KANTECH
From Tyco Security Products

EntraPass 8.0 Network & Security White Paper

Telephone: 1 (450) 444-2030 • Toll free: 1-888-222-1560 • www.kantech.com

KANTECH
From Tyco Security Products

Introduction 4
Transactions between EntraPass applications 4
Communication protocols 4
Triple-DES (3DES) 128-bit encryption 4
32/64 bits encryption 5
UDP protocol 5
Serial communications 5
Transactions between the EntraPass gateway and Kantech IP devices 6
AES 128-bit encryption 6
Message wrapping 6
Communication between workstation and server 7
Component status query 9
Manual operations 10
Saving and modifying data 11
Between workstation and server 11
Polling between server and applications 14
Communication with global gateway, reloading data 14
Controller 14
Global gateway and the multi-site gateway 15
Example of data reloads: 19
Reloading firmware to controllers 20
Update between components 21
Polling between gateway and controllers 23
Controller events 24
Communication between server and SmartLink 27
Interaction between applications 27
Bandwidth required to send command lines 28
Communication between web and mobile to SmartLink 29
Communication between main server and mirror database/redundant server 30
Bandwidth used by the mirror database 31
Bandwidth used by the redundant server 31
Copy/synchronization between mirror database and main server 32
Report process 32
Communication between main server and database access 34
Communication between main server and video vault 35
System in idle mode 35

Telephone: 1 (450) 444-2030 • Toll free: 1-888-222-1560 • www.kantech.com

KANTECH
From Tyco Security Products

Telephone: 1 (450) 444-2030 • Toll free: 1-888-222-1560 • www.kantech.com

KANTECH
From Tyco Security Products

Introduction

EntraPass is a suite of high performance software solutions that delivers reliable access control for facilities of every size. Available in Special, Corporate, and Global editions, EntraPass offers single and multiple workstation access control solutions, and is compatible with Kantech entire line of door controllers. It is also network-ready, providing maximum flexibility for managing remote sites with connectivity using direct, dial-up modem, and TCP/IP using the Kantech IP-Link. Standard features include context-sensitive help, elevator control, automatic backup of system data, the ability to interface with external alarm systems, and definition of operator workspaces. Advanced features, such as EntraPass WebStation, account management for managed access control, redundant servers, video integration, automated e-mails, and real-time interfacing with paging systems, reinforce your protection. Whether you have one, or thousands doors, EntraPass gives you the control you need to determine who gets in, and who stays out.

EntraPass bandwidth & encryption

This section informs users about the bandwidth usage for an EntraPass system on an Ethernet network. Tables detailing the number of bytes used for each type of operation and components are available later on in this document. We describe operations such as saving and modifying data in detail. However, you must take into account that each operation, such as sending messages to the server and to the workstations, can generate additional bandwidth usage.

Transactions between EntraPass applications

Each transaction that takes place between EntraPass applications adds sixteen bytes. Each of these transactions can contain up to 4,000 bytes of data.
For example, when uploading cards, you can send up to 125 user/cards per packets to a gateway instead of sending each card individually, see table 9.
You can customize ports between server and applications.

Communication protocols

In order to get a fair evaluation of the quantity of data used, you must take into account the minimum number of bytes required for each protocol used by the EntraPass system.

Triple-DES (3DES) 128-bit encryption

The system uses 3DES Encryption, with a fixed key, to encrypt all sensitive fields in the EntraPass database such as password, pin, etc.

Telephone: 1 (450) 444-2030 • Toll free: 1-888-222-1560 • www.kantech.com

32/64 bits encryption

This encryption, based on a randomly generated key, is used for transactions between all EntraPass applications, such as the server, workstation, multi-site gateway, global gateway, KT-NCC, video vault, SmartLink, mirror database and redundant server and Oracle MS/SQL Interface (card gateway). The 32-bit or 64-bit encryption method will be set according to the key value.

UDP protocol

The UDP protocol requires a minimum of 54 bytes for each packet sent on the network. By default, the maximum UDP packet size is 1500 bytes to prevent packet fragmentation and increase communication performance.

Table 1: UDP Protocol

TCP/IP Protocol	Data
54 bytes	1 - 1460 bytes

Serial communications

For serial communications between the gateway and the controllers, you must add a minimum of 4 bytes per packet of data sent on the network.

Table 2: Serial communications

Serial communications	Data
4 bytes	1 - 255 bytes

KANTECH
From Tyco Security Products

Transactions between the EntraPass gateway and Kantech IP devices

AES 128-bit encryption

The Kantech IP devices (Kantech IP Link, KT-400 Ethernet Four-Door Controller and KT-1 Ethernet (PoE/PoE+) one door controller) use the AES 128-bit encryption to communicate with the EntraPass multi-site gateway. We even encrypt the pulse heartbeat sent to the EntraPass multi-site gateway that contains the MAC address of the IP Device.

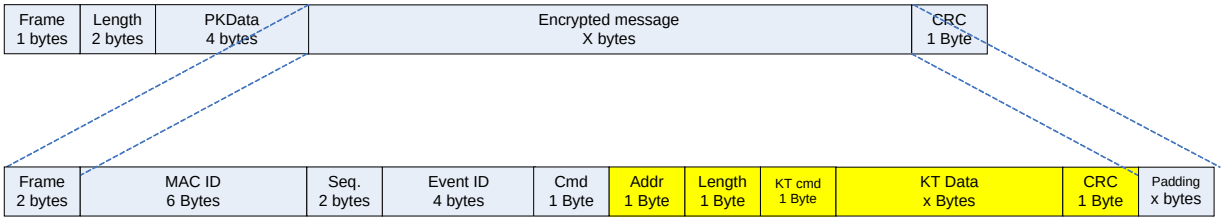
This feature prevents any hacking from the Internet and avoids the requirement of establishing the multi-site gateway/IP device connection through an IPSEC tunnel (by the same token, avoiding the need for additional routing equipment or software).

The algorithm uses the Advanced Encryption Standard (AES), also known as Rijndael. The encryption uses a 16-character key that must be identical between the IP device and the multi-site gateway. While the user can provide a key with less than 16 characters, the longer the key, the more secure the communication will be.

Message wrapping

The following diagram presents an example of the structure of a message between a Kantech IP device and the multi-site gateway. The upper part represents the encrypted message while the lower part is a breakdown of the encrypted message.

Figure 1: Message wrapping structure



The first byte is a synchronization frame byte (0x99) followed by the length of the message to follow (excluding the length itself, but including the checksum). The PkData is a 4 bytes long site identifier from EntraPass. The last 2 bytes are a validity checksum to confirm the integrity of the message. The checksum includes the entire message, starting at the frame byte 0x99 but excluding the checksum itself.

The following values are part of the encrypted section. The first block of 2 bytes is an encryption validation frame with a fixed value of 0x3021. Followed by the MAC ID, or session ID to identify the sender. The sequence number is used for synchronization purposes and to ensure that each encrypted message will be different. The event field is a window event

created by the multi-site gateway to act as a call back identifier. When the IP device initiates the communication, this field is blank. The event ID is followed by the IP device command that must be executed and the data specific to each command.

The last field, “Padding”, is required since the encryption algorithm requires the message length to be in multiple of 16. If it is not the case, the algorithm will pad with ‘0’ and increase the size of the message to match a multiple of 16.

Table 3: Encrypted message section

Field	Description
MAC ID	Unique identifier of the device.
Sequence	Message counter to synchronize the communication. Also used to randomize the effect of encryption on similar messages.
Event ID	This is a Windows event created by the gateway to act as a call back identifier. When the IP Link initiates the communication, this field is bland (0x00000000)
Command	Specific command for the IP Link/KT-400. See following table.
Data	Data specific to each command.
Padding	0 padding for the encryption algorithm.

Note: If the message originates from the IP device, its MAC address is used. If the message comes from the multi-site gateway instead, a unique identifier is generated representing this conversation.

Communication between workstation and server

The majority of EntraPass operations are directed to the workstation to inform users about the system status. You must take into account that each type of operation generates event traffic between the server and the workstation.

Version 6.04 and higher allows status requests between workstations/SmartLink to the gateway in order to remove unnecessary traffic with the server. This process requires that the communication port is open both ways between workstations/SmartLink to the gateway. If there is no direct communication process, traffic is redirected to server.

KANTECH
From Tyco Security Products

Display of events, pictures, and graphics on the workstations

Table 4 details the number of bytes used when deploying data from the server to the workstation.

Note: Pictures and graphical components are transferred only once to the workstations unless they are modified.

Table 4: Data transmission between workstation and server

Component types	Number of bytes using one language	Number of bytes using two languages
Per message	662	990
Per picture		
Information	100	100
Image	+-60K (once) **	+-60K (once) **
Per alarm	662	990
Instruction	4574 (once)	4574 (once)
Comment	XML	XML
Per graphic		
Information	207 (once)	207 (once)
Item	119 (once)	119 (once)
Image	100k to 3mb (once)	100k to 3mb (once)

** Add +/- 60K per image and per signature assigned to each card.

Component status query

You can perform two types of queries: per component, or per list. **Table 5** details the traffic generated during a status query from a workstation.

