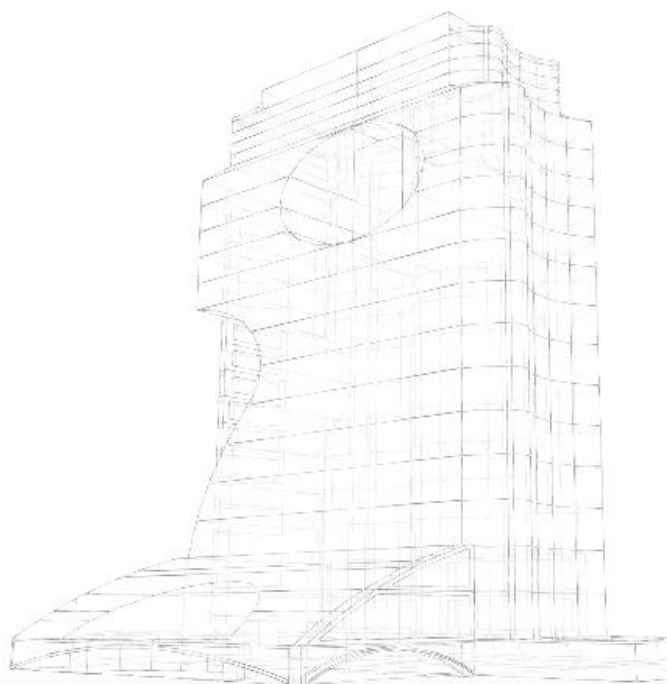




ENTRAPASS

Security Management Software



CORPORATE EDITION

KANTECH
A Tyco International Company

Niniejszy dokument jest tłumaczeniem angielskiej wersji instrukcji firmy Kantech – EntraPass 8.10 User manual CE.



Spis treści

Nowe Funkcje (Release Notes) 8.10.....	1
Jak to zrobić?	5
Jak utworzyć kopię systemu (Backup)	5
Jak zdefiniować szablon foto-identyfikatora (Badge).....	6
Jak dodać nowego użytkownika karty (Card)	7
Jak zdefiniować nowy terminarz (Schedule)	8
Jak zdefiniować prosty raport (Simple Report)	9
Jak utworzyć nowy poziom dostępu (Access Level)	10
Jak wydrukować listę kart (Print a Card List).....	11
Jak wydrukować listę poziomów dostępu (Print a List of Access Levels).....	12
Jak Wydrukować Listę Drzwi (Print a List of Doors)	13
Jak skonfigurować pulpity (Setup the Desktops).....	14
Jak używać skrótów klawiszy	15
Jak spersonalizować okno logowania w EntraPass WEB.....	16
Jak udostępnić Go Pass dla użytkownika.....	17
Jak użyć HID Mobile Access	18
Jak migrować z Parametrów zdarzeń do Zdarzeń Przypisanych do operatora	20
Jak przełączyć bazę w tryb tylko do odczytu	21
Jak włączyć tryb serwisowy	22
Jak skonfigurować czytniki ioSmart	23
F.A.Q.....	25
Czy można użyć wejścia linii dozoru do odblokowania grupy pięter i jak długo pozostaną one odblokowane?	25
Czy można zaimportować poziomy dostępu (Import Access Levels)?	25
Jakie są numery portów komunikacyjnych w systemie EntraPass: serwera, stacji operatora, Smartlinka, bramki, serwera zapasowego, stacji wideo oraz EntraPass WEB?	25
Jakie są opcje rozbrajania wirtualnego systemu alarmowego?	25
Jakie są opcje uzbrajania wirtualnego systemu alarmowego?	25
Jakiego rodzaju opcje są dostępne w przypadku operacji grupowych (batch operations)?	25
Do czego można użyć funkcji Przekazniki zdarzeń i jakie są w niej opcje do wyboru?	26
Jak jest różnica pomiędzy Dostępem jednorazowym a Czasowym odryglowaniem drzwi w KT-100, KT-200, KT-300 oraz KT-400?	26



Do czego służy opcja <i>Zdarzenia klienta</i> ?	26
Dlaczego używamy grup kart dostępu?	27
Gdzie mogę zsynchronizować operatorów z Active Directory?	27
Wstęp	28
Co to jest EntraPass?	28
Główne funkcje EntraPass	29
Instalacja	38
Minimalne wymagania systemowe	38
Jak zwiększyć bezpieczeństwo? Poradnik	39
Instalacja systemu	40
Rejestracja Systemu	43
Dodawanie składników programu (Adding System Components)	45
Edycja składników programu	49
Rozpoczęcie pracy z programem	52
Funkcje podstawowe	52
Szczegóły funkcji Usuń (Delete details)	61
Wyświetlanie linków pomiędzy elementami systemu (Displaying Components Links)	61
Paski narzędzi EntraPass (EntraPass Toolbars)	62
Instalacja ekspresowa (Express Setup)	64
Wyszukiwanie elementów (Finding Components)	65
Uruchamianie i zamykanie aplikacji (Session Start and End)	67
Struktura systemu w formie drzewa (System Tree View)	73
Pulpity	76
Pulpit alarmów	76
Personalizacja wyświetlania zdarzeń w oknie zdarzeń (Customizing Event Display in the Message Desktops)	86
Okna map (Graphic Desktop)	88
Okno zdarzeń (Message List Desktop)	90
Transferowanie dostosowanego pulpitu (Transferring a Customized Desktop)	100
Status	101
Status aplikacji (Application Status)	101
Status tekstowy (Text Status)	102
Status liczbowy (numerical status)	103



Status w postaci graficznej (Graphic Status)	104
Status bazy danych (Database Status).....	106
Stan serwera Video (Video Server Status).....	107
Stan serwera (Server State)	110
Logowanie (Logins)	111
Operacje	113
Operacje na Bramce GSI (Manual Operations on Gateway)	113
Operacje na Wirtualnych lokalizacjach i magistralach (Manual Operations on Sites).....	115
Operacje na kontrolerach (Manual Operations on Controllers)	117
Operacje dotyczące drzwi (Manual Operations on Doors)	120
Operacje dotyczące wind (Manual Operations on Elevator Doors)	123
Operacje dotyczące przekaźników (Manual Operations on Relays)	126
Operacje na liniach dozorowych (Manual Operations on Inputs)	128
Operacje dotyczące raportu śledzącego (Manual Operations on View Roll Call)	129
Operacje dotyczące systemów zintegrowanych (Manual Operations on Integrated Panels)	130
Operacje Harmonogramy akcji (Manual Operations on Action Scheduler).....	131
Użytkownicy.....	135
Poziom dostępu - wyjątki (Access Exception)	135
Definiowanie poziomów dostępu (Access Levels Definition).....	135
Projektowanie foto-identyfikatorów (Badges Designing)	136
Operacje na grupach kart (Batch Operations on Cards)	146
Definiowanie grup dostępu (Card Access Groups Definition)	148
Definiowanie opcji kart (Card Options Definition)	149
Nadruk na kartach (Card Printing)	151
Definiowanie typów kart (Card Type Definition).....	153
Przypisywanie poziomów dostępu (Cardholder Access Levels Assignment)	154
Definiowanie kart (Cards Definition)	163
Historia zmian karty (Card audit trail)	166
Tworzenie nowego szablonu do importu/eksportu kart (Creating a New Import/Export Pattern).....	182
Definiowanie karty gościa w szablonie definiowania nowej karty (Creating a Visitor Card When Creating a New Card)	183
Import/eksport kart do pliku CSV (CSV Files Import and Export)	183



Personalizacja pól informacyjnych karty (Customizing Card Information Fields)	188
Definiowanie kart gości jednodniowych (Day Passes Definition)	189
Wprowadzanie nowej karty w Zaawansowanym zarządzaniu (Issuing a New Card in Enhanced User Management Environment)	190
Dodawanie kart przez czytnik kontrolera (Issuing Cards Using the "Batch Load" Feature)	192
Wyświetlanie listy ostatnich transakcji (Last Transactions Display).....	193
Lista drzwi z dostępem wybranej karty (Quick Access to Door List per Card)	195
Lista abonentów (Tenants List).....	195
Dodawania obiektów do szablonu foto-identyfikatora (To Add Objects to a Badge Layout)	200
Modyfikacja właściwości zdjęcia (To Modify Picture Properties)	201
Weryfikacja poziomu dostępu wybranej karty (Validating Card Access)	202
Definiowania kart gości (Visitor Cards Definition).....	202
Definiowanie.....	203
Definiowanie terminarzy (Schedules Definition).....	203
Definiowanie pięter (Floors Definition)	206
Definiowanie map (Graphics Definition)	206
Definiowanie dni świątecznych (Holiday Definition).....	210
Wyzwalacz i alarm, wcześniej Przełącznik makro SML (previously Event Trigger)	211
Definiowanie nowych powiadomień o alarmie (Create a new Alarm notification).....	212
Kreator makro SML (Task Builder Definition).....	214
Grupy	227
Grupy Kontrolerów (Controller Group Creation)	227
Grupy Drzwi (Door Group Creation).....	227
Grup wyjść sterujących (Relay Group Creation).....	228
Grupy Linii dozorowych (Input Group Creation)	228
Grupy poziomów dostępu (Access Level Groups Grouping)	229
Grupy pięter (Floor Group Creation)	229
Grupy przełączników (Trigger Group Creation).....	230
Urządzenia	231
Aplikacja EntraPass (Application Configuration)	231
Określanie ogólnych parametrów (Defining General Parameters)	232
Definiowanie kontroli wiadomości (Defining Message Controls)	237



Konfiguracja bramek EntraPass (EntraPass Gateways Configuration)	260
Konfiguracja wirtualnych magistrali (Site configuration)	263
Zmiana nazwy/opisu (Change Site Labels)	266
Konfiguracja magistrali (Connection Configuration)	266
Konfiguracja parametrów czasowych komunikacji (Setting up Communication Timing) ..	278
Konfiguracja kontrolerów (Controllers Configuration)	278
Rejestrowanie Bramki Viedo lub Video Vault (Video Gateway or Video Vault enrolment)	312
Konfiguracja modułów Combust KT-300 (KT-300 Combust modules).....	315
Konfiguracja modułów rozszerzeń (Expansion Modules Setup)	317
Konfiguracja Kantech Telephone Entry System (KTES) (Kantech Telephone Entry System (KTES) Configuration).....	318
Konfiguracja drzwi (Doors Configuration)	329
Konfigurowanie wyjść sterujących (Relay Configuraiton)	344
Konfiguracja linii dozorowych (Input Configuration)	345
Konfiguracja wyjść sterujących sygnalizatorami (Output Device Configuration)	350
Szablony Czytników (Reader Templates).....	353
Konfiguracja zintegrowanych urządzeń (Integrated Panel Configuration)	354
Konfiguracja zintegrowanych modeli (Integrated Component Configuration)	363
Zakładka Wyzwalacz i Alarm (Trigger and Alarm tab)	366
Pole komentarza (Comment Field)	367
Wideo	370
Definiowanie kamer (Camera Definition).....	370
Bieżące nagrania (Current Recording)	374
EntraPass Video Vault (EntraPass Video Vault Browsing)	375
Przeglądanie eksportowanych plików wideo (Exported Video Viewing)	375
Eksport plików wideo (Exporting Video Files)	376
Wyszukiwanie zdarzeń wideo (Finding Video Events)	377
Parametry nagrywania (Recording Parameters)	379
Pulpit wideo (Video Desktop)	381
Lista zdarzeń wideo (Video Event List)	382
Odtwarzanie nagrań wideo (Video Playback).....	389
Konfiguracja serwera wideo (Video Server Configuration)	390
Przełączniki wideo (Video Triggers)	398



Tworzenie i modyfikacje okien wideo (Video Views Creation and Modification)	399
Definiowanie okien wideo (Video Views Definition)	401
System	405
Active Directory	405
Powiązania (Associations).....	430
Raport z uruchomienia (Commissioning)	431
Tworzenie/modyfikowanie poziomu dostępu dla operatora (Creating/Modifying an Operator Security Level)	432
Tworzenie / modyfikacja operatorów (Creating or Editing an Operator)	433
Filtrowanie zdarzeń pulpitu (Filtering Desktop Events), ...	437
Struktura bazy danych (Database Structure Definition)	438
Definiowanie parametrów zdarzeń (Event Parameters Definition)	439
Definiowanie instrukcji (Instructions Definition)	445
Definiowanie filtrów zdarzeń (Message Filters Definition)	445
Definiowanie operatorów (Operators Definition).....	447
Definiowanie poziomów dostępu dla operatorów (Security Level Definition)	454
Definiowanie poziomu dostępu do programu dla operatorów (Workspace Definition) ...	459
Historia Zmian (Audit).....	468
Raporty	471
Archiwum raportów zdarzeń (Archive Viewing).....	471
Raport użycia kart (Card Use Report)	474
Definiowanie szablonów raportów (Custom Reports Definition)	475
Definiowanie formatu wyjściowego raportu (Defining a Report Output Format).....	480
Definiowanie terminarza automatycznego generowania raportu (Defining Automatic Report Schedules).....	482
Definiowanie szablonów raportów RCP (In/Out Reports Definition).....	484
Generowanie raportów RCP (In/Out Reports Request)	486
Korekty raportów RCP (Operations on In/Out)	487
Podgląd raportów RCP (Previewing In/Out Reports)	489
Podgląd raportów (Previewing Reports)	490
Szybki raport (Quick Report Definition)	491
Historia generowania raportów (Report Log)	493
Stan generowania raportu (Report State)	494
Podgląd raportów zdarzeń (Requesting Reports)	495



Raport śledzący (Roll Call Reports)	497
Specyfikacja specjalnych opcji dla automatycznego generowania raportów (Specifying Additional Options for an Automatic Report)	498
Opcje	500
Terminarz kopii systemu (Backup Scheduler)	500
Modyfikacja hasła do rejestracji aplikacji (Connection Password Modification)	503
Parametry definiowania kart (Credentials Parameters)	504
Zdarzenia definiowane przez klienta (Custom Messages)	505
Informacje dotyczące dystrybutora (Dealer Information)	505
Format wyświetlania numeru karty (Defining a Card Display Format)	507
Kolor i priorytet zdarzenia (Event Color and Priority)	509
Integracja (Integration)	510
Info podczas logowania operatora (Login Messages)	510
Konfigurowanie urządzeń multimedialnych (Multimedia Devices Configuration)	512
Definiowanie opcji wideo (Defining Video Options)	513
Wybór i konfiguracja drukarki zdarzeń (Printers Selection and Configuration)	514
Rejestracja (Registration)	516
Logowanie do trybu serwisowego (Service Login Information)	517
Ustawienie Daty i Czasu (System Date & Time Modification)	517
Wybór języka (System Language Selection)	518
Konfiguracja parametrów systemu (System Parameters Configuration)	519
Synchronizacja czasu w systemie (Time Parameters)	536
Format nazwy użytkownika karty (User Name Format)	537
Serwer EntraPass	538
Aplikacja	538
Błędy w systemie (Error Log)	538
Zdarzenia systemowe (Log)	539
Rejestracja aplikacji (Registration)	540
Logi raportów Historia generowania raportów (Report Log)	540
Kopia systemu (Backups)	541
Odtworzenie kopii (Restores)	543
Format wyświetlania numeru karty (Defining a Card Display Format)	544
Zmiana format wyświetlania kart z 24 bit do 32 bit (Changing from a 24 bit to 32-bit Global Card Format)	546



Modyfikacja hasła do rejestracji aplikacji (Connection Password Modification).....	547
Wybór języka (System Language Selection)	547
Ustawienie Daty i Czasu (System Date & Time Modification).....	548
Konfiguracja parametrów systemu (System Parameters Configuration)	549
Terminarz kopii systemu (Backup Scheduler)	568
Zdarzenia definiowane przez klienta (Custom Messages)	571
Info podczas logowania operatora (Login Messages)	572
Dodatkowe aplikacje i narzędzia programistyczne	574
Konfiguracja kontrolerów pomocą Instalacji ekspresowej (Configuring a KTES Using Express Setup).....	574
Narzędzia bazy danych (Database Utility)	576
Stacja EntraPass Video (EntraPass Video Vault).....	580
Aplikacja Instalacja ekspresowa (Express Setup Program)	583
Diagnostyka PING (PING Diagnostic)	591
Przeglądarka raportów (Quick Report Viewer)	592
Aplikacja SmartLink Interface (The SmartLink Interface)	593
Edytor słownika (Vocabulary Editor)	595
Ikony w programie EntraPass	600



EULA

TYCO INTERNATIONAL LTD

END-USER LICENSE AGREEMENT (Oryginalna licencja firmy Kantech)

IMPORTANT - READ THIS END-USER LICENSE AGREEMENT ("EULA") CAREFULLY BEFORE OPENING THE DISK PACKAGE, DOWNLOADING THE SOFTWARE OR INSTALLING, COPYING OR OTHERWISE USING THE SOFTWARE. THIS EULA IS A LEGAL AGREEMENT BETWEEN YOU AND SENSORMATIC ELECTRONICS, LLC ("TYCO"), AND GOVERNS YOUR USE OF THE SOFTWARE ACCOMPANYING THIS EULA WHICH SOFTWARE INCLUDES COMPUTER SOFTWARE AND MAY INCLUDE MEDIA, PRINTED MATERIALS, AND "ON-LINE" OR ELECTRONIC DOCUMENTATION (COLLECTIVELY, THE "SOFTWARE"). BY BREAKING THE SEAL ON THIS PACKAGE, DOWNLOADING THE SOFTWARE OR INSTALLING, COPYING OR OTHERWISE USING THE SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA. IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS EULA, DO NOT OPEN, DOWNLOAD, INSTALL, COPY OR OTHERWISE USE THE SOFTWARE.

1 - SCOPE OF LICENSE. The Software may include computer code, program files and any associated media, hardware or software keys, printed material and electronic documentation. The Software may be provided to you pre-installed on a storage device (the media) as part of a computer system or other hardware or device ("System"). The Software is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. All title and intellectual property rights in and to the Software (including but not limited to any images, photographs, and text incorporated into the Software), the accompanying printed materials, and any copies of the Software, are owned by Tyco and/or its suppliers. The Software is licensed, not sold. All rights not expressly granted under this EULA are reserved by Tyco and its suppliers.

2 - GRANT OF LICENSE. This EULA grants you the following rights on a non-exclusive basis:

a - General. This EULA permits you to use the Software for which you have purchased this EULA. Once you have purchased licenses for the number of copies of the Software that you require, you may use the Software and accompanying material provided that you install and use no more than the licensed number of copies at one time. The Software is only licensed for use with specified Licensor-supplied Systems. If the Software is protected by a software or hardware key or other device, the Software may be used on any computer on which the key is installed. If the key locks the Software to a particular System, the Software may only be used on that System.

b - Locally Stored Components. The Software may include a software code component that may be stored and operated locally on one or more devices. Once you have paid the required license fees for these devices (as determined by Tyco in its sole discretion), you may install and/or use one copy of such component of the Software on each of the devices as licensed by Tyco. You may then use, access, display, run or otherwise interact with ("use") such component of the Software in connection with operating the device on which it is installed solely in the manner set forth in any accompanying documentation or, in the absence of such, solely in the manner contemplated by the nature of the Software.

c - Remotely Stored Components. The Software may also include a software code component for operating one or more devices remotely. You may install and/or use one copy of such component of the Software on a remote storage device on an internal network with all of the devices and may operate such component with each device over the internal network solely in the manner set forth in any accompanying documentation or, in the absence of such, solely in the manner contemplated by the nature of the Software; provided however, you must still acquire the required number of licenses for each of the devices with which such component is to be operated.

d - Embedded Software/Firmware. The Software may also include a software code component that is resident in a device as provided by Tyco for operating that device. You may use such component of the Software solely in connection with the use of that device, but may not retrieve, copy or otherwise transfer that software component to any other media or device without Tyco's express prior written authorization.

e - Backup Copy. You may make a back-up copy of the Software (other than embedded software) solely for archival purposes, which copy may only be used to replace a component of the Software for which you have



EntraPass - Instrukcja instalacji i obsługi programu
Nowe Funkcje (Release Notes) 8.10

current valid license. Except as expressly provided in this EULA, you may not otherwise make copies of the Software, including the printed materials.



EULA

3 - OTHER RIGHTS AND LIMITATIONS. Your use of the Software is subject to the following additional limitations. Failure to comply with any of these restrictions will result in automatic termination of this EULA and will make available to Tyco other legal remedies.

a - Limitations on Reverse Engineering and Derivative Works. You may not reverse engineer, decompile, or disassemble the Software, and any attempt to do so shall immediately terminate this EULA - except and only to the extent that such activity may be expressly permitted by applicable law notwithstanding this limitation. You may not make any changes or modifications to any portion of the Software, or create any derivative works, without the written permission of an officer of Tyco (except as provided in Section 3(f) of this EULA with respect to "open source" software). You may not remove any proprietary notices, marks or labels from the Software. You shall institute reasonable measures to ensure compliance with the terms and conditions of this EULA by your personnel and agents.

b - Copyright Notices. You must maintain all copyright notices on all copies of the Software.

c - Transfer. You may only transfer your rights under this EULA (i) as part of a permanent sale or transfer of all of the devices for which the Software is licensed as applicable; (ii) if you transfer all of the Software (including all component parts, the media and printed materials, any upgrades and this EULA); (iii) if you do not retain any copies of any portion of the Software; (iv) if the recipient agrees to the terms of this EULA; and (v) if the Software is an upgrade, such transfer must also include all prior versions of the Software. You agree that failure to meet all of these conditions renders such transfer null and void.

d - Termination. Without prejudice to any other rights, Tyco may terminate this EULA if you fail to comply with the terms and conditions herein. In such event, you must immediately destroy all copies of the Software and all of its component parts. To the extent the Software is embedded in hardware or firmware, you will provide prompt access to Tyco or its representative to remove or lock Software features or functionality as Tyco determines.

e - Subsequent EULA. Tyco may also supersede this EULA with a subsequent EULA pursuant to providing you with any future component, release, upgrade or other modification or addition to the Software. Similarly, to the extent that the terms of this EULA conflict with any prior EULA or other agreement between you and Tyco regarding the Software, the terms of this EULA shall prevail.

f - Incorporation of "Open Source" and other Third Party Software. Portions of the Software may be subject to certain third party license agreements governing the use, copying, modification, redistribution and warranty of those portions of the Software, including what is commonly known as "open source" software. No warranty is provided for open source software. By using the Software you are also agreeing to be bound to the terms of such third party licenses. If provided for in the applicable third party license, you may have a right to receive source code for such software for use and distribution in any program that you create, so long as you in turn agree to be bound to the terms of the applicable third party license, and your programs are distributed under the terms of that license. If applicable, a copy of such source code may be obtained free of charge by contacting your Tyco representative.

g - Trademarks. This EULA does not grant you any rights in connection with any trademarks or service marks of Tyco, its affiliates or its suppliers.

h - Rental. You may not sub-license, rent, lease or lend the Software. You may not make it available to others or post it on a server or web site or otherwise distribute it.

i - Software Keys. The hardware/software key, where applicable, is your proof of license to exercise the rights granted herein and must be retained by you. Lost or stolen keys will not be replaced.

j - Demonstration and Evaluation Copies. A demonstration or evaluation copy of the Software is covered by this EULA; provided that the licenses contained herein shall expire at the end of the demonstration or evaluation period.

k - Registration of Software. The Software may require registration with Tyco prior to use. If you do not register the Software, this EULA is automatically terminated and you may not use the Software.



