, на этой вкладке отображается состояние подключения.

Цвета значка на панели команд

Цвет значка  на панели команд экрана «Today» (Сегодня) меняется в зависимости от состояния радиосистемы.

Цвет	Значение	Соответствующее состояние
Серый 	Радиосистема: <ul style="list-style-type: none">отключенанаходится в режиме ожиданияне подключена	NO RADIO (Радиосистема отсутствует) RADIO OFF (Радиосистема выключена) DISCONNECTED (Соединение разорвано) INACTIVE (Не активна)
Желтый 	Состояние подключения: <ul style="list-style-type: none">Привязка (значок прекращает вращение)Аутентификация (значок прекращает вращение)Согласование адреса по DHCP (значок вращается по часовой стрелке)За пределами зоны действия сети	ASSOCIATING (Привязка) AUTHENTICATING (Аутентификация)
Красный 	Аутентификация не выполнена, поэтому соединение не установлено.	ASSOCIATED (Привязка выполнена) (но без аутентификации)
Зеленый 	Подключение аутентифицировано и использует действующий DHCP-адрес.	COMPLETE (Готово)

Примечание. Цвет значков соответствует состоянию, для отображения которого используется Вкладка «Status» (Состояние) (см. стр. 1-16).

Индикатор состояния соединения

На панели команд размещен индикатор уровня сигнала.



Полоски отражают уровень сигнала. когда радиосистема находится в режиме передачи. Если радиосистема не передает сигнал, над полосками отображается небольшой символ «X».

Включение драйвера радиосистемы WLAN

Чтобы радиосистема могла передавать сигнал, необходимо включить драйвер радиосистемы. Если радиосистема не включена, подключение к сети невозможно.

Конфигурация терминала	Необходимые действия
Dolphin 6100/6500/7600 с ОС Windows CE 5.0	Нажмите направленную вверх стрелку в правом нижнем углу экрана.
Dolphin 6000 с ОС Windows Mobile 6.5 Dolphin 6100 с ОС Windows Embedded Handheld 6.5 Dolphin 6500 с ОС Windows Embedded Handheld 6.5 Dolphin 7600 с ОС Windows Mobile 6 Dolphin 9900 с ОС Windows Mobile 6.1 Dolphin 9700 с ОС Windows Mobile 6.5 Dolphin 99EX с ОС Windows Embedded Handheld 6.5	Выберите Start (Пуск) > Settings (Параметры) > вкладка Connections (Подключения) > Dolphin Wireless Manager.
Dolphin 7850	Выберите Start (Пуск) > Settings (Параметры) > вкладка Connections (Подключения) > Radio Manager.


Для получения сведений о включении и отключении радиосистемы на конкретном терминале, обратитесь к руководству пользователя соответствующего терминала, которое можно загрузить по адресу: www.honeywellaidc.com.

Установка соединения

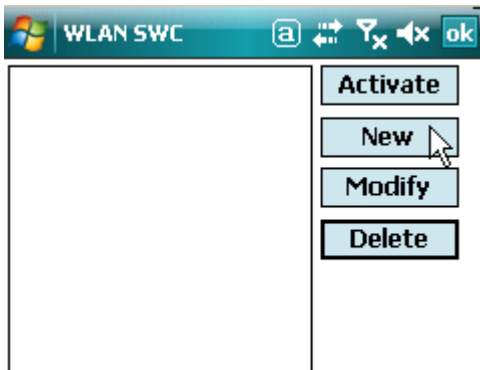
Требования



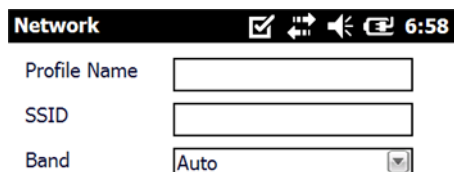
Значения параметров, устанавливаемые в SWC, полностью зависят от используемой на предприятии беспроводной сети. Если вы не знаете, что ввести в описанные ниже поля, обратитесь к администратору сети.

1. При отображении экрана «Today» (Сегодня) или рабочего стола нажмите на панели команд значок .

- Выберите вкладку **Config** (Конфигурация) и нажмите **New** (Создать).



- Вы можете создать несколько профилей, которые используют один и тот же SSID, задав каждому профилю уникальное имя в поле «Profile Name» (Имя профиля) в окне «Network» (Сеть).



- Введите **SSID**.
- Выберите определенный диапазон, если соединение должно быть ограничено стандартами b/g/n или a/n (2,4 ГГц или 5,0 ГГц).
- Из раскрывающегося списка **Assoc. Mode** выберите режим привязки, который соответствует конфигурации сети.

Режим	Особенности подключения	Дополнительная информация
Нет	Без аутентификации или шифрования.	Вариант «None» (Нет) (стр. 1-9)
WEP	Шифрование с использованием алгоритма WEP.	WEP (стр. 1-11)
IEEE 802.1X (WEP)	Аутентификация по протоколу EAP.	IEEE 802.1X (WEP) (стр. 1-9)
WPA-Personal (PSK) WPA2-Personal (PSK)	Шифрование WPA и аутентификация PSK.	WPA-Personal (PSK) и WPA2-Personal (PSK) (стр. 1-11)
WPA-Enterprise (EAP) WPA2-Enterprise (EAP)	Шифрование WPA и аутентификация EAP.	WPA-Enterprise (EAP) и WPA2-Enterprise (EAP) (стр. 1-12)

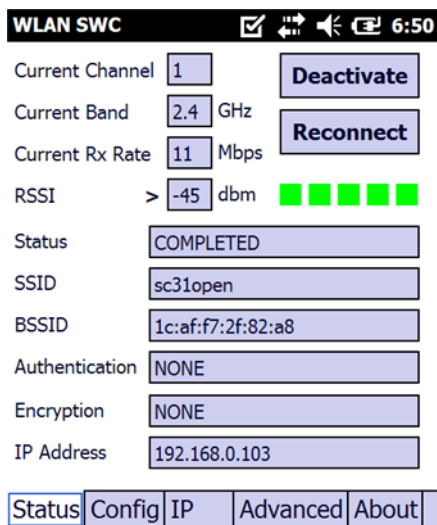
Примечание. Терминал Dolphin 7600 с ОС Windows CE 5.0 не поддерживает методы EAP.

- Для отображения полей и параметров, требуемых для выбранного режима привязки, шифрования и методов EAP, используется **Окно «Network» (Сеть)** (см. стр. 1-8).