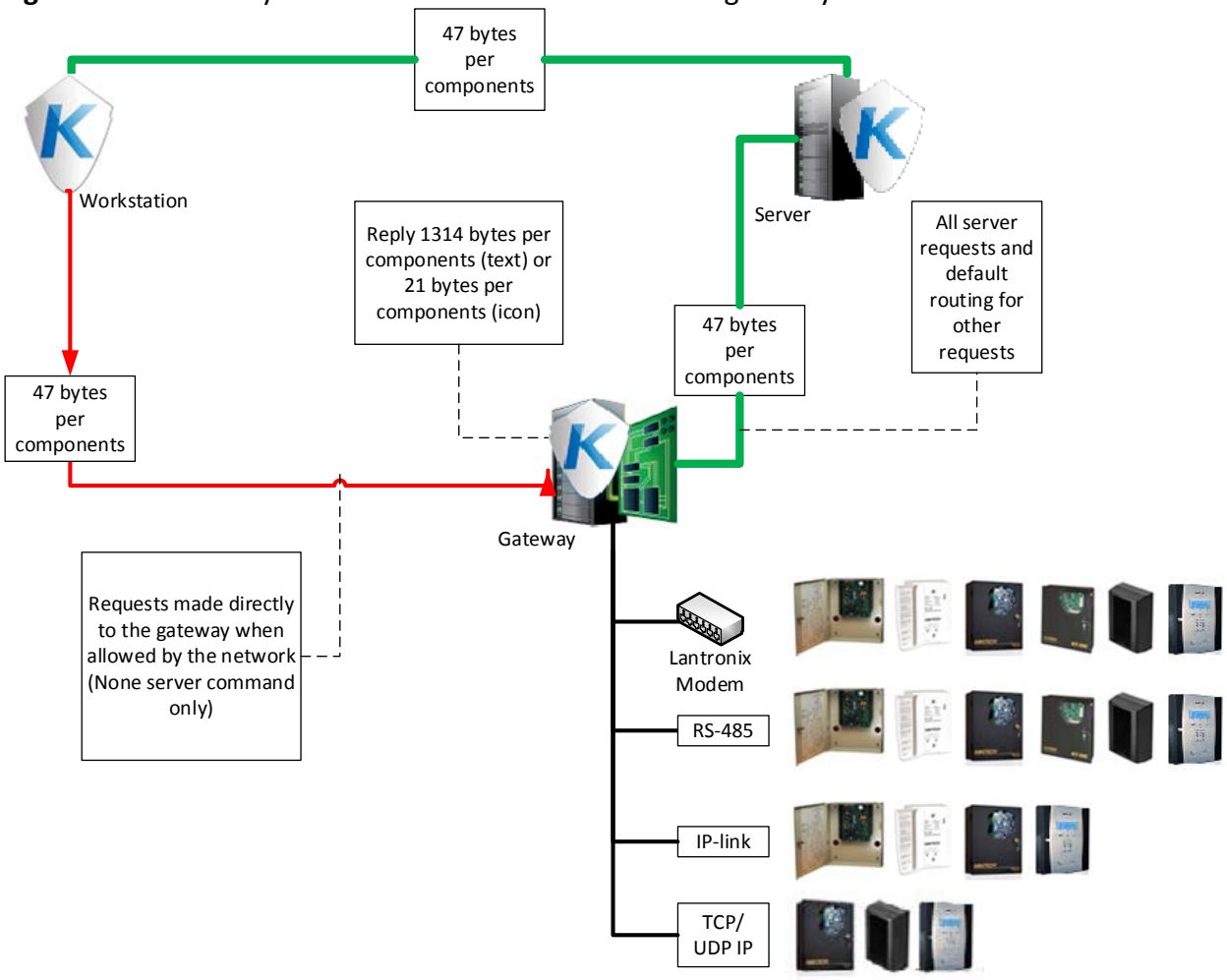
Table 5: Component status query

Query type	Number of bytes
Component status query	47
Component text status reply by item	1314
Component image status reply by item	21
List query	4277
List reply by item	322

Manual operations

During manual operation queries, the workstations send data to the server at 68 bytes per component. The server then deploys to the gateway. At that point, the controllers send an 8 bytes reply per activated component.

Figure 2: Transfer bytes from workstation to server to gateway



KANTECH
From Tyco Security Products

Saving and modifying data

Between workstation and server

When saving a component on a workstation, the system must calculate the saving value for this component. For more information, see the following table. It also adds 39 bytes for each backup query to the server.

Table 6: Data backup

Type of components	Number of bytes	Number of bytes per sub-items
Modification query	56	—
Information for 1 access level	484	19 + XML
Information for 1 group of access level	483	19
Information for 1 alarm system	693	XML*
Information for 1 area	531	XML*
Information for 1 area group	483	—
Information for 1 badging	506	119 + XML* + Front image** + Back image**
Information for 1 card	5070	119 + XML* + Photo** + Signature**
Information for 1 group of cards	481	119
Information for 1 action scheduler	723	—
Information for 1 group of access cards	139	104
Information for 1 card type	482	—
Information for 1 controller	14541	19
Information for 1 group of controller	483	19
Information for 1 door	4297	XML*
Information for 1 group of doors	483	819
Information for 1 event parameter	103	—

KANTECH
From Tyco Security Products

Type of components	Number of bytes	Number of bytes per sub-items
Information for 1 event relay	83	—
Information for 1 floor	478	—
Information for 1 group of floors	483	19
Information for 1 graphic	1197	119 + background plan** + backgroup video**
Information for 1 gateway	15792	XML*
Information for 1 guard tour	1497	19 + XML*
Information for 1 holiday	492	19
Information for 1 input	606	XML*
Information for 1 input group	483	19
Information for 1 instruction	4574	—
Information for 1 trigger	1440	19 + XML*
Information for 1 roll call report	1903	—
Information for 1 card filter	477	—
Information for 1 trigger group	485	19
Information for 1 reader template	514	XML*
Information for 1 device association	482	19 + XML*
Information for 1 video record	511	XML*
Information for 1 integration panel	1352	XML*
Information for 1 integration panel component	527	XML*
Information for 1 site	2560	XML*
Information for 1 muster report	1907	—

KANTECH
From Tyco Security Products

Type of components	Number of bytes	Number of bytes per sub-items
Information for 1 active directory	25204	XML*
Information for 1 tenant	700	—
Information for 1 camera	3651	XML
Information for 1 messages filter	3564	19
Information for 1 EntraPass application	8333	XM
Information for 1 operator	4292	11 + XML* + Photo**
Information for 1 security level	1777	19
Information for 1 auxiliary output	563	XML*
Information for 1 video trigger	875	—
Information for 1 relay	530	XML*
Information for 1 group of relays	483	19
Information for 1 report	14527	19
Information for 1 schedule	601	—
Information for 1 connection	3588	XML*
Information for 1 time and attendance report	14527	19
Information for 1 tenant group	12492	—
Information for 1 Master account	2656	XML*
Information for 1 account	73149	XML*
Information for 1 filter	901	19
Information for 1 macro maker	4575	—
Information for 1 DVR	1456	—
Information for 1 view	858	—

* Text value, size from 1kb to 3mb

** Image value, size from 20kb to 3mb

Telephone: 1 (450) 444-2030 • Toll free: 1-888-222-1560 • www.kantech.com

Polling between server and applications

Polling is bidirectional. On the one hand, each EntraPass application sends a query to the server every 2 minutes. On the other hand, the server sends a query every 2 minutes to all applications. In both cases, this delay can be lower when specific notifications must be send immediately.

The video vault queries the server every 5 seconds.

Communication with global gateway, reloading data

With EntraPass, it is possible to reload data at different levels: with controllers and with the gateway.

Controller

The controller performs the reload during the system hard reset, or during gateway reloading. When reloading a controller, the number of data transferred must be evaluated to include the data loaded by default such as system and controller information as well as date and time information (minimum of 106 bytes). In addition, all components configured at the controllers must be included. See **Table 7**.

Table 7: Data reload to controllers

Components types	Number of bytes
Global system information	83
Per controller - Controller - Per reader driver - Floor assignation (when elevator) - Serial number (KT-300) - DSC module (KT-300) - SPI module (KT-400)	 40 253 512 115 204 90
Per floor definition	64
Per door	27
Per relay	6

KANTECH
From Tyco Security Products

Components types	Number of bytes
Per input	14
Per output	15
Per card - KT-100/KT-200/KT-300 - KT-400/KT-1	 7-17 78
Per schedule - KT-100/KT-200/KT-300 - KT-400/KT-1/KTES	 21 41
Access level (reload)	249
Per floor group (reload)	249
Per floor group mask	33
All holiday	200
Per relay group	3
Per input group	3
Per action scheduler	22
Per reader driver	203
Date/Time	7
Program download	130

Global gateway and the multi-site gateway

The gateway performs the reload manually or during the gateway start up. During information reload between the server and the gateway, the amount of data transferred is calculated according to the gateway type and the number of components configured in the system.

Note: Take into account that all site controllers connected to the gateway will reload automatically when the gateway is reloading.

