Kommunikation

Übersicht

Über den Menüpunkt Kommunikation können Netzwerkprotokolle wie SMTP, SNMP, LDAP und das Übertragungsprotokoll für Gefahrenmeldeanlagen (gemäß VdS-Richtlinie 2465) konfiguriert werden.

E-Mail

Bei Alarmen und Warnungen kann das System E-Mails mit den entsprechenden Meldungen versenden. Diese Funktion ist standardmäßig deaktiviert.

Um die Funktion zu aktivieren, muss die E-Mail-Adresse und die Adresse des SMTP-Servers (Simple Mail Transfer Protocol) eines E-Mail-Kontos eingegeben werden. Das Simple Mail Transfer Protocol überträgt E-Mails standardmäßig unverschlüsselt im Klartext. Eine Verschlüsselung ist möglich und wird vom SMTP-Client initiiert. Wird ein Verschlüsselungsmodus verwendet, muss dieser angegeben werden. Die unterstützten Verschlüsselungsmodi sind SSL und STARTTLS. Je nach Verschlüsselungsmodus wird der entsprechende Standardport voreingestellt, der jederzeit manuell geändert werden kann. Wenn der SMTP-Server eine Authentifizierung erfordert, müssen zusätzlich der Benutzername und das Passwort des E-Mail-Kontos angegeben werden.

Zusätzlich besteht bei aktiviertem KentixONE Plan die Möglichkeit, E-Mails über den KentixONE Onlinedienst zu versenden. Hierfür sind keine weiteren Einstellungen notwendig. Der KentixONE Maildienst verwendet STARTTLS als Verschlüsselungsmodus.

SNMP

SNMP (Simple Network Management Protocol) ist ein Netzwerkprotokoll um Netzwerkelemente überwachen und verwalten zu können. Hierüber kann ein Manager Messwerte, Alarme und weitere Variablen eines SNMP-Agenten abfragen. KentixONE ist in der Lage sowohl Datenpakete an einen Manager zu versenden als auch von einem Agenten Datenpakete zu empfangen. In diesem Fall ist KentixONE der Manager. SNMP bietet zusätzlich die Möglichkeit, eigenständig Nachrichten an den Manager zu versenden, sobald ein bestimmtes Ereignis eintritt. Eine solche Initiativbenachrichtigung wird als „Trap“ bezeichnet.

SNMP Konfiguration

Um SNMP auf einem Kentix Gerät zu aktivieren, muss die entsprechende Checkbox ausgewählt werden. Anschließend kann eine Liste in Form einer CSV-Datei mit allen von KentixONE zur Verfügung gestellten Mess- und Konfigurationswerten heruntergeladen werden. Jeder Wert hat einen eindeutigen Identifikator (OID), der durch den ASN.1 Standard definiert ist. Zusätzlich kann auf der Kentix Homepage im Bereich Software eine MIB-Datei (Management Information Base) heruntergeladen werden, die die OID-Baumstruktur enthält. Jede Verzweigung der Baumstruktur hat einen Namen und eine Nummer. Beim Durchlaufen der Baumstruktur (MIB-Walk) werden die

einzelnen Knoten immer spezifischer.

Nach Aktivierung der SNMP Funktion kann für jedes Element in der DetailView (Alarmgruppen und Geräte) eine Liste der für das Element erzeugten OIDs angezeigt werden.

Wenn KentixOne eine Trap von einem Agenten empfängt, kann KentixONE alle überwachten OIDs des Agenten erneut abrufen. Für jede konfigurierte OID wird eine separate Abfrage gestartet.

Der Empfang eines Traps löst eine sofortige Aktualisierung aller OIDs des den Trap versendenden Agents aus.
Dies ermöglicht eine zeitnahe Alarmierung durch OID Werte.
Im Normalbetrieb werden diese Werte in vom Benutzer eingestellten Abständen von 1, 3, 10 oder 20 Minuten von Kentix ONE aktualisiert.

SNMP Zugänge

Damit ein Datenaustausch zwischen Agent und Manager stattfinden kann, muss zunächst ein Zugang zwischen Agent und Manager konfiguriert werden. In der Tabelle sind alle angelegten Zugänge aufgelistet. Durch Klicken auf den Reiter „+“ wird ein neuer Zugang angelegt und ein neues Konfigurationsfenster erscheint.