8. Если это предусмотрено для данного режима привязки, выберите метод шифрования (**Encryption**).
9. Если это предусмотрено для данного режима привязки, выберите метод аутентификации (**EAP Method**) (см. стр. 1-9).
10. Если необходимо или по желанию, введите ключи и пароли.
11. Нажмите **OK**. На экране снова отображается вкладка «Config» (Конфигурация), где в списке отображается введенный SSID.
12. Выберите устройство из списка и нажмите **Activate** (Активировать). Выполняется активация конфигурации и терминал Dolphin предпринимает попытку подключиться к сети с использованием заданных параметров.

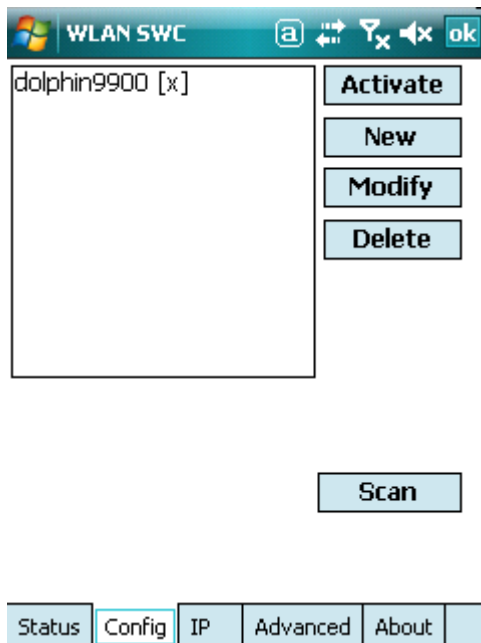


13. На экране отображается вкладка «Status» (Состояние) с информацией о состоянии соединения.



Вкладка «Config» (Конфигурация)

Вкладка «Config» предназначена для управления соединениями и конфигурациями. Здесь задается конфигурация, которую использует терминал для подключения к сети.



Активация конфигурации

Для подключения к сети **необходимо** выбрать конфигурацию из списка и нажать кнопку **Activate** (Активировать). Терминал не будет выполнять подключение к сети до нажатия кнопки **Activate**.

На вкладке «Config» показан список, содержащий все созданные конфигурации, но активировать можно только одну из них. Для выбора другого подключения просто выберите нужное подключение из списка на вкладке «Config» и нажмите кнопку **Activate**.

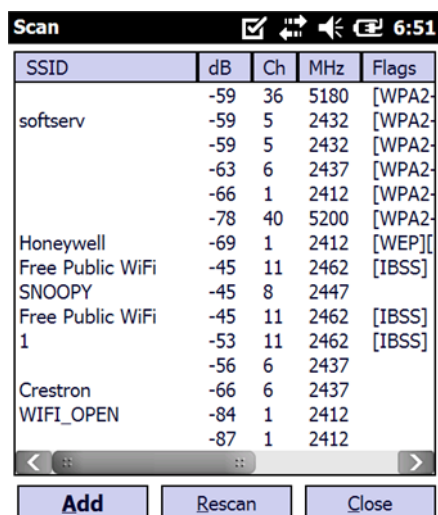
Рядом с активированной конфигурацией на вкладке «Config» отображается символ [x].

Кнопки на вкладке «Config» (Конфигурация)

- Modify** (Изменить) Для изменения существующей конфигурации выберите ее в списке и нажмите кнопку **Modify**. Отображается окно «Network» (Сеть) с данными выбранной конфигурации. Внесите требуемые изменения и нажмите **OK** для их сохранения. Затем для установления соединения нажмите кнопку **Activate** (Активировать).
- Add** (Добавить) Чтобы вручную добавить подключение, нажмите кнопку **Add**. На экране отображается пустое окно «Network» (Сеть). Выполните шаги 5–8 раздела [Установка соединения](#) (см. стр. 1-3).
- Delete** (Удалить) Для удаления подключения выберите его в списке и нажмите кнопку **Delete**.

Использование функции поиска

С помощью кнопки «Scan» (Поиск) на вкладке «Config» (Конфигурация) осуществляется поиск местных настроенных беспроводных сетей, в зоне действия которых находится терминал. Нажатие кнопки **Scan** запускает процедуру поиска, результаты которого отображаются в окне «Scan» (Поиск).



SSID	dB	Ch	MHz	Flags
	-59	36	5180	[WPA2-PSK]
softserv	-59	5	2432	[WPA2-PSK]
	-59	5	2432	[WPA2-PSK]
	-63	6	2437	[WPA2-PSK]
	-66	1	2412	[WPA2-PSK]
	-78	40	5200	[WPA2-PSK]
Honeywell	-69	1	2412	[WEP][TKIP]
Free Public WiFi	-45	11	2462	[IBSS]
SNOOPY	-45	8	2447	
Free Public WiFi	-45	11	2462	[IBSS]
1	-53	11	2462	[IBSS]
	-56	6	2437	
Crestron	-66	6	2437	
WIFI_OPEN	-84	1	2412	
	-87	1	2412	

Кнопки

Add (Добавить) Нажмите эту кнопку после выбора нужного элемента в списке. Открывается [Окно «Network» \(Сеть\)](#) (см. стр. 1-8), которое позволяет настроить подключение.

Rescan (Повторить поиск) Нажмите эту кнопку, чтобы повторить поиск беспроводной сети, если в списке отсутствует искомая точка доступа.

Close (Закреть) Нажмите эту кнопку, чтобы закрыть окно «Scan» (Поиск) и вернуться на вкладку «Config».

Столбцы

SSID Отображает идентификатор SSID точки доступа (это имя точки доступа к которой выполняется подключение).

db Отображает уровень сигнала в дБм.

Ch Отображает номер используемого канала.

MHz Отображает рабочую частоту в МГц.

Flags (Флаги) Отображает режим привязки и алгоритм шифрования для подключения устройства.

BSSID Отображает полный идентификатор BSSID (это MAC-адрес точки доступа).

Окно «Network» (Сеть)

Окно «Network» содержит параметры конфигурации, определяющие подключение терминала к беспроводной сети.

Для доступа к окну «Network» используется Вкладка «Config» (Конфигурация) (см. стр. 1-6). Чтобы открыть это окно:

- нажмите кнопку **New** (Создать) на вкладке «Config»;
- выполните поиск устройств, предоставляющих доступ к беспроводной сети, и добавьте их в свою сеть; см. [Использование функции поиска](#) на стр. 1-7.
- выберите существующую конфигурацию и нажмите кнопку **Modify** (Изменить).