Figure 3: Global gateway and multi-site gateway reload

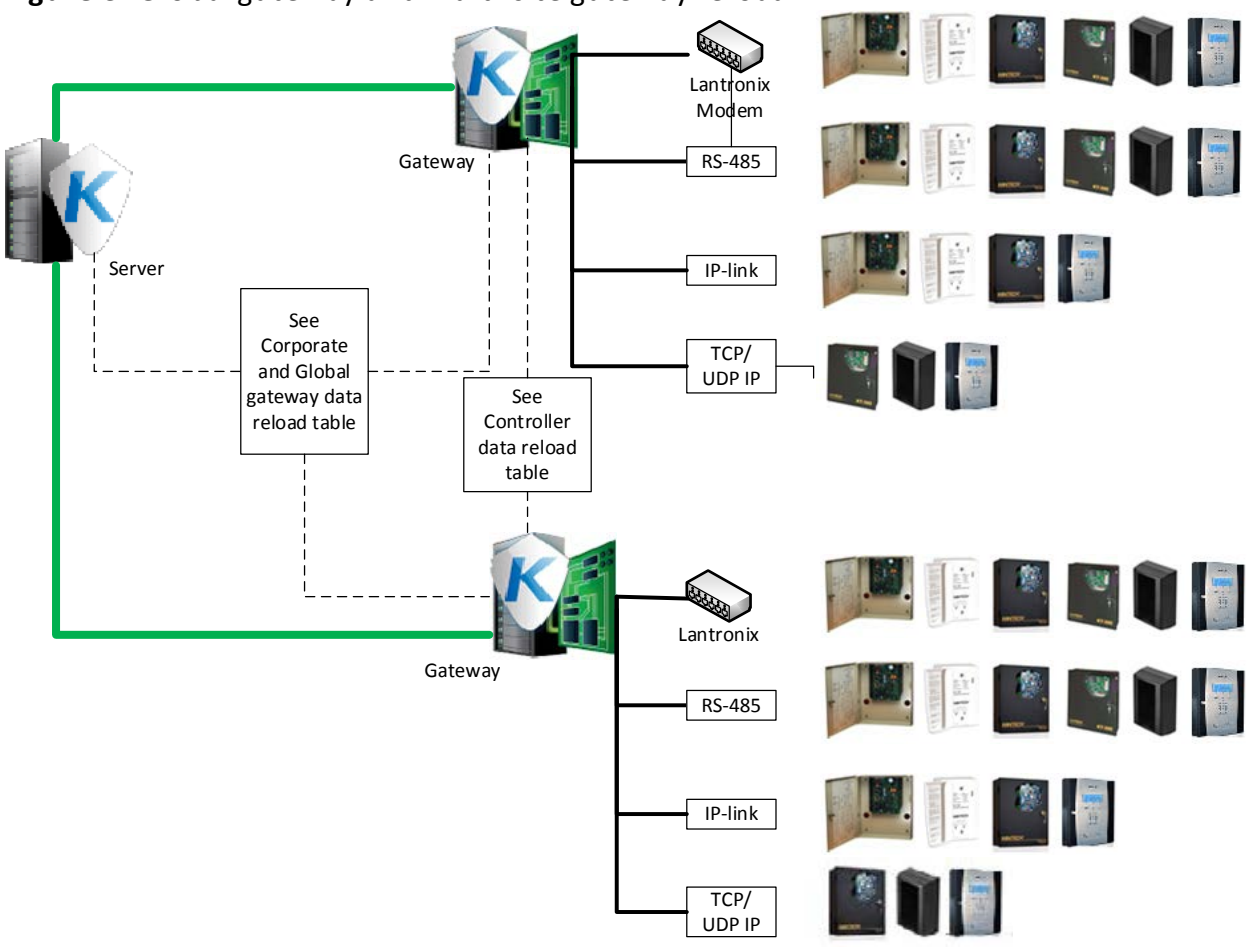


Table 8: Data reload —multi-site gateway

Components types	Number of bytes
General information	14342
Information for 1 account	413
Information for 1 site	392
Information for 1 controller	9040
Information for 1 door	342
Information for 1 relay	22
Information for 1 input	66
Information for 1 auxiliary output	52
Information for 1 access level	780
Information for 1 schedule	133
Information for 1 holiday	10255
Information for 1 floor	10
Information for 1 card	35 + 34 * Number of sites
Information for 1 controller group	268
Information for 1 door group	268
Information for 1 relay group	268
Information for 1 input group	268
Information for 1 floor group	1074
Information for 1 access level group	49
Information for 1 panel	8222
Information for 1 panel component	2062
Information for 1 tenant group	15
Information for 1 tenant	215
Information for 1 action scheduler	137

Table 9: Data reload – Global gateway

Components types	Number of bytes
General information	823
Information for 1 loop	1024
Information for 1 controller	6416
Information for 1 door	190
Information for 1 relay	24
Information for 1 input	64
Information for 1 auxiliary output	56
Information for 1 access level	16396
Information for 1 schedule	129
Information for 1 action scheduler	133
Information for 1 holiday	6
Information for 1 floor	12
Information for 1 card	91
Information for 1 controller group	273
Information for 1 door group	4113
Information for 1 relay group	65553
Information for 1 input group	65553
Information for 1 floor	10
Information for 1 floor group	1073
Information for 1 panel	8222
Information for 1 panel component	2062
Information for 1 access level	262153
Information for 1 access level group	48

KANTECH
From Tyco Security Products

Components types	Number of bytes
Information for an alarm system	204
Information for an area	50
Information for an area group	416
Information for a guard tour	722
Information for an event relay	28

Example of data reloads:
For a system with a multi-site gateway with two sites of 10 controllers each, 200 cards, 12 schedules and 20 access levels:

To reload the multi-site gateway:

General information	= 14, 342 bytes
Sites	= 2 x 392 = 784 bytes
Controllers	= 20 x 9040 = 180,800 bytes
Doors	= 40 x 342 = 13,680 bytes
Relays	= 2 x 22 = 44 bytes
Inputs	= 8 x 66 = 528 bytes
Outputs	= 2 x 52 = 104 bytes
Access level	= 20 x 780 = 15,600 bytes
Schedules	= 12 x 133 = 1,596 bytes
Schedules	= 12 x 133 = 1,596 bytes
Cards	= 35 + (34 x 2) = 200 cards x 103 bytes = 20,600 bytes
Total	**= 248,078 bytes**

To reload the controllers:

Global system information	= 83 bytes
Date/Time	= 7 bytes
Controller	= 40 bytes
Door	= 2 x 27 = 54 bytes
Input	= 8 x 14 = 112 bytes
Relays	= 2 x 6 = 12 bytes
Output	= 2 x 15 = 30 bytes
Card	= 200 x 78 = 1600 bytes
Schedule	= 12 x 81 = 252 bytes
Access level	= 248 bytes
Total	**= 2355 bytes per controller x 20 = 47100 bytes**

Telephone: 1 (450) 444-2030 • Toll free: 1-888-222-1560 • www.kantech.com

Note: Serial communication protocols and TCP/IP are not included in the calculation.

Reloading firmware to controllers

Controllers' firmware size.

- KT-100 Application: 64kb
- KT-300 Application: 64kb
- KT-NCC OS and Application: 8mb
- KT-400 OS and Application: 6mb
- KT-400 v1 OS and Application: 10mb
- KT-1 OS and Application: 10mb
- KT-400 Application: 450kb
- KT-400 v1 Application: 900kb
- KT-1 Application: 913kb
- KTES Application: 380kb

During the reload operation, the firmware is transferred from the workstation to the gateway and is then deployed to the selected controllers. Take into account that the controllers will start reloading data following the firmware reload.
Reloading is done one controller at the time, per packets of 134 bytes (130 for reload and 4 for the protocol).
Altogether, with the TCP/IP protocol, 500 packets of 188 bytes will be sent to the controllers (KT-100/KT-300).
For example, a site with 16 controllers requires:
500 packets x 188 bytes x 16 Controllers = 500 x 188 x 16 = **1,504 Mb to transfer**

Note: Serial communication protocols and TCP/IP are not included in the calculation.

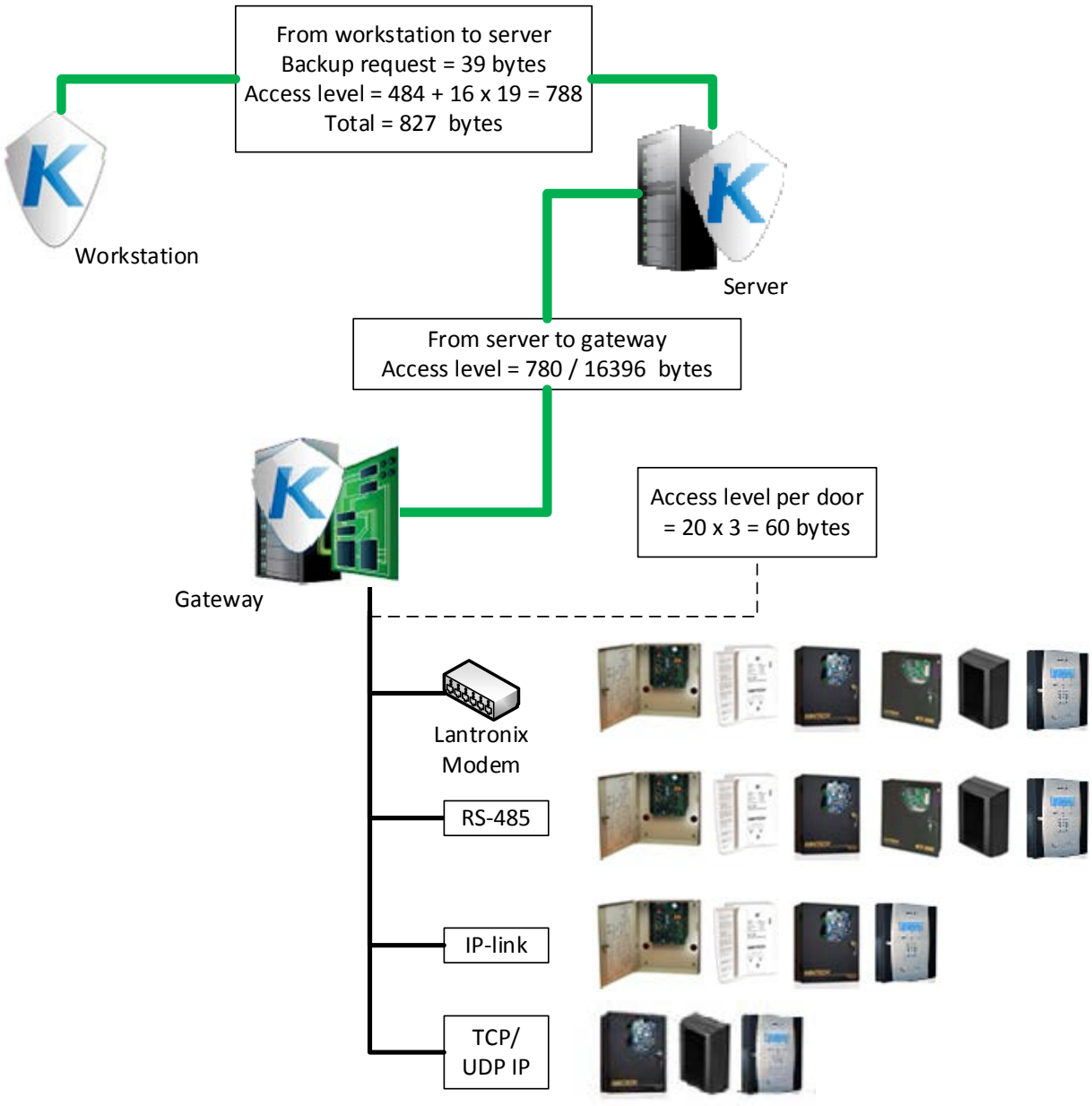
KANTECH
From Tyco Security Products

Update between components

Backups or modifications are automatically loaded to the gateway and the controllers. It is possible to evaluate the number of bytes sent to the gateway and the controllers according to the given reload data. See **Table 9***: Data reload – Global gateway* for global gateways, see **Table 8:** Data reload —multi-site gateway for multi-site gateways, and **Table 7**: Data reload to controllers for Data Reload to Controllers.

Telephone: 1 (450) 444-2030 • Toll free: 1-888-222-1560 • www.kantech.com

Figure 4: Access level backup



For an access level backup for 20 doors, calculate 500 bytes per transaction between the workstation and the server, 528 bytes from server to gateway and 60 bytes between the gateway and the controllers.

Example of calculations for a group of 40 doors:

During a door group backup, calculate 141 bytes for the group and add 8 bytes per door included in that group.
39 bytes per modification query
141 bytes per door group
8 bytes per door * 40 = 320 bytes
Therefore: 39 + 141 + 320 = **Total of 500 bytes**

Note: Serial communication protocols and TCP/IP are not included in the calculation.

