Communication

Overview

The Communication menu item can be used to configure network protocols such as SMTP, SNMP, LDAP and the transmission protocol for hazard alarm systems (in accordance with VdS guideline 2465).

e-mail

In the event of alarms and warnings, the system can send e-mails with the corresponding messages. This function is deactivated by default.

To activate the function, the e-mail address and the address of the SMTP server (Simple Mail Transfer Protocol) of an e-mail account must be entered. The Simple Mail Transfer Protocol transmits e-mails unencrypted in plain text by default. Encryption is possible and is initiated by the SMTP client. If an encryption mode is used, this must be specified. The supported encryption modes are SSL and STARTTLS. Depending on the encryption mode, the corresponding default port is preset, which can be changed manually at any time. If the SMTP server requires authentication, the user name and password of the e-mail account must also be entered.

If the KentixONE-GO subscription is activated, it is also possible to send e-mails via the KentixONE-GO service. No further settings are required for this. The KentixONE-GO server uses STARTTLS as encryption mode.

SNMP

SNMP (Simple Network Management Protocol) is a network protocol for monitoring and managing network elements. A manager can use this to query measured values, alarms and other variables of an SNMP agent. KentixONE is able to send data packets to a manager as well as receive data packets from an agent. In this case, KentixONE is the manager. SNMP also offers the option of independently sending messages to the manager as soon as a certain event occurs. Such an initial notification is referred to as a “trap”.

SNMP configuration

To activate SNMP on a Kentix device, the corresponding checkbox must be selected. A list in the form of a CSV file with all measurement and configuration values provided by KentixONE can then be downloaded. Each value has a unique identifier (OID), which is defined by the ASN.1 standard is defined. In addition, an MIB file (Management Information Base) containing the OID tree structure can be downloaded from the Software section of the Kentix homepage. Each branch of the tree structure has a name and a number. As you move through the tree structure (MIB walk), the individual nodes become more and more specific.

When KentixOne receives a trap from an agent, KentixONE can retrieve all monitored OIDs of the

agent again. A separate query is started for each configured OID.

The receipt of a trap triggers an immediate update of all OIDs of the agent sending the trap.
This enables prompt alerting through OID values.
In normal operation, these values are updated by Kentix ONE at user-defined intervals of 1, 3, 10 or 20 minutes.

SNMP accesses

In order for data to be exchanged between the agent and manager, access between the agent and manager must first be configured. The table lists all accesses created. Click on the “+” tab to create a new account and a new configuration window will appear.

General

To set up SNMP access, you must specify whether KentixONE is to act as an agent or as a manager. Three different SNMP types can be set for this purpose. KentixONE is the agent for the SNMP types “Provide data” and “Trap”. KentixONE is the manager for the “Receive data” type. A name and the SNMP version must be assigned to the access. The name of the access appears in the table of all created accesses and when adding SNMP sensors in the detail view and helps with their management. The SNMP version must match for both the agent and the manager. KentixONE supports SNMPv2 and SNMPv3, which differ mainly in the security of data packet transmission. Set the version accordingly. Newly created accounts are not active by default. This must be changed manually by clicking on the corresponding checkbox.

If KentixONE acts as a manager, SNMP sensors can be added in the Detail View. The sensor is assigned the corresponding OID there.

Traps

The menu item only appears if “Trap” is set as the SNMP type. Traps can be sent for the following events:

1. Coldstart / An interruption in the power supply triggers a trap.
2. Warm start / A restart of the device triggers a trap.
3. Alarm / As soon as an alarm occurs, a trap is triggered.
4. Alarm status change / As soon as the status of the alarm changes from alarm to no alarm or from no alarm to alarm, a trap is triggered. The change from acknowledgeable alarm to alarm also triggers a trap.
5. Access / As soon as an attempt is made to open a SmartAccess component, a trap is triggered.

You can choose between two different display types for alarm and access traps. Bei einem strukturierten Alarm- oder Zutrittstrap werden die Alarmwerte in einem Datenpaket in einzelne OIDs gepackt und gesendet. Bei einem normalen Alarmtrap werden alle Alarmwerte, nur durch ein Komma getrennt, in einen einzigen OID gepackt und gesendet. Beim SNMP-Typ Änderung Alarmstatus werden die Traps immer als strukturierter Trap gesendet.

Authentication

The authentication depends on the SNMP version used.

Version 2 uses so-called communities for authentication between agent and manager. Communities are names that are transmitted by the SNMP service together with the request and represent a previously agreed key (pre-shared key).

From version 3, an authentication protocol and a privacy protocol can be selected. In addition to the two protocols, a user name must be assigned. This is used for authentication. SNMP 3 supports the following combinations:

1. No authentication and no privacy protocol
2. Authentication and no privacy protocol
3. Authentication and privacy protocol

HMAC-MD5 (hash-based message authentication code) and HMAC-SHA can be selected as authentication protocols. SHA and MD5 are two different hash functions. As soon as an authentication protocol is used, the authentication password is also required.