EULA

l - Additional Restrictions. The Software may be subject to additional restrictions and conditions on use as specified in the documentation accompanying such Software, which additional restrictions and conditions are hereby incorporated into and made a part of this EULA.

m - Upgrades and Updates. To the extent Tyco makes them available, Software upgrades and updates may only be used to replace all or part of the original Software that you are licensed to use. Software upgrades and updates do not increase the number of copies licensed to you. If the Software is an upgrade of a component of a package of Software programs that you licensed as a single product, the Software may be used and transferred only as part of that single product package and may not be separated for use on more than one computer or System. Software upgrades and updates downloaded free of charge via a Tyco authorized World Wide Web or FTP site may be used to upgrade multiple Systems provided that you are licensed to use the original Software on those Systems.

n - Tools and Utilities. Software distributed via a Tyco-authorized World Wide Web or FTP site (or similar Tyco-authorized distribution means) as a tool or utility may be copied and installed without limitation provided that the Software is not distributed or sold and the Software is only used for the intended purpose of the tool or utility and in conjunction with Tyco products. All other terms and conditions of this EULA continue to apply.

4 - EXPORT RESTRICTIONS. You agree that you will not export, re-export or transfer any portion of the Software, or any direct product thereof (the foregoing collectively referred to as the "Restricted Components"), to IRAN, NORTH KOREA, SYRIA, CUBA and SUDAN, including any entities or persons in those countries, either directly or indirectly ("Tyco's Position"). You also agree that you will not export, re-export or transfer the Restricted Components to any other countries except in full compliance with all applicable governmental requirements, including but not limited to applicable economic sanctions and constraints administered by the U.S. Treasury Department and applicable export control measures administered by the U.S. Department of Commerce and U.S. Department of State, any other U.S. government agencies, and measures administered by the European Union or the government agencies of any other countries. Any violation by you of the applicable laws or regulations of the U.S. or any other government, or where you breach Tyco's Position notwithstanding whether or not this is contrary to any aforementioned applicable laws or regulations, will result in automatic termination of this EULA.

5 - U.S. GOVERNMENT RESTRICTED RIGHTS. The Software is Commercial Computer Software provided with "restricted rights" under Federal Acquisition Regulations and agency supplements to them. Any use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in sub-paragraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFAR 255.227-7013 et. seq. or 252.211-7015, or sub-paragraphs (a) through (d) of the Commercial Computer Software Restricted Rights at FAR 52.227-19, as applicable, or similar clauses in the NASA FAR Supplement. Contractor/manufacturer is Sensormatic Electronics, LLC, 6 Technology Park Drive, Westford, MA 01886.

6 - LIMITED WARRANTY.

a - Warranty. Tyco warrants that the recording medium on which the Software is recorded, hardware key, and the documentation provided with it, will be free of defects in materials and workmanship under normal use for a period of ninety (90) days from the date of delivery to the first user. Tyco further warrants that for the same period, the Software provided on the recording medium under this license will substantially perform as described in the user documentation provided with the product when used with specified hardware.

THE FOREGOING EXPRESS WARRANTY REPLACES AND IS IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING BUT NOT LIMITED TO, ANY IMPLIED OR OTHER WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT OR NON-MISAPPROPRIATION OF INTELLECTUAL PROPERTY RIGHTS OF A THIRD PARTY, CUSTOM, TRADE, QUIET ENJOYMENT, ACCURACY OF INFORMATIONAL CONTENT, OR SYSTEM INTEGRATION. TYCO MAKES NO WARRANTY THAT ANY PORTION OF THE SOFTWARE WILL OPERATE ERROR-FREE, FREE OF ANY SECURITY DEFECTS OR IN AN UNINTERRUPTED MANNER. TYCO SHALL NOT BE RESPONSIBLE FOR PROBLEMS CAUSED BY CHANGES IN THE OPERATING CHARACTERISTICS OF THE DEVICE(S) UPON WHICH THE SOFTWARE IS OPERATING, OR FOR PROBLEMS IN THE INTERACTION OF THE SOFTWARE WITH NON-TYCO SOFTWARE OR HARDWARE PRODUCTS. TYCO NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON PURPORTING TO ACT ON ITS BEHALF TO MODIFY OR TO CHANGE THIS WARRANTY, NOR TO ASSUME



EntraPass - Instrukcja instalacji i obsługi programu
Nowe Funkcje (Release Notes) 8.10



EULA

FOR IT ANY OTHER WARRANTY OR LIABILITY CONCERNING THIS SOFTWARE. THE WARRANTY MADE BY TYCO MAY BE VOIDED BY ABUSE OR MISUSE. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS UNDER MANDATORY LAW THAT VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

b - Exclusive Remedy. Tyco's entire liability and your exclusive remedy under the warranty set forth in this Section 6 will be, at Tyco's option, to (i) attempt to correct Software errors with efforts Tyco believes suitable to the problem, (ii) replace at no cost the recording medium, Software or documentation with functional equivalents as applicable, or (iii) refund a pro-rated portion of the license fee paid for such Software (less depreciation based on a five-year life expectancy) and terminate this EULA, provided, in each case, that Tyco is notified in writing of all warranty problems during the applicable warranty period. Any replacement item will be warranted for the remainder of the original warranty period. No remedy is provided for failure of the Software if such failure is the result of accident, abuse, alteration or misapplication with respect to the Software or any hardware on which it is loaded. Warranty service or assistance is provided at the original point of purchase.

7 - LIMITATION OF LIABILITY & EXCLUSION OF DAMAGES.

a - LIMITATION OF LIABILITY. IN NO EVENT WILL TYCO'S AGGREGATE LIABILITY (INCLUDING, BUT NOT LIMITED TO, LIABILITY FOR NEGLIGENCE, STRICT LIABILITY, BREACH OF CONTRACT, MISREPRESENTATION AND OTHER CONTRACT OR TORT CLAIMS) ARISING FROM OR RELATED TO THIS EULA, OR THE USE OF THE SOFTWARE, EXCEED THE GREATER OF USD\$5.00 OR THE AMOUNT OF FEES YOU PAID TO TYCO OR ITS RESELLER FOR THE SOFTWARE THAT GIVES RISE TO SUCH LIABILITY. BECAUSE AND TO THE EXTENT THAT SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSIONS OR LIMITATIONS OF LIABILITY ABOVE, THESE MAY NOT APPLY TO YOU.

b - EXCLUSION OF OTHER DAMAGES. UNDER NO CIRCUMSTANCES SHALL TYCO OR ANY OF ITS RESELLERS OR LICENSORS BE LIABLE FOR ANY OF THE FOLLOWING: (I) THIRD PARTY CLAIMS; (II) LOSS OR DAMAGE TO ANY SYSTEMS, RECORDS OR DATA, OR LIABILITIES RELATED TO A VIOLATION OF AN INDIVIDUAL'S PRIVACY RIGHTS; OR (III) INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE, RELIANCE, OR COVER DAMAGES (INCLUDING LOST PROFITS AND LOST SAVINGS), IN EACH CASE EVEN IF TYCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOU ARE SOLELY RESPONSIBLE AND LIABLE FOR VERIFYING THE SECURITY, ACCURACY AND ADEQUACY OF ANY OUTPUT FROM THE SOFTWARE, AND FOR ANY RELIANCE THEREON. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR THE LIMITATION ON HOW LONG AN IMPLIED WARRANTY LASTS, SO SOME OF THE ABOVE LIMITATIONS MAY APPLY TO YOU ONLY TO THE EXTENT PERMITTED BY THOSE LAWS.

8 - GENERAL. If any provision of this EULA is found to be unlawful, void, or for any reason unenforceable, then that provision shall be severed from this EULA and shall not affect the validity and enforceability of the remaining provisions. You should retain proof of the license fee paid, including model number, serial number and date of payment, and present such proof of payment when seeking service or assistance covered by the warranty set forth in this EULA. This EULA is governed by the laws of the State of New York, without regards to its conflicts of law principles. The parties hereby irrevocably agree that they submit themselves to the personal jurisdiction of the state and federal courts of New York for purposes of resolving any and all disputes arising under or related to these terms and conditions. The parties specifically exclude the application of the provisions of the United Nations Convention on Contracts for the International Sale of Goods.



Nowe Funkcje (Release Notes) 8.10

Moduł wejść/wyjść ioModule

KT-MOD-IO16 to dodatkowy moduł dla KT-400 i kontrolerów KT-1. Płyta posiada 16 wejść/wyjść, które można konfigurować w czterech grupach z EntraPass. Moduł można zdefiniować jako wejścia linii dozorowych, przekaźniki lub jako winda. Istnieje możliwość użycia zacisków 9-12 jako przekaźników SPI oprócz obecnych 32 modułów przekaźnikowych SPI zdefiniowanych w zakładce SPI. Ponadto pełny status stanu czytnika ioSmart i ioModule jest dostępny z kontrolera do którego są podłączone. Aby uzyskać więcej informacji, zobacz stan modułu. Nowa ikona w menu kontrolera ułatwia znajdowanie nieprzypisanych modułów.

Użyliśmy tej samej funkcjonalności, aby znaleźć nieprzypisane ioModules jak używamy dla czytników ioSmart. Aby uzyskać więcej informacji, zobacz [żądanie nieprzypisanych modułów](#).

Aby uzyskać kompatybilność z ioModule, należy użyć najnowszy firmware w kontrolerach KT-1 i KT-400.

Historia zmian

Aby przyspieszyć inspekcję i rozwiązywanie problemów, dodaliśmy nową funkcję historii zmian(audytu). Raporty z historii zmian są dostępne na podstawie kart, komponentów i operatorów.

Funkcja historii zmian zawiera szczegółowy raport o tym, kto dokonał zmian, kiedy zmiany wystąpiły na karcie lub do komponentu systemu. Szczegółowe informacje obejmują niektóre z następujących czynności: typ zmiany, menu, które zostało zmienione, liczbę zmienionych pól, nazwę pola, wartość przed zmianą, wartość po zmianie i typ danych. Ikona historii jest dostępna w dowolnym menu, w którym można edytować kartę lub komponent, a raport oparty na operatorach znajduje się w menu systemowym. Aby uzyskać więcej informacji, zobacz [Historia zmian karty \(Card audit trail\)](#).

Dodatkowe pola informacji o karcie

EntraPass Corporate Edition ma teraz 20 dostępnych pól informacyjnych, dodano dziesięć dodatkowych pól. Pola informacyjne mają edytowalne etykiety i są przydatne do przechowywania informacji dotyczących posiadacza karty, na przykład działu, adresu, numeru pracownika. Aby uzyskać więcej informacji, zobacz [wydawanie nowej karty](#).

Ostatnio otwierane drzwi użytkownika

Dodaliśmy dodatkowe pole do raportu karty użytkownika. Ostatni dostęp jest teraz opcją w obszarze drukowania zaznaczonych pól okna wydruku karty. Jeśli ta opcja jest zaznaczona, w raporcie pojawiają się trzy dodatkowe kolumny: ostatnio otwierane drzwi, ostatnio użyte (Data i godzina) oraz ostatni komunikat o zdarzeniu. Aby uzyskać więcej informacji, zobacz [Drukowanie kart](#).



Unikatowy identyfikator do importowania i eksportowania kart

Aby ulepszyć funkcję importowania/eksportowania informacji o kartach, dodaliśmy UniqueID do listy dostępnych pól. Podczas tworzenia wzorca importu i wybierz UniqueID, dzięki temu można importować bez numeru karty. Można również usuwać użytkowników bez numeru karty. Aby uzyskać więcej informacji, zobacz [Tworzenie nowego wzorca importu/eksportu](#).

Okrągłe obrazy na fotoidentyfikatorze

Ulepszono właściwości szablonu dla projektowania fotoidentyfikatora. Dostępne są dwie nowe opcje, pierwszy to standardowy prostokątny obraz z zaokrąglonymi narożnikami, a drugi to obraz okrągły lub eliptyczny. Aby uzyskać więcej informacji, zobacz [Projektowanie fotoidentyfikatorów](#).

Wyświetlanie pola użytkownika w łączach poziomu dostępu

Dodaliśmy dodatkowe pole do głównych linków w module poziomu dostępu. Przed 8.10, główne łącza wykazały listę wszystkich posiadaczy kart, którzy mają dostęp do wybranego poziomu dostępu. Aby ułatwić rozpoznawanie, użytkownik może dodać kolumnę dla pól informacji o karcie, z możliwością wybrania jednego z pól informacji o karcie użytkowników. EntraPass zachowuje wybór, aby upewnić się, że jest on dostępny dla kolejnych loginów.

Usunięto opcję skompresowanych kopii zapasowych

Ze względu na uprawnienia administratora systemu Windows ograniczające poprawne wykonanie samorozpakowującego się skompresowanego pliku kopii zapasowej, usunęliśmy tę opcję z danych, archiwów, kopii zdarzeń RCP i kopii zapasowych wideo oraz terminarza kopii zapasowych. Zamiast tego użyj oddzielnych plików kopii zapasowej. Aby uzyskać więcej informacji, zobacz [kopie zapasowe](#).

Zapobieganie konfliktom wersji w danych kopii zapasowej

Aby uniknąć przywracania niepoprawnej wersji danych i tworzenia konfliktów bazy danych, gdy operator przywraca kopie zapasową danych, EntraPass sprawdza poprawność pierwszych dwóch cyfr wersji i jeśli wersja, który operator przywraca różni się od bieżącej wersji oprogramowania, wyświetli się komunikat informujący operatora, aby upewnił się, że wersje są zgodne. Jest to dostępne dla wszystkich typów kopii zapasowych. Aby uzyskać więcej informacji, zobacz [odtworzenie kopii](#).

Ukrywanie miniatur obrazów z pól informacyjnych

Aby ułatwić różne wymagania poziomów bezpieczeństwa, EntraPass oferuje możliwość ukrywania pól informacji o kartach z widoku. Miniatury obrazów dla operatorów i użytkowników mają teraz tę funkcjonalność i można wybrać, aby zobaczyć zdjęcia tylko wtedy, gdy jest to potrzebne. Jeśli ustawienie jest ustawione na brak, Miniaturka obrazu zostanie wyświetlona w prawym górnym rogu strony użytkownika i operatora. Aby uzyskać więcej informacji, zobacz [ukrywanie informacji o karcie](#).



Personalizowanie wiadomości powitalnej

Aby spersonalizować środowisko użytkownika, można dostosować powitalne wiadomości e-mail wysyłane przez EntraPass dla nowych użytkowników i operatorów. W sytuacjach, gdy trzeba wyłączyć operatora, można również napisać wiadomość, aby wyjaśnić, dlaczego.

Zamknij ekran potwierdzenia po potwierdzeniu alarmu

Aby wyeliminować wiele odpowiedzi w przypadku systemu z wieloma stacjami roboczymi, okna powiadomień automatycznie zamykają się na innych stacjach roboczych, gdy ktoś potwierdza alarm. Aby uzyskać więcej informacji, zobacz [status aplikacji](#).

8 drzwi bezprzewodowych ASSA-ABLOY na KT-1

Ze względu na sukces KT-1, jednodrzwiowy kontroler może teraz obsługiwać osiem drzwi bezprzewodowych ASSA-ABLOY. Dodanie sześciu bezprzewodowych zamków zmniejsza koszty instalacji poprzez zminimalizowanie ilości kontrolerów potrzebnych do dużych ilości zamków bezprzewodowych, a także pracy wymaganej do ich dopasowania.

Uruchamianie raportu aktywności z ekranu użytkownika

Nowa ikona w kartach generuje nowy raport dla ostatnich transakcji karty. Ten szybki raport jest dodatkiem do istniejącej listy znajdującej się na pulpicie wiadomości, ale zawiera więcej opcji raportów z nieograniczonym wynikiem. Aby uzyskać więcej informacji, zobacz [Raport aktywności](#).

Dodano simplex 4007ES do naszego zakresu integracji i uproszczone nazwy i opisy integracji w GUI

Panel przeciwpożarowy simplex 4007ES został dodany do listy paneli przeciwpożarowych, które EntraPass integruje z. Dodatkowo, aby ułatwić instalację podczas integracji z wtargnięciem lub sygnalizacją pożaru, mamy przepisany tekst rozwijany i opis dla wszystkich typów DLL. Aby uzyskać więcej informacji, zobacz zintegrowana konfiguracja panelu.

Aktualizacja Sybase

Aby umożliwić EntraPass uruchamiania w systemie Windows Server 2016 i Windows Server 2019, uaktualniono bazy danych Sybase do najnowszej.

Oczyszczanie bazy danych

Poprawiliśmy efektywność bazy danych Sybase, dodając funkcje do automatycznego oczyszczania i pakowania plików, które osiągają pewien rozmiar. Ponadto EntraPass automatycznie usunie rekordy kart, które nie zostały zmodyfikowane w ciągu pięciu lat.



Zgodność z systemem Windows Server 2019

EntraPass jest teraz kompatybilny z Windows Server 2019 Standard. Aby uzyskać więcej informacji, zobacz [minimalne wymagania systemowe](#).

Drukuj poziomy dostęp bezpośrednio w formacie PDF

Jeśli chcesz drukować poziomy dostęp, masz teraz możliwość zapisania poziomego dostępu do formatu PDF i formatu pliku CSV, jest to uzupełnienie istniejących funkcji drukowania. Opcja zapisania elektronicznej kopii wspiera ekologiczne biuro.

Małe ulepszenia stacji roboczej

Po zaktualizowaniu do najnowszej wersji EntraPass, można zauważyć kilka ulepszeń podczas uruchamiania systemu. Wersja produktu pojawi się w prawej górnej części ekranu i eliminuje konieczność kliknięcia w sekcji about, aby uzyskać informacje. Ponadto aby zmniejszyć liczbę kliknięć, po zalogowaniu się automatycznie wyświetla okno poświadczeń z wypełnioną nazwą użytkownika.

Rozszerzona usługa internetowa EntraPass

Aby uwzględnić okoliczności, gdy EntraPass Web jest zainstalowany w innym folderze Internet Information Services (IIS), operator kontroluje teraz link do powitalnego e-mail dla EntraPass Web, EntraPass go i EntraPass go install. Operator może wprowadzać modyfikacje bezpośrednio w GUI. Ta aktualizacja ułatwia również wiele połączeń SmartLink, gdzie można wybrać, które aplikacje mobilne do nawiązania połączenia jak smartlink wykorzystują. Aby uzyskać więcej informacji, zobacz [Konfigurowanie aplikacji SmartLink](#).



Jak to zrobić?

Jak utworzyć kopię systemu (Backup)

1. Wybierz zakładkę **Opcje (Options)**.
2. Kliknij **Terminarz Kopii Zapasowej (Backup Scheduler)**.
3. Wybierz rodzaj danych z zakładek znajdujących się na górze (**Dane (Data)**, **Archiwum (Archive)**, **Czas pracy (In/Out)** albo **Zdarzenie Wideo (Video Event)**).
4. Kliknij i zaznacz pole **Automatyczna Kopia Zapasowa (Automatic Backup)**, aby aktywować funkcję, a następnie wprowadź **Czas Rozpoczęcia (Start Time)**.
5. Jeśli została wybrana **Automatyczna Kopia Zapasowa (Automatic Backup)**, należy wybrać częstotliwość.
6. Kliknij i zaznacz pole **Teraz (Now)** aby utworzyć kopię zapasową od razu.

Aby dowiedzieć się więcej o Kopiach Zapasowych, sprawdź [KOPIA SYSTEMU \(BACKUPS\)](#)



Jak zdefiniować szablon foto-identyfikatora (Badge)

1. Wybierz zakładkę **Użytkownicy (Users)**.
2. Kliknij przycisk **Identyfikator (Badge)**.
3. Kliknij przycisk **Nowy (New)**  na pasku narzędzi.
4. Wybierz właściwości i kliknij **OK**.
5. Wprowadź nazwę Identyfikatora dla obu języków.
6. Kliknij ***Kliknij tutaj, aby zmienić szablon Identyfikatora (Click here to modify the badge layout)*** na dole ekranu.
7. W oknie **Design Identyfikatora** wybierz elementy, które mają być dodane do Identyfikatora.
8. Po zakończeniu kliknij **menu Szablon** i wybierz **Wyjście (Exit)**.
9. Zapisz przy pomocy przycisku **Zapisz (Save)**

Aby dowiedzieć się więcej o konfigurowaniu Identyfikatorów w EntraPass, sprawdź [Projektowanie foto-identyfikatorów \(Badges Designing\)](#)



Jak dodać nowego użytkownika karty (Card)

!!! [Bramka](#) albo Połączenie muszą zostać utworzone przed utworzeniem Karty

!!! [Poziom dostępu](#) musi zostać utworzony przed utworzeniem Karty

1. Wybierz zakładkę **Użytkownicy (Users)**.
2. Kliknij przycisk **Karta (Card)**.
3. Kliknij przycisk **Nowy (New)**  na pasku narzędzi. Aktywuje się wtedy pole **Numer Karty (Card number)**.
4. Wprowadź numer karty i naciśnij **Enter**.
5. Wprowadź **Nazwę Użytkownika Karty (Card user name)**
6. Kliknij przycisk **Poziom dostępu (Access level)**
7. Wybierz Poziom dostępu z rozwijanej listy
8. Zapisz przy pomocy przycisku **Zapisz (Save)**

Aby dowiedzieć się więcej o tworzeniu kart, sprawdź [Definiowanie Kart \(Cards Definition\)](#)

Notatka:

Jeżeli włączono **Zaawansowane zarządzanie (Enhanced User Management)**, sprawdź **Wprowadzanie nowej karty w Zaawansowanym zarządzaniu (Issuing a New Card in Enhanced User Management Environment)**.