Polling between gateway and controllers

During the communication in active mode between gateway and controllers, the gateway queries each controller sequentially with a 4 byte command. Then, if the controller has no message to send, it transmits a 1 byte presence notification to the gateway. The query sequence is repeated systematically from the first to the last controller.
The following table contains the average value of the bandwidth measured for each of the gateway type with a TCP/IP site:

Table 10: Bandwidth gateway/controller

Gateway	Default Value	Slowest	Fastest
Corporate	1000 bytes per second	200 bytes per second	7200 bytes per second
Global Gateway	7400 bytes per second	3800 bytes per second	7800 bytes per second

For a multi-site gateway with three TCP/IP sites with default values:
1000 bytes per second x 3 sites = 3000 bytes per second used for querying 3 sites.

Table 11: Idle site query

Message type	Number of bytes
Gateway query	4
Controller reply	1

During the controller query with a TCP/IP site, the packets sent will be at least 54 + 5 bytes for the gateway and 54 + 1 bytes for the controllers. There will be an alternate transmission of 59 bytes and 55 or 60 bytes packets for the bandwidth measure for gateway and controller queries.

Note: Bandwidth will not increase with the number of controllers connected to the site. In fact, the polling frequency remains the same. The increase is caused by the query delay per controller that increases with the addition of a controller to the site.

Controller events

Controller events are treated directly at the Gateway, see **Table 12***: Messages from the controller*

. The gateway sends each event to the main server, in 100 byte packets. The main server will deploy the messages to the workstations. See **Table 4**: Data transmission between workstation and server

.

For example, for an access with a 32-bit card, the information provided will be event date/time, door and the access request that contains the card number.

Packet transmission	= 4 bytes
Date/Time	= 7 bytes
Door	= 1 bytes
Access request	= 5 bytes
Total	**= 17 bytes per access**

Figure 5: Gateway controller events

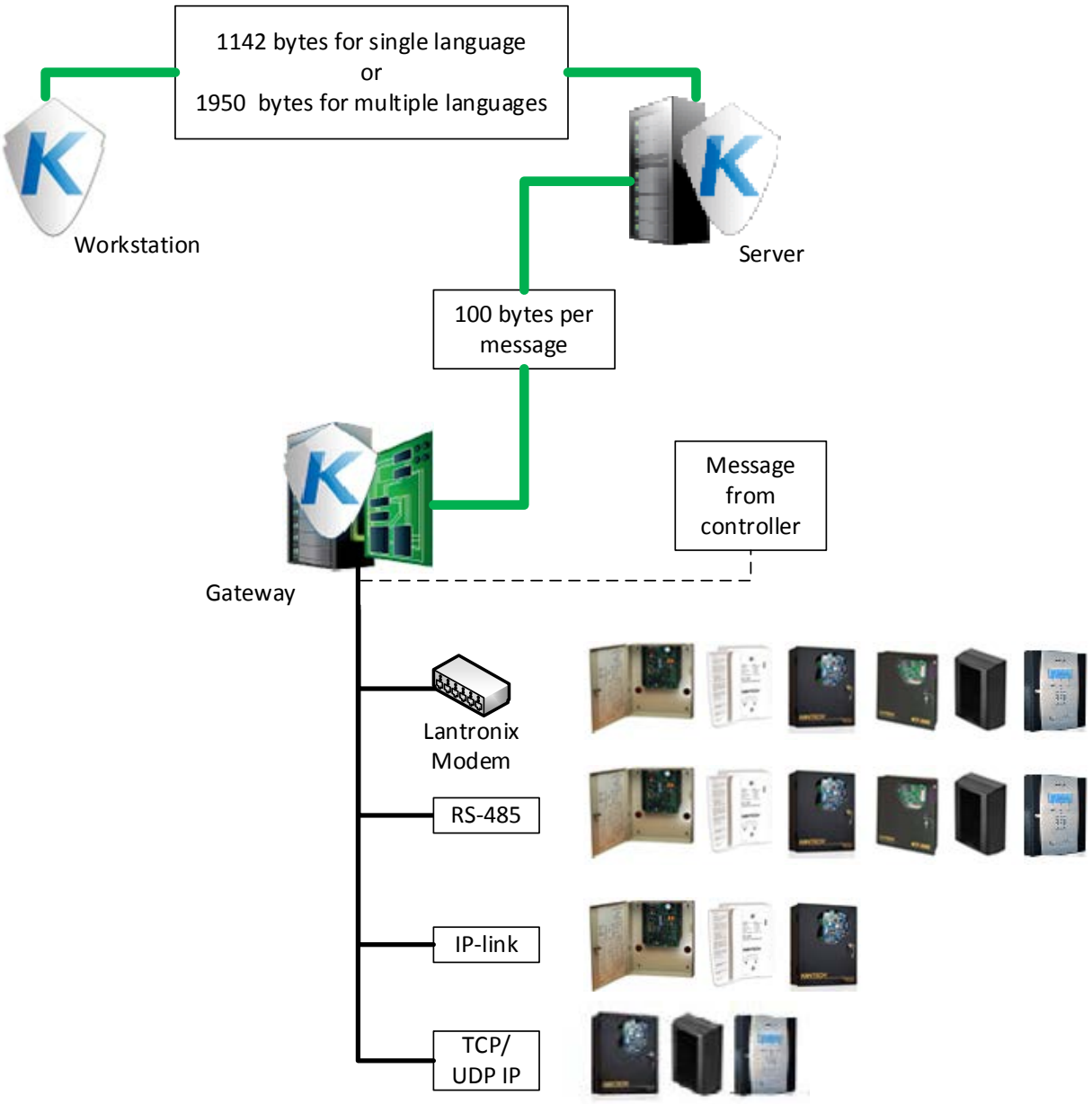


Table 12: Messages from the controller

Data Types	Number of bytes
Communication protocol	4
Controller's complete status	63
Date and times	7
System report	4
Report following a command on the network	1
Door Report	1
Inputs in alarm report	1
Shunt inputs report	2
Temporarily shunt inputs report	2
Supervised inputs report	1
Relay activation status	2
Door status	2
Internal/external card number status	4
Output by event activation status	1
Access request results	5 with 32-bit card 11 with BCD card
Valid or invalid floor selection results	6 with 32-bit card 10 with BCD card
Status on unlocking door in stand-alone mode	2
Status on disabling door in stand-alone mode	1
Status on activating relay in stand-alone mode	2

KANTECH
From Tyco Security Products

Communication between server and SmartLink

SmartLink is an external application that integrates itself to the EntraPass system allowing the following functionality:

- Receive request from RS-232 port.
- Receive request from IP using SmartService.
- Execute macro command base on system trigger.
- Execute macro command base on manual request.
- Send e-mail.

SmartLink can handle the following request:

- Login/Logout
- Database creation/View/Modification/Deletion.
- Manual action like unlock a door/activate a relay/etc.
- Component state
- Component list
- User and operator picture.
- Events report
- Live events
- Badging

SmartLink can execute the following macro command:

- Send an e-mail.
- Send to a pager.
- Save data to a file.
- Execute a manual action like unlock a door/activate a relay/etc.
- Create specific output data.

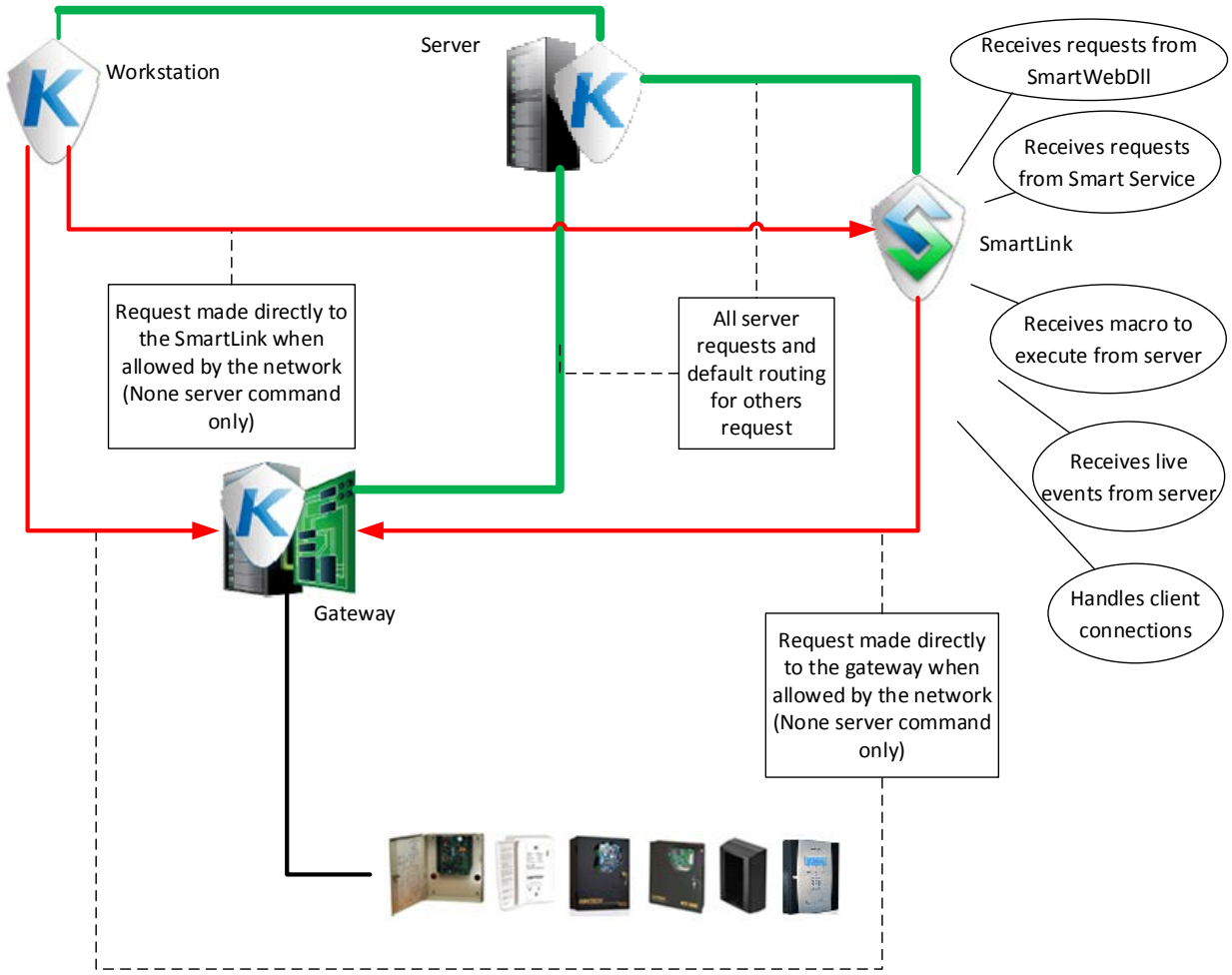
The SmartLink, through the SmartService, is the EntraPass Interface for the following application:

