# Icotera **(**

# User guide

# for Icotera i4882-00 gateways with the firmware version 2.2.5

Published: September 2024

**Document version: 1.0** 

# **Table of contents**

Product overview
Physical description
Connector panel
Status LED indicators
Connectors
Ethernet ports
USB port
Power port
On/Off switch
Reset button
Serial number
Recommended Wi-Fi mesh installation scenarios
Scenario 1: Connecting an Icotera gateway with wired access points
Scenario 2: Connecting an Icotera gateway with wireless access points
Scenario 3: Connecting an Icotera gateway with wired and wireless access points 8
Setting up the Wi-Fi mesh network
Establishing a wired connection
Establishing a wireless connection
Adding a wired access point
Adding a wireless access point
Changing the installation setup of an access point
Changing a wired connection to a wireless connection
Changing a wireless connection to a wired connection
Resetting your Icotera i3560 access point
Troubleshooting
Configuring and managing the gateway
Logging in to the web interface
Overview
Top bar
Menu
Management area
Bottom bar
Viewing status information
Connected devices
General system information
WAN information
LAN information
Wi-Fi information
Managing LAN and Wi-Fi settings
LAN settings
Wi-Fi settings
Backup

Using network o	liagnostic tools			 	 	 	 26
Ping				 	 	 	 26
Traceroute				 	 	 	 27
Wi-Fi scan				 	 	 	 27
Reset				 	 	 	 28
Configuring adr	ninistrator settir	ngs		 	 	 	 29
Managing use	er credentials .			 	 	 	 29
Managing the	behaviour of L	ED indica	tors .	 	 	 	 29
Configuring r	emote access .			 	 	 	 30
Managing servio	es			 	 	 	 30
Port forwardi	ng			 	 	 	 30
DMZ				 	 	 	 31
ALG				 	 	 	 31
Wake On LAN	۰			 	 	 	 32
DDNS				 	 	 	 32
UPnP				 	 	 	 33
IPv6 firewall.				 	 	 	 33
Legal notice				 	 	 	 34

# **Product overview**

This chapter provides a general overview of the Icotera i4882-00 gateway, its components, features and characteristics. For specifications, see the product datasheet at https://icotera.com.

# **Physical description**

This section describes the physical components of the Icotera i4882-00 gateway, such as connectors, LED indicators, and buttons.

# **Connector panel**

The Icotera i4882-00 connector panel, shown in the following figure, contains the WAN port, LAN ports, USB port, WPS button, power port, on/off switch, and reset button.



Figure 1. The Icotera i4882-00 connector panel

# Status LED indicators

You can see the status LED indicators on the left of the front panel. The middle LED indicator is unused in Icotera i4882-00 gateways.

Also, you can see the link activity and status LED indicators on each of the Ethernet ports of the connector panel.



Figure 2. Status LED indicators

The following table shows the status LED indicator descriptions. *Table 1. The status LED indicator descriptions* 

LED type	Туре	Colour	State	Description
Link activity	Ethernet port ac-	Green	Solid	The gateway established a communication link.
	tivity		Blinking	Network activity occurs on this port.
			Off	The Ethernet connection is down for this port.
Link status	LAN port status	Orange	Solid	The port operates at 1 Gbps for the 1 Gbps port or 2.5 Gbps for the 2.5 Gbps port.
			Off	The port operates at a lower throughput. For example, the 2.5 Gbps port operates at 10, 100, or 1000 Mbps.
System	System status and activity	N/A	Off	When the auto-off feature is enabled, users can shortly press the WPS button to trigger the system LED indicator.
		Green	Blinking	The firmware upgrade is in progress.
			Solid	The gateway established an Internet connection.
		Red	Blinking	The gateway did not boot, initialise or provision correctly.
			Blinking fast	The firmware upgrade failed.
			Solid	The gateway did not obtain the IP address, or the Internet connection is unavailable.
		Orange	Blinking	The gateway is booting, initialising, or provision- ing.
Wi-Fi	Wi-Fi status and activity	N/A	Off	When the auto-off feature is enabled, users can shortly press the WPS button to trigger the Wi-Fi LED indicator.
		Blue	Blinking	The pairing is in progress.
			Blinking fast	The pairing failed. Users can start a new pairing session while the LED indicator blinks.
			Solid	The gateway t completed the pairing. The LED indicator lights solid blue for 15 seconds.
		Green	Solid	Wi-Fi is active.
		Red	Solid	Wi-Fi is active, and users can access the web interface. The gateway did not obtain the IP address, or the Internet connection is unavailable.

# Connectors

The i4882-00 connector panel includes 1 RJ45 100/1000/2500 BaseT WAN port, 1 RJ45 connector 100/1000/2500 BaseT LAN port, two RJ45 connectors 10/100/1000 BaseT(x) ports, and 1 USB 2.0 port.

#### **Ethernet ports**

The Icotera i4882-00 uses 100/1000/2500 Base Tx and 10/100/1000 BaseTx port connectors configured as MDI/ MDIX. The gateway uses auto-sense ports that are designed to operate at 10 Mbps, 100 Mbps, or 1000 Mbps (2500 Mbps WAN), depending on the connecting device. These ports support the IEEE 802.3u auto-negotiation standard, which means that when a port is connected to another device that also supports the IEEE 802.3u standard, then the two devices negotiate the best speed and duplex mode. The 10Base-T/100Base-TX/1000Base-T RJ-45 switch ports also support half- and full-duplex mode operation and can connect to 10 Mbps, 100 Mbps or 1000 Mbps Ethernet segments or nodes.

# **USB port**

The Icotera i4882-00 has one USB 2.0 port that supplies 5 V at 500 mA.

# **Power port**

The power port accepts a DC 12 V power source. Make sure that the power adapter is suitable for your region.

# **On/Off** switch

You can use the On/Off switch to turn on or off the gateway, as well as reboot it and restore the last saved configuration.

# **Reset button**

You can use the reset button to restart the gateway, restore the factory default settings, or switch to a different memory bank.

To restart your working gateway, press the reset button for up to 5 seconds

To restore the factory default settings on your working gateway, press the reset button for 5-30 seconds. To restore the factory default settings on the gateway that is turned off, press the reset button for 5 seconds.

To switch the gateway that is turned off to a different memory bank, press the reset button for more than 30 seconds. The memory in Icotera i4882-00 gateways is divided into two banks. At a single point in time, the gateway can use one of these banks. You might switch to a different memory bank, for example, when the gateway stops responding after a firmware upgrade.

# Serial number

The serial number of the lootera gateway consists of 13 digits. The format of the serial number is PPPPCCXXXXXX. where PPPP is the product identifier, CC is the product variant, and XXXXXXX is the running serial number. For example, 4882001234567 is the serial number of the Icotera i4882-00 gateway with a running number of 1234567.

# **Recommended Wi-Fi mesh installation scenarios**

This chapter describes possible connection scenarios between your gateway and supported access points. This chapter also includes best practices for creating a mesh network and provides troubleshooting suggestions.

The Icotera i4882 gateways and the Icotera i3560 access point (AP) can support up to four access points in a mesh network with a single controller access point and up to three wired or wireless APs. This configuration helps deliver a strong Wi-Fi signal to virtually every spot of the residential premises.

Turn on SONiQ on your gateway. Make sure that your gateway runs on the firmware version 2.2.0 or higher. Also, make sure that your access points run on the firmware version 1.1.2 or higher.

You can accomplish this configuration by using one of the following scenarios.

# Scenario 1: Connecting an Icotera gateway with wired access points

In the first scenario, you use an Icotera i4882 gateway as a controller access point. Optionally, you can use an unmanaged third-party switch that is transparent to 802.1Q VLANs.

You use Ethernet cables to connect up to three wired Icotera i3560 access points to the gateway or the third-party switch.

You can connect wired access points to any available LAN port of the gateway or another access point. The following image shows the architecture of this scenario.



Figure 3. Connecting up to three wired access points to the gateway or switch

Alternatively, you can connect wireless access points to the gateway or another access point by using Wi-Fi. When your Wi-Fi devices move around your premises, they automatically steer to the most suitable access point.

#### Scenario 2: Connecting an Icotera gateway with wireless access points

In the second scenario, you also use an Icotera i4882 gateway as a controller access point. You use Wi-Fi to connect up to three wireless Icotera i3560 access points to your gateway.

In this scenario, wireless access points can connect to the gateway or other access points, depending on the controller's guidance.



Figure 4. Connecting up to three wireless access points to the gateway

# Scenario 3: Connecting an Icotera gateway with wired and wireless access points

In the third scenario, you use an Icotera i4882 gateway as a controller access point. You use an Ethernet cable to connect one access point. Also, you use Wi-Fi to connect up to two wireless Icotera i3560 access points to your gateway. Depending on the controller guidance, wireless access points can connect to the gateway or other access points.