В окне «Network» следует заполнить поля, определяемые выбранными параметрами подключения. Например:

Без аутентификации или шифрования

Network 6:58

Profile Name

SSID

Band

Assoc Mode

Network Id

WPA (EAP)

Network 7:01

Profile Name

SSID

Band

Assoc Mode

Network Id

Encryption

EAP Method

Identity

Password

Prompt Id/Passwd When Connecting

Anony ID

Identity

Password

Prompt Id/Passwd When Connecting

Anony ID

File Store Cert Store

CA Cert.

Tunnel PAC

Machine PAC

Provisioning

WEP

Network 7:01

Profile Name

SSID

Band

Assoc Mode

Network Id

Encryption

Key Length 64 bits 128 bits

Key Type ASCII HEX

Key 1

Key 2

Используйте кнопку **Browse** (Обзор) для загрузки в эту конфигурацию файлов, хранящихся на терминале.

Режимы привязки

Режим привязки, выбранный из раскрывающегося списка «Assoc. Mode», определяет поля, отображающиеся в окне «Network» (Сеть). Разные режимы привязки требуют ввода разной информации или предлагают определенные параметры конфигурации.

Доступные режимы привязки:

- [Вариант «None» \(Нет\)](#) (см. стр. 1-9)
- [WEP](#) (см. стр. 1-11)
- [IEEE 802.1X \(WEP\)](#) (см. стр. 1-9)
- [WPA-Personal \(PSK\)](#) и [WPA2-Personal \(PSK\)](#) (см. стр. 1-11)
- [WPA-Enterprise \(EAP\)](#) и [WPA2-Enterprise \(EAP\)](#) (см. стр. 1-12)

Примечание. Терминал Dolphin 7600 с ОС Windows CE 5.0 не поддерживает методы EAP.

Вариант «None» (Нет)

Выбор для режима привязки варианта **None** означает, что в процессе подключения не используется аутентификация или шифрование.

IEEE 802.1X (WEP)

Доступные методы EAP

[IEEE 802.1X \(WEP\)](#) (стр. 1-9) и [WPA-Enterprise \(EAP\)](#) и [WPA2-Enterprise \(EAP\)](#) (стр. 1-12) поддерживают следующие методы EAP:

- LEAP
- PEAPv0-MSCHAPV2
- PEAPv1-MSCHAPV2
- PEAPv1-GTC
- PEAPv1-TLS
- FAST-MSCHAPV2
- FAST-GTC
- FAST-TLS
- TLS
- TTLS-MD5
- TTLS-MSCHAPV2
- TTLS-GTC

Заполнение полей EAP

В зависимости от выбранного метода EAP могут отображаться следующие поля (отображение тех или иных полей зависит от того, что требует или что предлагает выбранный протокол для конфигурации):

Поле	Описание
Identity (Идентификационный код)	Это идентификационный код, предусмотренный стандартом 802.1X и предоставляемый аутентификатору. Идентификационный код может содержать до 63 ASCII-символов (с учетом регистра).

Поле	Описание
Password (Пароль)	Это пароль, используемый для запроса MD5 или аутентификации EAP. Пароль может содержать до 63 ASCII-символов (с учетом регистра). В целях дополнительной защиты вместо символов пароля на экране отображаются звездочки.
Anonymous ID (Анонимный идентификатор)	Введите в это поле анонимный идентификатор. Этот идентификатор используется для создания туннеля, через который передается реальный идентификатор (введенный в поле «Identity»). В целях дополнительной защиты в это поле рекомендуется вводить код, отличающийся от кода в поле «Identity».
File Store (В файле) Cert Store (В хранилище сертификатов)	Нажмите одну из этих кнопок, чтобы выбрать место хранения сертификата(-ов). Например, если сертификат хранится в папке IPSM или на SD-карте в виде файла, выберите File Store . Если сертификат помещен в хранилище сертификатов Windows данного устройства, выберите Cert Store .
CA Cert. (Сертификат СО) и Client Cert. (Клиентский сертификат) CA Cert. <input type="text"/> Client Cert. <input type="text"/>	Нажмите кнопку Browse (Обзор) <input type="button" value="..."/> для загрузки сертификата сертифицирующего органа (СО) или клиентского сертификата, хранящегося на терминале. <ul style="list-style-type: none"> Сертификаты СО — это любые сертификаты, выпущенные сертифицирующим органом. Клиентские сертификаты содержат информацию, идентифицирующую пользователя, а также сведения об организации, выпустившей сертификат. Это обеспечивает полномасштабное шифрование данных.
Private Key (Закрытый ключ) Private Key <input type="text"/>	Нажмите кнопку Browse (Обзор) <input type="button" value="..."/> для загрузки закрытого ключа, хранящегося на терминале.
Priv Key Pass (Пароль закрытого ключа)	Если загружен закрытый ключ, введите пароль, который разблокирует этот закрытый ключ.
Tunnel PAC (PAC туннеля) и/или Machine PAC (PAC машины)	Нажмите кнопку Browse (Обзор) <input type="button" value="..."/> для загрузки PAC-ключа туннеля или машины, хранящегося на терминале. <i>Примечание.</i> При использовании метода EAP-FAST выполняется однократный регистрационный обмен данными, в результате которого формируется общий секретный код, называемый ключом PAC (ключом удостоверения защищенного доступа). Этот PAC-ключ используется во всех последующих сеансах аутентификации.
Provisioning (Подготовка)	Подготовка включает в себя активацию службы и занесение в различные базы данных информации заказчика. Выберите один из следующих методов подготовки: <ul style="list-style-type: none"> Без подготовки Анонимно С аутентификацией Анонимно с аутентификацией

WEP

Если в качестве режима привязки выбран WEP, можно выбрать открытое или общее шифрование (**Encryption**) и ввести свои ключи.

The screenshot shows a 'Network' configuration dialog box. The 'Assoc Mode' is set to 'WEP'. The 'Encryption' is set to 'OPEN'. Under 'Key Length', '64 bits' is selected. Under 'Key Type', 'ASCII' is selected. There are two input fields for 'Key 1' and 'Key 2', both of which are currently empty.

WPA-Personal (PSK) и WPA2-Personal (PSK)

The screenshot shows a 'Network' configuration dialog box. The 'Assoc Mode' is set to 'WPA-Personal (PSK)'. The 'Encryption' is set to 'TKIP'. There is one input field for 'PSK', which is currently empty. Below the 'PSK' field, there is a note: 'Use 8 to 63 chars for ASCII or 64 digits for HEX'. At the bottom of the dialog, there are 'OK' and 'Cancel' buttons.