- EntraPass web (web based application)
- EntraPass go (mobile application)
- go Pass (mobile application)
- go Install (mobile application)
- LDAP

Interaction between applications

The query frequency between the server and the SmartLink is the same for all workstations and gateways. For more information, see **Figure 4**: Access level backup

Figure 6: Polling between server and applications



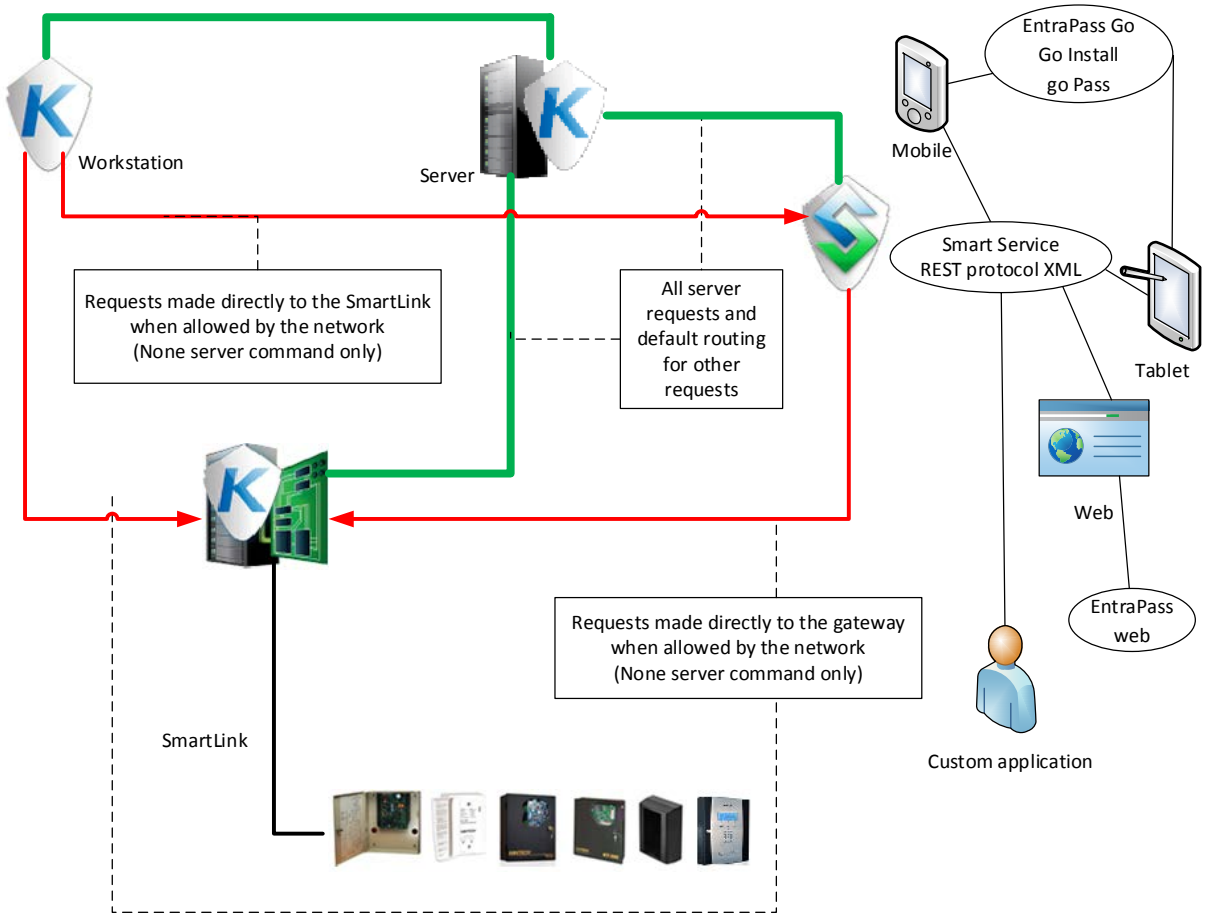
Bandwidth required to send command lines

To calculate the bandwidth used during the execution of a command line, count 1 byte per character used. For example:
<2>''COMMAND=ACTIVATERELAY''<28>''RELAYID=525''<28><3>
50 bytes must be transmitted for the execution of this command line.

KANTECH
From Tyco Security Products

Communication between web and mobile to SmartLink

Figure 7: SmartServer REST API



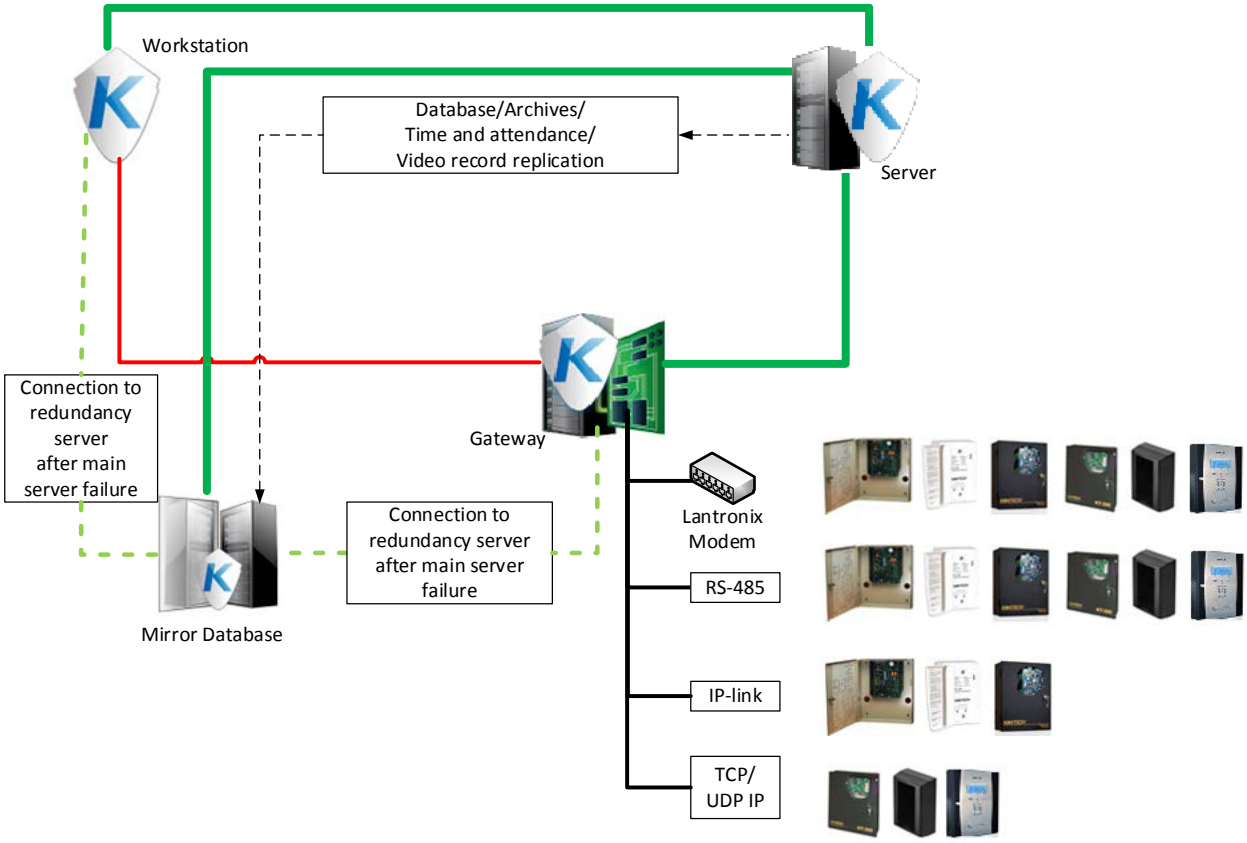
Communication between Entrapass web/mobile application is done through a web service called SmartService. SmartService is a base REST API that allows connection with the EntraPass systems. REST API is a public interface that customers use to build their own application. To use Kantechs APIs, customers must purchase a connected program license.

KANTECH
From Tyco Security Products

Communication between main server and mirror database/redundant server

The mirror database/redundant server application offers resilience to increasing power failures when the EntraPass server shuts down. As soon as communication is broken between an EntraPass application and server, the application tries to establish connection to an redundant server. The redundant server starts when communication is broken between the mirror database and server according to the configuration, which is start on normal shutdown or/and start on abnormal shutdown).

Figure 8: Mirror database and redundant server communications



Bandwidth used by the mirror database

Every five seconds, the redundant server replicates the database and the data stored on the main server.

The number of bytes used to replicate the backups and modifications is identical to those used for the main server backups. See **Table 6**: Data backup

Note: To obtain the number of transactions and bytes received, see **Table 13**. The number on the left indicates the number of transactions and the number on the right indicates the number of bytes sent to the redundant database.

Table 13: Transactions report

Number of transactions to process	Number of bytes sent to redundant database
# of data transactions processed	868 – 2,307,586
# of archive transactions processed	5 – 6,425
# of time and attendance transactions processed	0 – 0
# of Windows registry transactions processed	74 – 2,809
Transaction errors	0

Bandwidth used by the redundant server

When the application can no longer detect the main server, it starts the redundant server to take charge of the system management. The redundant server is an exact copy of the main server. The bandwidth used for poling, data backup and messages management will be identical to the main server.

KANTECH
From Tyco Security Products

Copy/synchronization between mirror database and main server

Once the main server is functional again, the redundant server shuts down and sends the information according to the parameters configured by the operator before the main server power failure.

Restore database: complete copy of mirror database to the main server.

Restore archived data: sends all archived data to the main server.

Merge archives: sends only archived data accumulated since the last redundant server start-up.

Restore time and attendance: sends all time and attendance archives.

Merge time and attendance: sends only time and attendance archives accumulated since the last redundant server start-up.