Jak zdefiniować nowy terminarz (Schedule)

1. Wybierz zakładkę **Definicje (Definition)**.
2. Kliknij przycisk **Terminarz (Schedule)**.
3. Kliknij przycisk **Nowy (New)**  na pasku narzędzi.
4. Wprowadź nazwę Terminarza w dwóch językach.
5. Zapisz przy pomocy przycisku **Zapisz (Save)**
6. Wprowadź czas: **Rozpoczęcia** oraz **Zakończenia**.
7. Wprowadź dni tygodnia, dla których obowiązuje Terminarz.
8. Wybierz (do czterech) święta, które mają być uwzględnione.

Aby dowiedzieć się więcej o definiowaniu świąt w EntraPass, sprawdź [Definiowanie Świąt \(Holiday Definition\)](#)



Jak zdefiniować prosty raport (Simple Report)

Aby dowiedzieć się więcej o tworzeniu raportów w EntraPass, sprawdź Definiowanie [Szybkich Raportów \(Quick Report Definition\)](#)

1. Wybierz zakładkę **Raport (Report)**.
2. Kliknij **Szybki Raport (Quick Report)**.
3. Wybierz rodzaj **Zdarzenia (Event)** z listy.
4. Po prawej stronie okna wprowadź nazwę w dwóch językach w polu **Nazwa raportu (Report name)**
5. Kliknij przycisk **Wykonaj (Execute)**



Jak utworzyć nowy poziom dostępu (Access Level)

!!! Bramka albo Połączenie muszą zostać utworzone przed utworzeniem nowego Poziomu Dostępu

1. Wybierz zakładkę **Użytkownicy (Users)**.
2. Kliknij przycisk **Poziom dostępu (Access level)**.
3. Wybierz **Bramkę / Połączenie (Gateway / Connection)** z listy.
4. Kliknij przycisk **Nowy (New)**  na pasku narzędzi. Zostanie odblokowane pole Numer Karty.
5. Wprowadź nazwę dla Poziomu dostępu w dwóch językach.
6. Zapisz przy pomocy przycisku **Zapisz (Save)**

Aby dowiedzieć się więcej o tworzeniu kart, sprawdź [Definiowanie Poziomu Dostępu \(Access Level Definition\)](#)



Jak wydrukować listę kart (Print a Card List)

1. Wybierz zakładkę **Użytkownicy (Users)**.
2. Kliknij przycisk **Karta (Card)**.
3. Kliknij przycisk **Drukuj (Print)**
4. Wybierz **Index Karty (Index Card)** z listy.
5. Ewentualnie można zdefiniować zakres numerów kart, wyfiltrować, a następnie wybrać pola karty do wydruku (aby poznać szczegóły sprawdź [Drukowanie Kart \(Card Printing\)](#)).
6. Kliknij przycisk **Drukuj (Print)**
7. Wybierz drukarkę z listy i kliknij **OK**.



Jak wydrukować listę poziomów dostępu (Print a List of Access Levels)

1. Wybierz zakładkę **Użytkownicy (Users)**.
2. Kliknij przycisk **Poziom Dostęp (Access level)**.
3. Kliknij przycisk **Drukuj (Print)**
4. Wybierz **Stronę / Bramkę / Połączenie (Site / Gateway / Connection)** z listy.
5. Wybierz poziomy dostęp do wydrukowania.
6. Kliknij przycisk **Drukuj (Print)**
7. Wybierz drukarkę z listy i kliknij **OK**.



Jak Wydrukować Listę Drzwi (Print a List of Doors)

1. Wybierz zakładkę **Urządzenia (Devices)**.
2. Kliknij przycisk **Drzwi (Door)**.
3. Kliknij przycisk **Drukuj (Print)**
4. Wybierz **Stronę / Bramkę / Połączenie (Site / Gateway / Connection)** z listy.
5. Wybierz **Drzwi** do wydrukowania.
6. Kliknij przycisk **Drukuj (Print)**
7. Wybierz drukarkę z listy i kliknij **OK**.



Jak skonfigurować pulpity (Setup the Desktops)

Aby dowiedzieć się więcej o konfiguracji pulpitów w EntraPass, sprawdź **Pulpity** (Desktops)

1. Wybierz zakładkę **Pulpity (Desktops)**.
2. Kliknij prawym przyciskiem myszy na przycisku **Pulpit (Desktop)** i wybierz **Właściwości (Properties)**.
3. Wprowadź nazwę dla pulpitu w polu **Nazwa Pulpitu (Desktop Name)**.
4. Wybierz pulpity do wyświetlenia.
5. Wybierz **Zatwierdź i uruchom (OK and GO)**, aby zapisać i uruchomić zmiany.



EntraPass - Instrukcja instalacji i obsługi programu Jak to zrobić?

Jak używać skrótów klawiszowych

EntraPass pozwala na korzystanie z klawiszy skrótów w celu przyspieszenia działań.

Przycisk	Aktywowany z	Funkcja
F1	Dowolne menu	Pomoc
F2	Dowolna lista	Rozszerzony wybór
F3	Dowolne menu	Wyświetl wszystkie otwarte okna
F4	Dowolne menu z listą	Otwórz listę
F5	Tam gdzie możliwe	Odśwież
F8	Wszędzie	Wyszukaj
F10	Wszędzie	Wyloguj
F11	Wszędzie	Przestrzeń robocza
F12	Wszędzie	Zmień konto



Jak spersonalizować okno logowania w EntraPass WEB

Możesz dowolnie spersonalizować ekran powitalny oraz ikonę logowania dla EntraPass Web w następujący sposób:

- 1** – przy pomocy edytora tekstu otwórz plik web.cfg (C:\inetpub\wwwroot\).
- 2** – znajdź `<add key="WelcomeMessage" value="EntraPass Web"/>`.
- 3** – zastąp "EntraPass Web" dowolną wiadomością. Nie przekraczaj limitu 30 znaków, aby uniknąć nieprawidłowego wyświetlenia wiadomości. Znaki specjalne są [dostępne \(HTML ASCII\)](#).
- 4** - znajdź `<add key="WelcomeImage" value="Resources/Images/chip_bw.png"/>`
- 5** - zastąp "Resources/Images/chip_bw.png" adres swojego preferowanego obrazu w formacie JPG albo PNG.
- 6** – domyślny rozmiar obrazu to 57 x 57 pikseli. Aby to zmienić edytuj wartości "WelcomeImageHeight" oraz "WelcomeImageWidth". Nie przekraczaj rozmiaru 155 x 155 pikseli, aby mieć pewność, że obraz będzie prawidłowo wyświetlony.



Jak udostępnić Go Pass dla użytkownika

Użytkownik może otworzyć drzwi przy pomocy smartfonu dzięki aplikacji GO Pass.

Aby skorzystać z GO Pass musisz dodać GO Pass do [komponentów systemu](#) oraz udostępnić GO Pass aplikacji SmartLink. Aby udostępnić GO Pass wykonaj następujące czynności:

- 1** – wybierz **Urządzenia, Aplikacje** i zaznacz SmartLink, który zostanie wykorzystany dla twojej aplikacji GO Pass.
- 2** – wybierz zakładkę **Usługa Web** oraz opcję **Udostępnij GO Pass**.
- 3** – upewnij się, że **Nazwa połączenia, Adres IP / Nazwa domeny** oraz **numery portu** są wprowadzone dla połączenia SmartLink.
- 4** – wybierz zakładkę **E-mail SmartLink**.
- 5** – upewnij się, że Parametry serwera E-mail są wprowadzone dla połączenia.

Aby udostępnić GO Pass dla użytkownika i wysłać uwierzytelnienia wykonaj następujące czynności:

- 1** – w zakładce **Użytkownicy** wybierz **Karta**.
- 2** – wybierz istniejącego **Użytkownika** albo stwórz Nowego.
- 3** – zaznacz pole **GO Pass**.
- 4** – wprowadź adres e-mail użytkownika. Zostanie on wykorzystany do wysłania instrukcji.
- 5** – wybierz pole **Powiadom**, aby umożliwić wysłanie e-maila.
- 6** – wybierz język.
- 7** – zapisz.

E-mail jest automatycznie wygenerowany i wysłany do użytkownika ze szczegółami, w jaki sposób pobrać aplikację na ich smartfon. Uwierzytelnienia są automatycznie wprowadzone do aplikacji.

System wykorzystuje informacje Karty #1 w zakładce Karty, aby przyznać dostęp. Upewnij się, że to pole jest wypełnione.

Zmiana portu albo adresu SmartLink przerwie dostęp GO Pass. GO Pass wymaga zaktualizowanego uwierzytelnienia.

Aby wysłać zaktualizowane uwierzytelnienia do wszystkich użytkowników GO Pass wykonaj następujące czynności:

- 1** – w zakładce **Opcje** wybierz **Parametry systemu**.
- 2** – z menu wybierz **EntraPass Web**; następnie **wybierz Wyślij ponownie do wszystkich użytkowników GO Pass**.

Zaktualizowane uwierzytelnienia są automatycznie wysłane do wszystkich użytkowników GO Pass poprzez e-mail.

Notatka: musisz posiadać ważny KAP, aby korzystać z opcji GO Pass.



Jak użyć HID Mobile Access

HID Mobile Access daje użytkownikowi dostęp do drzwi za pomocą smartfona. HID Mobile Access jest konfigurowany z poziomu stacji roboczej EntraPass razem z uprawnieniami dla użytkownika.

Aby skorzystać z HID Mobile Access musisz dodać HID Mobile Access do [komponentów systemu](#).

Aby włączyć HID Mobile Access wykonaj następujące czynności:

- 1 - Wybierz kartę Opcje, a następnie wybierz z menu **Parametry systemu**.
- 2 - Wybierz przycisk Integracja i wybierz kartę **HID Mobile Access**.
- 3 - Wprowadź **identyfikator klienta** i **hasło**. Sprawdzanie poprawności certyfikatu PKI nie jest obecnie obsługiwane. Możesz je zdobyć poświadczenia z konta systemowego HID. Adres **URL portalu**, adres **URL logowania** i **ścieżka** są automatycznie zakończone, ale możesz edytować, jeśli potrzebujesz.
- 4 - Wybierz przycisk **Konfiguruj numery części**. Spowoduje to otwarcie okna **Konfiguracja numeru części**.
- 5 - Wybierz **Aktualizuj z HID Portal**, aby zaktualizować listę.
- 6 - Wprowadź swój **Facility Code** i wybierz **format wyświetlania karty**. Kod obiektu i format wyświetlania karty są specyficzne dla zakupionych kart HID. Wybierz OK, aby zapisać konfigurację.
- 7 - Wybierz OK, aby zapisać parametry dostępu mobilnego HID.

Aby dodać nowego użytkownika HID Mobile Access w systemie, wykonaj następujące kroki:

- 1 - Z zakładki **Użytkownicy** wybierz **Karta**.
- 2 - Wybierz istniejącą **nazwę użytkownika karty**. Ta integracja działa na istniejących kontach użytkowników.
- 3 - Wybierz przycisk **HID Mobile Access**. Spowoduje to otwarcie okna **HID Mobile Access**.
- 4 - Wybierz numer części z **listy numerów części**. Każdy numer części reprezentuje pudełko kart. Ilość pole wyświetla liczbę pozostałych numerów kart.
- 5 - Wybierz opcję **Wyślij zaproszenie i wydaj mobilny identyfikator**, aby poprosić użytkownika o zarejestrowanie smartfona.
- 6 - Wybierz OK.

Aby wyświetlić status istniejącego użytkownika HID Mobile Access, wykonaj następujące kroki:

- 1 - Z zakładki **Użytkownicy** wybierz **Karta**.
- 2 - Wybierz istniejącą **nazwę użytkownika karty**.
- 3 - Wybierz przycisk **HID Mobile Access**. Spowoduje to otwarcie okna **HID Mobile Access**.
- 4 - Zaznacz pole wyboru **Zaawansowane**.



EntraPass - Instrukcja instalacji i obsługi programu Jak to zrobić?

5 - W sekcji **Zaproszenia** wyświetlany jest status zaproszenia. Tutaj możesz ponownie wysłać lub usunąć zaproszenia. Lista **kontenerów poświadczeń** wyświetla wszystkie urządzenia, które zostały już powiązane z użytkownikiem.

6 - Wybierz **OK**.

Aby dodać wiele urządzeń do jednego użytkownika, wykonaj następujące czynności:

1 - W oknie **HID Mobile Access** wybierz numer części z listy numerów części.

1 - Zaznacz pole wyboru **Zaawansowane**.

2 - Wybierz przycisk **Wyślij zaproszenie**. Gdy użytkownik rejestruje swoje urządzenie, tworzony jest nowy kontener **listę kontenerów poświadczeń**.

3 - Wybierz nowe urządzenie z listy **kontenerów poświadczeń**.

4 - Wybierz przycisk **Wyдай mobilny identyfikator**.

5 - Wybierz **OK**.

Aby dodać wiele kart do jednego użytkownika, wykonaj następujące kroki:

1 - W oknie **HID Mobile Access** wybierz numer części z listy numerów części.

1 - Zaznacz pole wyboru **Zaawansowane**.

2 - Wybierz kontener z listy **kontenery poświadczeń**.

3 - Wybierz przycisk **Wyдай identyfikator** telefonu komórkowego. Powoduje to wysłanie kolejnego **identyfikatora mobilnego** do smartfona użytkownika.

4 - Wybierz **OK**.

UWAGA: Każde urządzenie może posiadać 1 identyfikator mobilny z każdego numeru części. Urządzenie może pomieścić do 5 różnych identyfikatory mobilne, jeśli pochodzą z 5 różnych numerów części.



Jak migrować z Parametrów zdarzeń do Zdarzeń Przypisanych do operatora

Tryb Zdarzeń Przypisanych do Operatora zastępuje tryb parametrów zdarzeń do zarządzania zdarzeniami. Nowe instalacje od wersji 7.30.48 będą używały domyślnie tryb Zdarzeń Przypisanych do Operatora. Aktualizowane systemy z wcześniejszych wersji muszą włączyć tryb ręcznie. Aby włączyć tryb Zdarzeń Przypisanych do Operatora podejmij następujące kroki:

- 1 - Zaloguj się do serwera EntraPass lub aplikacji stacji roboczej.
- 2 - Kliknij **Opcje**, a następnie **Parametry systemu**.
- 3 - Kliknij ikonę **serwera**.
- 4 - Kliknij kartę **Alarmy – zarządzanie**.
- 5 - Wybierz **Migruj z parametrów zdarzeń do Zdarzeń Przypisanych do Operatora**.
- 6 - Wybierz **OK**, aby rozpocząć migrację.
- 7 - Wybierz **OK**, aby potwierdzić operację. Aby zapewnić bezpieczeństwo, wykonywana jest automatyczna kopia zapasowabaza danych jest zablokowana.
- 8 - Podczas migracji zdarzenia są wyświetlane na domyślnym pulpicie operatora.
 - Jeśli wybrana jest opcja **Nadpisz obszar roboczy stacji roboczej**, zdarzenia są wyświetlane w polu obszar roboczy zdefiniowany na karcie Zabezpieczenia.
 - Jeśli opcja **Nadpisz obszar roboczy stacji roboczej** nie jest zaznaczona, zdarzenia są wyświetlane w polu domyślny pulpit.
 - Jeśli operator nigdy nie zalogował się do stacji roboczej lub ostatni login operatora nie był się na stacji roboczej, operator otrzyma wszystkie zdarzenia.
 - Jeśli ostatni login operatora był na stacji roboczej i opcja **Zastosuj obszar roboczy stacji roboczej i parametry zdarzeń** jest wybrana, operator otrzyma zdarzenia w obszarze roboczym zdefiniowanym w opcji **Kiedy Zalogowany** iz harmonogramem zdefiniowanego w Parametrach Zdarzeń dla stacji roboczej.
 - Jeśli ostatni login operatora był na stacji roboczej i opcja **Zastosuj obszar roboczy stacji roboczej i parametry zdarzeń** nie jest wybrana, operator otrzyma zdarzenia z zdefiniowanym harmonogramem wyświetlania w Parametrach Zdarzeń dla tej stacji roboczej.
- 9 - Istniejące parametry zdarzeń są scalane w pojedyncze wyzwalacze i alarmy w oparciu o ich typ (aplikacja, Drzwi, wejście itp.), Ich harmonogramy alarmu i instrukcje. Makropolecenia zdefiniowane w Parametrach Zdarzeń również są migrowane.
- 10 - Model zarządzania alarmami jest przesyłany do każdego wyzwalacza i alarmu. Kompatybilność i Priorytet Zdarzenia są przekazywane do potwierdzenia dla wszystkich podłączonych stacji roboczych.
- 11 - Po migracji wszystkie aktywne stacje robocze muszą być wylogowane i zalogowane, aby wyświetlić zmiany.

UWAGA: Nie można odwrócić migracji z trybu parametru zdarzenia do Zdarzenia Przypisane do Operatora.



Jak przełączyć bazę w tryb tylko do odczytu

Gdy włączony jest tryb tylko do odczytu bazy danych, nie można wprowadzać żadnych modyfikacji do bazy danych. Wiadomości, alarmy i operacje ręczne będą nadal działać normalnie. Aby ręcznie ustawić bazę danych EntraPass do trybu tylko do odczytu wykonaj następujące czynności:

- 1** - Zaloguj się do serwera EntraPass lub aplikacji stacji roboczej.
- 2** - Kliknij prawym przyciskiem myszy w dowolnym miejscu głównego okna, aby uruchomić menu.
- 3** - Kliknij opcję **Tryb bazy danych - tylko do odczytu**.
- 4** - Kliknij **Tak**, aby potwierdzić akcję.
- 5** - Kliknij **OK**, aby zamknąć okno potwierdzenia. Wskaźnik stanu bazy danych sieci, umieszczony w lewym dolnym rogu ekranu zmieni kolor z zielonego na czarny.
- 6** - Aby przywrócić bazę danych do normalnego trybu, kliknij prawym przyciskiem myszy w dowolnym miejscu głównego okna i kliknij **Tryb bazy danych - tylko do odczytu**. Wskaźnik stanu znajdujący się w lewym dolnym rogu ekranu zmieni kolor z czarnego na zielony.

UWAGA: Baza danych pozostanie w trybie tylko do odczytu do momentu wyłączenia jej przez operatora lub serwera zrestartowany.



Jak włączyć tryb serwisowy

Po włączeniu trybu serwisowego w EntraPass wszystkie powiadomienia alarmowe są pomijane. Obejmuje to wszystko alarm potwierdzania komunikatów wyskakujących i wiadomości e-mail wysyłanych z wyzwalacza zdarzeń. Ten tryb nie ma wpływu raporty wysyłane e-mailem i e-maile z przypomnieniem KAP.

Aby włączyć tryb konserwacji, wykonaj następujące kroki:

- 1 - Zaloguj się do serwera EntraPass lub aplikacji stacji roboczej.
- 2 - Kliknij prawym przyciskiem myszy w dowolnym miejscu głównego okna, aby uruchomić menu.
- 3 - Kliknij **tryb serwisowy**.
- 4 - Kliknij **Tak**, aby potwierdzić akcję.
- 5 - Kliknij **OK**, aby zamknąć okno potwierdzenia. Gdy tryb serwisowy jest włączony, **wiadomość tryb serwisowy** jest wyświetlana w dolnej części okna.
- 6 - Aby wyłączyć tryb konserwacji, kliknij prawym przyciskiem myszy w dowolnym miejscu głównego okna i kliknij **Tryb serwisowy**.

UWAGA: Tryb serwisowy pozostanie aktywny do momentu wyłączenia go przez operatora lub ponownego uruchomienia serwera.



Jak skonfigurować czytniki ioSmart

Czytnik kart Kantech ioSmart musi być podłączony do kontrolera (KT-400 lub KT-1). Czytnik ioSmart obsługuje połączenia wiegand i RS-485 ze sterownikiem.

Podczas łączenia za pomocą połączenia wiegand użyj programu Express Setup, aby skonfigurować czytnik. Podczas łączenia za pomocą połączenia RS-485 wykonaj następujące czynności:

- 1 - Kliknij kartę **Urządzenia**.
- 2 - Wybierz ikonę **kontrolera**.
- 3 - Wybierz kontroler i kliknij zakładkę **ioSmart**.
- 4 - Wybierz symbol +, aby dodać czytnik ioSmart do kontrolera.
- 5 - Wprowadź **numer seryjny** czytnika ioSmart.
- 6 - Wybierz skojarzone drzwi.
- 7 - Wybierz opcję Klawiatura, jeśli czytnik ioSmart zawiera klawiaturę.
- 8 - Aby skonfigurować wejścia i wyjścia czytnika, kliknij przycisk terminala i wybierz I1 i I2O funkcja terminalu.

- **Wyłączone**
- **Pojedyncze wejście linii dozorowej**
- **Podwójne wejście linii dozorowej**
- **Wyjście sterujące zamkiem**
- **Przełącznik**

Możliwe jest skonfigurowanie I1 i I2O dla maksymalnie 4 wejść linii dozorowych (przy użyciu I1 i I2O w trybie Podwójnego wejścia linii dozorowej) lub 2 wejścia i 1 wyjście (Wyjście sterujące zamkiem lub przełącznik).