Поддерживаемые методы шифрования

- TKIP
- AES-CCMP
- TKIP+CCMP

PSK (предварительно согласованный ключ)

В поле PSK следует ввести предварительно согласованный ключ. В это поле можно ввести код, включающий от 8 до 63 ASCII-символов. Вместо ASCII-ключа также можно использовать шестнадцатеричный ключ PSK. Шестнадцатеричные ключи PSK должны иметь длину строго 64 символа и могут содержать только шестнадцатеричные цифры (A–F, 0–9).

При первом вводе данных в это поле вводимые символы отображаются на экране, но когда эта конфигурация будет открыта в следующий раз, символы будут заменены звездочками (*).

Секретные пароли или ключи шифрования вводятся обеими сторонами информационного обмена заранее. Предварительно согласованные ключи (PSK) вводятся на клиентах и на серверах (серверы аутентификации, точки доступа и пр.).

WPA-Enterprise (EAP) и WPA2-Enterprise (EAP)

The screenshot shows a network configuration interface with the following fields and options:

- Profile Name: [Text Input]
- SSID: [Text Input]
- Band: [Auto] (Dropdown)
- Assoc Mode: [WPA-Enterprise (EAP)] (Dropdown)
- Network Id: [Text Input]
- Encryption: [TKIP] (Dropdown)
- EAP Method: [FAST-MSCHAPV2] (Dropdown)
- Identity: [Text Input]
- Password: [Text Input]
- Prompt Id/Passwd When Connecting
- Anony ID: [Text Input]

Примечание. Терминал Dolphin 7600 с ОС Windows CE 5.0 не поддерживает методы EAP.

Поддерживаемые методы шифрования

- TKIP
- AES-CCMP
- TKIP+CCMP

Доступные методы EAP

Поддерживаются следующие методы EAP:

- LEAP
- PEAPv0-MSCHAPV2
- PEAPv1-MSCHAPV2
- PEAPv1-GTC
- PEAPv1-TLS
- FAST-MSCHAPV2
- FAST-GTC
- FAST-TLS
- TLS
- TTLS-MD5
- TTLS-MSCHAPV2
- TTLS-GTC

Более подробная информация: см. [Заполнение полей EAP](#) на стр. 1-9.

Если установлен флажок, расположенный ниже поля «Password» (Пароль), то при каждой попытке подключения пользователю предлагается ввести SSID и пароль.


Общие конфигурации

В этом разделе подробно рассмотрены некоторые наиболее распространенные конфигурации сетей, включая:

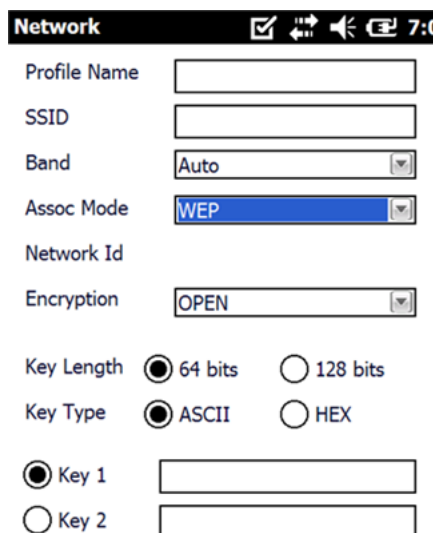
- [WEP](#) (см. стр. 1-13)
- [PEAPv1-MSCHAPV2](#) (см. стр. 1-14)
- [WPA-PSK](#) (см. стр. 1-14)

WEP

Если в качестве режима привязки выбран WEP, можно выбрать открытое (Open) или общее (Shared) шифрование для аутентификации с помощью определенного ключа.

1. На панели команд экрана «Today» (Сегодня) нажмите значок .
2. Выберите вкладку **Config** (Конфигурация).
3. Нажмите **New** (Создать).
4. В окне «Network» (Сеть) введите **SSID**.
5. В качестве режима привязки (**Assoc. Mode**) выберите **WEP**.
6. Можно выбрать один из следующих методов шифрования (**Encryption**):

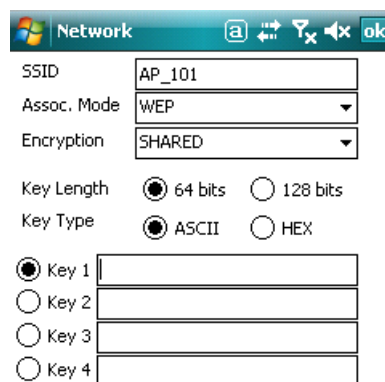
Encryption=OPEN (открытое)



The screenshot shows the 'Network' configuration window with the following settings:

- Profile Name: []
- SSID: []
- Band: Auto
- Assoc Mode: WEP
- Network Id: []
- Encryption: OPEN
- Key Length: 64 bits (selected), 128 bits
- Key Type: ASCII (selected), HEX
- Key 1: []
- Key 2: []

Encryption=SHARED (общее)




The screenshot shows the 'Network' configuration window with the following settings:


- SSID: AP_101
- Assoc. Mode: WEP
- Encryption: SHARED
- Key Length: 64 bits (selected), 128 bits
- Key Type: ASCII (selected), HEX
- Key 1: []
- Key 2: []
- Key 3: []
- Key 4: []

- В поля **Key 1—Key 4** (Ключ 1—Ключ 4), введите ключ. Формат каждого ключа *должен учитывать* длину (Key Length) и тип (Key Type) ключа, выбранные на шаге 6. SWC проверяет длину ключа и не позволяет сохранить ключ в неверном формате.
 - Нажмите **OK**, выполняется возврат на вкладку «Config» (Конфигурация).
7. На вкладке «Config» выберите из списка сеть и нажмите **Activate** (Активировать).
 8. Терминал начнет процедуру подключения.
 9. После установления соединения на экране отображается [Вкладка «Status» \(Состояние\)](#) (стр. 1-16) с результатами.

PEAPv1-MSCHAPV2

1. На панели команд экрана «Today» (Сегодня) нажмите значок .
2. Выберите вкладку **Config** (Конфигурация).
3. Нажмите **New** (Создать).
4. В окне «Network» (Сеть) ведите **SSID**.
5. В качестве режима привязки (**Assoc. Mode**) выберите **IEEE 802.1X (WEP)**.
6. Выберите в качестве метода EAP (**EAP Method**) вариант **PEAPv1-MSCHAPV2**.
7. Введите идентификационный код (**Identity** (см. стр. 1-9)) и пароль (**Password** (см. стр. 1-10)).
8. При необходимости можно также задать анонимный идентификатор (**Anonymous ID** (см. стр. 1-10)) или выбрать тип сертификата — **CA** (Сертифицирующий орган) или **Client** (Клиентский) (см. стр. 1-10).
При выборе PEAPv1-TLS можно также загрузить **Private Key (Закрытый ключ)** (стр. 1-10) и ввести пароль для закрытого ключа.
9. Нажмите **OK**, выполняется возврат на вкладку «Config» (Конфигурация).
10. На вкладке «Config» выберите из списка сеть и нажмите **Activate** (Активировать).
11. Терминал начнет процедуру подключения.
12. После установления соединения на экране отображается вкладка «Status» (Состояние) (см. стр. 1-16) с результатами.