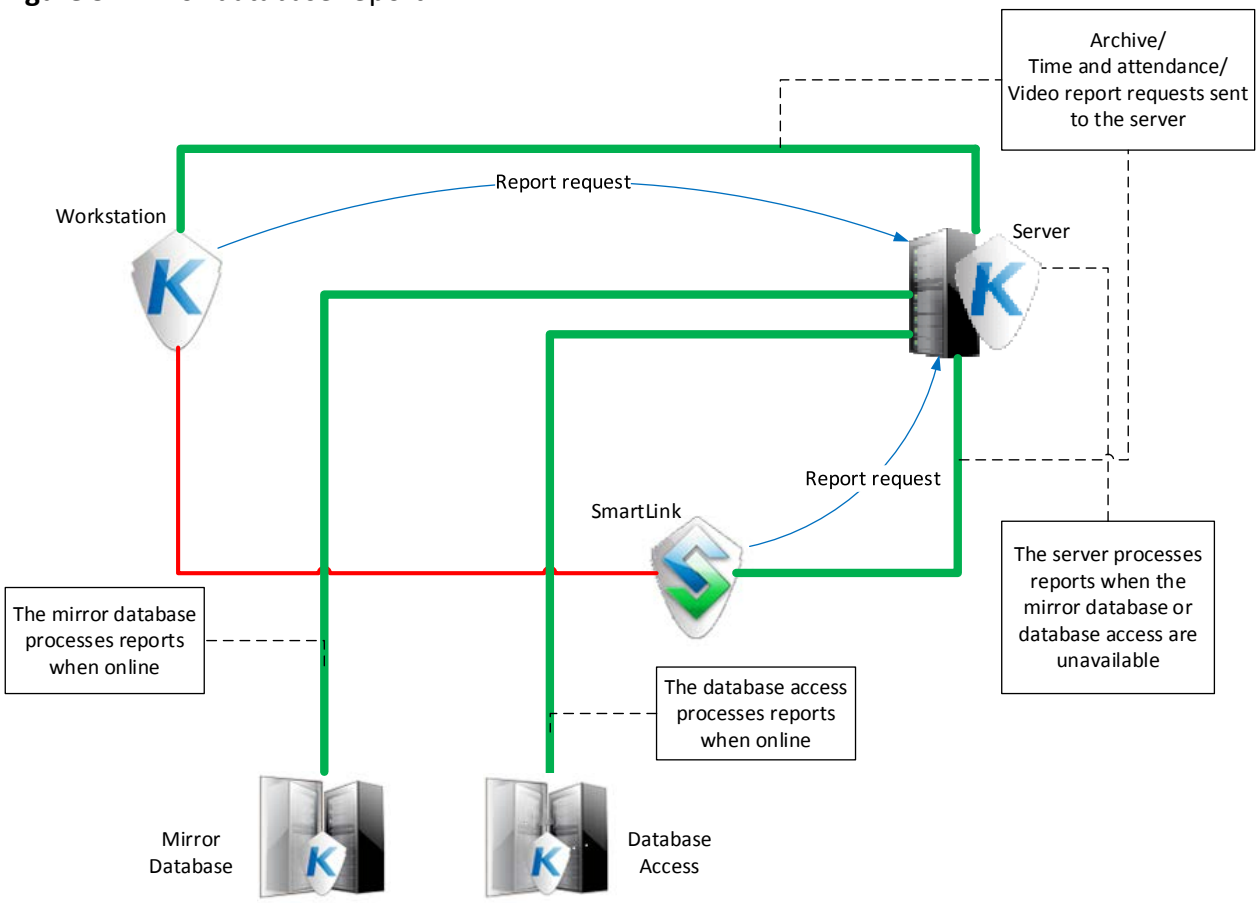
Merge video: sends only events related to video recordings accumulated since the last redundant server start-up.

Report process

Use the mirror database to process archival, time and attendance and video reports. When the mirror database is connected to the primary server and when the synchronisation is done, the mirror database can receive report requests from the server and process using the local copy of the database. At the end, the information is directly returned to the requester without using main server.

Telephone: 1 (450) 444-2030 • Toll free: 1-888-222-1560 • www.kantech.com

Figure 9: Mirror database report

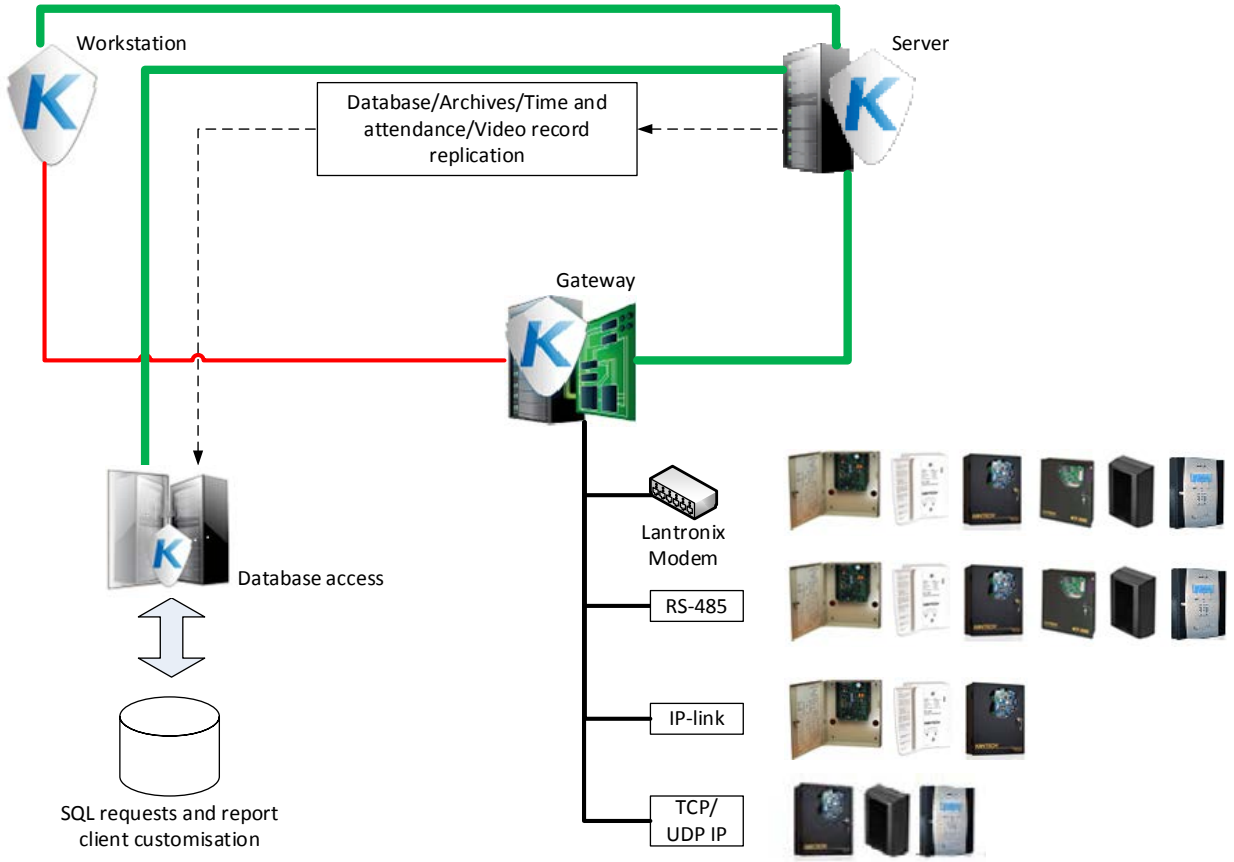


KANTECH
From Tyco Security Products

Communication between main server and database access

The database access offers an SQL, read only, access to a copy of the EntraPass database. Database access is synchronised to the system database using the same mechanism than the mirror database.

Figure 10: SQL copy of EntraPass database

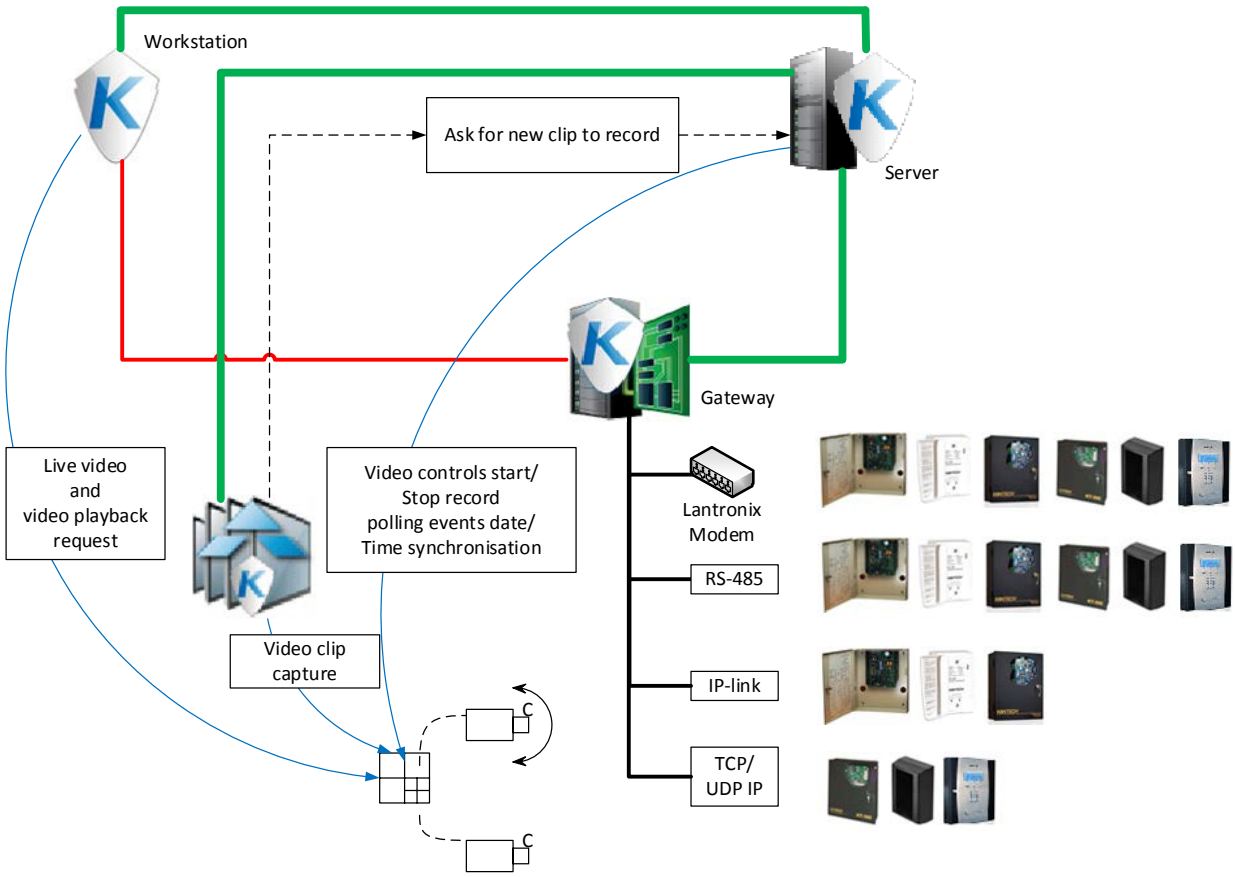


KANTECH
From Tyco Security Products

Communication between main server and video vault

The video vault is an EntraPass application used to automate video clip backup.

