Netzwerk

Übersicht

Verwenden Sie den Menüpunkt Netzwerk, um Netzwerkdienste wie DHCP und VPN einzurichten oder Sicherheitseinstellungen wie SSL-Zertifikate und Port Authentifizierung nach IEEE 802.1X zu verwalten.

Einstellungen

Netzwerkeinstellungen

Die verfügbaren Einstellungen hängen vom gewählten Netzwerkdienst ab.

Bei Verwendung eines DHCP-Dienstes erhält das Gerät die IP-Adresse automatisch vom DHCP-Server. Daher sind bei der Auswahl von DHCP als Netzwerkdienst die IP-Adresse und die Subnetzmaske inaktiv und können nicht bearbeitet werden. Zusätzlich kann die Option einer statischen IP-Adresse als Fallback verwendet werden. Das Gerät ist unter der statischen Adresse erreichbar, sobald der DHCP-Dienst nicht verfügbar ist. Dazu müssen die statische IP-Adresse und die Subnetzmaske eingegeben werden.

Bei der manuellen Konfiguration der Netzwerkeinstellungen müssen die IP-Adresse, die Subnetzmaske und das Gateway eingetragen werden.

Zusätzlich müssen die IP-Adressen der DNS-Server (Domain Name System) eingetragen werden. Diese ordnen die Domain-Namen den IP-Adressen zu. Dies wird zum Beispiel für KentixONE-GO benötigt.

IEEE 802.1X

Um eine Verbindung zu einem mit 802.1X geschützten Netzwerk herzustellen, muss die Port Authentifizierung aktiviert werden. Danach können der Benutzername und das Passwort für die Authentifizierung mit der Authentifizierungsmethode EAP (Extensible Authentication Protocol) eingegeben werden. Falls das Passwort bereits vom Authentifizierungsserver gehasht wurde, muss die Funktion „Passwort ist bereits gehasht“ aktiviert werden.

Andere Authentifizierungsmethoden als EAP werden derzeit nicht unterstützt.

SSL-Zertifikat

Für eine sichere Verbindung zwischen dem integrierten Webserver des Kentix Gerätes und einem Browser kann ein SSL-Zertifikat auf das Gerät geladen werden. Die Datei, die hochgeladen wird, enthält das Zertifikat und einen Schlüssel. Diese können zum Beispiel mit OpenSSL erzeugt werden.

Beispiel zum Erstellen eines selbstsignierten Zertifikats mit OpenSSL

Temporären Ordner erstellen

$ mkdir ~/Desktop/cert

Zertifikat und Keydatei erstellen

$ 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

Kombinieren der Keydatei und des Zertifikats

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

Satellite-Einstellungen

Die Ethernet-fähigen Kentix Geräte können in den Betriebsarten Main Device, Stand-Alone Device oder als Satellite Device betrieben werden. Durch die Wahl der Betriebsart unterscheiden sich die Funktionalitäten, die im geräteeigenen KentixONE Webinterface zur Verfügung stehen.

Satellite Devices werden im Verbund mit anderen Kentix Geräten betrieben. Die Administration erfolgt zentral am Main Device. Satellite Devices können als Gateway für weitere Sensoren oder DoorLocks dienen. Die Konfiguration der Sensoren und DoorLocks erfolgt nicht auf dem Satellite Device, sondern auf dem Main Device.

Um ein Gerät auf die Betriebsart Satellite Device zu stellen, wird die IP-Adresse des Main Device benötigt. Zusätzlich muss das Satellite Device auf dem Main Device über den Menüpunkt Dashboard eingelernt werden.

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

Auflistung der Geräte und unterstützten Betriebsarten

VPN

Ein virtuelles privates Netzwerk (VPN) dient dazu, ein Netzwerk aufzubauen, das für andere Netzwerkteilnehmer nicht einsehbar ist. Um eine VPN-Verbindung vom Kentix Gerät zu einem Server aufzubauen, wird ein OpenVPN-Server benötigt.

Für den Verbindungsaufbau zu einem VPN wird eine vom VPN-Server erzeugte Konfigurationsdatei und ein Zertifikat der zuständigen Zertifizierungsstelle benötigt. Sobald die Konfigurationsdatei und das Zertifikat hochgeladen wurden, kann die Verbindung durch Klicken auf den Button „Aktiv“ und anschließendes Speichern aktiviert werden. Bei erfolgreichem Verbindungsaufbau erscheinen in den ausgegrauten Feldern die Adresse und die Subnetzmaske der VPN-Verbindung.