WPA-PSK

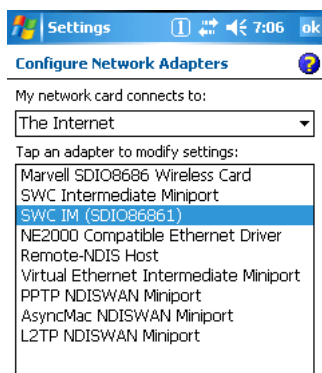
1. На панели команд экрана «Today» (Сегодня) нажмите значок .
2. Выберите вкладку **Config** (Конфигурация).
3. Нажмите **New** (Создать).
4. В окне «Network» (Сеть) ведите **SSID**.
5. В качестве режима привязки (**Assoc. Mode**) выберите **WPA-Personal (PSK)**.
6. Выберите метод шифрования (**Encryption**): TKIP, AES-CCMP или TKIP + CCMP.
7. Введите предварительно согласованный ключ (см. стр. 1-11) в поле **PSK**.
8. Нажмите **OK**, выполняется возврат на вкладку «Config» (Конфигурация).
9. На вкладке «Config» выберите из списка сеть и нажмите **Activate** (Активировать).
10. Терминал начнет процедуру подключения.
11. После установления соединения на экране отображается **Вкладка «Status» (Состояние)** (стр. 1-16) с результатами.

Статический IP-адрес

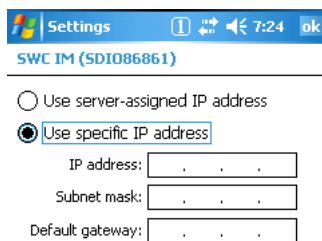
Статический IP-адрес устанавливается не в SWC, а с помощью драйвера радиосистемы. После задания в драйвере радиосистемы статического IP-адреса беспроводное соединение настраивается с помощью программы SWC как обычно.

Установка статического IP-адреса в устройствах с ОС Windows Mobile (7600, 7850, 9700, 9900 и 99EX)

1. Выберите **Start (Пуск) > Settings (Параметры) > вкладка Connections (Подключения) > Network Cards (Сетевые платы)**.



2. Выберите сетевой адаптер. Имя адаптера начинается с «SWC IM», после чего в скобках следует имя драйвера радиосистемы.
3. Открывается вкладка «IP address» (IP-адрес). Выберите вариант **Use specific IP address** (Указать IP-адрес).



- a. Введите значение в поле **IP address** (IP-адрес).
 - b. Введите значение в поле **Subnet mask** (Маска подсети).
 - c. Введите значение в поле **Default gateway** (Шлюз по умолчанию).
4. Нажмите **ОК**.
 5. Откройте программу SWC и настройте беспроводное подключение.

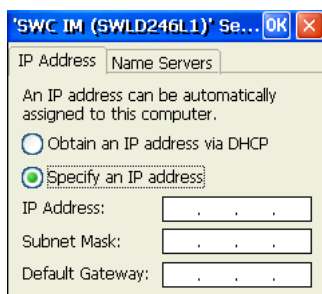
Установка статического IP-адреса в ОС Windows CE 5.0 (6100/6500/7600)

1. Выберите **Start (Пуск) > Control Panel (Панель управления) > Network and Dial-up Connections (Сеть и удаленный доступ к сети)**.

2. Выберите двойным нажатием драйвер радиосистемы.




3. Драйвер радиосистемы открывается, отображая вкладку «IP address» (IP-адрес). Выберите вариант **Specify an IP address** (Указать IP-адрес).

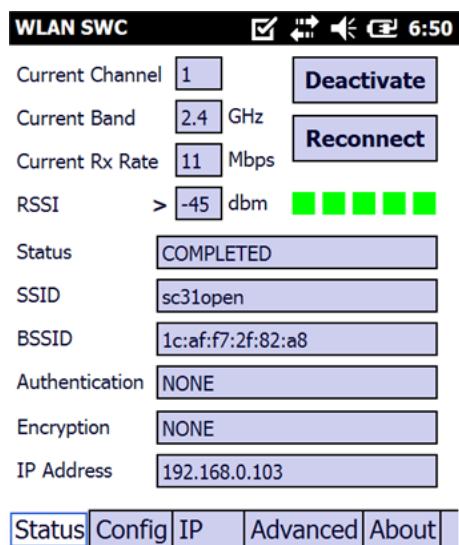


- a. Введите значение в поле **IP address** (IP-адрес).
 - b. Введите значение в поле **Subnet mask** (Маска подсети).
 - c. Введите значение в поле **Default gateway** (Шлюз по умолчанию).
4. Нажмите **OK**.
 5. Откройте программу SWC и настройте беспроводное подключение.

Вкладка «Status» (Состояние)

На вкладке «Status» отображается состояние текущего активного подключения; см. [Активация конфигурации](#) на стр. 1-6.

Если радиосистема включена и активирована требуемая конфигурация, то при нажатии значка  на панели команд экрана «Today» (Сегодня) открывается вкладка «Status» с информацией о текущем состоянии соединения.



Кнопка «Deactivate» (Деактивировать)

При нажатии кнопки «Deactivate» устройство отключается от сети и соответствующий профиль деактивируется.

Кнопка «Reconnect» (Повторное подключение)

Используйте кнопку «Reconnect» для обновления подключения путем предварительного принудительного отключения клиента.

Поле «Status» (Состояние) Status

COMPLETED

NO RADIO (Радиосистема отсутствует)	Программа SWC не распознает драйвер радиосистемы WLAN.
RADIO OFF (Радиосистема выключена)	Радиосистема выключена.
DISCONNECTED (Соединение разорвано)	Радиосистема не подключена к сети.
INACTIVE (Бездействие)	На вкладке «Config» отсутствуют профили или профили не активированы.
ASSOCIATING (Привязка)	Выполняется привязка подключения терминала.
ASSOCIATED (Привязка выполнена)	Подключение терминала привязано к сети.
AUTHENTICATING (Аутентификация)	Выполняется аутентификация.
COMPLETE (Готово)	Подключение привязано, аутентификация завершена успешно, подключение активно.