- 9 - Kliknij zakładkę **KT-1 / KT-400** i wybierz odpowiednią szybkość transmisji dla swojego systemu.

- 10 - Kliknij przycisk z trzema kropkami, aby przypisać **szablon czytnika**. Użyj zakładki Urządzenia → Szablon czytnika, aby go skonfigurować.

Możesz również skonfigurować swój czytnik ioSmart w zakładce Operacje.

- 1 - Kliknij kartę **Operacje**.
- 2 - Wybierz odpowiednią ikonę kontrolera i zostaną wyświetlone okna kontrolera.
- 3 - Wybierz odpowiednie urządzenie, kliknij kontroler prawym przyciskiem myszy i wybierz opcję Żądanie nieprzypisanych modułów.
- 4 - Kliknij prawym przyciskiem kontroler i kliknij Nieprzypisany moduł. Spowoduje to utworzenie modułu nieprzypisanego kontrolera wymagane przez zdarzenie operatora na pulpicie.



EntraPass - Instrukcja instalacji i obsługi programu Jak to zrobić?

5 - Kliknij prawym przyciskiem myszy zdarzenie, aby przypisać czytnik. Numer seryjny czytnika ioSmart jest automatycznie wypełnione na karcie konfiguracji.

UWAGA: Zobaczysz komunikat o błędzie **Nie można dodać modułu do tego kontrolera**, gdy dodatkowe czytniki nie można dodać do kontrolera z powodu limitu.

Status czytników ioSmart jest wyświetlany w menu Operacje → Drzwi. Kliknij prawym przyciskiem myszy na odpowiednie drzwi, aby wyświetlić status. Wyświetlany jest status wszystkich skonfigurowanych czytników ioSmart podłączonych do kontrolera Operacje → Kontrolery.



F.A.Q.

Czy można użyć wejścia linii dozorowej do odblokowania grupy pięter i jak długo pozostaną one odblokowane?

Tak, linia dozorowa może zostać wykorzystany do odblokowania pojedynczego piętra albo grupy. Piętro albo grupa pozostanie dostępna tak długo, jak odryglowane pozostaną drzwi. Czas domyślny to 10 sekund, ale istnieje możliwość modyfikacji tego okresu.

Czy można zaimportować poziomy dostęp (Import Access Levels)?

Nie, Poziomy Dostępu nie mogą być importowane.

Jakie są numery portów komunikacyjnych w systemie EntraPass: serwera, stacji operatora, Smartlinka, bramki, serwera zapasowego, stacji wideo oraz EntraPass WEB?

- Serwer: TCP 18000
- Stacja: TCP 18101
- Bramka: TCP 18102
- Smartlink: TCP 18103
- Dublowanie bazy danych: TCP 17999
- Video Vault: TCP18107
- EntraPass WEB: TCP 8801

Jakie są opcje rozbrajania wirtualnego systemu alarmowego?

System Wirtualnych Alarmów można wyłączyć zdalnie przy pomocy software'u oraz manualnie przy pomocy karty magnetycznej i czytnika przy drzwiach.

Jakie są opcje uzbrajania wirtualnego systemu alarmowego?

System Wirtualnych Alarmów jest dostępny wyłącznie w EntraPass Global. Istnieją trzy metody uzbrajania Systemu Wirtualnych Alarmów:

- aktywacja przy użyciu karty magnetycznej
- aktywacja przy pomocy karty oraz aktywującego sygnału wejściowego
- aktywacja sygnałem wejściowym

Jakiego rodzaju opcje są dostępny w przypadku operacji grupowych (batch operations)?

Operacje grupowe umożliwiają użytkownikowi dokonywanie znaczących zmian w bazie danych przy pomocy jednego kliknięcia. Pola, które można zmieniać przy pomocy operacji grupowych to: Stan Karty, Poziom Nadzorcy (GE), Karta śledzona, Data Rozpoczęcia, Data zakończenia, Usuń po terminie ważności, Oczekiwanie na kod PIN z klawiatury, Poziom dostępu karty, Szablon identyfikatora. Operacje grupowe mogą być również przeprowadzone poprzez Typ Karty (Card Type).



Do czego można użyć funkcji Przekazniki zdarzeń i jakie są w niej opcje do wyboru?

Ta funkcja jest dostępna tylko dla konkretnych zdarzeń w EntraPass Global. Można ustawić opcję, aby każdy przekaznik uruchamiał się okresowo, albo aktywował się / wyłączał według zdefiniowanego Terminarza.

Co się dzieje gdy zdjęcia do kart są zapisane w oddzielnym folderze zamiast w bazie danych serwera?

Ustawienia umożliwiają zapisać zdjęcia użytkowników kart, wzory podpisów oraz grafikę tła w postaci oddzielnych plików zamiast bezpośrednio do bazy danych. Oferujemy tą opcję dla lokalizacji, które mają duże ilości w/w obrazów i grafik. Baza danych obrazów, podpisów i grafik może aktualnie zawierać 2 Gb danych. Parametr będzie używany w przypadkach, gdy połączenie może wymagać więcej miejsca na zapisywanie obrazów, podpisów oraz grafik.

Jak jest różnica pomiędzy Dostępem jednorazowym a Czasowym odryglowaniem drzwi w KT-100, KT-200, KT-300 oraz KT-400?

Jednorazowy dostęp dla KT-100-200-300-400

To polecenie może być wyegzekwowane poprzez menu operacyjne drzwi – drzwi zostaną odryglowane na określony czas. Jeśli drzwi pozostaną otwarte dłużej niż określony czas zostanie wygenerowane zdarzenie alarmu wstępnego. Jeśli po tym zdarzeniu drzwi nie zostaną zamknięte w określonym czasie zostanie wygenerowane zdarzenie drzwi otwarte zbyt długo.

Czasowe odblokowaniu dla KT-100-200-300

To polecenie może być wyegzekwowane poprzez menu operacyjne drzwi – drzwi zostaną odryglowane na określony czas. Jeśli drzwi pozostaną otwarte dłużej niż określony czas zostanie wygenerowane zdarzenie alarmu wstępnego. Jeśli po tym zdarzeniu drzwi nie zostaną zamknięte w określonym czasie zostanie wygenerowane zdarzenie Drzwi otwarte zbyt długo.

Czasowe odryglowanie dla KT-400

To polecenie może być wyegzekwowane poprzez menu operacyjne drzwi w momencie otwarcia drzwi. Jeżeli drzwi pozostaną otwarte dłużej niż określony czas odblokowania zostanie wygenerowane nowe zdarzenie Alarm przy ponownym zamknięciu.

Do czego służy opcja Zdarzenia klienta?

Opcja Zdarzeń definiowanych przez klienta (Custom messages) umożliwia operatorowi, który posiada odpowiednie uprawnienia bezpieczeństwa, zdefiniowanie niestandardowych komunikatów, które mogą być generowane poprzez zdarzenia zależne od terminarza. Każdy komunikat może być aktywowany, kiedy terminarz staje się aktywny, nieaktywny lub w obu przypadkach.

Każde zdarzenie jest wyświetlane w Liście Komunikatów (Messages List) na pulpicie.



Dlaczego używamy grup kart dostępu?

Zaprogramowane grupy odczytu kart pozwalają na szybką selekcję poziomów dostępu do różnych elementów systemu. Grupa odczytu karty może zostać wykorzystana podczas programowania karty zamiast wprowadzania poziomu dostępu dla każdego połączenia. Tylko informacje dotyczące grupy odczytu karty są powiązane z kartą; tym samym można modyfikować te informacje bez modyfikowania dostępu karty.

Grupy odczytu kart mogą być importowane z pliku CSV.

Gdzie mogę zsynchronizować operatorów z Active Directory?

Możliwe jest uruchomienie synchronizacji z wielu lokalizacji, w tym:

- **System / Active directory:** użyj przycisku **Synchronizuj teraz**, aby ręcznie rozpocząć synchronizację z wybranym aktywnym serwerem katalogów.
- **Status / Aplikacja:** kliknij prawym przyciskiem myszy SmartLink, aby zobaczyć dwie opcje synchronizacji:
 - **Wymuś Synchronizację wszystkich LDAP** wymusza wszystkie synchronizowanie wszystkich aktywnych serwerów katalogów.
 - **Wymuś Synchronizację LDAP** zsynchronizuje tylko jeden konkretny serwer Active Directory.
- **Kontrola usług LDAP:** kliknij prawym przyciskiem myszy ikonę Active Directory na pasku zadań Windows, aby zobaczyć Synchronizację

Opcja „**teraz**”:

- Ta opcja synchronizuje wszystkie aktywne serwery katalogów na wybranym łączu SmartLink.



Wstęp

Co to jest EntraPass?

Co to jest EntraPass?

EntraPass jest wszechstronnym, opartym na sterowaniu poprzez menu pakietem oprogramowania kontroli dostępu. Wśród wielu funkcji, EntraPass może m.in. zaoferować:

- Nowy silnik zarządzania bazami danych (Sybase)
- Możliwość komunikacji zdalnej
- Aplikacja SmartLink Interface (systemy przywoławcze, systemy HVAC, e-mail i nie tylko)
- Serwer redundancji dla bezawaryjnego działania (opcjonalnie)
- Podłączenie do Kantech IP Link
- Kompatybilność z KT-1 i KT-400 oraz KT-300, KT-100, KT-200

Notatka:

Możesz stworzyć magistralę kontrolerów KT-200 na porcie RS-485 kontrolera KT-400 w przypadku nie korzystania z pozostałych typów kontrolerów (KT-100, KT-300 oraz KT-400)

- KTES – Kantech Telephone Entry System
- Integracja ze sprzętem od innych producentów
- Ekspresowe ustawienia
- Lokalny anti-passback, interakcję pomiędzy kontrolerami drzwi
- Kontrola wind
- Zintegrowane funkcje identyfikowania
- Interaktywne plany pięter
- Pulpity konfigurowalne przez operatora
- CardGateway (opcjonalnie)



EntraPass - Instrukcja instalacji i obsługi programu

Wstęp

- Czytniki w technologii multi-formatowej
- Powiązanie systemów alarmów zewnętrznych
- Raportowanie wej./wyj.; możliwość raportowania na/przez e-mail
- Diagnostyka wizualna
- Integracja wideo z systemem Intellex firmy American Dynamics
- Obsługa 40 TVR II
- Obsługa 40 NVR
- Wyświetlanie strumienia live, odtwarzanie nagrań wideo, lokalne rejestrowanie zdarzeń i zapisywanie
- Archiwizacja wideo poprzez EntraPass Video Vault
- Edytor słownika
- Zintegrowane systemy alarmowe
- Obsługa Windows 7 Pro 64-bit

Czym jest Kontrola Dostępu?

Kontrola dostępu składa się z wielu elementów, m.in.: czytników, detektorów wyjścia, czujników ruchu, etc.; które są profesjonalnie zainstalowane w obrębie kontrolowanego przejścia i sterowane z kontrolera dostępu. Stacje systemowe służą m.in. do odbierania zdarzeń, potwierdzanie alarmów czy modyfikowania bazy danych systemu. Zaletą kontroli dostępu jest to, że wszystkie zdarzenia systemowe są starannie archiwizowane i z łatwością mogą zostać pobrane do celów kontrolnych.

Główne funkcje EntraPass

Kantech Advantage Program (KAP) – Program Korzyści Kantech

KAP zapewnia 12 miesięcy dostępu do darmowych aktualizacji oraz do szkoleń online dla użytkowników końcowych. Aby dowiedzieć się więcej, sprawdź Aplikacji Zgłoszeniowej Nowego Opcjonalnego Programu Korzyści Kantech (New Optional Kantech Advantage Program), DN1874.



SmartLink

EntraPass - Instrukcja instalacji i obsługi programu

Wstęp

EntraPass umożliwia połączenie wspólnym interfejsem najbardziej zaawansowanych urządzeń, takich jak: multipleksery CCTV, alfanumeryczne systemy przywoławcze, automatyczne e-maile, systemy HVAC, panele LCD czy krosownice wideo; za pomocą połączenia RS-232 lub sieci, pomiędzy jednym ze stanowisk EntraPass SmartLink, a zdalnymi stacjami sieciowymi EntraPass WebStations. Zaawansowana integracja systemu może zostać przeprowadzona za pomocą dwukierunkowego połączenia SmartLink, wykorzystanego do komunikacji z aplikacjami takimi jak: systemy wej./wyj., systemy identyfikowania, systemy zarządzania zasobami ludzkimi czy systemy rejestracji studentów; poprzez TCP/IP, port RS-232 lub DLL. Pozwala to na pełną i wykonaną w czasie rzeczywistym wymianę danych pomiędzy systemami, eliminując zbędne wprowadzanie danych.

Lustrzana baza danych oraz serwer redundantny

Dublowanie baz danych oraz serwery redundantne zapewniają alternatywy mechanizm dublowania danych w przypadku błędów lub awarii Głównego Serwera. Dublowanie bazy danych tworzy bieżącą i rzeczywistą kopię bazy danych na serwerze redundantnym. W przypadku błędu lub awarii na serwerze głównym, serwer redundantny zostaje uruchomiony automatycznie podtrzymując tym samym wszystkie funkcje i zastosowania serwera głównego (za wyjątkiem programu Card Gateway). W momencie, kiedy serwer główny uzyska na nowo sprawność, wszystkie wpisy zostają wcielone, a cała baza danych przeniesiona na niego z serwera redundantnego.

Notatka: Card Gateway nie jest kompatybilny z 64bit serwerem windows. Należy zainstalować 32bit klienta.

Drzwi z zamkiem bezprzewodowym opcja licencjonowana

Funkcja bezprzewodowej licencji na drzwi obsługuje dodawanie bezprzewodowych drzwi do systemu EntraPass.

EntraPass wspiera dodawanie drzwi bezprzewodowych Assa Abloy. Drzwi bezprzewodowe można skonfigurować do pracy ze sterownikami Kantech KT-1 i KT-400.

Notatka: Licencje na drzwi należy zakupić dla każdego drzwi bezprzewodowych.

Kantech IP Link

EntraPass jest kompatybilny z Kantech IP Link, który zapewnia bezpieczne połączenie Ethernet, służące, jako urządzenie kontrolujące przepustowość poprzez komunikowanie się bramkami tylko wtedy, gdy jest to konieczne. Główną funkcją Kantech IP Link jest przekazywanie informacji pomiędzy kontrolerami, a bramkami.



Kontrolery KT-400 i KT-1 oraz KT-300, KT-100, KT-200

EntraPass jest kompatybilny z kontrolerami KT-100, KT-200, KT-300 oraz KT-400 i KT-1. Jest to dodatkowa zaleta w przypadku modernizacji istniejących instalacji, które wymagają większej elastyczności i ulepszanego interfejsu użytkownika. Pozwala także instalatorom na dobór kontrolera w taki sposób, aby ten jak najlepiej pasował do potrzeb i możliwości finansowych klientów.

KT-400

Kontroler KT-400 jest szyfrowanym przy pomocy Ethernet kontrolerem sterowania drzwi, który jest stosowany, jako regulator drzwi oraz jako urządzenie do komunikacji IP.

Dodatkowe moduły dla KT-400

Kontroler KT-400 umożliwia podłączenie modułów rozszerzających. *Podłączenie mieszanych modułów rozszerzających wejściowych i wyjściowych daje możliwość podłączenia do 256 dodatkowych wejść i 256 dodatkowych wyjść na kontroler.*

- KT-MOD-REL8 : Ten moduł rozszerzający jest 8-przełącznikowym modulem wykorzystywanym, jako przełącznik ogólny albo wyjście sterujące windą. Moduł obsługuje łańcuchowe połączenie, które może dodać do 32 modułów KT-MOD-REL8 (w sumie 256 przełączników zewnętrznych na kontroler KT-400).
- KT-MOD-INP16 : Ten moduł rozszerzający jest modulem wejściowy, który dodaje do 16 stref do kontrolera KT-400. Moduł obsługuje łańcuchowe łączenie, które może dodać do 15 modułów KT-MOD-INP16 (w sumie 240 wejść zewnętrznych na kontroler KT-400. Dodanie 16 pokładowych wejść do KT-400 daje w sumie 256 wejść na KT-400).
- KT-MOD-OUT16 : Moduł rozszerzający do 12 VDC 16. Może być stosowany do kontroli dostępu windy (może wymagać dodatkowego sprzętu). Moduł obsługuje łańcuchowe łączenie, które może podłączyć do 16 modułów KT-MODOUT16 (w sumie 256 wyjść zewnętrznych na KT-400).



EntraPass - Instrukcja instalacji i obsługi programu

Wstęp

Czytniki Kantech ioSmart

Czytnik kart Kantech ioSmart umożliwia użytkownikom dostęp do karty za pośrednictwem kontrolera drzwi Kantech (KT-400 i KT-1). ioSmart obsługuje transmisję numerów kart za pomocą protokołu RS-485 lub Wiegand. Utrzymane formaty obejmują standardowy format 32-bitowy, standardowy format 26-bitowy i inne zastrzeżone firmy Kantech formaty takie jak eXtended Secure Format (XSF) i Smartcard Secure Format (SSF). Aby zapewnić łatwą aktualizację ścieżka do klientów, niektóre modele obsługują zarówno technologię Smart Card, jak i bliskość Kantech technologia (ioProx).

HID Mobile Access

Integracja systemu HID Mobile Access z EntraPass umożliwia dostęp do drzwi za pomocą uwierzytelnienia w smartfonie. Rejestracja i zarządzanie poświadczeniami jest kontrolowane przez EntraPass.

Kantech Telephone Entry System (KTES)

KTES umożliwia użytkownikom nadania prawa dostępu do budynku dla gości za pośrednictwem telefonu stacjonarnego lub telefonu komórkowego. Ta linia telefoniczna może również służyć, poprzez zintegrowany modem, jako łącznik programowania lub link monitoringu. KTES został zaprojektowany, jako jednostka samodzielna, ale może również stanowić część kompletnego systemu kontroli dostępu (takich jak EntraPass lub dowolnego innego systemu kontroli dostępu). Może komunikować się z EntraPass przez bramkę do programowania i monitorowania. Instalacja KTES może także uwzględniać kontrolery Kantech (KT-100, KT-300 oraz KT-400), jak również dowolny kontroler, który obsługuje port interfejsu Wiegand. Ponadto, w celu ułatwienia procesu importowania i eksportowania np. listy najemców, została wdrożona automatyzowana procedura, która prowadzi użytkownika przez kolejne etapy operacji. Aby dowiedzieć się więcej na temat instalacji i programowania KTES sprawdź *KTES Installation Manual*, DN1769 oraz *KTES Programming Manual*, DN1770.

Ekspresowe ustawienia (Express Setup)

Program Express Setup pozwala instalatorom automatycznie zdefiniować i skonfigurować większość standardowych komponentów systemu. Oszczędza tym samym czas montażu i zapobiega błędom konfiguracji. Dzięki programowi Express Setup, system jest w pełni sprawny i gotowy do testowania sprzętu i okablowania zanim instalator wprowadzi indywidualne zmiany niezbędne do konkretnej instalacji.

Kontrola wind (Elevator Control Capability)

EntraPass umożliwia instalatorom zaprogramowania do 64 pięter dla jednej kabiny windy przy użyciu urządzeń rozszerzających, takich jak: KT-PC4216, KT-PC4204 (max. 16 pięter) z KT-300; lub takich jak: KT-MOD-OUT16, KT-MOD-INP16 lub KT-MOD-REL8 z KT-400. Ten element pozwala zarządcy obiektu ograniczyć dostęp do konkretnego piętra dla osób nieposiadających odpowiednich uprawnień/autoryzowanych kart.



Definiowanie szablonów identyfikatorów (Integrated Badging)

Opcja projektowania szablonów foto-identyfikatorów została dodana do programu EntraPass, aby umożliwić użytkownikom projektowanie i drukowanie foto-identyfikatorów. Zdjęcia użytkowników oraz ich podpisy mogą być importowane z pliku lub, korzystając z odpowiednich urządzeń (np. wbudowana kamera) przechwytywane, a następnie implementowane we właściwe pola szablonu foto-identyfikatora danej karty i drukowane.

Interaktywne Plany Pięter (Interactive Floor Plans)

EntraPass potrafi zaimportować oraz wyświetlać grafiki w wysokiej rozdzielczości stworzone w systemach CAD (przekonwertowane do formatu .jpg albo .bmp), umożliwiając tym samym projektowanie systemów opartych na grafikach, które operator może używać po minimalnym przygotowaniu. Interaktywne przyciski mogą być dodawane na plan piętra w celu zobrazowania poszczególnych komponentów, oferując jednocześnie pełne zastosowanie komponentu.

Pulpity Konfigurowalne przez operatora (Configurable Desktops by Operator)

Dzięki EntraPass do każdego Operatora można przypisać 8, w pełni konfigurowalnych, pulpitów. Te pulpity wyświetlają wybrane okna z informacjami na temat zdarzeń, zdjęcia oraz grafiki użytkownika, wyfiltrowane zdarzenia, grafiki oraz nagrania wysokiej rozdzielczości oraz instrukcje alarmów. Pulpity mogą zawierać dowolną konfigurację okien.

Powiązanie systemów alarmów zew. (Interfacing with External Alarm Panels)

Kontrolery KT-100, KT-300 oraz KT-400 pozwalają użytkownikom uzbroić, rozbroić oraz wstrzymać uzbrojenie zewnętrznego panelu alarmowym. Pozwala to na łatwą integrację EntraPass z dowolnym, zewnętrznym systemem alarmowym.

Funkcja rejestracji czasu pracy (In/Out Feature)

Zintegrowana z system EntraPass funkcjonalność RCP jest taną alternatywą dla dedykowanych, a co za tym idzie droższych, systemów rejestracji czasu pracy. Funkcja umożliwia operatorowi wydrukowanie raportów w formacie CSV lub przesłanie ich do programu kadrowego.