Figure 5. Connecting one wired access point and up to two wireless access points to the gateway

# Setting up the Wi-Fi mesh network

This section describes best practices for creating a mesh network for wired and wireless connections.

#### Establishing a wired connection

The following image shows the Wi-Fi coverage of a three-floor house. In this image, the gateway uses an Ethernet cable to connect to WAN and to access points. In turn, access points use an Ethernet cable to connect to devices that require high throughput, such as a gaming computer or a television. With other devices, access points establish wireless connections.



Figure 6. Covering a house with the Wi-Fi signal by using wired access points

In this image, solid lines show connections with an Ethernet cable; dashed lines show wireless connections. The gateway and access points cover the area highlighted in green. In these areas, the Wi-Fi signal strength is less than -82 dBm. User devices connect to the gateway where possible, even when they are closer to the access point.

We recommend using the Ethernet cable to connect all access points to your gateway or switch. Avoid connecting access points with each other.

To ensure a strong Wi-Fi signal, install one access point on each floor and place it centrally. After you install access points in your mesh network, check the download speed at all places of interest and on static Wi-Fi devices. Make sure that you can download data at more than 200 Mbps rate. Cover all places that do not provide such speed with additional access points. To measure the download speed, use the Speedtest application. For more information, see <a href="https://www.speedtest.net/">https://www.speedtest.net/</a>.

The coverage areas of wired access points can overlap. In this case, the access points do not interfere and improve seamless roaming.

We recommend that you avoid installing more access points than required to cover the premises. Installing many access points degrades Wi-Fi performance.

#### **Establishing a wireless connection**

The following image shows the Wi-Fi coverage of a three-floor house. In this image, the gateway uses an Ethernet cable to connect to WAN. Also, the gateway establishes wireless connections with access points. In turn, access points use an Ethernet cable to connect to devices that require high throughput, such as a gaming computer or a television. With other devices, access points establish wireless connections.



Figure 7. Covering a house with the Wi-Fi signal by using wireless access points

In this image, solid lines show connections with an Ethernet cable; dashed lines show wireless connections. The gateway and access points cover the area highlighted in green. In these areas, the Wi-Fi signal strength is less than -82 dBm. Make sure that you place each access point in the area where the strength of the Wi-Fi signal from the gateway is less than -82 dBm. User devices connect to the gateway where possible, even when they are closer to the access point.

We recommend connecting your access points to the gateway with an Ethernet cable when possible. When you establish a wireless connection between the gateway and an access point, expect up to 50% lower throughput.

Place your gateway so that it can cover most of the house. Add wireless access points only when needed. Installing many access points degrades Wi-Fi performance.

Connect your wireless access points to the gateway or to a wired access point. Avoid connecting a wireless access point to another wireless access point.

After you install access points in your mesh network, check the download speed at all places of interest and on static Wi-Fi devices. Make sure that you can download data at least at a 100 Mbps rate. Cover all places that do not provide such speed with additional access points. To measure the download speed, use the Speedtest application. For more information, see <a href="https://www.speedtest.net/">https://www.speedtest.net/</a>.

To reduce in-home interference, use an Ethernet cable to connect devices that frequently transfer large files to the access point.

# Adding a wired access point

• Check that the system and Wi-Fi LED indicators on the gateway light solid green.



• Power on your Icotera i3560 access point and wait until the LED indicator lights solid white.



- Connect an Ethernet cable to one of the free LAN ports on the supported gateway and one of the free LAN ports on your access point.
- Wait until the LED indicator on the access point lights solid green.



- The wired access point is configured with the same SSID and password as on the gateway. You can use the access point.
- For troubleshooting, see <u>Status LED indicators</u> or contact your ISP support department.

# Adding a wireless access point

• Check that the system and Wi-Fi LED indicators on the gateway light solid green.



• Place the Icotera i3560 access point in the same room as the gateway. Turn on your access point and wait until the LED indicator on the access point lights solid white. The access point is ready for pairing.



• Press and hold the WPS button on your gateway for at least three seconds until the Wi-Fi LED indicator starts blinking blue. Release the WPS button. The gateway is ready for pairing with the access point.



• Now press and hold the WPS button on the access point for at least three seconds until the Wi-Fi LED indicator starts blinking blue. Release the WPS button.



• The pairing process is in progress. This process takes up to two minutes. Wait until the Wi-Fi LED indicators on the router and the access point light solid blue. After 15 seconds, the LED indicator on your access point starts blinking green. Next, the Wi-Fi LED indicators on the router and the access point light solid green.



- The wireless access point is now correctly configured with the same SSID and password as on the gateway. You can turn it off and move it to the target location in your home. After you turn the access point on again, the Wi-Fi LED indicator shows solid green. The access point is in the operation mode.
- For troubleshooting, see the <u>Status LED indicators section</u> or contact your ISP support department.

# Changing the installation setup of an access point

• Check that the gateway and the access point are correctly configured and fully operational. The system and Wi-Fi LED indicators on the gateway light solid green. The Wi-Fi LED indicator on the access point lights solid green. Now you can change the installation setup for the lcotera i3560 access point.



#### Changing a wired connection to a wireless connection

• The Icotera i3560 access point automatically switches from a wired connection to a wireless connection. Remove the Ethernet cable from the LAN port of your access point. The Wi-Fi LED indicator lights solid red and the access point switches to a wireless connection.



• After up to 5 minutes, the LED indicator lights solid green, which means that the access point is correctly configured and ready to work in the wireless mode.



- You can move the Icotera i3560 access point to a new location. To do so, turn it off, move the access point, and turn it on again. When the Wi-Fi LED indicator lights solid green, you can use your access point.
- For troubleshooting, refer to the LED section or contact your ISP support department.

#### Changing a wireless connection to a wired connection

• The lootera i3560 access point automatically switches from a wireless connection to a wired connection. You can connect an Ethernet cable to one of the free LAN ports on the access point and one of the free LAN ports on the gateway. After up to 5 minutes, the access point establishes a wired connection and the LED indicator lights solid green.



- The access point is correctly configured and ready to work in the wired mode.
- You can move the Icotera i3560 access point to a new location. To do so, turn it off, move the access point, connect an Ethernet cable, and turn it on again. When the Wi-Fi LED indicator lights solid green, you can use your access point.
- For troubleshooting, see the <u>Status LED indicators section</u> or contact your ISP support department.

# Resetting your Icotera i3560 access point

To use your Icotera i3560 access point on another Wi-Fi network, you must do a factory reset.

• Check that the Wi-Fi LED indicator on your access point lights solid green. You can do a factory reset.



• Take a thin rod (such as a paper clip) and insert it into the Reset hole to press the hidden button.



• Keep the Reset button pressed for more than 5 seconds until the LED indicator lights solid orange.



- Release the Reset button.
- Wait until the access point completes the factory reset boot-up. When the Wi-Fi LED indicator lights solid white, the Icotera i3560 access point is ready for a new installation.

# Troubleshooting

- The Icotera i4882 system LED indicator blinks red:
  - \* The gateway did not initialize or provision correctly.
- The Icotera i4882 system LED indicator lights solid red:
- \* The gateway did not obtain the IP address or the Internet connection is unavailable.
- The Icotera i4882 Wi-Fi LED indicator lights solid red:
  - \* The Wi-Fi connection might be established with stations, but they do not have any service.
- The Icotera i3560 Wi-Fi LED indicator blinks red:
  - \* The access point established an Internet connection but the strength of the backhaul connection is less than -82 dBm. Try to move your Icotera i3560 access point closer to the gateway or another access point.
- The i3560 Wi-Fi LED indicator shows solid red:
  - \* The access point did not obtain the IP address or the Internet connection is unavailable.

# **Configuring and managing the gateway**

This chapter provides an overview of the Icotera gateway configuration and management features. It focuses on using the web interface to manage the gateway settings.

# Logging in to the web interface

To log in to the web interface, complete the following steps.

1. Enter **router/** or the IP address of your gateway in your web browser. The browser displays the following dialogue box.

i4883-00 Login	
Please input your username and password:	
Username:	
Password:	
Log in Clear	

Figure 8. Logging in to the web interface

- 2. Enter your username and password.
- 3. Choose *Log in* to log in. Alternatively, choose *Clear* to delete credentials and enter them again.



The first time you log in, use the username and password provided by your network operator. After the first login, you can change your password in the *Administration/UI login password* menu.