Figure 11: Video vault



System in idle mode

When the communication system is in idle mode, the bandwidth can be calculated as follows:

For an EntraPass system with 2 workstations, 1 multi-site gateway and 4 TCIP/IP sites:

Workstation	= 2 x 26 = 52 bytes
Gateway	= 26 bytes/sec.
Sites	= 4 x 1000 = 4000 bytes/sec.
Total	**= 4078 bytes/sec for system in idle mode**

KANTECH
From Tyco Security Products

IP port List
EntraPass Version 8.00

Telephone: 1 (450) 444-2030 • Toll free: 1-888-222-1560 • www.kantech.com

Ports in **bold green** are default values that the user can customize.

Table 14: Port list

Port #	From (Applications)	To (Applications)	Usage
8001	EntraPass web	SmartService	HTTP managed access control (REST)
8001	EntraPass go	SmartService	HTTP managed access control (REST)
8001	EntraPass Install go	SmartService	HTTP managed access control (REST)
8001	EntraPass go Pass	SmartService	HTTP managed access control (REST)
8002	SDK	SmartService	HTTP managed access control (WCF)
8003	EntraPass web	SmartService	UDP notification port
8003	EntraPass go	SmartService	UDP notification port
8003	EntraPass Install go	SmartService	UDP notification port
18200	SmartWebDLL	SmartLink	Listening TCP port (local and remote machine)
18200	SmartSDKDLL	SmartLink	Listening TCP port (local and remote machine)
18200	VKSmartWebDll	SmartLink	Listening TCP port (local and remote machine)
18200	PFSmartWebDll	SmartLink	Listening TCP port (local and remote machine)
80	Web browser	KT-NCC	HTTP Web page configuration (factory default mode only)
80	Web browser	IP-Link	HTTP Web page configuration (factory default mode only)
80	Web browser	KT-400	HTTP Web page configuration (factory default mode only)
80	Web browser	KT-1	HTTP Web page configuration (factory default mode only)
80	Web browser	KT-2	HTTP Web page configuration (factory default mode only)
80	Web browser	KTES	HTTP Web page configuration (factory default mode only)
17998	Server	Server service functions	Listening TCP port (local machine)
17998	Redundant server	Server service functions	Listening TCP port (local machine)

KANTECH
From Tyco Security Products

Port #	From (Applications)	To (Applications)	Usage
17998	Workstation	Server service functions	Listening TCP port (local machine)
17998	Gateway	Server service functions	Listening TCP port (local machine)
17998	SmartLink	Server service functions	Listening TCP port (local machine)
17998	Mirror database	Server service functions	Listening TCP port (local machine)
17998	MSSQL-Oracle HR Interface	Server service functions	Listening TCP port (local machine)
17998	Video Vault	Server service functions	Listening TCP port (local machine)
17998	Database access	Server service functions	Listening TCP port (local machine)
18000	Server workstation	Server	Listening TCP port (local machine)
18000	WorkStation	Server	Listening TCP port (local and remote machine)
18000	Gateway	Server	Listening TCP port (local and remote machine)
18000	SmartLink	Server	Listening TCP port (local and remote machine)
18000	Mirror database	Server	Listening TCP port (remote machine)
18000	MSSQL-Oracle HR Interface	Server	Listening TCP port (local and remote machine)
18000	Video vault	Server	Listening TCP port (local and remote machine)
18000	Database access	Server	Listening TCP port (remote machine)
17999	Workstation	Redundant Server	Listening TCP port (remote machine)
17999	Gateway	Redundant Server	Listening TCP port (remote machine)
17999	SmartLink	Redundant Server	Listening TCP port (remote machine)
17999	Video vault	Redundant Server	Listening TCP port (remote machine)
18001	IP-Link	Gateway	TFTP firmware update
18002	KT-NCC	Server	TFTP firmware update
18101	Server	Server workstation	Listening TCP port (local machine)

KANTECH
From Tyco Security Products

Port #	From (Applications)	To (Applications)	Usage
18101	Server	Workstation	Listening TCP port (local and remote machine)
18103	Server	Gateway	Listening TCP port (local and remote machine)
18104	Server	SmartLink	Listening TCP port (local and remote machine)
18105	Server	Mirror database	Listening TCP port (local and remote machine)
18106	Server	MSSQL-Oracle HR Interface	Listening TCP port (local and remote machine)
18107	Server	Video vault	Listening TCP port (local and remote machine)
18108	Server	Database access	Listening TCP port (local and remote machine)
18300	EntraPass Ping	Server	Listening TCP port (local and remote machine)
18300	EntraPass Ping	Redundant Server	Listening TCP port (local and remote machine)
18301	EntraPass Ping	Workstation	Listening TCP port (local and remote machine)
18303	EntraPass Ping	Gateway	Listening TCP port (local and remote machine)
18304	EntraPass Ping	SmartLink	Listening TCP port (local and remote machine)
18305	EntraPass Ping	Mirror database	Listening TCP port (local and remote machine)
18306	EntraPass Ping	MSSQL-Oracle HR Interface	Listening TCP port (local and remote machine)
18307	EntraPass Ping	Video vault	Listening TCP port (local and remote machine)
18308	EntraPass Ping	Database access	Listening TCP port (local and remote machine)
18000	Server service control	Server	Listening TCP port (local machine)
18103	Gateway service control	Gateway	Listening TCP port (local machine)
18104	SmartLink Service control	SmartLink	Listening TCP port (local machine)

KANTECH
From Tyco Security Products

Port #	From (Applications)	To (Applications)	Usage
18105	Mirror database service control	Mirror database	Listening TCP port (local machine)
18106	MSSQL-Oracle HR Interface service control	MSSQL-Oracle HR interface	Listening TCP port (local machine)
18107	Video vault service control	Video vault	Listening TCP port (local machine)
18108	Database access service control	Database access	Listening TCP port (local machine)
18701	KT-NCC	Server	Listening UDP port (remote machine)
18702	KT-NCC	Redundant server	Listening UDP port (remote machine)
18703	Server	KT-NCC	Listening UDP port (Broadcast)
18704	Production	KT-NCC	Listening UDP port (remote machine)
18706	Web API	KT-NCC	Listening UDP port (local machine)
18707	KT-NCC	Web API	Listening UDP port (local machine)
18801	IP-Link/KT-400/KT1/KT2	Gateway/KT-Finder	Listening UDP port (remote machine)
18802	IP-Link/KT-400/KT1/KT2	Gateway/KT-Finder	Listening TCP port (remote machine)
18803	Gateway/KT-Finder	KT-400/KT1/KT2	Listening UDP port (broadcast)
18810	Gateway	IP-Link/KT-400/ KT-1/KT-2	Listening UDP port (remote machine)
18901	Remote video process	RVP poll	Listening TCP port (local machine)
18902	Remote video process	RVP event	Listening TCP port (local machine)
18903	Remote video process	RVP record	Listening TCP port (local machine)
18904	Remote video process	RVP control	Listening TCP port (local machine)
18905	Remote video process	RVP control	Listening TCP port (local machine)
18906	Remote video process	RVP control	Listening TCP port (local machine)
18907	Remote video process	RVP control	Listening TCP port (local machine)

KANTECH
From Tyco Security Products

Port #	From (Applications)	To (Applications)	Usage
18908	Remote video process	RVP control	Listening TCP port (local machine)
18909	Remote video process	RVP control	Listening TCP port (local machine)
18910	Remote video process	RVP control	Listening TCP port (local machine)
18911	Remote video process	RVP control	Listening TCP port (local machine)
18991	Server	Remote video process	Listening TCP port (local machine)
18991	Redundant server	Remote video process	Listening TCP port (local machine)
18992	Remote video process	Server	Listening TCP port (local machine)
18992	Remote video process	Redundant server	Listening TCP port (local machine)
35111	Video vault	Video vault gateway	TCP port
5000	Workstation	Intellex	Listening TCP port (remote machine)
5001	Workstation	Intellex	Listening TCP port (remote machine)
5000	Video vault	Intellex	Listening TCP port (remote machine)
5000	RVP poll	Intellex	Listening TCP port (remote machine)
5000	RVP record	Intellex	Listening TCP port (remote machine)
5000	Video vault	Intellex	Listening TCP port (remote machine)
5001	RVP control	Intellex	Listening TCP port (remote machine)
5003	RVP event	Intellex	Listening TCP port (remote machine)
22609	Workstation	Exacq	Listening TCP port (remote machine)
22609	Video vault	Exacq	Listening TCP port (remote machine)
80	RVP poll	Exacq web service	Listening TCP port (remote machine)
22609	RVP record	Exacq	Listening TCP port (remote machine)
22609	Video vault	Exacq	Listening TCP port (remote machine)
22609	Workstation	Exacq	Listening TCP port (remote machine)
22609	RVP control	Exacq	Listening TCP port (remote machine)
22609	RVP event	Exacq	Listening TCP port (remote machine)