Diagnostyka wizualna (Visual Diagnostics)

EntraPass jest w stanie wyświetlić w czasie rzeczywistym wizualną reprezentację urządzeń systemowych wraz z aktualizowanymi w czasie rzeczywistym warunkami, w tym wysokiej rozdzielczości plany pięter, które mogą być importowane i wyświetlane na ekranie. Interaktywne przyciski systemowe mogą być dodawane do grafik, aby wyświetlać status komponentu w czasie rzeczywistym. Dzięki temu wszelkie działania mogą być wykonywane z poziomu grafiki systemu w czasie rzeczywistym.



Rozszerzona integracja wideo (Enhanced Video Integration)

W odpowiedzi na rosnące znaczenie nagrań wideo w systemach kontroli dostępu, EntraPass dodaje możliwość monitorowania w czasie rzeczywistym. Integracja z systemem zarządzania Intellex firmy American Dynamics zapewnia monitoring wideo w czasie rzeczywistym oraz odtwarzanie wideo, poprzez Intellex Application Programming Interface (API). Obraz może być powiązany z monitoringiem wideo w czasie rzeczywistym, jak i odtwarzaniem nagrań wideo. Obraz może być powiązany ze odnotowanymi zdarzeniami i rejestrowany z szesnastu kamer z różnych jednostek Intellex jednocześnie. Presety, sekwencje, sterowania głowicą oraz widoki w siatce 1x1, 2x2, 3x3 czy 4x4 są dostępne za pośrednictwem oprogramowania EntraPass. Wszystkie kamery mogą być wywoływane bezpośrednio z planu piętra poprzez dwukrotne kliknięcie na przycisk aparatu. Operatorzy mogą konfigurować parametry wyświetlania za pośrednictwem interfejsu użytkownika EntraPass.

EntraPass Video Vault

EntraPass Video Vault umożliwia automatycznie zapisywanie wszystkich nagrań alarmowych od Intellex lub EntraPass w formacie Audio Video Interlaced (.AVI), Kantech Video Intellex (.KVI), Kantech Video Archive (.KVA) oraz American Dynamics

Network Client's Video (.IMG). Wszystkie mogą być chronione hasłem. Każdy EntraPass Video Vault może być połączony z tak wieloma jednostkami Intellex, jak to jest zdefiniowane w oprogramowaniu EntraPass. Nagrania wideo mogą być zapisywane w 24 różnych, zdefiniowanych wcześniej, lokalizacjach zapisu. Obraz .bmp może zostać przypisany do każdego pliku wideo, a miniatura może zostać utworzona na pierwszej klatce nagrania.

Edytor słownika (Vocabulary Editor)

Nieskomplikowany i łatwy w użyciu program służący do przetłumaczenia oprogramowania na wybrany język. Domyślnie EntraPass jest dostępny w następujących językach: angielskim, francuskim, hiszpańskim, niemieckim oraz włoskim. Może zostać przetłumaczony na 99 języków przy wykorzystaniu tej funkcji.

Zintegrowane systemy alarmowe (Intrusion Integration)

Pełny dostęp do Panelu Wirtualnej Klawiatury dołączonej do KT-400 jest obecnie dostępny. Funkcja autodetekcji została dodana, aby umożliwić pobieranie danych bezpośrednio z panelu w celu optymalizacji procesu obsługi administracyjnej. Nowy typ parametru dla zdarzeń został dodany do obsługi większości zdarzeń związanych z włamaniami.



EntraPass - Instrukcja instalacji i obsługi programu

Wstęp

Pomoc techniczna

Jeżeli poniższa instrukcja nie dostarcza odpowiedzi na którekolwiek pytania, ani nie możesz znaleźć informacji w plikach Pomocy, sugerujemy abyś skontaktował się z instalatorem systemu. Twój instalator posiada wiedzę na temat twojego systemu i powinien być w stanie udzielić ci wszystkich niezbędnych odpowiedzi. Jeżeli będziesz potrzebować jednak dodatkowej informacji prosimy skontaktować się z działem Wsparcia Technicznego dla twojego regionu.

North America Toll Free +888 222 1560 (GMT -05:00)

US and Canada: +450 444 2030, Fax: +450 444 2029 | 8:00 to 20:00 | kantechsupport@tycoint.com

Latin America (GMT -03:00)

Argentina: +5411 4711 8711, Fax: +5411 4711 8201 | 9:00 to 18:00 | ingenieria@tycoint.com

Asia (GMT +08:00)

Asia Pacific: | 8:30 to 18:00 | apac.support@tycoint.com

Europe Toll Free +800 CALL TYCO / +800 2255 8926 (GMT +01:00)

Wprowadzenie

EntraPass – wsparcie techniczne

Bahrain +800 04127	8:00 to 18:00	emea.support@tycoint.com
France +33 04 72 79 14 83	8:00 to 18:00	emea.support@tycoint.com
Greece +00 800 31 22 94 53	8:00 to 18:00	emea.support@tycoint.com
Russia +8 10 800 2052 1031	8:00 to 18:00	emea.support@tycoint.com
Spain +900 10 19 45	8:00 to 18:00	emea.support@tycoint.com
Turkey +00 800 31 92 30 07	8:00 to 18:00	emea.support@tycoint.com
United Arab Emirates +800 0 31 0 7123	8:00 to 18:00	emea.support@tycoint.com
United Kingdom: +31 475 352 722	8:00 to 18:00	emea.support@tycoint.com



EntraPass - Instrukcja instalacji i obsługi programu

Wstęp



EntraPass - Instrukcja instalacji i obsługi programu

Wstęp



Instalacja

Minimalne wymagania systemowe

Obsługiwane systemy operacyjne

- Windows Server 2008 Standard/Enterprise
- Windows Server 2012 Datacenter X64
- Windows Server 2016 Standard and Windows Server 2016 Datacenter

Notatka: Aplikacja dostępu do bazy danych nie jest obsługiwana w systemie Windows Server 2016, dla której zaplanowano poprawkę następną wersją EntraPass.

- Windows Server 2019 Datacenter X64
- Windows 7 Pro / Enterprise / Ultimate (32 oraz 64-bit)
- Windows 8.1 Enterprise x86 / Windows 8.1 Enterprise x64
- Windows 10 Enterprise x86/Windows 10 Enterprise x64

Notatka: Wszystkie systemy operacyjne powinny mieć zainstalowane bieżące aktualizacje oraz bieżące Service Pack.

Upewnij się, że komputer, na którym instalujesz oprogramowanie spełnia poniższe wymagania minimalne:

- Procesor Dual Core
- 4GB RAM
- Karta graficzna AGP albo PCI Express 8X z 64 MB oraz wsparciem DirectX 9.0
- Karta sieciowa 10/100 Base-T EntraPass

Serwer Web

- Procesor Pentium IV 1.8GHz
- Min. miejsce na dysku: 10 GB
- 1 GB RAM
- Microsoft Internet Information Services (IIS) 5.1 lub nowsza z bieżącymi aktualizacjami
- Microsoft.NET Framework 2.0 z bieżącymi aktualizacjami
- Adobe Flash Player 9.0 musi być zainstalowany na komputerze.

Wsparcie Virtual Environment

- VMware Workstation Version 7 lub nowsza

Dodatkowe wymagania



EntraPass - Instrukcja instalacji i obsługi programu Instalacja

Dla niektórych aplikacji można używać następujących urządzeń:

- Karta graficzna – do zachowania obrazów użytkownika
- Karta dźwiękowa – dla dźwięków alarmowych w przypadku alarmu
- Drukarka Identyfiaktów – do drukowania identyfikatorów
- Urządzenie do zapisywania podpisów – do zachowywania podpisów (Identyfikowanie)
- Drukarka logów – do drukowania zdarzeń (wiadomości i alarmy)
- Drukarka raportów – do drukowania raportów

Jak zwiększyć bezpieczeństwo? Poradnik

Przewodnik zwiększenia poziomu zabezpieczeń Kantech zaleca następujące działania instalacyjne, konfiguracyjne i instalacyjne, aby zapewnić najwyższy poziom bezpieczeństwa EntraPass. Niezastosowanie się do poniższej konfiguracji zabezpieczeń może skutkować osłabionym stanem operacyjnym z lukami w zabezpieczeniach. Aby uzyskać więcej informacji, zobacz swój produkt instrukcja instalacji dla konkretnych instrukcji. Aby spełnić zalecane standardy bezpieczeństwa, wypełnij następujące kroki:

1 - Wdrożenie EntraPass w wyseparowanej wirtualnej sieci lokalnej (VLAN).

2 - Aby zaszyfrować warstwę bezpieczeństwa podczas przesyłania danych, użyj protokołu Hypertext Transfer Protocol Secure (HTTPS) zamiast HTTP. Musisz uzyskać certyfikat Secure Socket Layer (SSL) od urzędu certyfikacji (CA), i wygeneruj go na stronie internetowej EntraPass. Zobacz, jak zaimplementować SSL w IIS (Internet Usługi informacyjne) na stronie internetowej Microsoft.

<https://support.microsoft.com/enz/help/299875/how-to-implement-ssl-in-iis>

UWAGA: Ten link jest tylko w celach informacyjnych, skontaktuj się z firmą Microsoft w celu uzyskania pomocy dotyczącej implementacji protokołu SSL.

3 - Zmień domyślne hasła podczas instalacji.



Instalacja systemu

Notatka: po zakończeniu instalacji EntraPass zwykły użytkownik nie może uruchomić oprogramowania bez zmodyfikowania pozwolenia dostępu do folderów. Aby rozwiązać ten problem użytkownik musi otrzymać uprawnienia administratora:

- dla systemów 64-bit:

- Foldery: C:\Program files(x86)\Advantage 10.10 oraz C:\Program files(x86)\Kantech.

- Rejestr danych:

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Kantech

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Advantage Data Architect.

- dla systemów 32-bit:

o Foldery: C:\Program files(x86)\Advantage 10.10 oraz C:\Program files(x86)\Kantech.

o Rejestr danych:

- HKEY_LOCAL_MACHINE\SOFTWARE\Kantech

- HKEY_LOCAL_MACHINE\SOFTWARE\Advantage Data Architect.

1 – Zanim rozpoczniesz instalację upewnij się, że żadna aplikacja EntraPass nie jest uruchomiona.

2 – Umieść dysk CD w napędzie (albo pamięć USB w porcie). Instalacja powinna rozpocząć się automatycznie, jeżeli komputer ma ustawioną funkcję autorun. Jeżeli instalacja nie rozpocznie się automatycznie z poziomu systemu operacyjnego wybierz Uruchom (Start > Uruchom), wpisz D:/Setup.exe (gdzie D: określa napęd CD-ROM).

3 – Zanim instalacja przejdzie dalej zostaniesz poproszony o wybór języka. Angielski jest językiem domyślnym.

Notatka: język ustawiony w trakcie instalacji (InstallShield) nie może zostać zmieniony później, kiedy użytkownik chce zainstalować aktualizację EntraPass albo zainstalować komponent w innym języku. Jeżeli istnieje potrzeba zmienienia języka ustawionego w trakcie instalacji należy usunąć oraz przeinstalować oprogramowanie.

Notatka: język systemowy oraz język bazy danych zależy od języka, który został wybrany w trakcie instalacji oprogramowania. Na przykład, jeżeli został wybrany „English”, to właśnie angielski będzie językiem domyślnym przy uruchomieniu. Język systemowy oraz język bazy danych może zostać zmieniony z Serwera EntraPass oraz Stacji roboczej EntraPass.



EntraPass - Instrukcja instalacji i obsługi programu Instalacja

4 – Kliknij OK. Zostanie wyświetlony ekran startowy.

- Wszystkie okna instalacji wyglądają tak samo, jak okno startowe
- Wersja oprogramowania, które instalujesz, znajduje się w lewym górnym rogu
- Środkowa część ekranu zawiera instrukcje, których należy przestrzegać w trakcie całego procesu instalacji. Instrukcje opisujące kolejne etapy instalacji będą wyświetlane po kliknięciu przycisku Następne (Next).
- Przyciski Wstecz (Back) oraz Następny (Next) znajdują się na dole ekranu i umożliwiają nawigację pomiędzy ekranami instalacji oraz zapewniają możliwość zmiany ustalonych wcześniej parametrów.
- Możesz Anulować (Cancel) instalację dowolnym momencie.

5 – Kliknij Następny (Next), aby kontynuować instalację. Zostanie wyświetlone okno Ustawienia Start (Setup Start).

6 – Wybierz działanie / działania, które chcesz przeprowadzić. Pierwsza grupa opcji jest dla nowych instalacji, ostatnia opcja dla uaktualnień. W trakcie pierwszej instalacji będziesz miał możliwość wybrać tylko jedną opcję instalacji. Sugerujemy, abyś zainstalował pierwszą opcję z listy.

- **Zainstaluj Serwer, Bazę Danych oraz Stację roboczą (Install Server, Database and Workstation):** ta opcja zainstaluje EntraPass Corporate Edition. Ta opcja będzie wyszarzona, jeżeli aplikacja jest już zainstalowana na komputerze.
- **Zainstaluje dodatkową Stację roboczą (Install Additional Workstation):** ta opcja powinna zostać wybrana, jeżeli chcesz zainstalować dodatkową stację roboczą. Ta opcja będzie wyszarzona, jeżeli serwer albo stacja robocza są już zainstalowane na komputerze.
- **Zainstaluje komponenty EntraPass System (Install EntraPass System Components):** ta opcja umożliwia zainstalowanie opcjonalnych lub dodatkowych komponentów EntraPass, takich jak: bramki, stacje sieciowe, SmartLink, Video Vault, interfejs Oracle/MS-SQL, etc. Ta opcja będzie wyszarzona, jeżeli dany komponent jest już zainstalowany na komputerze.

Notatka: bramka redundantna jest instalowana przy wykorzystaniu opcji Bramki. Numer seryjny wykorzystany przy rejestracji zaznaczy ją, jako bramkę redundantną.

- **Zainstaluje Narzędzia Systemowe EntraPass (Install EntraPass System Tools):** ta opcja pozwala zainstalować Narzędzia systemowe EntraPass. Ta opcja będzie wyszarzona, jeżeli dane narzędzie jest już zainstalowane na komputerze.



EntraPass - Instrukcja instalacji i obsługi programu Instalacja

- **Aktualizuje Zainstalowaną Aplikację (Update Installed Applications):** ta opcja będzie wyszarzona, jeżeli system nie jest jeszcze zainstalowany na komputerze. Aby zaktualizować EntraPass, zobacz Aktualizacja EntraPass.

7 – Kliknij Następny (Next). Zostanie wyświetlone okno na Numer Seryjny.

8 – Wprowadź numer seryjny dla EntraPass Corporate Server albo dla oprogramowania. Numer seryjny znajduje się na opakowaniu płyty. Upewnij się, że wprowadziłeś prawidłowy numer. Przycisk Następny (Next) jest aktywny tylko w przypadku wprowadzania prawidłowego numeru seryjnego.

9 – Kliknij Następny (Next). Zostanie wyświetlona Licencja Użytkownika oprogramowania.

10 – Wybierz Akceptuję (I accept), jeżeli rozumiesz i akceptujesz warunki opisane w licencji, albo Nie akceptuję (I do not accept), jeżeli chcesz przerwać instalację.

Notatka: Nie będziesz w stanie ukończyć instalacji, jeśli nie potwierdzisz warunków umowy licencyjnej. Przycisk Następny (Next) stanie się aktywny w momencie kliknięcia Akceptuję (I accept).

11 – Kliknij Następny (Next). Okno Informacje o Kliencie (**The Customer Information**) zostanie wyświetlone.

12 – Wprowadź Nazwę Użytkownika (User Name) oraz Nazwę Firmy (Company Name)

13 – Wybierz rodzaj użytkownika: Każdy, kto będzie korzystać z tego komputera albo Wyłącznie osoba zalogowane i zarejestrowana w systemie.

14 – Kliknij Następny (Next). Zostanie wyświetlono okno Wybierz Lokalizację Docelową (**Choose Destination Location**).

15 – Możesz zostawić docelową lokalizację i kliknąć Następny (Next), albo wybrać inną.

- Jeśli chcesz zmienić folder, w którym aplikacja ma zostać zainstalowana, kliknij Zmień (Change). Zostanie wyświetlone okno Wybierz Folder (**Choose folder**), w którym możesz wybrać nowy adres instalacji.

- Wprowadź adres folderu, w którym chcesz zainstalować EntraPass albo rozwiń i wybierz adres instalacji. Następnie wciśnij OK. Adres nowego folderu zostanie wyświetlony w oknie Wybierz Lokalizację Docelową (**Choose Destination Location**)

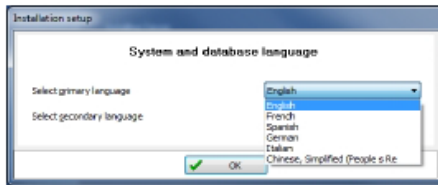
16 – Kliknij Następny (Next). Zostanie wyświetlone okno Gotowy do instalacji Programu (**Ready to Install the Program**).

17 – Jeśli potrzebujesz sprawdzić lub zmienić wprowadzone parametry, kliknij Wstecz (Back). Jeśli wszystko jest gotowe do instalacji, kliknij Następny (Next). Instalacja się rozpocznie.



EntraPass - Instrukcja instalacji i obsługi programu Instalacja

18 – Podczas instalacji zostaniesz poproszony o wybór głównego i drugiego języka. Ten wybór zdefiniuje język do zbudowania bazy danych oraz język do używania EntraPass.



19 – Kliknij OK, instalacja będzie kontynuowana.

20 – W trakcie instalacji pojawi się możliwość zainstalowania Intellex API:

- Jeśli Intellex API jest wymagany, kliknij Tak (Yes) i postępuj według instrukcji.

21 – Możesz również zainstalować aplikację, jako usługę Windows. Aplikacje działające, jako usługi Windows zostaną automatycznie zrestartowane po zamknięciu systemu (nawet przypadkowym).

22 – Na tym etapie możesz wybrać restart komputera, albo zdecydować się na niego później.

23 – Usuń dysk CD z napędu CD-ROM (albo pamięć USB z portu).

24 – Kliknij Zakończ (Finish) aby zakończyć instalację.

Notatka: po instalacji należy zrestartować komputer.

25 – Następnym krokiem jest skontaktowanie się z Działem Wsparcia Technicznego Kantech w celu uzyskania numeru aktywacji dodatkowych komponentów system. Więcej informacji w kolejnym punkcie instrukcji.

Rejestracja Systemu

Zalecany jest, aby jak najszybciej zarejestrować system. Dzięki temu użytkownicy będą mogli zainstalować dodatkowe opcje oraz będą mieli dostęp do systemu bez żadnych ograniczeń. Chociaż system jest funkcjonalny nawet przed jego rejestracją, jest ograniczony do wyłącznie 10 kart.

Ponadto, w przypadku, gdy system nie jest zarejestrowany, operatorzy są wylogowywani po każdej godzinie pracy; następnie muszą wprowadzić losowo generowany, 20 znakowy kod.

Rejestrowanie systemu (Registering the System)

1 – Kliknij przycisk Serwer (Server) na pulpicie komputera. Możesz również uruchomić EntraPass Server z menu startowego Windows (Start > EntraPass Corporate Edition > Server > Server)

2 – Kliknij Login / Logout, aby się zalogować / wylogować. Zostanie wyświetlone okno logowania.



EntraPass - Instrukcja instalacji i obsługi programu Instalacja

Unregistered system, Please use the following temporary password: **NWFHCLNKTSZEUAANGR**

System niezarejestrowany, użyj hasła tymczasowego: **NWFHCLNKTSZEUAANGR**

3 – W pole Nazwa użytkownika (User name) wpisz Kantech. Wprowadź czasowe, 20 literowe hasło wyświetlone na dole okna Login Operatora (Operator login). Hasło czasowe pojawia się tylko w trakcie nowych instalacji i jest podświetlone na żółto. Zostanie wyświetlone okno rejestracji.

System registration

System serial number

Temporary password in use - Click here to register

System Components - Features Options serial numbers Installation dates

System option 3/11/2011 9:20:35 AM

Components	Installation codes	First time connected
(2) Workstation	XXXX-XXXX-XXXX-XXXX	
(3) Workstation	XXXX-XXXX-XXXX-XXXX	
Corporate Gateway	XXXX-XXXX-XXXX-XXXX	
SmartLink	XXXX-XXXX-XXXX-XXXX	

Activate Edit Print Express Setup Close Help

Rejestracja w systemie

Numer serwera systemu

Kliknij, aby zarejestrować system

Elementy systemu - opis	Numer serwera opcji	Data zarejestrowania
Wszystkie elementy		
Opis systemu		11.10.2016 21:17:31
EntraPass Web (1)		11.10.2016 21:17:34

Elementy	Kod instalacji	Pierwsze połączenie
(2) Workstation		29.11.2016 11:59:51
(3) Workstation		29.11.2016 12:01:59
Multi-Site Gateway		
SmartLink		

Wyświetl informacje dot. KAP Włacz Edycja Drukuj Konfig. automat. Zakończ Pomoc

4 – Kliknij żółty przycisk Czasowe hasło w użyciu (Temporary password in use), aby zarejestrować system. Przycisk jest widoczny tylko przy nowych instalacjach.

Zostanie wyświetlone okno Rejestracji Systemu.

Notatka: istnieją dwie metody rejestracji nowego systemu; zarejestruj online na stronie www.kantech.com albo skontaktuj się ze swoim lokalnym wsparciem technicznym, aby otrzymać kod potwierdzający rejestrację.

5 – Idź na stronę www.kantech.com i zaloguj się do Strefy Użytkowników (Member Center).



EntraPass - Instrukcja instalacji i obsługi programu Instalacja

Notatka: jeżeli jeszcze nie jesteś członkiem, wyślij zgłoszenia, a potwierdzenie członkostwa powinno zostać wysłane na skrzynkę mailową w przeciągu 1-2 dni roboczych.

6 – Kliknij na Rejestracja Kantech (Kantech Registration).

7 – Wprowadź Systemowy Numer Seryjny (System Serial Number) i postępuj według instrukcji online.