# **Overview**

After a successful login, the browser displays the start window of the web interface. By default, it is the **Connected** *devices* section of the *Status* menu. The following figure presents the structure of the web interface.

lco	tera 🌗	i4883-00 Ethernet Router	English V Log out	Top bar
Status 🔻				
Connected devices	Connected devices			
System information	Connected devices			
WAN				Management area
LAN	All			
Wi-Fi 2.4 GHz				
Wi-Fi 5 GHz	IP address MAC Address	Hostname	DHCP	
VoIP			Refresh	
Settings 🔹		Bot	tom bar	
LAN	Reset Save Apply		combar	
Wi-Fi 2.4 GHz				
Wi-Fi 5 GHz				
Backup	Mana			
Diagnostic 🔹	Menu			
Ping				
Traceroute				
Wi-Fi scan				
Reset				
Administration 🔻				
UI login password				
LEDs				
Remote Access				
Services 🔹				
Port Forwarding				
DMZ				
ALG				
Wake On LAN				
DDNS				
UPnP				
IPv6 firewall				
	Figure 9 Web Interface s	start screen		

Figure 9. Web Interface start screen

#### Top bar

The top bar contains the Icotera logo, device designation, a dropdown list where you can choose the interface language, and the *Log out* button.

#### Menu

The menu is a collapsible list of available options, which are grouped into two levels: main and secondary. The main level provides access to general gateway management categories. The secondary level presents a submenu of available options for a given category. By default, the web interface expands all menu options. To collapse a menu section, click on its name.



Depending on the particular configuration, the menu layout varies. Internet service providers can customize and turn off specific menu sections.

#### Management area

The management area is where all the gateway management and status information are displayed and modified. Depending on the selected option, it can display a set of particular configuration options or a list of current gateway status information.

#### **Bottom bar**

In the centre of the bottom bar, there are three buttons:

- **Reset**: resets all changes made in the current session.
- **Save**: saves all changes made in the current session.
- **Apply**: applies all changes saved during the current session.

# Viewing status information

The *Status* menu provides tools for listing connected devices, viewing general gateway system information, as well as to obtain information about WAN, LAN and wireless interfaces operating on the device. You can also view phone info, VoIP call log, and information about the WDS status and associated clients in this menu.

#### **Connected devices**

The **Connected devices** section of the **Status** menu contains information about devices connected to the gateway.

Status	-							
Connected device	es			Connected (	devices			
System informati	ion							
WAN		Connected devi	ces					
LAN								
Wi-Fi 2.4 GHz		A. •						
Wi-Fi 5 GHz			IP address	MAC Address	Hostname	Link	RSSI	Mode
VoIP		5GHz AP 1	192.168.7.184	ac:19:8e:66:9d:29	hp_840_G9	432 Mbps	-81	AX
Settings	•							Refresh
Diagnostic	•			Parat Sava	Apply			
Administration	•			Reset Save				
Services	•							

Figure 10. The Connected devices section of the Status menu

You can use the dropdown lists to choose a particular interface. The table woth connected devices contains the following information.

- The IP address column shows the IP address of the connected device,
- The MAC address column shows the physical address of the connected device.
- The *Hostname* column shows the name of the connected device.
- The *Link* column shows the data transfer rate.
- The **RSSI** column shows the received signal strength indicator in dBm.
- The *Mode* column shows the wireless network mode.

To refresh the data in this table, choose **Refresh**.

Because this menu does not include any configurable options, the **Reset**, **Save**, and **Apply** buttons are inactive.

#### **General system information**

To access general information about the gateway go to the **Status/System information** menu section.

The **System information** section contains general information about the gateway state.

- Current time: current time and date,
- Uptime: duration the device has been powered up,
- Firmware version: the current software version operating on the device,
- WAN MAC: the physical address of the device's WAN interface,
- **WAN IP**: the IP address of the WAN interface,
- Device name: the name of the device,
- Serial number: the serial number of the device,
- **Configuration mode**: **Unconfigured** (no steering or configuration propagation between the gateway and i3550) or **Master** (steering and configuration propagation active between the gateway and i3550),
- Wi-Fi 2.4 GHz: the status of the 2.4 GHz wireless interface, either On or Off,
- Wi-Fi 5 GHz: the status of the 5 GHz wireless interface, either On or Off.

Connected devices System information WAN LAN Wi-Fi 2.4 GHz Wi-Fi 5 GHz	Current t Upt Firmware vers	ime: 2023 ime: 0 d 2	<b>Syst</b> /08/01 16:11 2 h 32 m 28 s	em informatio	on Device name:	i4883-00	
System information WAN LAN Wi-Fi 2.4 GHz Wi-Fi 5 GHz	Current t Upt Firmware vers	ime: 2023 ime: 0 d 2	:/08/01 16:11 2 h 32 m 28 s		Device name:	i4883-00	
WAN LAN Wi-Fi 2.4 GHz Wi-Fi 5 GHz	Upt Firmware vers	ime: 0 d 2	h 32 m 28 s				
LAN Wi-Fi 2.4 GHz Wi-Fi 5 GHz	Upt Firmware vers	ime: 0 d 2	h 32 m 28 s				
Wi-Fi 2.4 GHz Wi-Fi 5 GHz	Firmware ver				Serial number:	4883000005	052
Wi-Fi 5 GHz		ion: 4883	-2.2.0_2	Conf	iguration mode:	Unconfigured	ł
	WAN	AC: 00:0	f:15:9b:34:f9		Wi-Fi 2.4 GHz:	On	
VoIP						0	
Settings 🔹 🕨	WAN	<b>IP:</b> 10.10	04.2.125		Wi-Fi 5 GHz:	On	
Diagnostic 🔶							
Administration >			Sy	stem counters	\$		
Services 🕨							
		Status	Pkts in	Pkts out	Errors	Collisions	Speed
	2.5G LAN	Down	0	0	0	0	Down
	LAN 1	Down	0	0	0	0	Down
	LAN 2	Down	0	0	0	0	Down
	WLAN 2.4 GHz	Up	0	0	-	-	-
	WLAN 5 GHz	Up	0	0	-	-	-
	WAN	Up	24394	4544	26	0	FD100
							Refresh

Figure 11. System information section of the Status menu

The **System counters** section contains statistical information about data entering and leaving the interfaces of the gateway, as well as error and collision counters:

- Status: current status of a given interface, either Up or Down,
- Pkts in: number of incoming packets in the current session,
- Pkts out: number of outgoing packets in the current session,
- Errors: transmission error counter,
- Collisions: collision counter,
- Speed: negotiated speed (FD1000 Full Duplex at 1000Mbps, FD100 Full Duplex at 100Mbps, FD10 Full Duplex at 100Mbps, HD100 Half Duplex at 100Mbps, HD10 Half Duplex at 100Mbps).

To refresh the information in this section, choose **Refresh**.

Because this menu does not include any configurable options, the **Reset**, **Save**, and **Apply** buttons are inactive.

#### WAN information

The **WAN** section of the **Status** menu lists basic information about the WAN interface and the statistics of data carried through the interface.

The **WAN** section presents basic information about the WAN interface:

• WAN IP type: IP address type of the WAN interface,

- IP address: IP address used by the WAN interface,
- Subnet mask: subnet mask used by the WAN interface,
- **Default gateway:** default gateway configured for the WAN interface,
- MAC address: interface's physical address,
- DNS: two IP addresses are displayed; 0.0.0.0 is shown if the DHCP server option provides only a single DNS server.

Status 🔻						
Connected devices			WAN			
System information	WAN IP type:	DHCP		Default gatewa	av: 10.104.0.	1
WAN	in a ciper	51101		Dendent gatern		-
LAN	IP address:	10.104.3.22		MAC Addre	ss: 00:0f:15:	66:68:55
Wi-Fi 2.4 GHz	Subnet mask:	255.255.252.0		DI	NS: 81.18.219	.100 0.0.0.0
Wi-Fi 5 GHz						
VoIP			WAN counte	rs		
Settings 🕨 🕨						
Diagnostic 🔹 🕨	Status	Pkts in	Pkts out	Errors	Collisions	Speed
Administration >	WAN Up	26293	4779	26	0	FD100
Services >						Refresh
		Res	et Save	Apply		

Figure 12. The WAN section of the Status menu

The **WAN counters** section displays statistical information about data:

- Status: current status of a given interface, either Up or Down,
- Pkts in: number of incoming packets in the current session,
- Pkts out: number of outgoing packets in the current session,
- Errors: transmission error counter,
- Collisions: collision counter,
- Speed: negotiated speed (FD1000 Full Duplex at 1000Mbps, FD100 Full Duplex at 100Mbps, FD10 Full Duplex at 100Mbps, HD100 Half Duplex at 100Mbps, HD10 Half Duplex at 100Mbps).

To refresh the WAN information, choose **Refresh**.

Because this menu does not include any configurable options, the *Reset*, *Save*, and *Apply* buttons are inactive.

#### LAN information

You can use the **LAN** section of the **Status** main menu to obtain information about the LAN interfaces and to configure static IP leases for connected devices.