Allgemein

Um einen SNMP-Zugang einzurichten, muss festgelegt werden, ob KentixONE als Agent oder als Manager agieren soll. Dazu können drei verschiedene SNMP-Typen eingestellt werden. Bei den SNMP-Typen „Daten bereitstellen“ und „Trap“ ist KentixONE der Agent. Beim Typ „Daten empfangen“ ist KentixONE der Manager. Dem Zugang muss ein Name und die SNMP-Version zugewiesen werden. Der Name des Zugangs erscheint in der Tabelle aller angelegten Zugänge und beim Hinzufügen von SNMP-Sensoren in der Detail View und hilft bei deren Verwaltung. Die SNMP Version muss sowohl beim Agent als auch beim Manager übereinstimmen. KentixONE unterstützt SNMPv2 und SNMPv3, die sich hauptsächlich in der Sicherheit der Übertragung der Datenpakete unterscheiden. Stellen Sie die Version entsprechend ein. Neu angelegte Zugänge sind standardmäßig nicht aktiv. Dies muss manuell durch Anklicken der entsprechenden Checkbox geändert werden.

Wenn KentixONE als Manager agiert, können in der Detail View mit „Gerät hinzufügen“ SNMP-Sensoren hinzugefügt werden. Dem Sensor wird dort die entsprechende OID zugewiesen.

Traps

Der Menüpunkt erscheint nur, wenn als SNMP-Typ „Trap“ eingestellt ist. Traps können bei folgenden Ereignissen gesendet werden:

1. Coldstart: Eine Unterbrechung der Spannungsversorgung löst einen Trap aus.
2. Warmstart: Ein Neustart des Gerätes löst einen Trap aus.
3. Alarm: Sobald ein Alarm auftritt, wird ein Trap ausgelöst.
4. Änderung Alarmstatus: Sobald sich der Status des Alarms von Alarm auf keinen Alarm bzw. von keinem Alarm auf Alarm ändert, wird ein Trap ausgelöst. Auch die Änderung von

quittierbarerer Alarm auf Alarm löst ein Trap aus.
5. Zutritt: Sobald ein SmartAccess Zutrittsereignis eintritt, wird ein Trap ausgelöst.

Für Alarm- und Zutrittstraps kann zwischen zwei verschiedenen Darstellungsarten gewählt werden. 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.

Authentifizierung

Die Authentifizierung ist abhängig der verwendeten SNMP-Version.

Bei der Version 2 werden zur Authentifizierung zwischen Agent und Manager sogenannte Communities verwendet. Communities sind Namen, die mit der Anfrage zusammen vom SNMP-Service übermittelt werden und stellen einen vorher vereinbaren Schlüssel dar (Pre-shared key).

Ab Version 3 kann ein Authentifizierungsprotokoll und ein Privacy Protokoll ausgewählt werden. Zusätzlich zu den beiden Protokollen muss ein Benutzername vergeben werden. Dieser wird zur Authentifizierung verwendet. SNMP 3 unterstützt folgende Kombinationen:

1. Keine Authentifizierung und kein Privacy Protokoll
2. Authentifizierung und kein Privacy Protokoll
3. Authentifizierung und Privacy Protokoll

Als Authentifizierungsprotokolle können HMAC-MD5 (hash-based message authentication code) und HMAC-SHA gewählt werden. SHA und MD5 sind zwei verschiedene Hash-Funktionen. Sobald ein Authentifizierungsprotokoll verwendet wird, wird zusätzlich das Authentifizierungspasswort benötigt.

Bei der Kombination „Authentication and Privacy Protocol“ muss zusätzlich zum oben genannten Authentifizierungsprotokoll ein Privacy-Protokoll ausgewählt werden. Unterstützt werden die Verschlüsselungsalgorithmen DES (Data Encryption Standard), 3DES (Triple-DES), AES (Advanced Encryption Standard) und IDEA (International Data Encryption Algorithm). Beim Advanced Encryption Standard muss zusätzlich die Schlüssellänge angegeben werden (AES128, AES192, AES256). Zusätzlich besteht beim Advanced Encryption Standard die Möglichkeit, einen 3DES-erweiterten Schlüssel zu verwenden. Zusätzlich zum Protokoll muss das Privacy Passwort angegeben werden.