8 – Wróć do Rejestracji Systemu EntraPass (**EntraPass System Registration**) i wprowadź Kod Zawierający Rejestrację (Registration Confirmation Code), następnie kliknij OK. Przycisk OK można kliknąć tylko wtedy, gdy kod jest prawidłowy.

Notatka: jeżeli opuścisz główne okno Serwera bez zarejestrowania systemu, zostanie wyświetlone okno Zmień hasło potwierdzenia (Change Authentication Password). Okno to nie jest wyświetlane po zarejestrowaniu systemu.

Dodawanie składników programu (Adding System Components)

Kiedy serwer jest już zarejestrowany można rozpocząć instalację dodatkowych komponentów systemu. Dodatkowe komponenty systemu obejmują również aplikacje EntraPass m.in. EntraPass Video Vault. Zanim zainstalujesz dodatkowe komponenty systemowe upewnij się, że twój komputer spełnia minimalne wymagania. W celu zainstalowania dwóch pierwszych aplikacji na stacji i pierwszej aplikacji na bramce nie trzeba się kontaktować z Działem Wsparcia Technicznego firmy Kantech – te elementy są częścią pakietu instalacyjnego.

Notatka: EntraPass Special Edition wspiera jedną Bramkę oraz jedną stację roboczą. Dodatkowe Bramki oraz Stacje nie mogą zostać dodane.

1 – W głównym oknie Serwera kliknij w pasek narzędzi Połączenie (Connection), ewentualnie z poziomu aplikacji Stacji w pasek narzędzi Opcje (Options), a następnie kliknij w Rejestracja Systemu (System Registration). Wyświetli się okno rejestracji systemu.

Notatka: serwer EntraPass jest sprzedawany z trzema aplikacjami stacji roboczej oraz jedną aplikacją bramki multi-site. Jedna stacja robocza jest automatycznie instalowana w trakcie instalowania serwera. Jest wykorzystywana w celach konfiguracyjnych. Nie jest wyświetlana w dolnym panelu, ponieważ jest automatycznie instalowana i rejestrowana. Wykorzystaj CD oraz kody instalacyjne, aby zainstalować dodatkowe aplikacje stacji roboczych. Upewnij się, że komputer, na którym mają być instalowane spełnia wymagania minimalne.

2 – Kliknij w przycisk Drukuj (Print) aby wydrukować kody Instalacji, abyś zawsze miał kody przy sobie w przypadku instalowania stacji lub bramek. Aby uniknąć błędów nie kopiuj, ani nie przepisyj raz wydrukowanej kartki.

Notatka: jeżeli zainstalujesz opcję zaawansowaną (np. dodatkową bramkę), możesz konfigurować jej ustawienia przy pomocy programu Express Setup.



EntraPass - Instrukcja instalacji i obsługi programu Instalacja

3 – Z okna Rejestracja systemu wybierz komponent, który chcesz zainstalować. Następnie kliknij przycisk Naciśnij tutaj, aby zainstalować komponent (Click here to install component). Wyświetli się okno Rejestracji komponentu (Nazwa komponentu).

4 – Wprowadź Numer Seryjny (Option Serial Number), zlokalizowany na Certyfikacie (Option Certificate).

Notatka: istnieją dwie metody rejestracji nowego systemu; zarejestruj online na stronie www.kantech.com albo skontaktuj się ze swoim lokalnym wsparciem technicznym, aby otrzymać kod potwierdzający rejestrację.

5 – Idź na stronę www.kantech.com i zaloguj się do Strefy Użytkowników (Member Center).

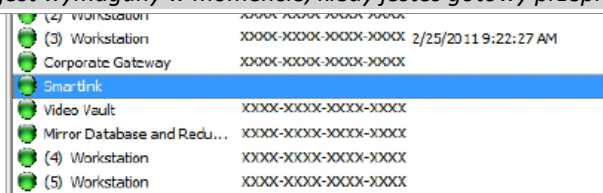
Notatka: jeżeli jeszcze nie jesteś członkiem, wyślij zgłoszenia, a potwierdzenie członkostwa powinno zostać wysłane na skrzynkę mailową w przeciągu 1-2 dni roboczych.

6 – Kliknij na Rejestracja Kantech (Kantech Registration).

7 – Wprowadź Systemowy Numer Seryjny (System Serial Number) i postępuj według instrukcji online.

8 – Wróć do okna Rejestracja komponentu EntraPass (EntraPass Component Registration), wprowadź Kod uwierzytelniający rejestrację (Registration Confirmation Code) i kliknij OK. Przycisk OK można kliknąć tylko wtedy, gdy oba kody są prawidłowe.

Notatka: po wprowadzeniu kodu uwierzytelniającego system generuje Kod instalacji na ekranie Rejestracji systemu. Niebieskie flagi (oznaczenia) identyfikują komponenty, które zostały utworzone, ale jeszcze nieaktywowane. Zielone flagi (oznaczenie) wskazują komponenty, które zostały aktywowane. Kod instalacyjny jest wymagany w momencie, kiedy jesteś gotowy przeprowadzić instalację z CD.



(2) Workstation	XXXX-XXXX-XXXX-XXXX
(3) Workstation	XXXX-XXXX-XXXX-XXXX 2/25/2011 9:22:27 AM
Corporate Gateway	XXXX-XXXX-XXXX-XXXX
SmartLink	
Video Vault	XXXX-XXXX-XXXX-XXXX
Mirror Database and Redu...	XXXX-XXXX-XXXX-XXXX
(4) Workstation	XXXX-XXXX-XXXX-XXXX
(5) Workstation	XXXX-XXXX-XXXX-XXXX

9 – Powtórz kroki od 3 do 8 dla każdego nowego komponentu systemu.

Notatka: musisz ustawić połączenie pomiędzy serwerem EntraPass a komputerem, na którym instalowane są nowe komponenty/opcje. Wykonaj ten krok wyłącznie wtedy, kiedy instalujesz komponent/opcję na komputerze, innym niż ten, na którym zainstalowana jest aplikacja EntraPass stacja robocza.



EntraPass - Instrukcja instalacji i obsługi programu Instalacja



EntraPass - Instrukcja instalacji i obsługi programu Instalacja



EntraPass - Instrukcja instalacji i obsługi programu Instalacja

Usługi Windows (Windows Services)

Składnik Active Directory jest instalowany automatycznie, jako usługa systemu Windows, gdy jest włączony. Na pasku systemowym Windows zostaną wyświetlone następujące ikony.

	Usługa nie została uruchomiona
	Usługa została uruchomiona, ale wystąpił błąd.
	Usługa działa
	Trwa synchronizacja

Po kliknięciu prawym przyciskiem na ikonę zostaną wyświetlone następujące opcje:

- **Start:** uruchamia usługę.
- **Stop:** zatrzymuje usługę.
- **Restart:** zatrzymuje, a następnie zrestartuje usługę.
- **Synchronizuj teraz:** wymusza natychmiastowe wprowadzenie zmian.
- **Sprawdź LOG:** otwiera folder, w którym zapisany jest plik log.txt.

Podmenu Informacje o (About) wyświetla ogólne informacje na temat aplikacji, takie jak: wersja, dane kontaktowe wsparcia technicznego, prawa autorskie.

Edycja składników programu

EntraPass umożliwia użytkownikowi przypisywanie dowolnych nazw do aplikacji dla łatwej identyfikacji wśród zdarzeń systemowych. Można również zmieniać nazwę komponentów w ich menu (Urządzenia > Aplikacje EntraPass).



EntraPass - Instrukcja instalacji i obsługi programu Instalacja

Przypisywanie nazwy opisowej do aplikacji

1 – Z okna Rejestracji wybierz aplikację, a następnie kliknij na przycisk Edytuj (Edit). Wyświetli się okno Edycji komponentu.

2 – Wprowadź opisową nazwę wybranej aplikacji EntraPass w polu Opis (Description). Zaleca się, aby wprowadzić dwie nazwy, jedną w języku głównym oraz drugą w dodatkowym języku, jeśli EntraPass działa w dwóch językach.

3 – Zaznacz jedną albo więcej opcji:

- Stacja robocza zablokowana (Workstation locked): zaznacz tę opcję, jeśli ta aplikacja zostanie zainstalowana na komputerze i będzie wykorzystywana tylko do odbierania zdarzeń systemowych.
- Zamknięty do uwierzytelniania (Locked for authentication): zaznacz tę opcję, jeśli chcesz, aby komputer, na którym zainstalowano aplikację EntraPass nie wysyłał swoich danych uwierzytelniających do serwera.
- Użyj konkretnego hasła do autoryzacji (Use specific password for authentication): zaznacz tę opcję, jeśli chcesz przypisać indywidualne hasło dla tej stacji roboczej. W przypadku wybrania tej opcji, wprowadź hasło w polu Hasło uwierzytelniania (Authentication password).

Notatka: pole Typ aplikacji wyświetla typ wybranej aplikacji EntraPass. Na przykład, wyświetli „Bramka multi-site”, jeżeli wybraną aplikacją jest Bramka multi-site. Identyfikacja jest również wyświetlona w oknie definiowania aplikacji EntraPass (Urządzenia > Definiowanie aplikacji EntraPass).



EntraPass - Instrukcja instalacji i obsługi programu Instalacja



Rozpoczęcie pracy z programem

Funkcje podstawowe

Poniżej znajdują się podstawowe funkcje systemu:

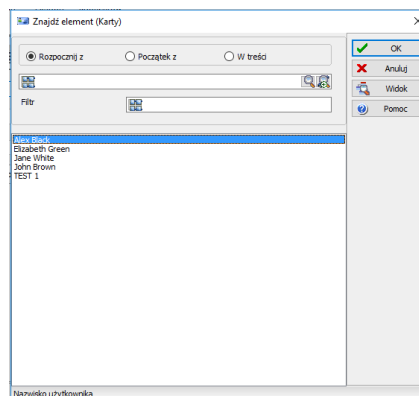
- Znajdź komponenty
- Użyj rozszerzonego pola wyboru
- Wybierz komponent, katalog, połączenie lub bramkę
- Wydrukuj listę lub raporty
- Zobacz powiązania pomiędzy komponentami
- Wywołaj widok drzewa systemu

Znajdź komponent (Finding Components)

Funkcja Znajdź component pozwala operatorowi znaleźć konkretny element albo komponent w bazie danych systemu przy użyciu odpowiednich komend.

Istnieją dwa rodzaje dialogu Znajdź komponent: dostęp do pierwszego można uzyskać z każdego paska narzędzi okna EntraPass. Dostęp do drugiego jest zapewniony przez działanie użytkownika (karty, karty gości, przepustki).

1 – W obu przypadkach musisz kliknąć na ikonę lornetki na pasku narzędzi, aby otworzyć Znajdź komponent.



- Okno po lewej jest wykorzystywane do znajdowania komponentów, a okno po prawej do znajdowania kart.

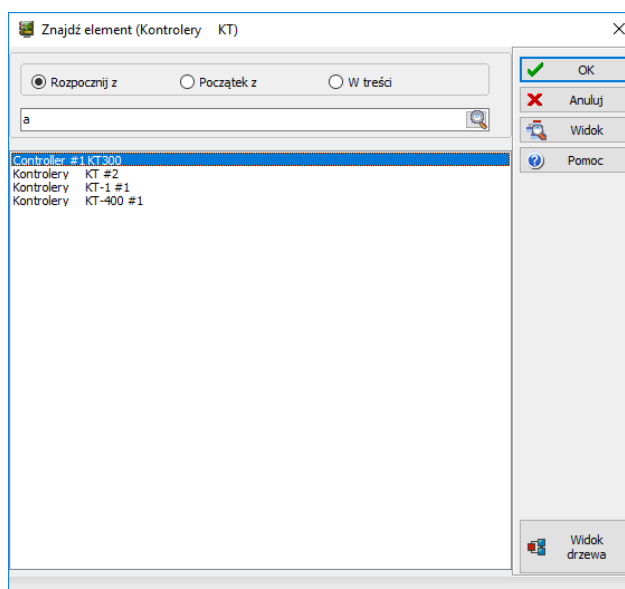


EntraPass - Instrukcja instalacji i obsługi programu Rozpoczęcie pracy z programem

-  Wyszuka w bazie danych komponent albo kartę
-  Przeszuka bazę danych pod kątem obrazu, który odpowiada karcie wybranej na liście.
-  Otworzy się menu, w którym wybierzesz, według jakiego indeksu karty chcesz wyszukiwać (numer karty, imię i nazwisko posiadacza karty, etc.).

2 – Aby rozpocząć wyszukiwanie wprowadź słowo klucz i kliknij ikonę lornetki po prawej. Aby ograniczyć liczbę rezultatów, odznacz jedno z pól:

- Rozpocznij od (Start with): wyświetlone zostaną wszystkie komponenty, które zaczynają się od wprowadzonego słowa klucza, w kolejności alfabetycznej; wyświetlone zostaną również pozostałe komponenty bazy danych.
- Zaczyna się od (Begins with): wyświetlone zostaną wyłącznie komponenty zaczynające od słowa klucza.
- Zawiera (Contains): wyświetlone zostaną wszystkie komponenty, które zawierają słowo klucz.



3 – Jeśli chcesz zobaczyć obraz korespondujący z wybraną z listy kartą, kliknij ikonę lornetki ze znacznikiem plus.

4 – Aby anulować proces wyszukiwania, kliknij przycisk Anuluj (Cancel)

5 – Kliknij OK. Zaznaczone komponenty na liście zostaną wyświetlone w oknie, w którym poszukiwanie zostało rozpoczęte.



Używanie Pola Rozszerzonego Wyboru (Extended Selection Box)

Pole rozszerzone wybory pozwala na podgląd wszystkich komponentów rozwijanej listy przez kliknięcie prawym przyciskiem na listę. Ta opcja jest odblokowana, jeżeli taka lista istnieje dla komponentów takich jak: aplikacje, kontrolery i drzwi. Jeżeli opcja jest odblokowana informacja na ten temat pojawia się w momencie najechania kursorem na rozwijaną listę.

- Filtry dostępne w rozszerzonym polu wyboru:

- Zawiera (Contains)
- Zaczyna się na (Starts with)
- Kończy się na (Ends with)
- Zawiera dokładnie (Exact words)
- Wybrane (Selected)

- Możesz również wprowadzić konkretne słowa w polu Filtr tekstu (Text filter), aby zlokalizować konkretny obiekt.

- Możesz również ustawić liczbę kolumn, w których mają zostać wyświetlone wyniki wyszukiwania.

Wybierania komponentów

Funkcja wybierania komponentów pozwala operatorowi na wybranie jednego, lub większej ilości komponentów. Metoda wyboru może zależeć od kontekstu wyszukiwania.

1 – Z aktywnego okna kliknij przycisk Wybierz Komponenty (Select Components). Zostanie otwarte okno pomocnicze, w którym można wybrać odpowiednie opcje.

2 – Możesz być zmuszony do zaznaczenia opcji, które są wyświetlone pojedynczo, albo skorzystać z przycisku Zaznacz wszystko (Select All), aby zaznaczyć wszystkie opcje. Możesz również wybrać komponenty, które nie są pogrupowane – Pojedyncze do poglądu (Single to view), albo wybrać Grupa (Group), aby wybrać istniejącą grupę.

3 – Z listy wybierz component/grupę, które chcesz wyświetlić.

4 – Jeżeli możliwe, korzystaj z przycisku Zaznacz wszystko (Select all), albo Odznacz wszystko (Clear all), aby usunąć wszystkie zaznaczenia.



EntraPass - Instrukcja instalacji i obsługi programu Rozpoczęcie pracy z programem

5 – Ustaw wymaganą licznę kolumnę w oknie Rozszerzonego Pola Wyboru, aby wyświetlić wszystkie komponenty. Filtr tekstu (Text filter) może zostać wykorzystany, aby zawęzić listę.

6 – Kliknij OK, aby zatwierdzić wybór i wrócić do poprzedniego okna.

Wybieranie konkretnego katalogu (Specific Folder)

Aby znaleźć – dla przykładu – konkretny katalog możesz musieć przejrzeć sieć albo dysk twardy.

1 – Z aktywnego okna, kliknij na przycisk Wybierz (Select) – jest zdefiniowany jako „...”. Otworzy się drugie okno, z którego możesz wybrać konkretny katalog.

2 – Aby zmienić miejsce docelowe katalogu, przejrzeć dostępne Dyski z listy (dolna część ekranu). Aby mieć pewność, że lista zawiera wszystkie dostępne dyski, kliknij przycisk Odśwież (Refresh).

3 – Kiedy zlokalizujesz katalog, kliknij OK, aby wrócić do aktywnego okna.

Wybieranie konkretnego połączenia lub bramki (Specific connection/Gateway)

EntraPass daje możliwość połączenia konkretnego komponentu z konkretną bramką/połączeniem. Dla przykładu, możesz przypisać konkretne święto do konkretnego połączenia lub bramki.

1 – Z aktywnego okna kliknij przycisk Nowy (New). System wyświetli okno Wybierz Bramkę/Połączenie (Select Gateway/connection).

2 – Kliknij podwójnie na połączenie/bramkę z wyświetlonej listy, kliknij OK.

3 – Podaj nazwę dla definiowanego komponentu.

4 – Postępuj według instrukcji, aby zakończyć proces.



EntraPass - Instrukcja instalacji i obsługi programu Rozpoczęcie pracy z programem

Drukowanie Listy albo Raportu (Printing a List or a Report)

Użytkownik może potrzebować funkcji Druku, aby:

- Wydrukować listę kart
- Wydrukować parametry zdarzenia
- Wydrukować informacje związane ze zdarzeniem
- Ustawić raport do wydrukowania

1 – Z okna EntraPass kliknij przycisk Drukuj (Print)

2 – Wybierz komponenty, które chcesz dodać do listy. Możesz użyć Zaznacz wszystko (Select All), aby dodać wszystkie wyświetlone komponenty.

3 – Jeśli zaznaczysz opcję Drukuj puste pola albo/i Drukuj opis komponentów, druk uwzględni tytuły pól, które są puste.

4 – Kiedy skończysz wybieranie pól, możesz przejrzeć listę przed wydrukiem. Przeglądając listę możesz:

- Zdefiniować ustawienia drukarki.
- Wydrukować kopię raportu lub listy.
- Zachować raport i listę do późniejszego użytku przy pomocy programu Quick Viewer albo wczytać istniejący raport. Aby uzyskać więcej informacji sprawdź [Quick Report Viewer](#).

5 – Jeśli chcesz zmodyfikować ustawienia, zamknij, zmień, a następnie wydrukuj listę.

6 – Użyj przycisku Czcionka (Font), aby zmienić rodzaj czcionki lub jej rozmiar.

7 – Aby wybrać lub zmienić czcionkę:

- Wybierz czcionkę menu. Podgląd wyboru pojawi się w polu podglądu.
- Wybierz format czcionki z menu Styl Czcionki (zwykła, kursywa, pogrubiona, pogrubiona kursywa)
- Wprowadź wielkość czcionki z menu (domyślny rozmiar: 10 albo 11). Im mniejsza czcionka, tym więcej pozycji zmieści się na liście.

8 – Możesz również wybrać kolor czcionki (domyślny kolor: czarny). Zmiany pojawiają się na bieżąco w polu podglądu. Kliknij OK, kiedy wszystkie zmiany zostały wprowadzone. Użyj przycisku Podgląd (Preview) w oknie Drukuj (Print), aby zobaczyć wszystkie zmiany przed wydrukiem.

Notatka: jeżeli żadna drukarka nie jest skonfigurowana, zostanie wyświetlona informacja o błędzie.



EntraPass - Instrukcja instalacji i obsługi programu Rozpoczęcie pracy z programem

Wyświetlanie powiązań między komponentami (Displaying Components Links)

Funkcja Pogląd połączeń (View links) pozwala na podgląd wszystkich wystąpień danego przedmiotu w innych menu. Tym samym można zobaczyć wszystkie połączenia danego komponentu z innymi komponentami.

Notatka: możesz korzystać z przycisku Podgląd połączeń zanim usuniesz komponent z bazy danych, aby sprawdzić, na które menu to usunięcie będzie oddziaływać. Możesz również wydrukować połączenia wybranego komponentu.

1 – Z dowolnego okna menu wybierz komponent i kliknij na przycisk Powiązanie (Link). Wszystkie komponenty, które są powiązane z wybranym komponentem zostaną wyświetlone.

2 – Przyciski zlokalizowane po lewej stronie komponentu wskazują na jego typ. Na przykład, jeżeli wybierzesz terminarz Zawsze ważne (Always valid) i klikniesz przycisk Połączenia (Link) system wyświetli listę wszystkich menu, w których ten terminarz jest ważny.

Notatka: w podanym przykładzie terminarz Zawsze ważne jest wykorzystany jako terminarz REX w menu Definiowania drzwi. Możesz kliknąć prawym przyciskiem na obiekt, aby wybrać kategorię. Na przykład, jeżeli klikniesz prawym przyciskiem i wybierzesz Poziomy dostęp (Access levels), zostaną wyświetlone wyłącznie te Poziomy dostęp, w których ten terminarz jest zdefiniowany.

3 – Aby zobaczyć wszystkie połączenia wybranych drzwi z innymi komponentami systemu zaznacz drzwi, a następnie kliknij przycisk Powiązanie (Link).

4 – Wszystkie komponenty powiązane z zaznaczonymi drzwiami zostaną wyświetlone. Dla przykładu, wybrane drzwi są używane na poziomie dostępu Admina; użytkownicy o uprawnieniach do korzystania z tego poziomu mają dostęp do drzwi.

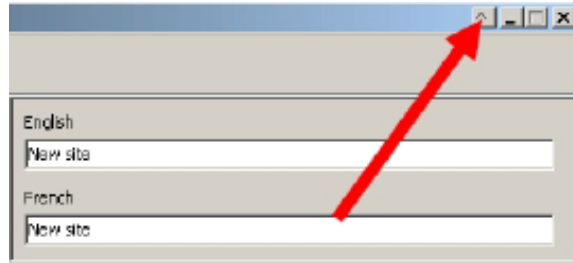
5 – Kliknij przycisk Drukuj (Print), aby wydrukować informacje wyświetlone na ekranie.