The **LAN** section contains the following general information about the LAN interface:

- *IP type*: IP type of the LAN interface,
- IP address: IP address used by the LAN interface,
- Subnet mask: subnet mask used by the LAN interface,
- Default gateway: default gateway configured for the LAN interface,
- MAC address: interface's physical address.

The **Counters** section displays statistical information about data:

- Status: current status of a given interface, either Up or Down,
- Pkts in: number of incoming packets,
- **Pkts out**: number of outgoing packets,
- Errors: transmission error counter,
- Collisions: collision counter,
- Speed: negotiated speed (FD1000 Full Duplex at 1000Mbps, FD100 Full Duplex at 100Mbps, FD10 Full Duplex at 100Mbps, HD100 Half Duplex at 100Mbps, HD10 Half Duplex at 100Mbps).

The **Dynamic Leases** section contains information about devices connected to LAN interfaces which have dynamically assigned IP addresses. Each device is described with the following parameters:

- IP address: IP address assigned to a device,
- MAC Address: physical address of a connected device, •
- Hostname: connected device's hostname, .
- Expires: lease time of the device's address,
- Remember: to turn a dynamic lease into a static lease, choose Make static. After you do so, you can see the entry in the **Static Leases** section.

Status 👻						
Connected devices			home_lan			
System information			-			
WAN	IP type: L	HCP server	D	efault gateway:	192.168.7.1	
LAN	IP address: 1	92.168.7.1		MAC Address:	00:0f:15:66	:68:57
Wi-Fi 2.4 GHz	Subnet mask: 2	55.255.255.0				
Wi-Fi 5 GHz						
VoIP	Counters					
Settings						
Diagnostic >	Status	Pkts in	Pkts out	Errors	Collisions	Speed
Administration	LAN 1 Down	0	0	0	0	Down
Services	LAN 2 Down	0	0	0	0	Down
	WIFI 1 AP 1 Up WIFI 2 AP 1 Up	0	0	0	0	-
	Dynamic Loasos					
	TP address MA	C Address	Hostname	Expin	es	Remember
	Static Labor					1
	Static Leases					
	TD addrocc	MAC Add	PASS	Hostnamo	Enab	Add / Remove
	IF dudiess	PIAC Add		nostiame	Enat	Addy Kelliove
	0.0.0.0	00:00:00:00:00	):00			Add
						Refresh
			quest lan			
			guest_lun			
	IP type:	HCP server	D	efault gateway:	192.168.100	0.1
	ID address:	92 168 100 1		MAC Address	00.0f.15.50	'de'56
	ir duress.			HAC Address.	00.01.15.50	
	Subnet mask: 2	55.255.255.0				
	Countors					
	Status	Pkts in	Pkts out	Errors	Collisions	Speed
	WIFI 1 AP 2 Down	0	0	0	0	-
	WIFI 2 AP 2 Down	0	0	0	0	-
						1
	Dynamic Leases					
					_	
	IP address MA	C Address	Hostname	Expire	25	Remember
	Static Leases					
	IP address	MAC Add	ress	Hostname	Enab	ole Add/Remove
	0.0.0.0	00:00:00:00:00	0:00			Add
						Refresh
		Reset	Save	Apply		

Figure 13. The **LAN** section of the **Status** menu

Icotera A/S, Hovedvejen 3A, 2600 Glostrup, Denmark - info@icotera.com Document version: 1.0

In the *Static Leases* section, you can manually add a static lease. To do so, apply the following steps.

- 1. For *IP address*, enter the IP address of a device to connect.
- 2. For MAC Address, enter the MAC address of the device.
- 3. For *Hostname*, enter the name of the device.
- 4. Check *Enable* to turn on the lease immediately. Keep the box unchecked to turn on the lease later.
- 5. To add the lease to the list, choose Add.
- 6. To save changes, choose **Save**.
- 7. To apply changes, choose **Apply**.

To refresh the LAN information, choose **Refresh**.

#### Wi-Fi information

The Wi-Fi 2.4 GHz and Wi-Fi 5 GHz menu sections contain information about the gateway wireless interfaces and their access points. Their layout is similar, and the Wi-Fi 5 GHz contains an additional Channel availability overview section as well **Rescan** button which are not present in the **Wi-Fi 2.4 GHz** section.

Status 🔻				
Connected devices			General	
System information	Status:	On	Mode:	802.11g/n/ax
WAN	Channel	1 (ontimal)	TX Dowor:	100
LAN	chunici	1 (optimal)	TX TOWEL	100
Wi-Fi 2.4 GHz	Band:	20MHz		
WI-FI 5 GHZ				
ettings		Access poin	t 1: homeWiFi2GHz	
iagnostic 🕨	SSID:	ICO-666855	Hidden:	no
dministration 🔸	BSSID:	00:0f:15:66:68:59	Encryption:	WPΔ2 ΔES
ervices 🕨	555151	-	Lifer y prom	
	Status:	On		
	Counters			
	Status	Pkts in Pkts out	Bytes in Bytes out	Errors Collisions
	AP 1 Up	0 0	0 0	0 0
	Associated clients			
	IP address MAC Address	Hostname Expires	10de Sleep RSSI TX bytes	TX rate TX failed RX bytes
	4			•
				Refresh
		Access poin	t 2: guestWiFi2GHz	
	SSID:	Guest	Hidden:	no
	BSSID	00.0f.15.50.de.5a	Encryption:	WDA2 AFS
	55510.		Encryption.	11 62 623
	Status:	Off		
	Counters			
	Status	Pkts in Pkts out	Bytes in Bytes out	Errors Collisions
	AP 2 Down	0 0	0 0	0 0
	Associated clients			
	TP address MAC Address	Hostname Expires	4ode Sleep RSSI TX bytes	TX rate TX failed RX bytes
	Image: 1 million of the second sec			
				Refresh
		Reset	Save	

Figure 14. The Wi-Fi 2.4 GHz section of the Status menu

20

Icotera A/S, Hovedvejen 3A, 2600 Glostrup, Denmark - info@icotera.com Document version: 1.0

The *General* section contains the following information about the Wi-Fi interfaces:

- Status: interface status, either On or Off,
- Channel: wireless channel on which the interface operates (choose Reselect to reselect channel if the Channel option in the Settings/Wi-Fi menu section is set to auto),
- Band: radio channel width used by the interface,
- Mode: wireless mode of the wireless interface (802.11ax, 802.11ac/ax, 802.11n/ac/ax or 802.11a/n/ac/ax),
- **Tx Power**: transmission power value (percentage) for the wireless interface.

tus 👻						
nnected devices				General		
stem information		Chathan	0-			000 11-1-1-1
AN		Status:	UII		Mode:	802.11a/n/ac/ax
N		Channel:	104 (auto)		TX Power:	100
IN						
-Fi 2.4 GHz		Band:	80MHz			
-Fi 5 GHz						
IP			Channel a	vailability overvie	2007	
tinas 🕨			Channer a			
	Channel	DFS	Beacons	Interference	Metric	: Status
jnostic 🕨	36	no	0	90	129	available
ninistration 🔸	40	no	9	20	139	available
/ices ▶	44	no	7	200	113	available
	48	no	2	90	129	available
	56	yes	2	20	142	CAC required
	60	Ves	0	0	142	CAC required
	64	ves	4	20	139	CAC required
	100	ves	7	40	164	available
	104	ves	2	10	174	available
	108	yes	4	40	164	available
	112	yes	0	40	164	available
	116	yes	0	100	153	CAC required
	120	yes	0	70	159	CAC required
	124	yes	0	150	145	CAC required
			Access noi	nt 1: homeWiFi5G	Hz	
			Access por	III 1. IIOIIIEWIFI3G	INZ	
		SSID:	ICO-666855		Hidden:	no
		BSSID:	00:0f:15:66:68:5d	E	ncryption:	WPA2 AES
		Status:	On			
	Counters					
		Status	Pkts in Pkts out	Bytes in B	sytes out	Errors Collisions
	AP 1	Up	0 0	0	0	0 0
	Associated clie	ents				
	TD address 1		Hasterne Fusies		TV hat a 1	
	IP address	MAC Address	Hostname Expires	Mode Sleep RSSI		IX rate IX failed RX by
	192.168.7.184 a	c:19:8e:66:9d:29	hp_840_G9 83300	AX N/A -81 dBr	m 890762 KiB 2	288 Mbps 0 104448
						Refresh
			Rent	Save Annly		
			Reset	Save		

Figure 15. The **Wi-Fi 5 GHz** section of the **Status** menu

The *Access point* sections contain the following information about every configured Wi-Fi access point:

- **SSID**: Service Set Identifier of the access point (Wi-Fi network name),
- **BSSID**: MAC address of the access point (Basic Service Set Identifier),
- Status: access point status, either On or Off,
- Hidden: visibility setting of the access point,
- **Encryption**: data encryption algorithm of the access point.

