

Wireless devices preparation



Successfully pass the free certification exam at IW Academy and become an Infinet Certified Engineer.

[To the certification exam](#)

- [InfiLINK 2x2, InfiMAN 2x2, InfiLINK Evolution, InfiMAN Evolution families](#)
 - [Configuration via CLI](#)
 - [Configuration via Web interface](#)
- [InfiLINK XG, InfiLINK XG 1000 families](#)
- [Quanta 5, Quanta 70 families](#)

InfiMONITOR NEXT polls the network nodes using SNMP. This means that in order to perform management and monitoring, an SNMP agent must be started and configured on each node.

By default, the "SNMP Agent" and the "SNMP Trap" notifications are disabled. To perform monitoring using **InfiMONITOR NEXT**, perform the necessary settings in the device's configuration: enable SNMP Agent and configure the SNMP Traps.

This article provides instructions to configure devices of the each Infinet Wireless families:

- [InfiLINK 2x2, InfiMAN 2x2, InfiLINK Evolution, InfiMAN Evolution families](#)
 - [Configuration via CLI](#)
 - [Configuration via Web interface](#)
- [InfiLINK XG, InfiLINK XG 1000 families](#)
- [Quanta 5, Quanta 70 families](#)



NOTE

The **InfiMONITOR NEXT** monitoring system supports "authNoPriv" protected mode only.

InfiLINK 2x2, InfiMAN 2x2, InfiLINK Evolution, InfiMAN Evolution families

There are 2 ways how to change the configuration:

1. Using the Command Line Interface (faster way).
2. Using the Web GUI.

Configuration via CLI

A detailed description of the WANFlex OS commands is available in the [snmpd command \(SNMP daemon\)](#) article. Connect to the device using Telnet or SSH and enter the following commands (the words USERNAME and PASSWORD must be replaced with the actual values):

```
snmpd user USERNAME add pass PASSWORD security authNoPriv accessRights readWrite class admin
```

Enable the SNMP Agent and save the configuration:

```
snmpd start  
config save
```

To enable and configure the SNMP Agent simultaneously for all the CPE devices connected to a BS (including the BS itself), run the following commands at the Base Station:

Title

```
mint rf5.0 rcmd -all -self "snmpd user USERNAME add pass PASSWORD security authNoPriv accessRights
readWrite class admin"
mint rf5.0 rcmd -all -self "snmpd start"
mint rf5.0 rcmd -all -self "config save"
```

To enable SNMP Traps simultaneously for all the CPE devices connected to a BS (including the BS itself), run the following commands at the Base Station: (replace "*P ADDRESS*" with the IP address assigned to **NEXT**):

```
mint rf5.0 rcmd -all -self "trapd start"
mint rf5.0 rcmd -all -self "trapd dst IP ADDRESS:162/v2"
mint rf5.0 rcmd -all -self "trapd type topoGroup enable"
mint rf5.0 rcmd -all -self "trapd type radioGroup enable"
mint rf5.0 rcmd -all -self "trapd type mintGroup enable"
mint rf5.0 rcmd -all -self "trapd type ospfGroup enable"
mint rf5.0 rcmd -all -self "trapd type linkEvent enable"
mint rf5.0 rcmd -all -self "trapd typetrapdColdStartEvent enable"
mint rf5.0 rcmd -all -self "trapd type snmpdAuthenticationFailureEvent enable"
mint rf5.0 rcmd -all -self "trapd type syslog enable"
mint rf5.0 rcmd -all -self "config save"
```

Configure the agent's IP address on each device (replace "*IP ADDRESS*" with the IP address of the device):

```
trapd agent IP ADDRESS
config save
```

Configuration via Web interface



NOTE

You can also use the Command Line section of the web interface to execute the commands described above.