EntraPass - Instrukcja instalacji i obsługi programu Rozpoczęcie pracy z programem

Ruchome Okno (Floating Windows)

Przycisk Ruchomego Okna (Floating Window) pozwala na przesunięcie okna poza ekran stacji roboczej. Przycisk znajduje się po lewej stronie przycisku Minimalizuj w oknach umożliwiających opcje Ruchome Okna.



Nie jest możliwe cofnięcie w trakcie przesuwania okna. Powinno zostać zamknięte i otwarte na nowo. Informacja o pozycji okna nie jest przechowywana w systemie.

Widok drzewa systemu (System Tree View)

Przycisk Widok drzewa systemu wyświetla listę komponentów w formacie hierarchii.

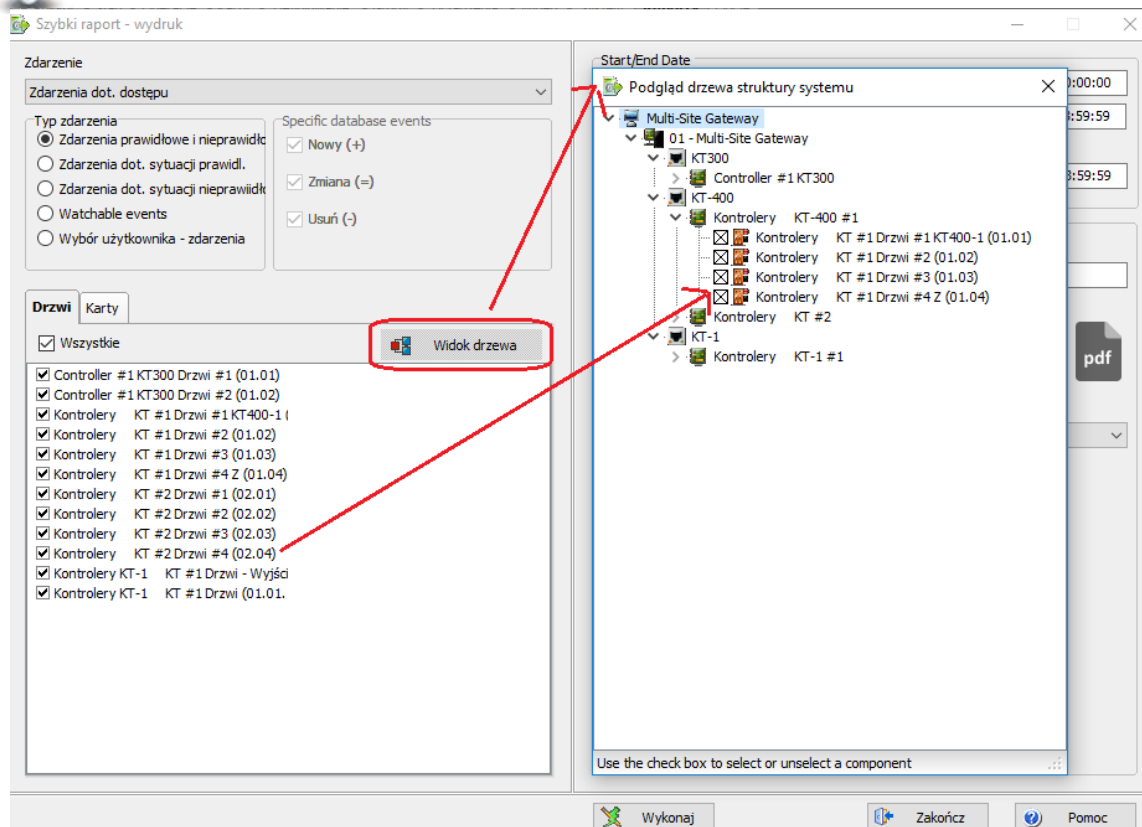
Wywołanie Widoku drzewa systemu

Kiedy możliwe, przycisk Widok drzewa systemu (System Tree View) jest dostępny, tak ja w oknie Żądanie Szybkiego Raportu (Quick Report Request).

1 – Z paska narzędzi Raporty (Reports) wybierz Żądanie Szybkiego Raportu (Quick Report Request). Kliknij przycisk Widok drzewa systemu (System Tree View).



EntraPass - Instrukcja instalacji i obsługi programu Rozpoczęcie pracy z programem

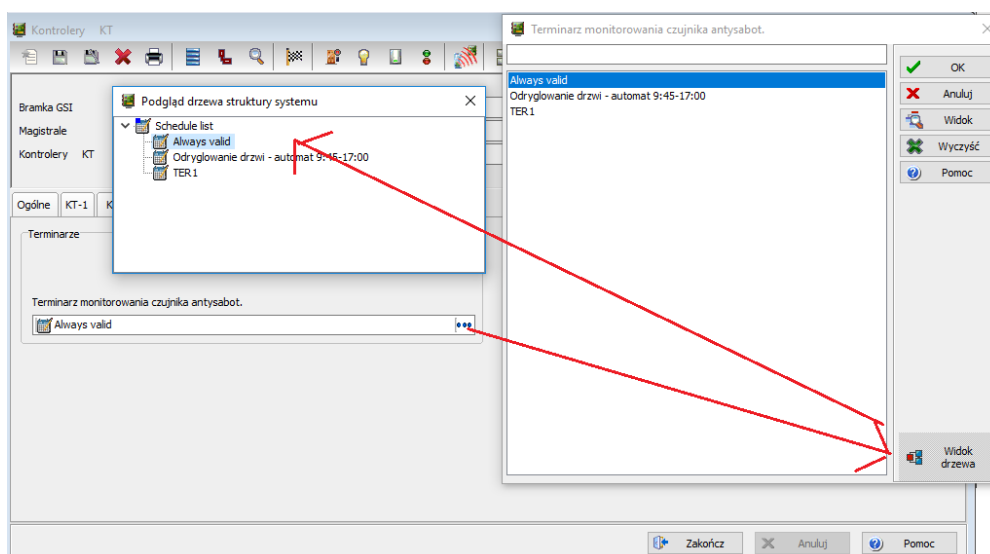


2 – Z Widoku drzewa systemu możesz poprzez podwójne kliknięcie zaznaczać lub odznaczać poszczególne komponenty. Zmiany są automatycznie uwzględniane na odpowiedniej zakładce.

3 – Kliknij ponownie na przycisk Widok drzewa systemu, aby ją zamknąć.

Wykorzystanie przycisku (•••) (Three-Dot button)

Na niektórych polach danych, wybierz przycisk (•••):

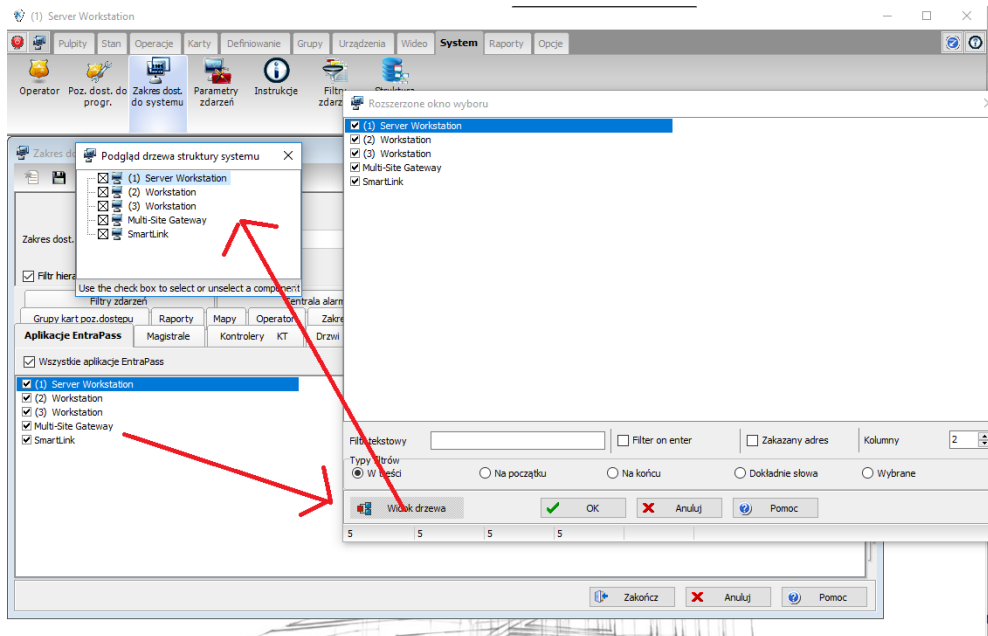




EntraPass - Instrukcja instalacji i obsługi programu Rozpoczęcie pracy z programem

Wykorzystanie Pola Rozszerzonego Wyboru (Using the Extended Selection Box)

1 – Idź do zakładki: Pasek narzędzi Systemu > Obszar Roboczy (Workspace) > Aplikacje EntraPass i kliknij prawym przyciskiem w Rozszerzone Pole Wyboru:



2 – Kliknij na przycisk Widok Drzewa Systemu. Poprzez podwójne kliknięcie możesz zaznaczać lub odznaczać poszczególne komponenty. Zmiany są automatycznie uwzględniane na Polu Rozszerzonego Wyboru.

3 – Kliknij ponownie na przycisk Widok Drzewa Systemu, aby zamknąć.

Wykorzystanie Pola Komentarzy, jako Notatnika (Comment Field as Notepad)

Pole Komend, które można znaleźć w oknie Kart i Urządzeń, może być edytowane bezpośrednio, ale również, jako okno Notatnika.

Dla przykładu, w oknie Karta kliknij podwójnie w puste pole. Edytuj tekst w oknie Notatnika, po czym je zamknij. Tekst zostanie wyświetlony w Polu Komentarzy. Kliknij przycisk Zapisz (Save).



Szczegóły funkcji Usuń (Delete details)

Przycisk Usuń (Delete) służy do usunięcia wybranego zapisu. W ramach zabezpieczenia przed przypadkowym usunięciem danych, ostrzeżenie z prośbą o potwierdzenie jest wyświetlane.

W momencie, kiedy komponent zostaje usunięty, wszystkie połączenia z innymi elementami również zostają skasowane. W Bazie danych zostają jednak zachowane rekordy (archives) po ich usunięciu.

Kiedy okno Usuniętych danych jest wyświetlone można w nim znaleźć:

- Usunięte komponenty
- Usunięte połączenia między komponentami

Zawsze będzie wyświetlony szacunkowy czas trwania operacji usunięcia.

Wyświetlanie linków pomiędzy elementami systemu (Displaying Components Links)

Funkcja Pogląd połączeń (View links) pozwala na podgląd wszystkich wystąpień danego przedmiotu w innych menu. Tym samym można zobaczyć wszystkie połączenia danego komponentu z innymi komponentami.

Notatka: możesz korzystać z przycisku Podgląd połączeń zanim usuniesz komponent z bazy danych, aby sprawdzić, na które menu to usunięcie będzie oddziaływać. Możesz również wydrukować połączenia wybranego komponentu.

1 – Z dowolnego okna menu wybierz komponent i kliknij na przycisk Powiązanie (Link). Wszystkie komponenty, które są powiązane z wybranym komponentem zostaną wyświetlone.

2 – Przyciski zlokalizowane po lewej stronie komponentu wskazują na jego typ. Na przykład, jeżeli wybierzesz terminarz Zawsze ważne (Always valid) i klikniesz przycisk Połączenia (Link) system wyświetli listę wszystkich menu, w których ten terminarz jest ważny.

Notatka: w podanym przykładzie terminarz Zawsze ważny jest wykorzystany jako terminarz REX w menu Definiowania drzwi. Możesz kliknąć prawym przyciskiem na obiekt, aby wybrać kategorię. Na przykład, jeżeli klikniesz prawym przyciskiem i wybierzesz Poziomy dostęp (Access levels), zostaną wyświetlone wyłącznie te Poziomy dostęp, w których ten terminarz jest zdefiniowany.

3 – Aby zobaczyć wszystkie połączenia wybranych drzwi z innymi komponentami systemu zaznacz drzwi, a następnie kliknij przycisk Powiązanie (Link).

4 – Wszystkie komponenty powiązane z zaznaczonymi drzwiami zostaną wyświetlone. Dla przykładu, wybrane drzwi są używane na poziomie dostępu Admina; użytkownicy o uprawnieniach do korzystania z tego poziomu mają dostęp do drzwi.

5 – Kliknij przycisk Drukuj (Print), aby wydrukować informacje wyświetlone na ekranie.



EntraPass - Instrukcja instalacji i obsługi programu Rozpoczęcie pracy z programem

Paski narzędzi EntraPass (EntraPass Toolbars)

EntraPass wyświetla większość poniższych przycisków. Stanowią one prosty sposób dostępu do funkcji systemu. Podpowiedź odnośnie zastosowania danego przycisku wyświetla się po „najechniu” kursorem nad przycisk.

Ikony różnią się od siebie zależnie od tego, jakie okno jest otwarte. Większość przycisków oraz funkcji z nimi powiązanych pokrywa się z innymi przyciskami i funkcjami, powszechnie stosowanymi w codziennej obsłudze komputera.



Przycisk Nowy (New) jest wykorzystywany do wprowadzenia nowych informacji do bazy danych. Może to być dodanie nowego połączenia, terminarza, kontrolera, etc.



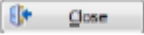
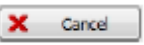
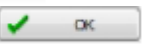
Przycisk Zapisz (Save) zapisuje wszystkie informacje, które zostały wprowadzone od ostatniego zapisu danych. Informacja jest zapisana bezpośrednio w systemie.



Przycisk Zapisz jako (Save as) pozwala na zapisanie wszystkich informacji o istniejącym komponencie pod nową nazwą, bez zmieniania oryginalnego komponentu. Kiedy stosuje się przy zmianach kart, możliwe jest utworzenie nowej karty.



EntraPass - Instrukcja instalacji i obsługi programu Rozpoczęcie pracy z programem

-  Przycisk Usuń (Delete) służy do usunięcia wybranego zapisu. W ramach zabezpieczenia przed przypadkowym usunięciem danych, ostrzeżenie z prośbą o potwierdzenie jest wyświetlane. W momencie, kiedy komponent zostaje usunięty, wszystkie połączenia z innymi elementami również zostają skasowane. W Bazie danych zostają jednak zachowane rekordy (archives) po ich usunięciu.
-  Przycisk Drukuj (Print) może zostać wykorzystany do wydruku raportu, list kart, parametrów zdarzenia, etc.
-  Przycisk Opiekun (Parent) pozwala wyświetlić wyszukiwania w hierarchii albo wyświetlić wyniki wyszukiwania w podziale na bramki, połączenia i kontrolery (według menu).
-  Przycisk Połączenie (Link) pozwala wyświetlić wszystkie połączenia danego elementu w innych menu.
-  Przycisk Znajdź (Find) pozwala wyszukać konkretny element albo komponent przy pomocy opisu.
-  Przycisk Ekspresowe Ustawienia (Express Setup) pozwala konfigurować system poprzez ustawienia domyślne.
-  Przycisk Widok drzewa systemu (System Tree View) wyświetla listę komponentów w formacie hierarchii.
-  Przycisk Zamknij (Close) służy do zamknięcia menu. Jeżeli przed zamknięciem nie zapisasz danych, system poprosi o zapisanie przed zamknięciem.
-  Przycisk Anuluj (Cancel) służy do anulowania wszystkich zmian, jakie zostały wprowadzone od ostatniego zapisu danych. System poprosi o potwierdzenie operacji.
-  Przycisk Pomoc (Help) wyświetla informacje pomocnicze na temat konkretnego tematu.
-  Przycisk OK jest wykorzystywany do akceptowania modyfikacji, dodawania i usuwania danych do bazy danych systemu.
-  Przycisk Zaznacz wszystkie (Select all) służy do zaznaczenia wszystkich elementów lub komponentów z wyświetlonej listy.
-  Przycisk Odznacz wszystkie (Unselect all) służy do odznaczenia wszystkich elementów lub komponentów z wyświetlonej listy, które zostały wcześniej zaznaczone.
-  W niektórych oknach występują przyciski dostępu do grafiki i animacji. Przycisk Włącz grafikę (Enable graphic) służy do wyświetlenia grafiki związanej z wybranym komponentem (np. drzwiami) oraz wyświetla powiązane komponenty (np. czynniki).



EntraPass - Instrukcja instalacji i obsługi programu Rozpoczęcie pracy z programem



Przycisk Włącz animację (Enable animation) służy do włączenia przycisku Włącz grafikę (Enable graphic). Uruchamia component i wyświetla jego status w czasie rzeczywistym.

Prawy przycisk: Pozwala użytkownikowi na wywołanie menu skrótów, z którego mogą wybrać konkretne polecenie, zależne od aktywnego menu.

Notatka: ikony funkcji, które nie są aktywne są automatycznie ukryte.

Instalacja ekspresowa (Express Setup)

Ekspresowe ustawienia pozwalają skonfigurować komponenty systemu, takie jak kontrolery, oraz urządzenia powiązane z komponentami, na przykład drzwiami. Funkcja redukuje potrzebę programowania do minimum, pozwalając instalatorowi poświęcić więcej czasu na sprawdzenie instalacji i samych komponentów systemu. Funkcje można wykorzystać do konfigurowania połączenia albo do zdefiniowania kontrolerów przypisanych do połączenia. Kiedy funkcja jest używana do konfigurowania połączenia, umożliwia instalatorowi przypisać połączenie do bramki.

Notatka: możesz uruchomić Express Setup z menu Windows: Start > Wszystkie programy > EntraPass Corporate Edition > Server > Express Setup; albo poprzez kliknięcie na przycisk Express Setup w oknach stacji roboczych EntraPass.

Kiedy funkcja jest używana do konfiguracji kontrolera pozwala użytkownikowi przypisać określone wartości do kontrolera i do powiązanych z nim urządzeń. W takim przypadku uruchamia się ją z pola wiadomości systemowych albo z menu kontrolera.

Notatka: musisz zalogować się do serwera, kiedy uruchamiasz Express Setup. Ponieważ program pozwala użytkownikowi na modyfikowanie konfiguracji urządzeń systemowych, kluczowym jest uwiarygodnienie użytkownika przed przystąpieniem do modyfikacji.



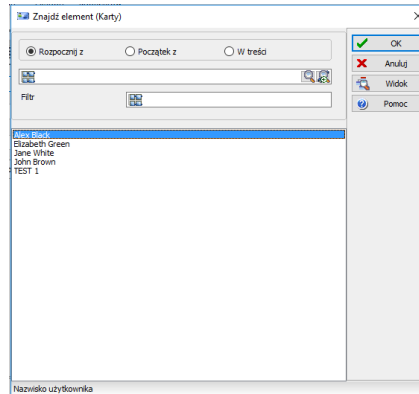
EntraPass - Instrukcja instalacji i obsługi programu Rozpoczęcie pracy z programem

Wyszukiwanie elementów (Finding Components)

Funkcja Znajdź component pozwala operatorowi znaleźć konkretny element albo komponent w bazie danych systemu przy użyciu odpowiednich komend.

Istnieją dwa rodzaje dialogu Znajdź komponent: dostęp do pierwszego można uzyskać z każdego paska narzędzi okna EntraPass. Dostęp do drugiego jest zapewniony przez działanie użytkownika (karty, karty gości, przepustki).

1 – W obu przypadkach musisz kliknąć na ikonę lornetki na pasku narzędzi, aby otworzyć Znajdź komponent.



- Okno po lewej jest wykorzystywane do znajdowania komponentów, a okno po prawej do znajdowania kart.



Wyszuka w bazie danych komponent albo kartę



Przeszuka bazę danych pod kątem obrazu, który odpowiada karcie wybranej na liście.



Otworzy się menu, w którym wybierzesz, według jakiego indeksu karty chcesz wyszukiwać (numer karty, imię i nazwisko posiadacza karty, etc.).

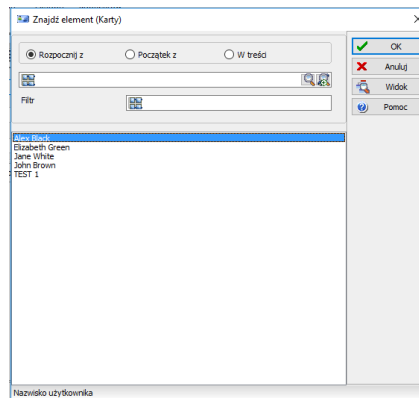
2 – Aby rozpocząć wyszukiwanie wprowadź słowo klucz i kliknij ikonę lornetki po prawej. Aby ograniczyć liczbę rezultatów, odznacz jedno z pól:

- Rozpocznij od (Start with): wyświetlone zostaną wszystkie komponenty, które zaczynają się od wprowadzonego słowa klucza, w kolejności alfabetycznej; wyświetlone zostaną również pozostałe komponenty bazy danych.
- Zaczyna się od (Begins with): wyświetlone zostaną wyłącznie komponenty zaczynające od słowa klucza.
- Zawiera (Contains): wyświetlone zostaną wszystkie komponenty, które zawierają słowo klucz.



EntraPass - Instrukcja instalacji i obsługi programu

Rozpoczęcie pracy z programem



3 – Jeśli chcesz zobaczyć obraz korespondujący z wybraną z listy kartą, kliknij ikonę lornetki ze znacznikiem plus.

4 – Aby anulować proces wyszukiwania, kliknij przycisk Anuluj (Cancel)

5 – Kliknij OK. Zaznaczone komponenty na liście zostaną wyświetlone w oknie, w którym poszukiwanie zostało rozpoczęte.



EntraPass - Instrukcja instalacji i obsługi programu Rozpoczęcie pracy z programem

Uruchamianie i zamykanie aplikacji (Session Start and End)

1 – Z menu Start Windows kliknij Start > Wszystkie > EntraPass Corporate Edition > Serwer / Stacja robocza, gdzie aplikacja EntraPass może być aplikacją wyłącznie do stacji roboczej, bramki, albo dowolnego urządzenia systemowego. Możesz również uruchomić program przez ikonę EntraPass znajdującą się na Pulpicie.