The **Counters** section contains statistical information about data entering and leaving the interfaces per access point:

- Status: current status of a given interface, either Up or Down,
- *Pkts in*: number of incoming packets,
- **Pkts out**: number of outgoing packets,
- **Bytes in:** number of incoming bytes,
- **Bytes out**: number of outgoing bytes,
- Errors: transmission error counter,
- **Collisions**: collision counter.

The *Associated clients* section lists all devices connected to the particular access point. Each device is described with the following parameters:

- IP address: IP address assigned to the device,
- MAC Address: physical address of the connected device,
- Hostname: connected device's hostname,
- **Expires**: lease time of the device's address,
- Mode: mode of operation,
- **Sleep**: when set to **Yes**, the client is present but does not exchange traffic with the host; when set to **No**, the client is present and active,
- **RSSI**: Received Signal Strength Indicator,
- **Tx bytes**: transmitted bytes,
- **Tx rate**: transmission rate,
- **Tx failed**: transmission failures,
- **Rx bytes**: received bytes.

To refresh the wireless interface information section, choose **Refresh**.

Because this menu does not include any configurable options, the **Reset**, **Save**, and **Apply** buttons are inactive.

# **Managing LAN and Wi-Fi settings**

The *Settings* menu provides advanced configuration options to control Layer 3 network parameters of the LAN and Wi-Fi networks. You can also upload and download configuration files.

# LAN settings

In the *LAN* section of the *Settings* menu, you can modify the parameters of the Local Area Network.

- *IPv4 Type*: if the *DHCP server* option is selected (default configuration), all hosts connected to LAN ports or over the Wi-Fi interface will obtain their IP addresses and other necessary information automatically. To change this setting choose the *Static* option from the drop-down menu and enter all network parameters manually,
- IP address: specifies the IP address of your network,
- IP netmask: specifies the network mask,
- Gateway (only for dynamic IP configuration): specifies the IP address of your network gateway,
- **Primary DNS** (only for dynamic IP configuration): specifies the primary Domain Name System server to be used to resolve DNS queries,
- **Secondary DNS** (only for dynamic IP configuration): specifies the secondary Domain Name System server to be used to resolve DNS queries,
- **WINS** (only for dynamic IP configuration): specifies the IP address of the Windows Internet Name Service server. This server is typically used in office environments,
- *IP range*: specifies the pool of IP addresses that the DHCP server can allocate.
- Lease time: specifies DHCP lease renewal time in seconds. The value in this field must range from 60 to 86400 and cannot be higher than the value in the **Max lease time** field. It is recommended to leave this value at its default setting.
- *Max lease time*: specifies the maximum time in seconds which can be assigned to a client, if it asks for a longer lease time than the standard one. The value in this field must range from 60 to 86400 and cannot be lower than the value in the *Lease time* field. It is recommended to leave this value at its default setting.

- **Enable Local Easy HostName**: when this box is checked, the web browser recognizes selected names from the list and opens the gateway web interface when you enter any of these names in the address bar.
- *IPv6 Router Advertisement*: when enabled, messages are sent by the router periodically and in response to Neighbor Solicitation packets.
- To reset all changes made during the current session, choose **Reset**. To save all changes made during the current session, choose **Save**. To applies all changes saved during the current session, choose **Apply**.

Status Settin LAN Wi-Fi Backu Diagno Admin

IPv4 Type.	DHCP server V	
IP address:	192.168.7.1	
IP netmask:	255.255.255.0	
Gateway:	192.168.7.1	
Primary DNS:	192.168.7.1	
Secondary DNS:	0.0.0.0	
WINS:	0.0.0.0	
IP range:	192.168.7.2 - 192.168.7.250	
Lease time:	86400	
Max lease time:	86400	
Enable Local Easy		
HostName:		
1	router home	
2		ſ
-	14882-00	ſ
3	14882-00	ſ
5	14882-00	ſ
5		l
6		l
/		l
8		l
IPv6 Router Advertisement:	Enable V	
	_	
Enabled:		
Enabled: IPv4 Type:	DHCP server	
Enabled: IPv4 Type: IP address:	DHCP server  192.168.100.1	
Enabled: IPv4 Type: IP address: IP netmask:	DHCP server 192.168.100.1 255.255.255.0	
Enabled: IPv4 Type: IP address: IP netmask: Gateway:	DHCP server 192.168.100.1 255.255.255.0 192.168.100.1	
Enabled: IPv4 Type: IP address: IP netmask: Gateway: Primary DNS:	DHCP server 192.168.100.1 255.255.255.0 192.168.100.1 192.168.100.1	
Enabled: IPv4 Type: IP address: IP netmask: Gateway: Primary DNS: Secondary DNS:	DHCP server 192.168.100.1 255.255.255.0 192.168.100.1 192.168.100.1 0.0.0.0	
Enabled: IPv4 Type: IP address: IP netmask: Gateway: Primary DNS: Secondary DNS: WINS:	DHCP server ▼         192.168.100.1         255.255.255.0         192.168.100.1         192.168.100.1         0.0.0.0         0.0.0.0	
Enabled: IPv4 Type: IP address: IP netmask: Gateway: Primary DNS: Secondary DNS: WINS: IP range:	□         □ <t< td=""><td></td></t<>	
Enabled: IPv4 Type: IP address: IP netmask: Gateway: Primary DNS: Secondary DNS: WINS: IP range: Lease time:	DHCP server ▼         192.168.100.1         255.255.255.0         192.168.100.1         192.168.100.1         0.0.0.0         0.0.0.0         192.168.100.2         192.168.100.250	
Enabled: IPv4 Type: IP address: IP netmask: Gateway: Primary DNS: Secondary DNS: WINS: IP range: Lease time: Max lease time:	□HCP server ▼         192.168.100.1         255.255.255.0         192.168.100.1         192.168.100.1         0.0.0.0         0.0.0.0         192.168.100.2         192.168.100.2         192.168.100.2         192.168.100.2         192.168.100.2         192.168.100.2	
Enabled: IPv4 Type: IP address: IP netmask: Gateway: Primary DNS: Secondary DNS: WINS: IP range: Lease time: Max lease time: Enable Local Easy	DHCP server          192.168.100.1         255.255.255.0         192.168.100.1         192.168.100.1         0.0.0.0         0.0.0.0         192.168.100.2         192.168.100.2         192.168.100.2         192.168.100.2	
Enabled: IPv4 Type: IP address: IP netmask: Gateway: Primary DNS: Secondary DNS: WINS: IP range: Lease time: Max lease time: Enable Local Easy HostName:	□         □	
Enabled: IPv4 Type: IP address: IP netmask: Gateway: Primary DNS: Secondary DNS: WINS: IP range: Lease time: Enable Local Easy HostName:	□HCP server ▼         192.168.100.1         255.255.255.0         192.168.100.1         192.168.100.1         0.0.0.0         0.0.0.0         192.168.100.2         192.168.100.2         192.168.100.2         192.168.100.2         192.168.100.2	
Enabled: IPv4 Type: IP address: IP netmask: Gateway: Primary DNS: Secondary DNS: WINS: IP range: Lease time: Max lease time: Enable Local Easy HostName:	□HCP server ▼         192.168.100.1         255.255.255.0         192.168.100.1         192.168.100.1         0.0.0.0         0.0.0.0         192.168.100.2         192.168.100.2         192.168.100.2         192.168.100.2         192.168.100.2	
Enabled: IPv4 Type: IP address: IP netmask: Gateway: Primary DNS: Secondary DNS: WINS: IP range: Lease time: Max lease time: Enable Local Easy HostName: 1 2	□HCP server ▼         192.168.100.1         255.255.255.0         192.168.100.1         192.168.100.1         0.0.0         0.0.0         192.168.100.2<	
Enabled: IPv4 Type: IP address: IP netmask: Gateway: Primary DNS: Secondary DNS: WINS: IP range: Lease time: Max lease time: Enable Local Easy HostName: 1 2 3	□HCP server ▼         192.168.100.1         255.255.255.0         192.168.100.1         192.168.100.1         0.0.0.0         0.0.0.0         192.168.100.2         192.168.10	
Enabled: IPv4 Type: IP address: IP netmask: Gateway: Primary DNS: Secondary DNS: WINS: IP range: Lease time: Max lease time: Enable Local Fasy HostName: 1 2 3 4	□HCP server ▼         192.168.100.1         255.255.255.0         192.168.100.1         192.168.100.1         0.0.0.0         0.0.0.0         192.168.100.2         192.168.10	
Enabled: IPv4 Type: IP address: IP netmask: Gateway: Primary DNS: Secondary DNS: WINS: IP range: Lease time: Enable Local Easy HostName: 1 2 3 4 5	□HCP server ▼         192.168.100.1         255.255.255.0         192.168.100.1         192.168.100.1         0.0.0         0.0.0         192.168.100.2<	
Enabled: IPv4 Type: IP address: IP netmask: Gateway: Primary DNS: Secondary DNS: WINS: IP range: Lease time: Max lease time: Enable Local Easy HostName: 1 2 3 4 5 6	□HCP server ▼         192.168.100.1         255.255.255.0         192.168.100.1         192.168.100.1         0.0.0         0.0.0         192.168.100.2<	
Enabled: IPv4 Type: IP address: IP netmask: Gateway: Primary DNS: Secondary DNS: WINS: IP range: Lease time: Max lease time: Enable Local Easy HostName: 1 2 3 4 5 6 7	□HCP server ▼         192.168.100.1         255.255.255.0         192.168.100.1         192.168.100.1         0.0.0         0.0.0         192.168.100.2         192.168.100.2         192.168.100.2         192.168.100.2         1800         1800         14882-00         14882-00         1000	
Enabled: IPv4 Type: IP address: IP netmask: Gateway: Primary DNS: Secondary DNS: WINS: IP range: Lease time: Max lease time: Enable Local Easy HostName: 1 2 3 4 5 6 7 8	□HCP server ▼         192.168.100.1         255.255.255.0         192.168.100.1         192.168.100.1         0.0.0         0.0.0         192.168.100.2<	