Login to the device's web interface. Go to the "Basic settings" page -> "SNMP" to the "Access" section:

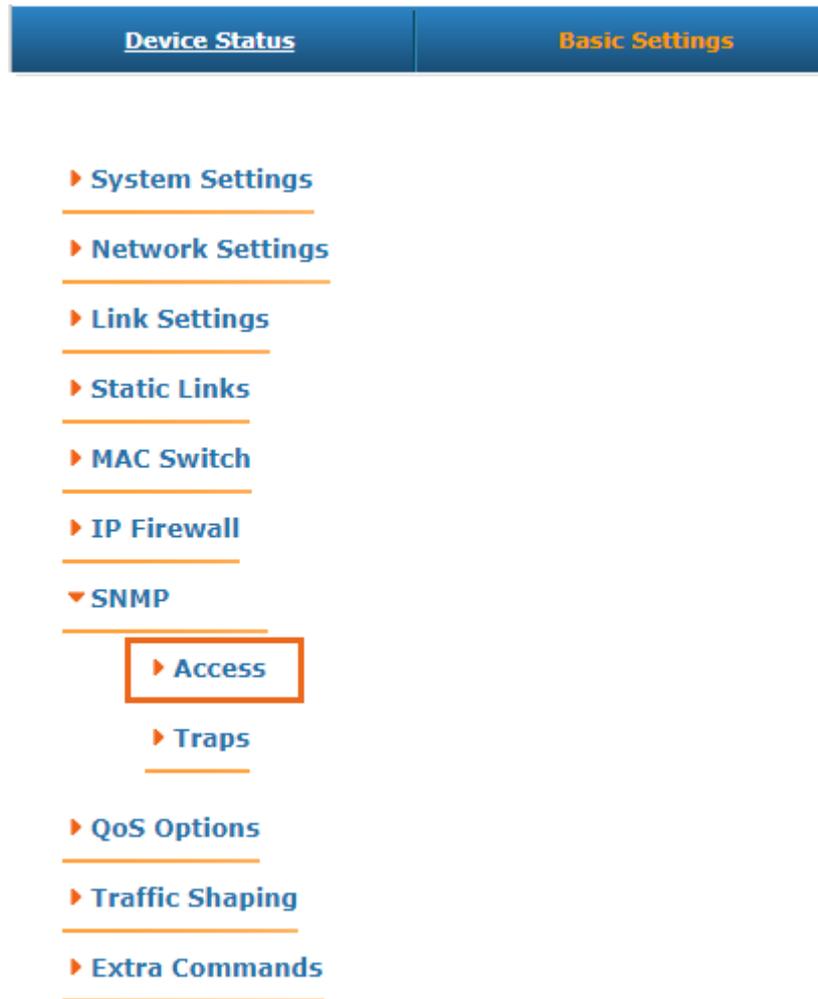


Figure - SNMP section

Perform the following steps:

- Set the "Start SNMP" flag to enable the SNMP Agent.
- Uncheck the "Version 1 enable" flag to disable the SNMPv1 version, which is enabled by default.
- Click the "Add SNMP v3 user" and enter the authentication data for accessing the network node via SNMP in the "Username" and "Password" fields.
- For the other parameters available in this section, keep the default values.

▼ SNMP

▼ Access

Help Start SNMP: Version 1 enable: Community: public Contact: Location:

User Name	Password	Security	Readonly	Admin	Privacy Password	Privacy Protocol	
admin	masterkey	Authorization No Privacy	<input type="checkbox"/>	<input checked="" type="checkbox"/>		DES	Remove User

Add SNMP v3 User

► Traps

► QoS Options

► Traffic Shaping

► Extra Commands

Apply Test Preview Configuration

Figure - SNMP authentication settings for InfiLINK 2x2, InfiMAN 2x2, InfiLINK Evolution, InfiMAN Evolution

Go to the "Traps" section where the following fields are available:

- "Enable SNMP Traps" - enable/disable traps. Check this flag.
- "Agent IP" - enter the device's IP address.
- "Destination" - the **NEXT** IP address and the UDP port, through which the polling subsystem receives notifications (by default it is port 162):
 - "V2" - enable/disable SNMP v2. Check this flag.
 - "Traps groups" - check flags for all the trap groups, that should be sent by the device.

▼ SNMP

▶ Access

▼ Traps

Help Enable SNMP Traps: Agent IP: ... X Transport: IP

Destination: ...: X + V2

topoGroup	<input checked="" type="checkbox"/>
topoEvent	<input checked="" type="checkbox"/>
newNeighborEvent	<input checked="" type="checkbox"/>
lostNeighborEvent	<input checked="" type="checkbox"/>

radioGroup	<input checked="" type="checkbox"/>
radioFreqChanged	<input checked="" type="checkbox"/>
radioBandChanged	<input checked="" type="checkbox"/>

mintGroup	<input checked="" type="checkbox"/>
mintRetries	<input checked="" type="checkbox"/>
mintBitrate	<input checked="" type="checkbox"/>
mintSignalLevel	<input checked="" type="checkbox"/>

ospfGroup	<input type="checkbox"/>
ospfNBRState	<input type="checkbox"/>

Figure - SNMP Traps configuration for InfiLINK 2x2, InfiMAN 2x2, InfiLINK Evolution, InfiMAN Evolution

To complete the setup, click on the "Apply" button.