Einstellungen

Sobald KentixONE Daten von einem Agenten abfragen möchte, wird die IP-Adresse des Hosts und der Port benötigt, auf dem der SNMP-Dienst Daten bereitstellt.

Da beim SNMP-Typ „Trap“ unaufgefordert ein Datenpaket an den Manager gesendet wird, muss auch hier die IP-Adresse des Hosts und der Port angegeben werden. Außerdem kann ein Heartbeat konfiguriert werden. Dieser dient zur zyklischen Funktionskontrolle des Agenten. Das Heartbeat-

Intervall gibt die Länge des Zeitintervalls zwischen zwei Heartbeat-Meldungen an. Zum Testen der Einstellungen kann auch eine einzelne Heartbeat-Nachricht durch Klicken auf den Button „Trap senden“ gesendet werden.

LDAP

Das Lightweight Directory Access Protocol (LDAP) ist ein Netzwerkprotokoll zum Abfragen und Ändern von Benutzer- und Adressdaten und deren Attributen, die in einer Datenbank gespeichert sind. In KentixONE ist ein LDAP-Client integriert, der mit einem LDAP-Server interagieren kann, auf dem die Benutzer- und Adressdaten in einer Datenbank gespeichert sind.

Der LDAP-Client dient dem Importieren und der automatisierten Verwaltung von Benutzern und deren Stammdaten. Bei der Authentifizierung eines aus LDAP importierten Benutzers in KentixONE gelten die aktiven Sicherheitsrichtlinien des LDAP-Servers.

LDAP-Server

Um Daten vom Server in KentixONE zu importieren, werden die IP-Adresse des Servers und die Portnummer benötigt. Soll die Kommunikation zwischen Client und Server verschlüsselt werden, muss sowohl auf dem Server als auch in KentixONE der Verschlüsselungsmodus SSL eingestellt werden. Die Daten sind auf dem LDAP-Server in einer Baumstruktur organisiert. Ein einzelnes Objekt in der Datenbank wird durch den Distinguished Name (DN) eindeutig identifiziert. Die Base-DN definiert, wo im Baum nach unten die Suche nach Objekten gestartet werden soll. Zusätzlich werden durch die Aktivierung der Funktion „Soft Delete“ bereits in KentixONE importierte Benutzer, die später auf dem LDAP-Server gelöscht werden, gesperrt anstatt gelöscht.

Authentifizierung

Um Benutzerdaten in KentixONE zu importieren, werden die Bind DN und das Passwort eines LDAP-Administrators benötigt. Mit der Bind DN wird dem Server mitgeteilt, wer den Zugriff durchführen möchte.

Systemberechtigungen

Derzeit können zwei Benutzergruppen, die in KentixONE angelegt wurden, zwei Benutzergruppen vom LDAP Server zugeordnet werden. Alle diese Benutzer haben die Berechtigungen, die der jeweiligen Benutzergruppe zugeordnet sind. Diese können unter dem Menüpunkt SMARTACCESS bearbeitet werden. Zusätzlich zu den beiden Gruppen können Administratoren separat vom LDAP-Server in KentixONE importiert werden.

Attribute

Für den Import der Benutzerdaten in KentixONE müssen zusätzlich die Typbezeichnungen der Attribute des LDAP-Verzeichnisses den entsprechenden Attributen in KentixONE zugeordnet werden.

Synchronisation

Damit der LDAP-Server und KentixONE den gleichen Datenbestand haben, muss in regelmäßigen Abständen ein Abgleich zwischen den beiden Datenbanken stattfinden. Dazu kann ein Synchronisations-Intervall eingestellt werden.

Externer Zugang

Unter diesem Menüpunkt kann eine externe Zutrittsauswertung aktiviert werden. Sobald die externe Zutrittsauswertung aktiviert ist, findet keine Auswertung der Buchungen auf dem AccessManager mehr statt.