23

Icotera A/S, Hovedvejen 3A, 2600 Glostrup, Denmark - info@icotera.com Document version: 1.0

#### Wi-Fi settings

In the *Wi-Fi* sections of the *Settings* menu, you can configure the general settings of the wireless interfaces, set access point parameters, as well as define Wi-Fi schedules and access lists.

The gateway displays the warning message that disabling Wi-Fi can disturb Wi-Fi extenders when the user unchecks the **Enable** check box for the 5 GHz interface and the **wifidomain** Note mode parameter is set to master. When the wifidomain mode is set to disabled, the gateway does not display the warning message. Status Wi-Fi 2.4 GHz Settings LAN Global Settings Wi-Fi 5 GHz ~ Enable: Backup Channel: Automatic selection 🗸 Diagnostic Administration Channel width: 20MHz 🗸 Services Mode: 802.11g/n/ax 🗸 TX Power: 100 🗸 % Wi-Fi 2.4 GHz APs guestWiFi2GHz homeWiFi2GHz Enable: ~ SSID: ICO\_50DE55 Encryption: WPA2 AES ~ Encryption key: Show password ..... Hidden: **Client isolation:** Enable WPS: ~ WPS: Please press the WPS button to activate WPS function. Start WPS ACL settings Client limit 0 client(s) allow 0 Access list behavior deny none 1 Clear Clear 16 Clear Reset Save Apply Figure 17. The Wi-Fi 2.4 GHz section of the Settings menu

The *Global Settings* section provides the general Wi-Fi performance settings, common for both 2.4 GHz and 5 GHz interfaces:

- Enable: enables or disables the radio interface,
- Channel: sets the channel number manually or relies on the automatic channel selection option,

- **Channel width**: channel width in MHz,
- Mode: available networking mode,
- **TX power**: Tx power level (percentage),
- **DFS Channel Cleaning mode**: use the dropdown list to choose when DFS and weather channels will be cleared:
  - \* **Auto**: when Wi-Fi is not being used,
  - \* Nightly-non-disruptive: at night.

		Wi-Fi 5 GHz
ettings 👻		
AN	Global Settings	
/i-Fi 2.4 GHz		
/i-Fi 5 GHz	Cookie.	
ackup	Enable:	
iagnostic 🔹 🕨	Channel:	Automatic selection, full DFS 🗸
dministration 🔸	Channel width:	80MHz 🗸
ervices >	Mode:	802.11a/n/ac/ax 🗸
	TX Power:	100 🕶 %
	DFS Channel Cleaning mode:	CAC nightly-non-disruptive V

The **APs** sections, common for both 2.4 GHz and 5 GHz interfaces, provide the following settings for every configured access point:

- **Enable**: enables or disables the particular access point,
- SSID: access point name that will be seen when scanning for available Wi-Fi networks,
- Encryption: type of encryption key and encryption algorithm used to secure Wi-Fi transmission between the access point and its clients. Available choices are None, WPA2 AES, WPA3 AES and WPA3-TRANSITION AES. Please note that None leaves the wireless AP unsecured and open for access from any Wi-Fi device.
- **Encryption key**: the password used to connect to the access point. The browser displays the entered characters when the **Show password** checkbox is turned on.
- *Hidden*: when checked, the chosen access point will not be detected by simple network scanning. We recommend keeping this box unchecked because hiding the access point name does not improve security
- *Client isolation*: when checked, the traffic between clients of the access point is blocked. You can use this option to create a guest access point. All devices connected to the guest access point are isolated.
- Enable WPS: turns on or off WPS.

In the **WPS** section, you can establish a WPS connection,

- Start WPS: activates the WPS procedure.
- **Reset**: resets all changes made to access point settings during the current session; **Save**: saves all changes made during the current session; **Apply**: applies all changes saved during the current session.

In the **ACL settings** section, you can configure the ACL protocol for a particular access point of a selected Wi-Fi interface.

- *Client limit*: the number of devices that can connect to the access point. Select the checkbox and enter the number of connected devices. The maximum value is 32 devices.
- Access list behaviour: defines the behaviour of the access list.
  - \* **allow**: only devices in the access list can connect to the gateway.
  - \* **deny**: prevents devices in the access list from connecting to the gateway. All other devices can connect to the gateway.
  - \* **none**: turns off the access list.
- Name: alias name for the MAC address.
- MAC Address: the physical address of the wireless adapter in a client device.
- **Enabled**: includes the device in the current access list. To temporarily exclude the device from the access list, uncheck it.

• **Clear**: removes the device from the access list.



You can connect up to 255 devices to your gateway.

#### Backup

The **Backup** section of the **Settings** menu provides tools for uploading and downloading the gateway configuration files.

In the **Upload config from local file** section, you can read the configuration from a local file:

- Choose *Choose file* to select a configuration file on your device. The gateway uploads the configuration from the chosen file.
- Check Status to see the status of the upload operation, such as no operation done or nothing to change.
- In the *Download file* section, you can save the current configuration to a local drive:
- Choose *Save* to generate and save the file with the current gateway configuration.

**Note** The backup file consists of the configuration and data modified by the user.

Status		
Settings	Upload config from local fi	le
LAN	Unload file	Chaose file
Wi-Fi 2.4 GHz	opioud nic	
Wi-Fi 5 GHz	Ctature	no exercise dans
Backup	Status	no operation done.
Diagnostic		
Administration	Download file	
Services	Click to download config:	Save
		Reset Save Apply

Figure 19. The Backup section of the Settings menu

# Using network diagnostic tools

The *Diagnostic* menu contains *Ping*, *Traceroute*, *Wi-Fi scan*, and *Reset* sections. You can use these menu sections to troubleshoot connection problems or reboot the gateway.

Because this menu does not include any configurable options, the **Reset**, **Save**, and **Apply** buttons are inactive.

#### Ping

You can use the **Ping** diagnostic tool to test the reachability of a host in an IP network.

status 🗸		pla -
Settings >		Ping
iagnostic 👻	Ping address:	0.0.0.0
ling	lice prodef val:	
Fraceroute	ose preder, var.	
Vi-Fi scan	Packet size:	32
leset	Packet count:	8
Iministration 🔸		
rvices 🕨 🕨		Ping Stop
	Results:	
	Status:	Not running
		A
		*
		11
		Reset Save Apply

Figure 20. The **Ping** tool of the **Diagnostic** menu

26

Icotera A/S, Hovedvejen 3A, 2600 Glostrup, Denmark - info@icotera.com Document version: 1.0

- **Ping address** the IPv4 address or hostname to ping.
- **Use predef. val** uses default ping parameters. By default, the ping operation sends 10 packets of 64 bytes each. If the **Use predef. val** option is inactive, then you can specify custom ping parameters.
  - \* **Packet size** the number of bytes in each ping packet.
  - \* **Packet count** the number of packets to be sent.
- **Ping** starts sending ping packets to the specified address.
- **Stop** interrupts the ping command.
- **Results** displays the output of the ping operation.
- Status shows the current state of the ping operation, such as Running or Not running.

#### Traceroute

You can use the *Traceroute* diagnostic tool to display the route and measure transit delays of packets across an IP network.