With the “Authentication and Privacy Protocol” combination, a privacy protocol must be selected in addition to the authentication protocol mentioned above. The encryption algorithms DES (Data Encryption Standard), 3DES (Triple-DES), AES (Advanced Encryption Standard) and IDEA (International Data Encryption Algorithm) are supported. With the Advanced Encryption Standard, the key length must also be specified (AES128, AES192, AES256). The Advanced Encryption Standard also offers the option of using a 3DES-enhanced key. In addition to the protocol, the privacy password must be entered.

Settings

As soon as KentixONE wants to query data from an agent, the IP address of the host and the port on which the SNMP service is running are required.

As the SNMP type “Trap” sends an unsolicited data packet to the manager, the IP address of the host and the port must also be specified here. A heartbeat can also be configured. This is used for cyclical function control of the agent. The heartbeat interval specifies the length of the time interval between two heartbeat messages. To test the settings, a single heartbeat message can also be sent by clicking on the “Send trap” button.

LDAP

The Lightweight Directory Access Protocol (LDAP) is a network protocol for querying and changing user and address data and their attributes that are stored in a database. KentixONE has an integrated LDAP client that can interact with an LDAP server on which the user and address data is stored in a database.

LDAP server

To import data from the server into KentixONE, the IP address of the server and the port number are required. If the communication between client and server is to be encrypted, the SSL encryption mode must be set both on the server and in KentixONE. The data is organized on the LDAP server in a tree structure. An individual object in the database is uniquely identified by the Distinguished Name (DN). The base DN defines where in the tree the search for objects should be started. In addition, by activating the “Soft Delete” function, users already imported into KentixONE who are later deleted on the LDAP server are blocked instead of deleted.

Authentication

To import user data into KentixONE, the bind DN and password are required. The bind DN tells the server who wants to perform the access.

System authorizations

Currently, two user groups created in KentixONE can be assigned to two user groups by the LDAP server. All these users have the authorizations that are assigned to the respective user group. These can be edited under the SMARTACCESS menu item. In addition to the two groups, administrators can be imported separately from the LDAP server into KentixONE.

Attributes

To import the user data into KentixONE, the type designations of the attributes of the LDAP directory must also be assigned to the corresponding attributes in KentixONE.

Synchronization

To ensure that the LDAP server and KentixONE have the same database, the two databases must be synchronized at regular intervals. A synchronization interval can be set for this purpose.

Once all settings have been made, they must be saved.

External access

External access evaluation can be activated under this menu item. As soon as external access evaluation is activated, bookings are no longer evaluated on the AccessManager.

For external evaluation, KentixONE offers the option of sending webhooks for bookings. A corresponding webhook must be configured for this. The DoorLock can be opened using the Kentix SmartAPI via an API call.

The Kentix SmartAPI documentation contains further information on the necessary parameters for the API request.

Example webhook

```
{
"UserRfidUid": "$USER_RFID_UID$",
"UserRfidData": "$USER_RFID_DATA$",
"UserRfidPin": "$USER_PIN$",
"DeviceWhichHasBeenBooked": "$DEVICE_ID$",
}
```

VdS 2465

KentixONE (from version 8.4.0) is able to transmit messages in accordance with the VdS 2456 directive (transmission protocol for hazard alarm systems) to corresponding control centers via networks of the TCP protocol family. This requires at least one KentixONE-GO license for 50 devices.

General

In order for KentixONE to be able to transmit messages to a control center, the IP address and port number of the control center via which the connection is to be established is required. An alternative IP address and port number can also be specified. Dies ist zum Beispiel bei einem Server mit zwei Netzwerkinterfaces oder bei einem gespiegelten System erforderlich.

The transmission units are provided with an identifier (VdS ID), which is uniquely assigned to each transmission unit by the control center. The VdS ID is used to uniquely assign the transmission units on the control center side and as an index for encryption.

The Advanced Encryption Standard (AES) is used as the encryption standard. To do this, an AES key and the key number generated by the control center must be entered. When establishing communication between the transmission unit and the control center, the first ticket is sent unencrypted from the transmission unit to the control center by default. The control center then sends an encrypted ticket (AES) containing the session keys for the encrypted communication. If the first ticket is to be sent to the control center already encrypted (AES), “Encrypted” must be entered in the Authentication menu field.

To check the function of the transmission unit and the control center, the tickets are transferred cyclically between the two. When the tickets are exchanged between the two can be set in the Routine time menu item. In addition, depending on the configuration of the control center, a routine ticket or an event notification with the message ID 0x53 is requested when a connection is established.

KentixONE checks the connection to the control center at cyclical intervals. If a connection is lost, it is possible to send a message. All users with activated system notifications receive an alarm message. To do this, the corresponding function must be activated.

Reporting lines

An alarm line (alarm group) is a group of alarms in an alarm area that has its own display for alarms in the control center with the aim of identifying the alarm location.

To configure a signaling line, the corresponding alarm group and alarm type must be assigned to the signaling line number. The alarm group can be configured in the Detail View menu item and maps the structure by building, floor, room or function depending on the configuration. Various alarm types can be configured. A message is only sent to the control center via the corresponding message line in the event of an alarm that corresponds to the set alarm type.