Figure 12: List of system IP ports - EntraPass Global and Corporate

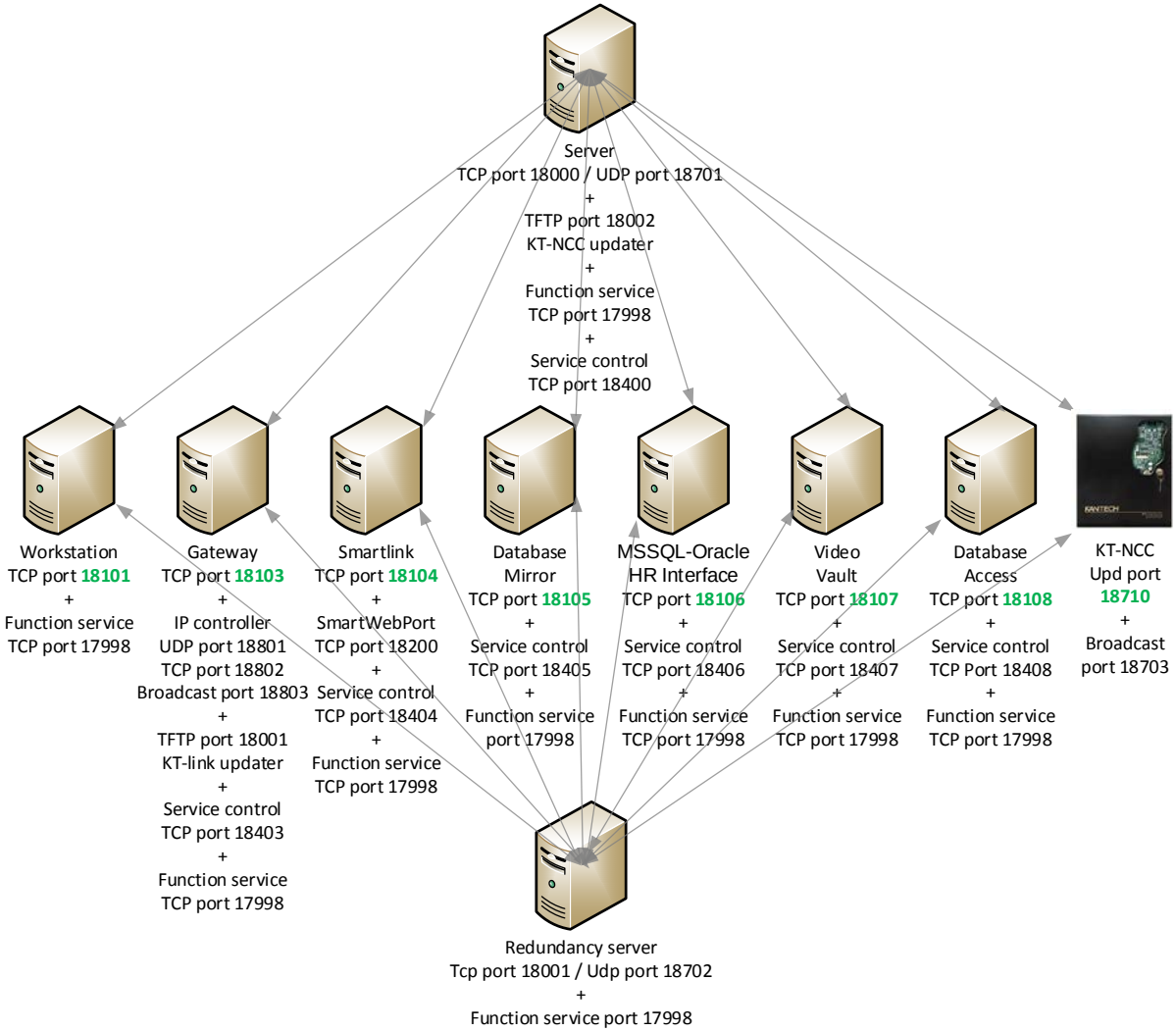


Figure 13: List of diagnostic IP ports (Kping) - EntraPass Global and Corporate

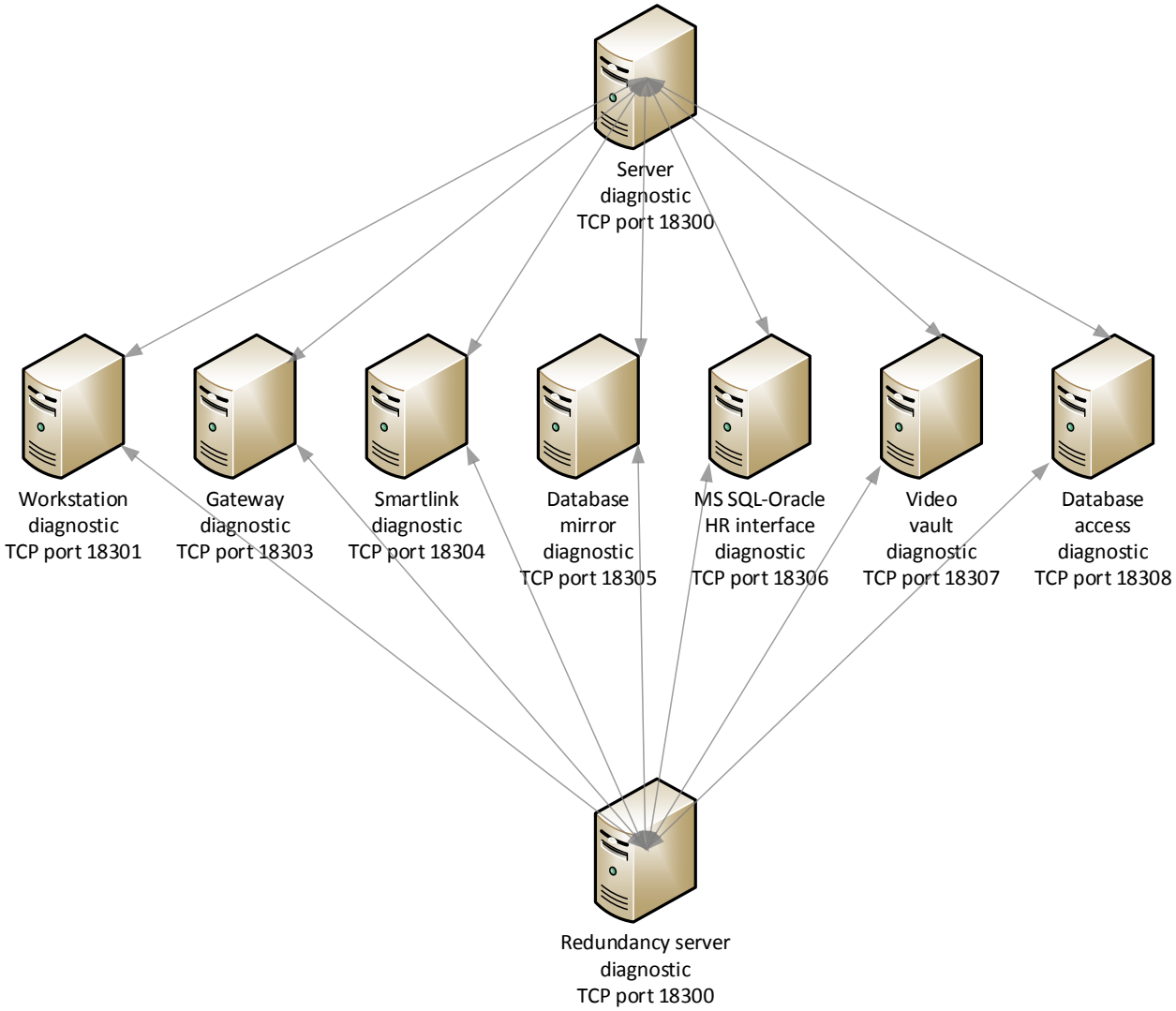
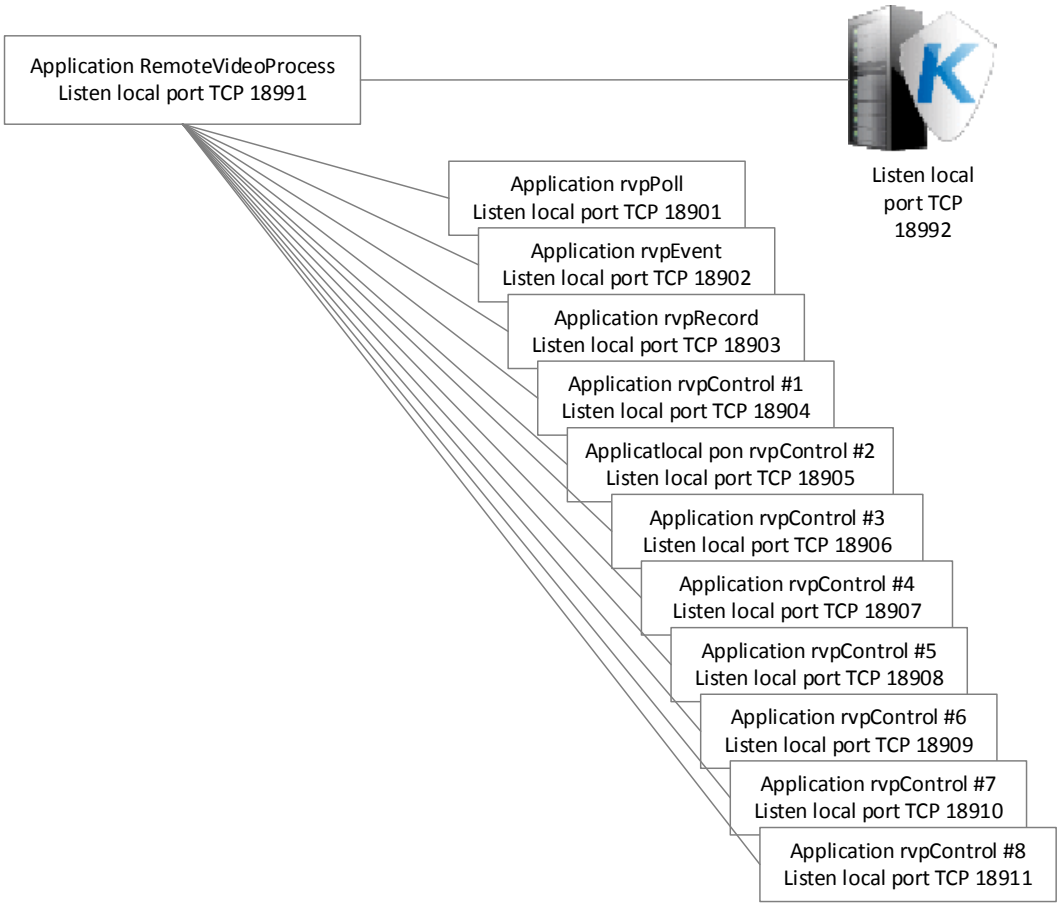


Figure 14: Server video inter-process port – EntraPass Global and Corporate

KANTECH
From Tyco Security Products



D29010396R001

Telephone: 1 (450) 444-2030 • Toll free: 1-888-222-1560 • www.kantech.com