- Address the IPv4 address or hostname of the destination where the command sends the ICMP packets.
- **Diag** starts tracing the route to the destination.
- **Stop** interrupts the traceroute operation.
- **Results** displays the output of the traceroute operation.
- Status shows the current state of the traceroute operation, such as Running or Not running.

Status 🔸			
Settings >			Traceroute
Diagnostic 🔹		Address:	0.0.0.0 Diag Stop
Ping			
Traceroute	Boculter		
Wi-Fi scan	Kesuits.		
Reset		Statuc	Not running
Administration >		Status.	Not running
Services >			
			*
			Reset Save Apply

Figure 21. The Traceroute tool of the Diagnostic menu

#### Wi-Fi scan

You can use the **Wi-Fi scan** tool to run a site survey for all wireless networks in the neighbourhood. As a result of this survey, the web interface displays a list of scanned access points. You can use two separate scanners for both radio interfaces.

- Scan starts the site survey process.
- Site survey information about detected networks.
  - \* **CH** the number of the operating channel.
  - \* **Type** the connection type.
  - \* **SSID** the access point name.
  - \* **BSSID** the MAC address of the access point.
  - \* **Encryption** the encryption type and method.
  - \* **Signal [dBm]** the signal strength in dBm.

To refresh the site survey list, choose **Scan**.

#### User guide for Icotera i4882 gateways with the 2.2.5 firmware version

•
×
•

Ne	twork sca	n			
re	ss the Sca	n button to execute site sur	vey:		Scan
lea	se he aware	that a Wi-Fi rescan may disrupt Wi	-Fi communication for a while		
-ica:	se be aware	that a wint rescan may disrupt wi	-ri communication for a while.		
Site	survey:				
Ch	Туре	SSID	BSSID	Encryption	Signal [dBm]
1	AP	FTTH_PY9030	00:1e:80:9d:5f:2c	WPA2-PSK	-63
1	AP	Vestas-corp	50:0f:80:35:72:e0	WPA2-EAP	-89
1	AP	FTTH_WD9178	00:1e:80:75:2f:0c	WPA2-PSK	-69
1	AP	ICO-E8464D	00:0f:15:e8:46:51	WPA2-PSK	-90
1	AP	OLA24	00:0f:15:b8:73:39	WPA2-PSK	-54
1	AP	Vestas-visitor	50:0f:80:35:72:e2	UNSECURED	-89
1	AP	ICO-5D2609	00:0f:15:5d:26:0d	WPA2-PSK	-53
1	AP	ICO-5D2441	00:0f:15:5d:24:45	WPA2-PSK	-50
1	AP	lastmile24	00:0f:15:5d:27:8d	WPA2-PSK	-90
6	AP	Vestas-corp	40:01:7a:f0:27:b0	WPA2-EAP	-82
6	AP	Vestas-visitor	40:01:7a:f0:27:b2	UNSECURED	-81
6	AP	DIRECT-JU-BRAVIA	da:0f:99:42:57:5f	WPA2-PSK	-80
6	AP	bramka GSM	0c:37:dc:38:87:d8	WPA2-PSK	-85
6	AP	FTTH_GQ5461_2	00:1e:80:9d:25:c0	WPA2-PSK	-73
6	AP	ICO-B870D1	00:0f:15:b8:70:d5	WPA2-PSK	-56
	AD	wnet24-iot	78-45-58-17-63-56	WDA2_DSK	-47

Wi-Fi 5 GHz

Press	the Cer				
	s the sta	n button to execute site sur	vey:		Sc
Please	he aware	that a Wi-Fi rescan may disrupt Wi	-Fi communication for a while		
ricuse	, be aware	that a wirring source of the			
Site 9	survey:				
					Signa
Ch	Туре	SSID	BSSID	Encryption	[dBm
36	AP		00:1e:80:70:9f:c8	WPA2-PSK	-90
36	AP	Vestas-visitor	50:0f:80:35:72:ed	UNSECURED	-90
36	AP	Icotera Office	78:45:58:1b:55:6e	WPA2-PSK	-72
36	AP	icotera-hotspot	7e:45:58:1b:55:6e	UNSECURED	-72
36	AP		82:45:58:1b:55:6e	WPA2-PSK	-72
36	AP	Vestas-corp	50:0f:80:35:72:ef	WPA2-EAP	-90
36	AP	T3493	00:0f:15:e8:46:55	WPA2-PSK	-90
44	AP	Vestas-corp	40:01:7a:f0:27:bf	WPA2-EAP	-90
44	AP	Vestas-visitor	40:01:7a:f0:27:bd	UNSECURED	-89
44	AP	Icotera Office	78:45:58:18:c3:5e	WPA2-PSK	-45
44	AP	icotera-hotspot	7e:45:58:18:c3:5e	UNSECURED	-45
44	AP		82:45:58:18:c3:5e	WPA2-PSK	-45
48	AP	Icotera Office	78:45:58:18:bf:b4	WPA2-PSK	-85
48	AP		82:45:58:18:bf:b4	WPA2-PSK	-85
48	AP	Icotera Office	78:45:58:18:c6:83	WPA2-PSK	-90
		A CONTRACTOR OF	7 45 50 40 6 00		0.0

Figure 22. The **Wi-Fi scan** tool of the **Diagnostic** menu

#### Reset

The *Diagnostic* menu also includes the *Reset* tab.

To reboot the gateway, choose **Reboot**.

To reset the gateway to the factory default settings, choose *Factory reset*.

Status 👂	
Settings )	Reset
Diagnostic 🔹	Please press the button to reboot the CPE.
Ping	This button will reset the device to factory settings, use only when advised by support
Traceroute	
Wi-Fi scan	
Reset	Reset Save Apply
Administration 🕨	
Services 🔹	
	- Figure 37 The Perst eaction of the Disgrestic many



28 Icotera A/S, Hovedvejen 3A, 2600 Glostrup, Denmark - info@icotera.com Document version: 1.0 Next, confirm the reset or reboot of the gateway.

	i4883-00 Warning	
	Reboot requested. Click to reboot CPE.	
Fig	gure 24. Request for reboot confirmation	วท
	i4883-00 Warning	
Are you sure you want to r	eset the device to factory settings? It will result in	resetting all configuration.
	Ok Cancel	

Because this menu does not include any configurable options, the **Reset**, **Save**, and **Apply** buttons are inactive.

# **Configuring administrator settings**

The *Administration* menu provides options for changing user credentials, managing the behaviour of LED indicators, and configuring remote access to the gateway. To restore the default values for these settings, choose *Reset*. Next, choose *Save* or *Apply*.

#### **Managing user credentials**

Status	•
Settings	•
Diagnostic	•
Administration	-
UI login passwor	d
LEDs	
Remote Access	
Services	•

Figure 26. Changing password in the **Administration** menu

You can use the **UI login password** tab of the **Administration** menu to change the password. To do so, enter your **Old password**. Next, enter your **New password**, and confirm it in the **Retype new password** input field.

#### Managing the behaviour of LED indicators

You can control the behaviour of LED indicators in the *LEDs* tab of the *Administration* menu.

- **LEDs** determines the behaviour of the LED indicators.
- \* **turn on** LED indicators remain turned on all the time.
- \* **turn off LEDs will be turned on again only if an event occurs** LED indicators remain turned off except in case of an event.
- \* **turn off LEDs will be turned on again only if an error occurs** LED indicators remain turned off except in case of an error.
- \* always off LEDs will be off after system will be up all LED indicators are off after the gateway boots up.
- LEDs' brightness determines the brightness level of LED indicators,
  - \* **high** LED indicators are visible in daylight.
  - \* **medium** LED indicators are barely visible in daylight.
  - \* **Iow** LED indicators are visible in darkness but not in daylight.

Status 🔸	
Settings >	LEDs
Diagnostic 🔹 🕨	LEDs: turn on
Administration 🔻	
UI login password	LEDs' brightness: high V
LEDs	
Remote Access	Reset Save Apply
Services >	



Icotera A/S, Hovedvejen 3A, 2600 Glostrup, Denmark - info@icotera.com Document version: 1.0

29

#### **Configuring remote access**

You can use the **Remote Access** tab of the **Administration** menu to configure access to the gateway from a WAN interface.

- To turn on the remote access by using the HTTPS protocol, select **Enable** in the **HTTPS settings** section.
- For **Port**, enter the port number for the remote access. The default value is 443.
- To turn on the remote access from the Internet, select *Enable* in the *Remote access from Internet* section. The *Public URLs* field displays the URL of the web interface that you can access from the public Internet.

To restore default values for the remote access settings, choose **Reset**. Next, choose **Save** or **Apply**.