InfiLINK XG, InfiLINK XG 1000 families

Title

Log in to the device's web interface. Go to the "SNMP" section.

Perform the following steps:

- Set the "Start SNMP" flag to enable the SNMP Agent.
- Uncheck the "Version 1 enable" flag to disable the SNMPv1 and v2c versions, which is enabled by default.
- Click the "Add SNMP v3 user" and enter the authentication data for accessing the network node via SNMP in the "Username" and "Password" fields.
- For the other parameters available in this section, keep the default values.

General Settings

Start SNMP: Contact: Location:

SNMP v1 and v2c (Read Only)

Enable SNMP v1 and v2c: Community:

SNMP v.3 Users

User Name	Password	Security	Readonly	Admin	Privacy Password	Privacy Protocol
<input type="text" value="admin"/>	<input type="text" value="masterkey"/>	Authorization No Privacy	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text"/>	DES
<input type="button" value="Add SNMP v3 User"/>						
<input type="button" value="Apply"/> <input type="button" value="Try"/>						

Figure - SNMP authentication settings for InfiLINK XG, InfiLINK XG 1000

In order to configure SNMP traps go to the "Traps" section and perform the following steps:

- Enable SNMP Traps by checking "Enable SNMP traps" flag.
- Enter the device's IP address.
- Click the "Configure SNMP traps and destinations" button and in pop-up window fill in the following fields:
 - "Destination address" - the NEXT IP address.
 - "v2c" - enable/disable SNMP v2. Check this flag.
 - "Traps groups" - check flags for all the trap groups, that should be sent by the device.

SNMP traps

Enable SNMP Traps:

Source IP Address: . . .

Edit

Destination address:

. . . . +

radioGroup

radioFreqChanged

radioBandChanged

others

linkEvent

trapdColdStartEvent

snmpdAuthenticationFailureEvent

syslog

Figure - SNMP Traps configuration for InfiLINK XG, InfiLINK XG 1000

Quanta 5, Quanta 70 families

Log in to the device's web interface. Go to the "SNMP" section.

Perform the following steps:

- Enable SNMP agent by activating the corresponding flag.
- Uncheck the "Version 1 enable" flag to disable the SNMPv1 version, which is enabled by default.
- Click the "Add SNMP v3 user"

Enabled:

Contact person:

Location:

SNMP v1/v2c

Enabled (read only):

Community:

SNMP v3

User Name	Password	Security	Readonly	Admin	Privacy Password	Privacy Protocol		
admin	masterkey	Auth / No privacy	No	Yes	-	DES		
-	-	No auth / No privacy	Yes	No	-	DES		

+ Add SNMP v3 User

Figure - SNMP authentication settings for Quanta 5, Quanta 70

- Select the "Auth/No privacy" mode
- Enter the authentication data for accessing the network node via SNMP in the "Username" and "Password" fields.
- For the other parameters available in this section, keep the default values.

Edit SNMP v3 User

User Name:

admin_122

Password:

admin122

Security:

Auth / No privacy

Readonly:



Admin:



Privacy Password:

Privacy Protocol:

des

Close

Figure - SNMP v3 settings for Quanta 5, Quanta 70

In order to configure SNMP traps go to the "Traps" section and perform the following steps:

- Enable SNMP Traps by checking "Enable SNMP traps" flag.
- Enter the device's IP address.
- Click the "Configure SNMP trap" button

SNMP Traps

Enable SNMP Traps:

Source IP address:

Destination address	Port	
192.168.11.26	: 162	 

+ Add SNMP Trap

Figure - SNMP traps settings for Quanta 5, Quanta 70

- In pop-up window fill in the following fields:
 - "Destination address" - the **NEXT** IP address and port.
 - "Traps groups" - check flags for all the trap groups, that should be sent by the device.

Edit SNMP Trap

Destination address: Port:

Radio Group

Radio Frequency Changed:

Radio Band Changed:

Others

Link Event:

Trapd Cold Start Event:

SNMP Authentication Failure Event:

Syslog:

Close

Figure - SNMP trap settings for Quanta 5, Quanta 70