Für die externe Auswertung bietet KentixONE die Möglichkeit, bei Buchungen Webhooks zu versenden. Dazu muss ein entsprechender Webhook konfiguriert werden. Das Öffnen des DoorLocks kann mit Hilfe der Kentix SmartAPI über einen API-Aufruf erfolgen.

Die Dokumentation der Kentix SmartAPI enthält weitere Informationen zu den notwendigen Parametern der API-Anfrage.

Beispiel Webhook

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

VdS 2465

KentixONE (ab Version 8.4.0) ist in der Lage, Meldungen nach der VdS 2465 Richtlinie (Übertragungsprotokoll für Gefahrenmeldeanlagen) an entsprechende Leitstellen über Netze der Protokollfamilie TCP zu übertragen. Hierzu ist mindestens eine KentixONE-GO Lizenz für 50 Geräte erforderlich.

Allgemein

Damit KentixONE Meldungen an eine Leitstelle übertragen kann, wird die IP-Adresse und Portnummer der Leitstelle benötigt, über die die Verbindung aufgebaut werden soll. Zusätzlich kann eine alternative IP-Adresse und Portnummer angegeben werden. Dies ist zum Beispiel bei einem Server mit zwei Netzwerkinterfaces oder bei einem gespiegelten System erforderlich.

Die Übertragungseinheiten werden mit einem Identifikator (VdS-ID) versehen, die von der Leitstelle für jede Übertragungseinheit eindeutig vergeben wird. Die VdS-ID dient der eindeutigen Zuordnung der Übertragungseinheiten auf Seiten der Leitstelle und als Index für die Verschlüsselung.

Als Verschlüsselungsstandard kommt der Advanced Encryption Standard (AES) zum Einsatz. Dazu muss ein AES-Schlüssel und die von der Leitstelle generierte Schlüsselnummer eingegeben werden. Beim Aufbau der Kommunikation zwischen der Übertragungseinheit und der Leitstelle wird standardmäßig das erste Ticket von der Übertragungseinheit unverschlüsselt an die Leitstelle gesendet. Die Leitstelle sendet daraufhin ein verschlüsseltes Ticket (AES), das die Sitzungsschlüssel für die verschlüsselte Kommunikation enthält. Soll das erste Ticket bereits verschlüsselt (AES) an die Leitstelle gesendet werden, muss im Menüfeld Authentifizierung „Verschlüsselt“ eingetragen werden.

Um die Funktion der Übertragungseinheit und der Leitstelle zu überprüfen, werden die Tickets zyklisch zwischen beiden übertragen. Wann die Tickets zwischen beiden ausgetauscht werden, kann im Menüpunkt Routinezeit eingestellt werden. Zusätzlich wird bei einem Verbindungsaufbau je nach Konfiguration der Leitstelle ein Routine-Ticket oder eine Eventbenachrichtigung mit der Meldungskennung 0x53 angefordert.

KentixONE prüft in zyklischen Intervallen die Verbindung zur Leitstelle. Bei einem Verbindungsverlust besteht die Möglichkeit eine Meldung zu versenden. Alle Benutzer mit aktivierten Systembenachrichtigungen erhalten eine Alarmmeldung. Dazu muss die entsprechende Funktion aktiviert werden.

Meldelinien

Eine Meldelinie (Meldergruppe) ist eine Zusammenfassung von Meldern eines Meldebereichs, für die eine eigene Anzeige für Meldungen in der Leitstelle vorhanden ist, mit dem Ziel, den Meldungsort zu kennzeichnen.

Um eine Meldelinie zu konfigurieren, muss der Meldeliniennummer die entsprechende Alarmgruppe und der Alarmtyp zugeordnet werden. Die Alarmgruppe kann im Menüpunkt Detail View konfiguriert werden und bildet je nach Konfiguration die Struktur nach Gebäude, Etage, Raum oder Funktion ab. Es können verschiedene Alarmtypen konfiguriert werden. Nur bei einem Alarm, der dem eingestellten Alarmtyp entspricht, wird über die entsprechende Meldelinie eine Meldung an die Leitstelle gesendet.