Поле «BSSID»

Идентификатор BSSID — это MAC-адрес точки доступа.



Работа в режиме прямого подключения

Введение

В настоящее время большинство установленных беспроводных сетей используют режим «инфраструктуры», который требует использования одной или нескольких точек доступа. В такой конфигурации точка доступа предоставляет интерфейс для подключения к системе распределения (например, Ethernet), которая обеспечивает доступ пользователей беспроводных каналов связи к корпоративным серверам и интернет-приложениям.

Однако в качестве дополнительной функции стандарт 802.11 определяет «специальный» режим, который позволяет сетевой плате с радиосистемой работать в сетевой конфигурации с независимым набором базовых услуг (IBSS). При использовании режима IBSS точки доступа не нужны. Пользовательские устройства связываются напрямую, используя модель связи равноправных узлов.


Несмотря на равноправность такого соединения в нем все равно необходимо определить управляющую сторону и сторону клиента; управляющее устройство инициирует прямое подключение, а клиент присоединяется к существующему прямому подключению.

Требования

Оба устройства, участвующие в равноправном соединении, должны иметь статические IP-адреса, кроме того, для них должен быть задан один и тот же шлюз по умолчанию. Кроме того, необходимо настроить статический IP-адрес на терминале (см. [Статический IP-адрес](#) на стр. 1-15).

Выполнение прямого подключения

В программе SWC необходимо настроить профиль прямого подключения.

1. Нажмите значок  на панели команд.
2. Выберите вкладку **Config** (Конфигурация) и нажмите **New** (Создать).
3. В окне «Network» (Сеть) для параметра **Assoc Mode** (Режим привязки) выберите значение **Ad Hoc** или **Ad Hoc (WEP)**.
4. В поле **SSID** введите сетевое имя для подключения.
5. Нажмите **OK**.
6. На вкладке «Config» (Конфигурация) выберите имя профиля (имя SSID) и нажмите **Activate** (Активировать) для выполнения подключения.



Настройка приложения WLAN SWC с помощью файла DeviceConfig

Обзор

Для настройки SWC можно использовать файл DeviceConfig. Для этого достаточно задать в файле DeviceConfig.exm требуемые параметры SWC, сохранить этот файл в папке \IPSM\Autoinstall и выполнить холодную перезагрузку терминала Dolphin. При включении радиосистемы WiFi приложение SWC выполнит подключение в соответствии с параметрами, заданными в файле DeviceConfig.exm.

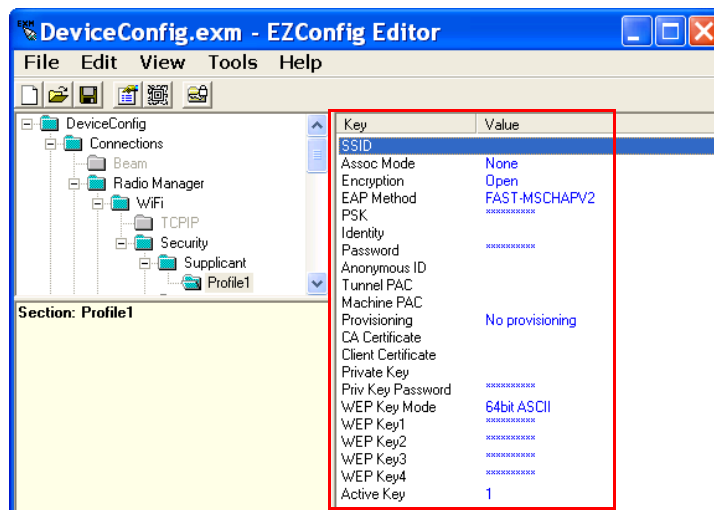
Редактирование файла DeviceConfig.exm

Откройте на своей рабочей станции или терминале файл DeviceConfig.exm, используя программу EZConfig. Описанные ниже инструкции демонстрируют работу с этим файлом на рабочей станции.

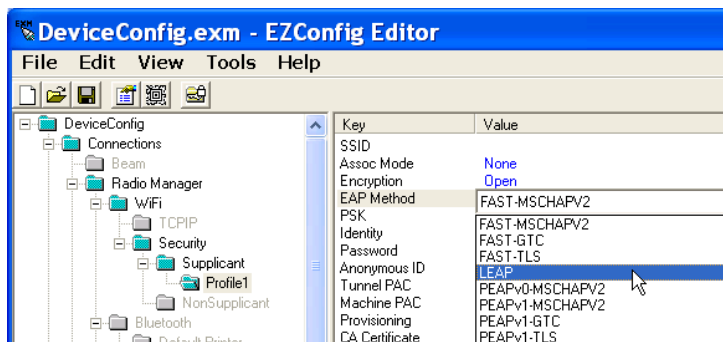
1. Выберите **Start (Пуск) > All Programs (Все программы) > Honeywell > Dolphin Power Tools and Demos (Служебные и демонстрационные программы Dolphin) > EZConfig Editor (Редактор EZConfig)**.



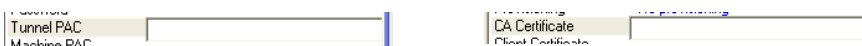
2. Нажмите значок **Open (Открыть)** и выберите файл DeviceConfig.exm.
3. Щелкните правой кнопкой мыши и выберите **Enable (Включить)** для следующих секций: **Radio Manager > WiFi > Security (Безопасность) > Supplicant (Запрашивающее устройство) > Profile 1 (Профиль 1)**.
Секция WiFi отключена по умолчанию. Включение этой секции обеспечивает включение радиосистемы 802.x при запуске устройства.
4. Выберите секцию **Profile 1**.



- Ключи в секции «Profile 1» соответствуют полям, которые содержит Окно «Network» (Сеть) (см. стр. 1-8). Для настройки требуемого ключа дважды нажмите этот ключ и выберите нужный вариант из раскрывающегося списка.



- Пункты каждого раскрывающегося списка соответствуют пунктам в списках, которые содержит Окно «Network» (Сеть) (см. стр. 1-8).
- Выберите или введите все необходимые параметры конфигурации.
 - Для параметров «Tunnel PAC» (PAC-ключ туннеля), «Machine PAC» (PAC-ключ машины), «CA Certificate» (Сертификат сертифицирующего органа) и «Client Certificate» (Клиентский сертификат) введите точный путь, по которому размещены файлы PAC-ключей и сертификатов на данном терминале.



Перед этим файлы PAC-ключей и сертификатов **необходимо сохранить** на этом терминале!


