Network

Overview

Use the Network menu item to set up network services such as DHCP and VPN or to manage security settings such as SSL certificates and port authentication in accordance with IEEE 802.1X.

Settings

Network settings

The available settings depend on the selected network service.

When using a DHCP service, the device automatically receives the IP address from the DHCP server. Therefore, when DHCP is selected as the network service, the IP address and subnet mask are inactive and cannot be edited. In addition, the option of a static IP address can be used as a fallback. The device can be reached at the static address as soon as the DHCP service is not available. To do this, the static IP address and the subnet mask must be entered.

When configuring the network settings manually, the IP address, subnet mask and gateway must be entered.

The IP addresses of the DNS servers (Domain Name System) must also be entered. These assign the domain names to the IP addresses. This is required for KentixONE-GO, for example.

IEEE 802.1X

To establish a connection to a network protected with 802.1X, port authentication must be activated. The user name and password for authentication using the EAP (Extensible Authentication Protocol) authentication method can then be entered. If the password has already been hashed by the authentication server, the “Password is already hashed” function must be activated.

Authentication methods other than EAP are currently not supported.

SSL certificate

For a secure connection between the integrated web server of the Kentix device and a browser, an SSL certificate can be loaded onto the device. The file that is uploaded contains the certificate and a key. These can be generated with OpenSSL, for example.

Example for creating a self-signed certificate with OpenSSL

Create temporary folder

$ mkdir ~/Desktop/cert

Create certificate and key file

$ openssl req -x509 -newkey rsa:2048 -keyout ~/Desktop/cert/key.pem -out ~/Desktop/cert/cert.pem \ -days 999 -subj "/C=DE/ST=RP/L=Idar-Oberstein/O=Kentix GmbH/OU=Org/CN=192.168.100.222" -nodes

Combining the key file and the certificate

$ cat ~/Desktop/cert/key.pem ~/Desktop/cert/cert.pem > ~/Desktop/cert/server.pem

Satellite settings

The Ethernet-enabled Kentix devices can operate in Main Device, Stand-Alone Device, or Satellite Device modes. The selection of the operating mode differentiates the functionalities that are available in the device's own KentixONE web interface.

Satellite Devices are operated in conjunction with other Kentix devices. The administration takes place centrally at the Main Device. Satellite Devices can serve as gateway for further sensors or DoorLocks. The configuration of the sensors and DoorLocks is not done on the Satellite Device, but on the Main Device.

To set a device to satellite device mode, the IP address of the main device is required. In addition, the satellite device must be taught in on the main device via the Dashboard menu item.

Devices	Main Device	Satellite Device	Stand-Alone Device
SiteManager AlarmManager			
MultiSensor			
AccessManager			
PowerManager			
SmartPDU			

Listing of devices and supported operating modes

VPN

A virtual private network (VPN) is used to set up a network that is not visible to other network participants. To establish a VPN connection from the Kentix device to a server, an OpenVPN server is required.

A configuration file generated by the VPN server and a certificate from the responsible certification authority are required to establish a connection to a VPN. As soon as the configuration file and the certificate have been uploaded, the connection can be activated by clicking on the "Active" button and then saving. If the connection is successfully established, the address and subnet mask of the

VPN connection appear in the grayed-out fields.