

SNMP settings



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

[To the certification exam](#)

SNMP allows the administrator to gather information about key device parameters and wireless links, including information about changes. The use of any monitoring system helps to timely receive information about the network infrastructure state using Infinet devices. Currently, the devices family supports SNMP protocol versions v1 v2c and v3.

The SNMP Protocol has two branches, the agent and the management stations:

- The agent sends data to the management station. Monitoring system - provides data gathering from all agents in the network.
- The monitoring system receives and processes events.
- The information is passed through requests and replies with the use of the MIB.
- The management station or monitoring system is responsible for decoding the SNMP packets and providing an interface to the administrator.

General settings

This section allow to enable/disable SNMP protocol support.

General settings

Enabled:



Contact person:

Max Mad

Location:

55.75, 37.6167

Figure - General SNMP settings

Parameter	Description
Enabled	Enable/disable the SNMP service in the device.
Contact person	A reference information about the device owner.
Location	The geographical location where the unit is installed, used as a reference information about the physical device's location.

SNMP v1/v2c

SNMP v1/v2c

Enabled (read only):



Community:

public

Figure - SNMP v1/v2c configuration

Parameter	Description
Enabled	Enable/disable the SNMP v.1 and v.2c support. The first version of the SNMP protocol lacks security, that hinders its use for network management, so SNMP v.1 and v.2c operates in read-only mode. Enabled by default.
Community	Set the community name for read-only mode of SNMP v.1 and v.2c, by default: " <i>public</i> ". The community name passes along with the data packet in clear text.

SNMP v3

Due to the security level of SNMP v.3 is higher than of SNMP v.1 and v.2c, it allows not only the data collection but also to manage devices. Detailed information about the devices management via the [monitoring system](#) is available in the corresponding article.

SNMP v3						
User Name	Password	Security	Readonly	Admin	Privacy Password	Privacy Protocol
admin	masterkey	Auth / No privacy	No	Yes	-	DES
root	root1234	Auth / No privacy	No	Yes	-	DES
+ Add SNMP v3 User						

Figure SNMP v3 configuration

To add an SNMP v3 user, click the corresponding button and fill in the following fields:

Parameter	Description
User name	SNMP v3 user name.
Password	SNMP v3 password.
Security	Security level: <ul style="list-style-type: none"> • "No auth / No privacy" – the lowest security level without authentication and privacy, only Username needs to be set. This level of protection does not allow management via the monitoring system. • "Auth / No privacy" – middle level with authentication but without privacy, Username and Password are required. • "Auth / Privacy" – highest level with authentication and privacy, Username, Password, Privacy Password and Privacy Protocol should be set.
Readonly	Enable/disable the read-only mode, readonly is set by default.
Admin	Enable/disable the full access to all parameters, for example, the ability to reboot the device. By default an access is limited.
Privacy password	Set the privacy password, it is necessary when privacy is enabled for the required security level.

Edit SNMP v3 User

User Name:

Password:

Security:

Auth / No privacy

Readonly:

Admin:

Privacy Password:

Privacy Protocol:

des

Close

Figure - SNMP v3 user configuration

SNMP traps

The devices polling cycle of the monitoring system is 5 minutes. To speed up the process of detecting incidents on devices, SNMP traps can be send each time an incident occurs, regardless of the polling process.

SNMP Traps

Enable SNMP Traps:

Source IP address:

192.168.103.11

Destination address

Port

192.168.200.55

:

162

+ Add SNMP Trap

Figure - SNMP traps configuration

Parameter	Description
Enable SNMP traps	Enable/disable SNMP traps sending.
Source IP address	Set the IP address of the device which sends traps.

To create a new record, click the "Add SNMP Trap" button.

Edit SNMP Trap

Destination address:

192.168.200.55

Port:

162

Radio Group

Radio Frequency Changed:

Radio Band Changed:

Others

Link Event:

Trapd Cold Start Event:

SNMP Authentication Failure Event:

Syslog:

Close

Figure - Create SNMP trap

In the new window select the traps type to send and fill in the following parameters:

Parameter	Description
Destination address	Set the monitoring system server IP address.
Port	Set the monitoring system UDP port.