- Если в конфигурации используется алгоритм WEP, выберите тип ключа из раскрывающегося списка.



При вводе ключа в поля «WEP Key1–4» проверка ключа не выполняется, эта проверка производится при активации файла DeviceConfig.exm на терминале.

- Сохраните файл DeviceConfig.exm на рабочей станции для использования в дальнейшем и закройте его.

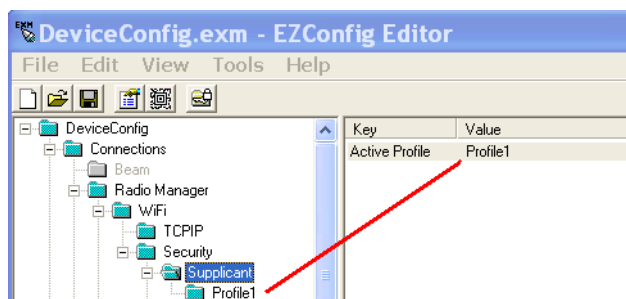
Настройка терминала

- Перенесите файл DeviceConfig.exm с настроенными параметрами в папку \IPSM\Autoinstall на терминале Dolphin.
- Выполните холодную перезагрузку терминала.
- Приложение SWC должно инициировать процедуру подключения с использованием значений параметров, заданных в файле DeviceConfig на этапе автоматической установки.
- После завершения автоматической установки нажмите значок SWC  на экране «Today» (Сегодня).
- Убедитесь, что конфигурация активна и правильна.

Выбор профиля

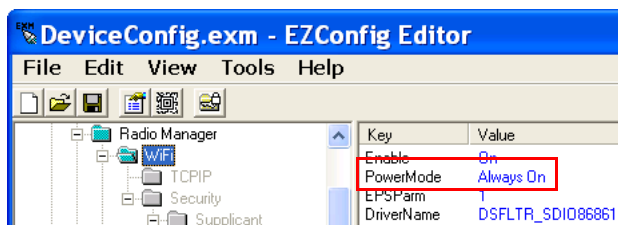
В секции SWC можно хранить несколько профилей, но для использования по умолчанию необходимо выбрать только один из них. Соответствующая профилю конфигурация будет использоваться для подключения при загрузке терминала.

Для выбора конфигурации по умолчанию введите имя профиля в поле **Active Profile** (Активный профиль) в секции **SWC**.



Изменение режима энергосбережения

Режим энергосбережения включен для данной радиосистемы по умолчанию.



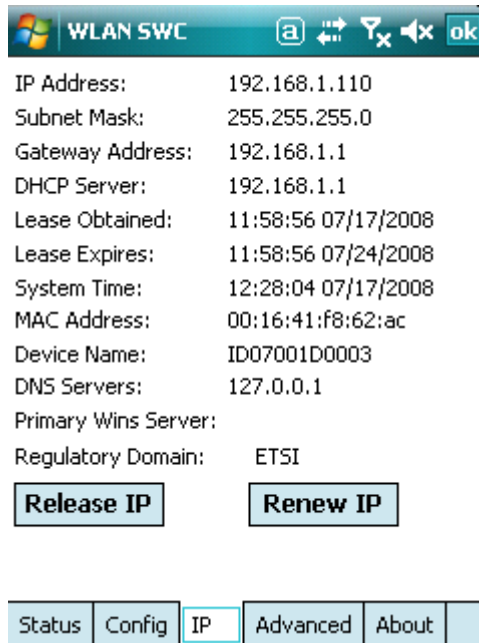


Обзор

Приложение SWC содержит ряд инструментов для администрирования сетевых конфигураций.

Вкладка «IP»

Вкладка «IP» позволяет просматривать статистику о работе терминала и активного сетевого подключения.

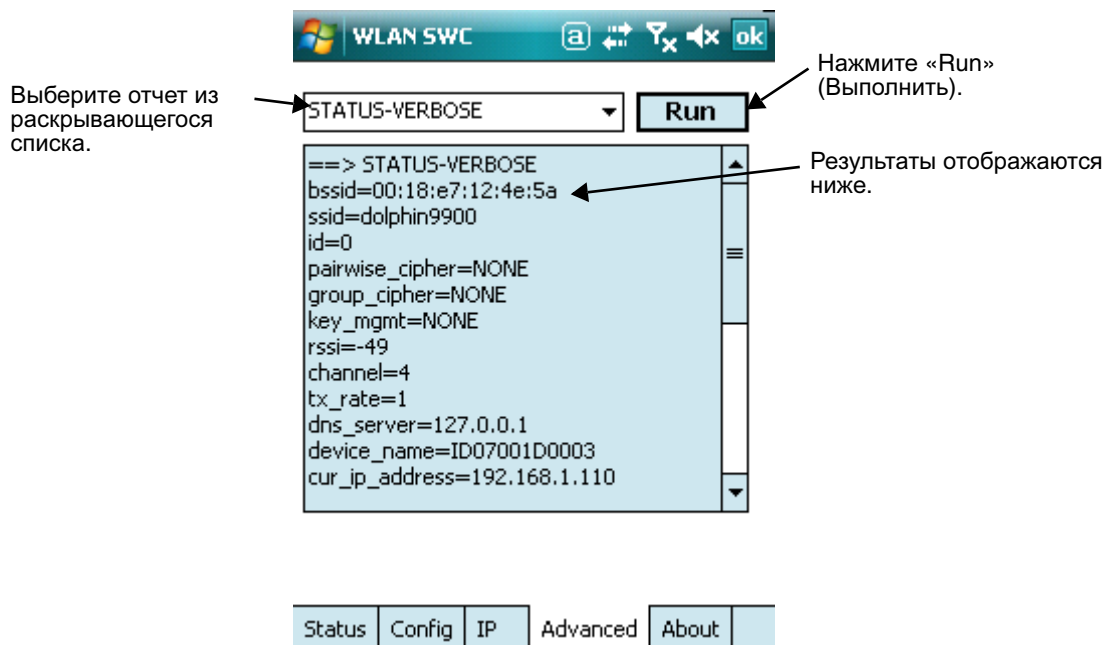


Кнопка «Release IP» (Освободить IP-адрес) Нажмите эту кнопку для освобождения используемого IP-адреса (обычно назначенного DHCP-сервером).

Кнопка «Renew IP» (Обновить IP-адрес) Нажмите эту кнопку для получения нового IP-адреса от DHCP-сервера.

Вкладка «Advanced» (Дополнительно)

На вкладке «Advanced» можно сформировать несколько отчетов, которые позволяют отслеживать фоновую обработку, выполняемую приложением SWC. Кроме того, здесь можно выполнять определенные команды.