Status 🔸	
Settings 🕨 🕨	Remote Access
Diagnostic 🔹 🕨	UTTDS sottings
Administration 👻	
UI login password	Enable: 🗹
LEDs	Port: 443
Remote Access	
Services >	Remote access from Internet:
	Enable: 🗹
	Public URLs: https://
	Reset Save Apply

Figure 28. The **Remote Access** section of the **Administration** menu

#### **Managing services**

The *Services* menu provides configuration options for controlling port forwarding, ALG, and UPnP.

#### Port forwarding

You can configure port forwarding rules in the **Port forwarding** tab of the **Services** menu.

By default, all rules are disabled and inactive. To configure the fields of a rule, select its checkbox.

You can define up to 128 rules.

- Name the name of a rule.
- **Protocols** one of the available protocols. Possible options include **TCP**, **UDP**, and **BOTH.**
- **Ext. ports** the external ports range.
- Int. IP the internal IP address.
- *Int. port* the internal port number. When you use a port range, the internal port number is a starting point for this range.
- Loopback turns on or off the NAT loopback feature for a given port. The NAT loopback, also known as NAT
  hairpinning, is a feature which permits access to service via the WAN IP address (often public IP address) from
  inside the local network. By default NAT loopback option for each port forwarding rule is disabled.
- **Enabled** turns on or off the port forwarding rule for editing. When you turn off this option, then the rule is inactive and not editable.

#### User guide for Icotera i4882 gateways with the 2.2.5 firmware version

Status 🔸									
Settings 🔹 🕨	Port Forwarding								
Diagnostic 🔹 🕨	No.	Name	Protocols	Ext. ports	Int. IP	Int. port	Loopback	Enabled	
Administration >	1	portForward1	UDP 🗸	0-	0.0.0	0			
Services	2	portForward2	UDP v	0	0.0.0	0			
DMZ	3	portForward3	UDP 🗸	0-	0.0.0	0			
ALG	4	portForward4	UDP 🗸	0	0.0.0	0			
Wake On LAN	5	portForward5	UDP 🗸	0-	0.0.0	0			
UPnP	6	portForward6		0	0.0.0	0			
	125	portForward125	UDP 🗸	0 -	0.0.0	0			
	126	portForward126	UDP 🗸	0	0.0.0	0			
	127	portForward127	UDP 🗸	0	0.0.0	0			
	128	portForward128	UDP 🗸	0	0.0.0	0			

Figure 29. The **Port forwarding** section of the **Services** menu

#### DMZ

You can configure a demilitarized zone in the **DMZ** section of the **Services** menu.

Status 🕨 🕨	
Settings 🔹 🕨	DMZ
Diagnostic 🔹 🕨	Enable:
Administration 🔸	
Services 🔻	DM2 destination IP:
Port Forwarding	Description:
DMZ	
ALG	Reset Save Apply
Wake On LAN	
DDNS	
UPnP	

Figure 30. The **DMZ** section of the **Services** menu

- Select **Enable** to activate DMZ.
- For *DMZ destination IP*, enter the IP address of the DMZ destination.
- For *Description*, enter the DMZ description. You can use up to 64 characters in this description.

# ALG

Application-level gateway options are available in the **ALG** tab of the **Services** menu. Select the appropriate checkbox to activate or deactivate a chosen protocol.

Status 🕨 🕨	
Settings 🕨 🕨	ALG
Diagnostic 🕨 🕨	ALG SIP: 🔽
Administration >	
Services 🔻	ALG RTSP: 🗸
Port Forwarding	ALG FTP: 🔽
DMZ	ALG PPTP: 🗸
ALG	
Wake On LAN	ALG LZIP. V
DDNS	ALG IPSEC: 🗸
UPnP	
	Reset Save Apply

Figure 31. The ALG section of the Services menu

#### Wake On LAN

You can use the Wake On LAN feature to send a magic packet to a chosen device.

Status 🕨 🕨									
Settings >	Wake On LAN								
Diagnostic 🔹 🕨	Destination MAC: ac:19:8e:6	6:9d:29 Sour	ce interface: home_lan 🗸	Send magic packet					
Administration 🔸									
Services 🔹		No pa	icket sent						
Port Forwarding	Click a lease row to set destinat	tion parameters							
DMZ	MAC	Hostname	Туре	Interface					
ALG	ac:19:8e:66:9d:29	hp_840_G9	Dynamic	home_lan					
Wake On LAN	ac:19:86:66:90:29		AKP	nome_ian					
DDNS									
LIDER									

#### Figure 32. The Wake On LAN section of the Services menu

- **Destination MAC** the MAC address to which the gateway sends a magic packet. Choose a matching entry from a list of MAC addresses to set destination parameters. You can also send a magic packet to a host which is not in the list, for example, a device that is connected to a LAN port but is not operating,
- Source interface the interface from which to send a magic packet.
- Send magic packet sends a magic packet.

Because this menu does not include any configurable options, the **Reset**, **Save**, and **Apply** buttons are inactive.

#### DDNS

You can use the **DDNS** menu to manage the Dynamic DNS feature.

To configure the DDNS feature, enter your information in the following fields.

- To use the DDNS feature, select *Enabled*.
- For Update interval, enter the time after which the gateway updates the DDNS settings.
- For Force update interval, enter the time after which the gateway forces the update of the DDNS settings.
- For *Select active profile*, choose one of the following options: *custom*, *opendns*, *no-ip*, *freedns*, *changeip*, *dynu*.
- For *User login*, enter your dyndns.org username.
- For User password, enter your dyndns.org password.
- For **User domain**, enter the fully-qualified domain name (FQDN) of the domain that you registered at dyndns.org.
- For Service URL, enter the URL of your DDNS.
- To display information about special sequences which you can enter in the fields of this section, choose Show help. The gateway substitutes these sequences with appropriate configuration data.

Status	•								
Settings 🕨 🕨		DDNS							
Diagnostic Administration	) )	Enabled:	User login:						
Services	• •	Update interval:	12 hours User password:						
Port Forwarding		Force update interval:	24 hours						
DMZ ALG		Select active profile:	custom V						
Wake On LAN		Service URL:							
DDNS		Help:	Show help						
UPnP			Following sequences in custom service URL have special meaning and are substituted with configuration data:						
			[USERNAME] User login used for authentication						
			[PASSWORD] User password used for authentication						
			[DOMAIN] Domain name configured by user						
			[IP] System IP						
			Reset Save Apply						
			32						

Figure 33. The **DDNS** section of the **Services** menu with help displayed

#### UPnP

You can activate the Universal Plug-and-Play feature in the **UPnP** section of the **Services** menu:

Status 🕨 🕨	
Settings 🔹 🕨	UPnP
Diagnostic 🔹 🕨	Enable:
Administration >	
Services 🔹	Barak Crue Aark
Port Forwarding	Neset Save Appy
DMZ	
ALG	
Wake On LAN	
DDNS	
UPnP	

Figure 34. The **UPnP** section of the **Services** menu

# IPv6 firewall

In the IPv6 firewall section of the Services menu, you can manually specify exceptions to the stateful IPv6 firewall.

- Use firewall exceptions: activate IPv6 firewall exceptions,
- **Description**: description of a given rule,
- **Protocols**: one of the available protocols:
  - \* **TCP**,
  - \* UDP.
  - \* **ANY**.
- Destination ports: single destination port or range of ports,
- **Source IPv6**: source IPv6 address,
- Destination IPv6: destination IPv6 address,
- **Enabled**: enables or disables chosen exception.

- ·					TD	6 firowall				
ngs 🕨 🕨					IPA	o mewan				
nostic 🔹 🕨	Firour	all avcantion	-							
inistration 🔸	Firew		5							
ices 🔻		Use fi excer	rewall ptions:							
Forwarding	No	Description	Drotocolo	Doct	ination porto	Sou		Doctir	nation IDv6	Enabled
Ζ	NO.	Description	Protocols	Dest		500		Desu		Enabled
	1		ANY 🗸	0	- 0		/ 0		/ 0	
e On LAN	2		ANY 🗸	0	- 0	::	/ 0	::	/ 0	
S	3									
P										
5 firewall										
	29									
	30		ANY 🗸	0	- 0	::	/ 0	::	/ 0	
	31		ANY 🗸	0	- 0	::	/ 0	::	/ 0	
	32		ANY 🗸	0	- 0	::	/0	::	/ 0	

Figure 35. The IPv6 section of the Services menu

# Legal notice

The information contained in this document represents the current view of Icotera on the issues discussed as of the date of publication and may be subject to change without notice. Because Icotera must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Icotera, and Icotera cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. Icotera MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of lcotera.

Icotera may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering the subject matter in this document. Except as expressly provided in any written license agreement from Icotera, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Icotera A/S Hovedvejen 3A 2600 Glostrup Denmark Phone: +45 7010 0033 Mail: info@icotera.com

© 2024 Icotera. All rights reserved.