Приложение SWC поддерживает следующие отчеты и команды (доступные варианты зависят от версии программного обеспечения):

- [STATUS \(Состояние\)](#) (см. стр. 4-3)
- [STATUS_VERBOSE \(Состояние подробно\)](#) (см. стр. 4-3)
- [SCAN \(Поиск\)](#) (см. стр. 4-3)
- [SCAN_RESULTS \(Результаты поиска\)](#) (см. стр. 4-3)
- [LIST_NETWORKS \(Список сетей\)](#) (см. стр. 4-4)
- [SELECT_NETWORK \(Выбор сети\)](#) (см. стр. 4-4)
- [ENABLE_NETWORK \(Включить сеть\)](#) (см. стр. 4-4)
- [SAVE_CONFIG \(Сохранить конфигурацию\)](#) (см. стр. 4-4)
- [DISCONNECT \(Разъединить\)](#) (см. стр. 4-4)
- [REASSOCIATE \(Повторить привязку\)](#) (см. стр. 4-4)
- [DHCP release \(Освободить адрес DHCP\)](#) (см. стр. 4-4)
- [DHCP renew \(Обновить адрес DHCP\)](#) (см. стр. 4-4)
- [REMOVE_NETWORK \(Удалить сеть\)](#) (см. стр. 4-4)

STATUS (Состояние)

При выборе отчета STATUS запрашивается и отображается текущая информация о состоянии WPA/EAPOL/EAP.

Например:

```
bssid=02:00:01:02:03:04
ssid=test network
pairwise_cipher=CCMP
group_cipher=CCMP
key_mgmt=WPA-PSK
wpa_state=COMPLETED
ip_address=192.168.1.21
Supplicant PAE state=AUTHENTICATED
suppPortStatus=Authorized
EAP state=SUCCESS
```

STATUS_VERBOSE (Состояние подробно)

Отчет STATUS_VERBOSE аналогичен отчету STATUS, но предоставляет более подробную информацию (т.е. содержит больше пар <.....>=<.....>).

Например:

```
bssid=02:00:01:02:03:04
ssid=test network
id=0
pairwise_cipher=CCMP
group_cipher=CCMP
key_mgmt=WPA-PSK
wpa_state=COMPLETED
ip_address=192.168.1.21
Supplicant PAE state=AUTHENTICATED
suppPortStatus=Authorized
heldPeriod=60
authPeriod=30
startPeriod=30
maxStart=3
portControl=Auto
Supplicant Backend state=IDLE
EAP state=SUCCESS
reqMethod=0
methodState=NONE
decision=COND_SUCC
ClientTimeout=60
```

SCAN (Поиск)

Выполняет поиск нового источника набора базовых услуг (BSS).

SCAN_RESULTS (Результаты поиска)

Отображает результаты последнего поиска. Поля разделяются наклонной чертой («/»).

Например:

```
bssid / channel / signal level / flags / ssid
00:09:5b:95:e0:4e 2412 208 [WPA-PSK-CCMP] jkm private
02:55:24:33:77:a3 2462 187 [WPA-PSK-TKIP] testing
00:09:5b:95:e0:4f 2412 209 jkm guest
```

LIST_NETWORKS (Список сетей)

Выводит список настроенных сетей. Поля разделяются наклонной чертой («/»).

Например:

```
network id / ssid / bssid / flags  
0 example network any [CURRENT]
```

SELECT_NETWORK (Выбор сети)

Выполняет выбор сети (и отключает другие сети). Идентификатор сети можно получить из результатов выполнения команды [LIST_NETWORKS \(Список сетей\)](#) (стр. 4-4).

ENABLE_NETWORK (Включить сеть)

Выполняет включение сети. Идентификатор сети можно получить из результатов выполнения команды [LIST_NETWORKS \(Список сетей\)](#) (стр. 4-4).

REMOVE_NETWORK (Удалить сеть)

Удаляет сеть. Идентификатор сети можно получить из результатов выполнения команды [LIST_NETWORKS \(Список сетей\)](#) (стр. 4-4).

SAVE_CONFIG (Сохранить конфигурацию)

Выполняет сохранение текущей конфигурации.

DISCONNECT (Разъединить)

Разрывает подключение и переводит систему в режим ожидания команды REASSOCIATE (Повторить привязку) перед подключением.

REASSOCIATE (Повторить привязку)

Выполняет принудительную повторную привязку текущего подключения.

DHCP release (Освободить адрес DHCP)

Освобождает текущий IP-адрес.

Выполнение этой команды имеет тот же эффект, что нажатие кнопки **Release IP** (Освободить IP-адрес) ([Вкладка «IP»](#) (стр. 4-1)).

DHCP renew (Обновить адрес DHCP)

Отправляет запрос в DHCP-сервер на получение нового IP-адреса.

Выполнение этой команды имеет тот же эффект, что нажатие кнопки **Renew IP** (Обновить IP-адрес) ([Вкладка «IP»](#) (стр. 4-1)).

DEBUG on (Включить режим отладки)

Включает функцию передачи отладочных данных в файл, хранящийся в папке IPSM.

DEBUG off (Отключить режим отладки)

Отключает включенную ранее функцию вывода отладочных данных в файл.

Техническая поддержка

Если вам нужна помощь при установке или устранении неполадок в устройстве, свяжитесь с нами, используя один из указанных ниже способов:

База знаний: www.hsmknowledgebase.com

Наша база знаний содержит информацию о тысячах готовых решений. Если нужное решение в базе знаний отсутствует, можно воспользоваться нашим порталом технической поддержки (см. ниже), который предлагает простой способ сообщить о возникшей проблеме или задать вопрос.

Портал технической поддержки: www.hsmsupportportal.com

Портал технической поддержки позволяет не только сообщить о проблеме, но также может предложить немедленное решение технической проблемы путем поиска различных вариантов в нашей базе знаний. С помощью портала вы можете задавать вопросы и отслеживать ход их обработки через Интернет, кроме того, он позволяет передавать и получать вложенные файлы.

Интернет-форма: www.hsmcontactsupport.com

Вы можете связаться с нашей службой технической поддержки непосредственно, заполнив интернет-форму запроса на техническую поддержку. Введите свою контактную информацию и описание вопроса/проблемы.

Телефон: www.honeywellaidc.com/locations

Для получения актуальной информации о наших контактах посетите наш сайт по указанной выше ссылке.

Honeywell Scanning & Mobility
Системы автоматизации и управления
121059, Россия
Москва, ул. Киевская 7
Тел. (7-495) 796 9800
www.honeywellaidc.com