2 – Z menu Start Windows kliknij Start > Wszystkie > EntraPass Global Edition > Serwer / Stacja robocza, gdzie aplikacja EntraPass może być aplikacją wyłącznie do stacji roboczej, bramki, albo dowolnego urządzenia systemowego. Możesz również uruchomić program przez ikonę EntraPass znajdującą się na Pulpicie.

3 – W trakcie uruchamiania, aplikacja próbuje nawiązać połączenie z serwerem. Język aplikacji jest zależny od ustawień wprowadzonych przez użytkownika. Język angielski jest językiem domyślnym.

Notatka: najpierw musisz uruchomić serwer EntraPass. Jeśli uruchomisz stację roboczą EntraPass przez uruchomieniem serwera, jesteś przekierowany do przypisania swojej aplikacji do serwera, nawet wtedy, kiedy aplikacja była już zarejestrowana. Jeżeli aplikacja była zarejestrowana musisz tylko uruchomić serwer.

Uruchamianie serwera EntraPass (Starting the EntraPass Server)

Serwer EntraPass jest wykorzystywany do:

- Wyświetlania wszystkich aplikacji podłączonych do serwera, wszystkich zdarzeń systemowych oraz logów błędów.
- Rejestrowania nowych połączeń (aplikacji stacji roboczych, aplikacji bramek, aplikacji klienckich takich jak: SmartLink, Video Vault, Report Viewer, etc.).
- Przygotowywania kopii zapasowych (danych, archiwów, baz danych)
- Odzyskiwania danych (danych, archiwów, baz danych)
- Weryfikowania zgodności bazy danych
- Zmieniania języka bazy danych.

1 – Uruchom Serwer (z menu Start Windows albo z pulpitu).

2 – Okno startowe serwera pokazuje postęp uruchamiania oraz informacje z nim związane. Kiedy proces się zakończy, okno logowania zostanie wyświetlone.

3 – Kliknij na przycisku Login/Logout, aby otworzyć ekran logowania się użytkownika.

4 – Wprowadź nazwę użytkownika oraz hasło. Domyślna nazwa użytkownika to kantech. Wielkość liter nie jest istotna. Domyślne hasło to kantech, z małych liter. Wielkość liter jest istotna.

Notatka: aby umożliwić użytkownikowi zalogowanie się do serwera Administrator Systemu musi zaznaczyć opcję „Zezwalaj na logowanie do serwera” podczas definiowania „Poziomy dostępu użytkownika” (System > Poziomy bezpieczeństwa). Sprawdź Definiowanie Poziomów bezpieczeństwa ([Security Level Definition](#)).

Notatka: system zachowuje ostatnich pięciu użytkowników, pozwalając na wybór ich nazwy z rozwijanej listy. Aby usunąć nazwę użytkownika z listy zaznacz go, a następnie kliknij Usuń (Delete) na klawiaturze. Domyślnie Wyświetlanie listy logowania (Display login list) jest wyłączone.

5 – Po wprowadzeniu poprawnego loginu i hasła zostanie wyświetlone główne okno EntraPass Serwer z aktywnym paskiem narzędzi. Zależnie od potrzeby, wybierz pasek narzędzi do przeprowadzenia konkretnej operacji albo do wyświetlenia informacji o systemie.



EntraPass - Instrukcja instalacji i obsługi programu Rozpoczęcie pracy z programem

Notatka: Pasek statusu wskazuje na status komunikacji: Zielony – komunikacja OK.; Czerwony – Problem w komunikacji.

6 – Umieść kursor na oznaczeniu statusu (kolorowy prostokąt) w celu zobaczenia wskazówki opisującej wyświetlaną informację.

- Jeśli pierwsze oznaczenie statusowe jest czerwone (flaga), wtedy baza danych systemu nie jest otwarta. Może to być spowodowane procesem weryfikacji danych. Jeśli jest fioletowe, oznacza to, że baza danych jest zamkniętych, ponieważ kopia zapasowa jest przywracana.
- Jeśli drugi oznaczenie statusowe jest czerwone (flaga), wtedy baza danych jest niedostępna. Jest to spowodowane przetwarzaniem danych albo aktualizowaniem bazy danych.
- Zielony kolor oznacza, że baza danych jest dostępna.



EntraPass - Instrukcja instalacji i obsługi programu Rozpoczęcie pracy z programem

Uruchamianie Bramki (Starting the Gateway Program)

Bramka może zostać zainstalowana na tym samym komputerze, co serwer albo aplikacja stacji roboczej EntraPass, ale zaleca się instalację programu na dedykowanym do tego komputerze.

1 – Uruchom bramkę (z menu Start albo z Pulpitu). Nie musisz wprowadzać hasła ani nazwy użytkownika. Uruchamia się główne okno EntraPass Corporate Edition.

2 – Uruchom bramkę (z menu Start albo z Pulpitu). Nie musisz wprowadzać hasła ani nazwy użytkownika. Uruchamia się główne okno EntraPass Global Edition.

3 – Możesz kliknąć prawym przyciskiem myszy gdziekolwiek w oknie Bramki, aby wyświetlić podmenu:

- **Minimalizuj** (Minimize) – minimalizuje okno Bramki
- **Wyślij na pasek** (Send to tray) – wysyła okna na pasek statusu.

4 – Zwróć uwagę na paski postępu:

- **Dane konfiguracyjne pobierane z serwera** (Configuration data received from the server): dane (np. modyfikacje karty) są przesyłane z serwera do bramki.
- **Dane wymagane przez stację roboczą** (Data requested by workstation): to są dane wymagane, np. statusy.
- **Wiadomości wysyłane do serwera**: wiadomości pochodzące od operatora są wysyłane do serwera.

5 – Z menu systemowego możesz wybrać: zaloguj (log in), wyloguj (log out), albo przeładowanie bramki.

6 – Z menu Bramki możesz wybrać element umożliwiający wybranie konkretnej bramki. Ilość bramek połączonych z serwerem jest wyświetlona na pasku statusu w głównym oknie Bramki.

Notatka: oznaczenie statusów (oflagowanie) informuje o statusie komunikacji. Pierwsze oznaczenie informuje o komunikacji z serwerem. Jeżeli jest czerwone, oznacza to, że serwer nie komunikuje się z Bramką. Ma to miejsce w momencie, kiedy serwer jest offline (możesz wtedy uruchomić serwer). Informacje dotyczące daty, czasu, liczbie bramek oraz adresie IP serwera również znajduje się na pasku statusu.

Notatka: pasek postępu to nie paski statusów. Nie musisz czekać, aż się wypełnią.



EntraPass - Instrukcja instalacji i obsługi programu Rozpoczęcie pracy z programem

Uruchamianie stacji roboczej EntraPass (Starting the EntraPass Workstation)

Stacją roboczą EntraPass nazywamy komputer, na którym jest zainstalowana aplikacja monitorująca EntraPass. Umożliwia ona dostęp i używanie bazy danych oraz wszystkich komponentów.

Upewnij się, że serwer jest online zanim uruchomisz oprogramowanie stacji roboczej EntraPass.

W trakcie uruchamiania, aplikacja próbuje nawiązać połączenie z serwerem. Język aplikacji jest zależny od ustawień wprowadzonych przez użytkownika. Język angielski jest językiem domyślnym.

Notatka: najpierw musisz uruchomić serwer EntraPass. Jeśli uruchomisz stację roboczą EntraPass przez uruchomieniem serwera, jesteś przekierowany do przypisania swojej aplikacji do serwera, nawet wtedy, kiedy aplikacja była już zarejestrowana. Jeżeli aplikacja była zarejestrowana musisz tylko uruchomić serwer.

1 – Uruchom stację roboczą EntraPass (z menu Start Windows albo z pulpitu).

2 – Okno logowania stacji roboczej EntraPass zostanie wyświetlone.

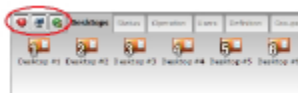
Notatka: jeżeli serwer jest offline, pierwsze oznaczenie (oflagowanie; kolorowe prostokąty na pasku) po lewej będzie czerwone; przycisk Logowanie/Wylogowanie jest wyłączony. W takim przypadku uruchom serwer; stacja robocza EntraPass wznowi działanie.

3 – Kliknij na przycisku Login/Logout, aby otworzyć ekran logowania się użytkownika.

4 – Wprowadź nazwę użytkownika oraz hasło. Domyślna nazwa użytkownika to kantech. Wielkość liter nie jest istotna. Domyślne hasło to kantech, z małych liter. Wielkość liter jest istotna.

Notatka: jeżeli nie możesz się prawidłowo zalogować, sprawdź czy Caps Lock nie jest włączony. Po wprowadzeniu prawidłowego Loginu zostaną wyświetlone menu systemu, pasek narzędzi oraz pasek statusów. Serwer musi być uruchomiony, jeśli chcesz zalogować się do systemu.

Notatka: domyślnie, użytkownicy nie mogą logować się do więcej niż jednej stacji roboczej na raz. Jeżeli istnieje taka potrzeba użytkownik może być jednak zalogowany wielokrotnie; zobacz Tworzenie oraz edytowanie operatora ([Creating or Editing an Operator](#)). Użytkownik może być zalogowany na serwerze EntraPass oraz stacji roboczej EntraPass w tym samym czasie.





EntraPass - Instrukcja instalacji i obsługi programu Rozpoczęcie pracy z programem

Uzyskiwanie informacji na temat stanu połączenia Stacji Roboczej Serwera (Accessing Information on the Server Workstation Connection Status)

- 1 – Kliknij w dowolny pasek narzędzi systemu albo wybierz opcję z menu, aby wejść do menu systemu. W dolnej części okna, kolorowe oznaczenia (flagi) wskazują stan połączenia: zielone – połączenie jest OK.; czerwone – problemy z połączeniem; niebieskie – raport w oczekiwaniu.
- 2 – Przesuń kursor nad kolorowe oznaczenie (prostokąt), aby wyświetlić szczegóły stanu sieci, szczegóły stanu bazy danych oraz stanu raportów stacji roboczej.
- 3 – Przesuń kursor nad wyświetlane wartości liczbowe, aby zobaczyć szczegóły. Zostaną wskazane, po kolei: data oraz czas, nazwa użytkownika, elementy w Alarmach, alarmy do zatwierdzenia, etc.
- 4 – Kliknij (albo kliknij podwójnie) na dowolny numer wyświetlany na pasku statusu, aby wyświetlić okno informacji (status information window)

Notatka: rekomenduje się korzystanie z przycisku Logowanie/Wylogowanie przy zamykaniu programu EntraPass. Zapewnia to prawidłowe zamknięcie baz danych.

Zmiana właściwości obszaru roboczego (Modifying your Work Area Properties)

- 1 – Kliknij prawym przyciskiem myszy w głównym oknie, aby wyświetlić okno Właściwości (Properties). Możesz teraz zmieniać przyciski okna oraz kolor tła.
- 2 – Aby zmodyfikować rozmiar przycisków paska narzędzi, wybierz jedną z opcji:
 - Małe przyciski (Small buttons): małe przyciski są wyświetlane poniżej elementów menu.
 - Duże przyciski z obrazami (Large buttons with images): przyciski komponentów są wyświetlane na dużych przyciskach.
 - Duże przyciski bez obrazów (Large buttons without images): nie są wyświetlone żadne przyciski.
- 3 – W sekcji Różne (Miscellaneous), wybierz:
 - Wyświetl menu: tylko pasek menu zostanie wyświetlony. Nie są wyświetlone żadne przyciski. Kliknij prawym przyciskiem, aby zmienić właściwości.
 - Wyświetl pasek narzędzi: pasek menu oraz pasek narzędzi są wyświetlone.
- 4 – Wybierz kolor tła.



EntraPass - Instrukcja instalacji i obsługi programu Rozpoczęcie pracy z programem

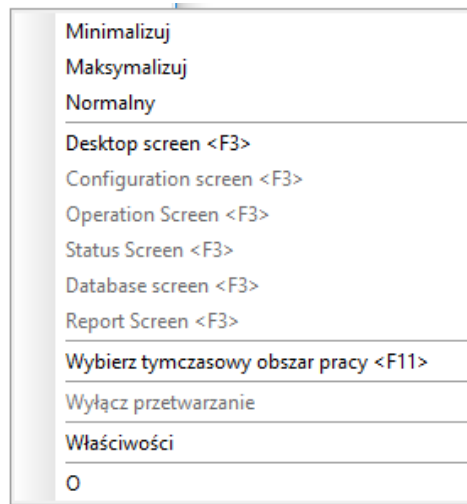
Przywracanie ukrytego okna (Retrieving Hidden Windows on the Desktop)

EntraPass pozwala pracować na wielu otwartych oknach. Kiedy okno zostanie zminimalizowane albo wysłane na tył, zupełnie znika z ekranu. Komenda w menu kontekstowym stacji roboczej może pomóc w odzyskaniu elementów.

- Jeśli okno zostało zminimalizowane, komenda z menu przywróci je na front ekranu, gdzie będziesz miał możliwość przywrócić ją do pełnego rozmiaru.
- Jeśli okno zostało wysłane na tył, komenda z menu przeniesie je na pierwszy plan.

Ta komenda działa dla: ekranów pulpitu, ekranów konfiguracji, ekranów operacyjnych, ekranów statusów, ekranów baz danych i ekranów raportowych.

1 – Kliknij prawym przyciskiem myszy w oknie stacji roboczej. Menu kontekstowe zostanie wyświetlone:



2 – W powyższym przykładzie, ekran Statusu został wysłany na tło. Kliknięcie komendy ekranu statusu przeniesie ekran na pierwszy plan.

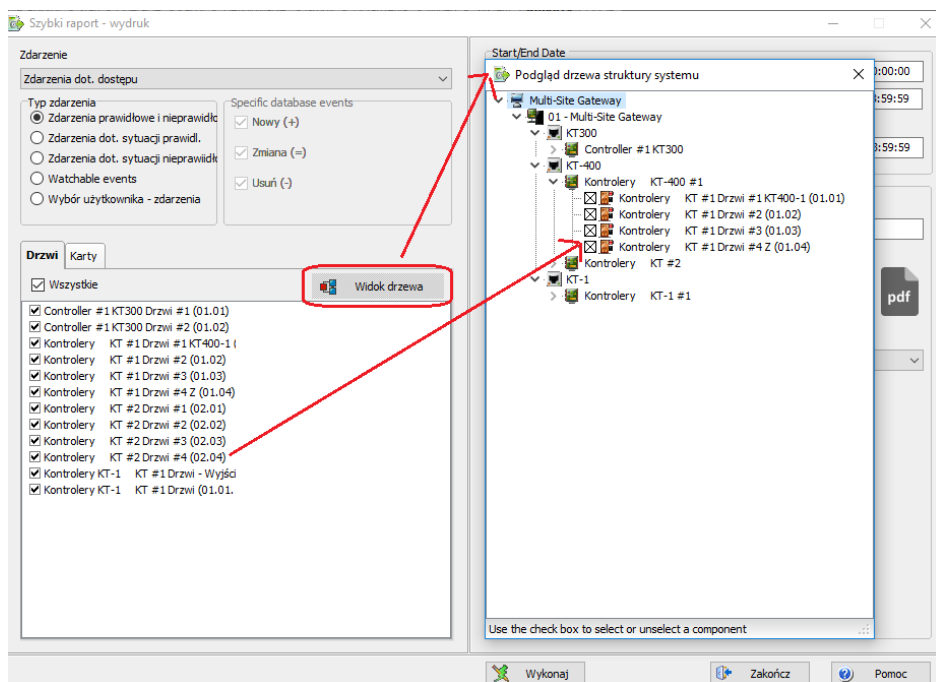


EntraPass - Instrukcja instalacji i obsługi programu Rozpoczęcie pracy z programem

Struktura systemu w formie drzewa (System Tree View)

Kiedy możliwe, przycisk Widok drzewa systemu (System Tree View) jest dostępny, tak ja w oknie Żądanie Szybkiego Raportu (Quick Report Request).

1 – Z paska narzędzi Raporty (Reports) wybierz Żądanie Szybkiego Raportu (Quick Report Request). Kliknij przycisk Widok drzewa systemu (System Tree View).

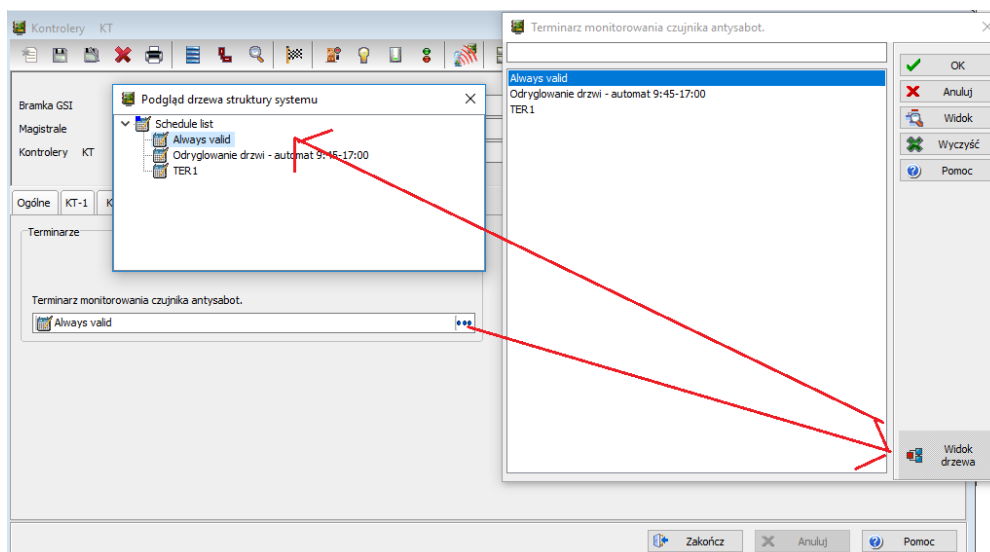


2 – Z Widoku drzewa systemu możesz poprzez podwójne kliknięcie zaznaczać lub odznaczać poszczególne komponenty. Zmiany są automatycznie uwzględniane na odpowiedniej zakładce.

3 – Kliknij ponownie na przycisk Widok drzewa systemu, aby ją zamknąć.

Wykorzystanie przycisku (•••) (Three-Dot button)

Na niektórych polach danych, wybierz przycisk (•••):





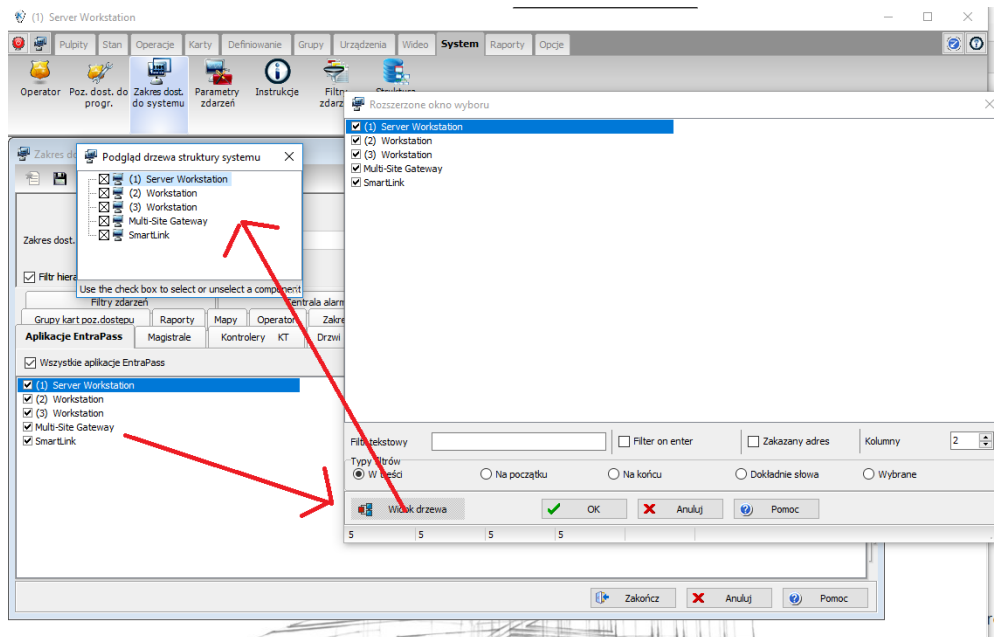
EntraPass - Instrukcja instalacji i obsługi programu Rozpoczęcie pracy z programem



EntraPass - Instrukcja instalacji i obsługi programu Rozpoczęcie pracy z programem

Użycie rozszerzonego okna wyboru (Using the Extended Selection Box)

1 – Idź do zakładki: Pasek narzędzi Systemu > Obszar Roboczy (Workspace) > Aplikacje EntraPass i kliknij prawym przyciskiem w Rozszerzone Pole Wyboru:



2 – Kliknij na przycisk Widok Drzewa Systemu. Poprzez podwójne kliknięcie możesz zaznaczać lub odznaczać poszczególne komponenty. Zmiany są automatycznie uwzględniane na Polu Rozszerzonego Wyboru.

3 – Kliknij ponownie na przycisk Widok Drzewa Systemu, aby zamknąć.



Pulpity

Pulpit alarmów

Pulpit alarmowy (Alarms Desktop)

Pulpit alarmów jest wykorzystywany do podglądu oraz monitorowania zdarzeń alarmowych. Zdarzenia alarmowe są definiowane w menu Parametry Zdarzeń (System > Event Parameter). Każde zdarzenie może zostać zdefiniowane, jako zdarzenie alarmowe. Zdarzenia alarmowe wymagają monitorowania użytkownika i są wyświetlane na Pulpicie alarmów. Terminarz musi zostać utworzony dla każdego typu alarmu (System > Parametry Zdarzeń, Ustawienia alarmów). Alarmy są wyświetlane z datą i konkretną godziną, opisem, szczegółami i instrukcją (o ile była zdefiniowana) oraz grafiką lub plikiem wideo. Nowe zdarzenia są dodawane na dole Pulpitu alarmów (w ustawieniach można ustawić odwrotny sposób wyświetlania – nowe zdarzenia na górze).

Definiowanie Pulpity alarmów (Defining an Alarms Desktop)

1 – Z głównego okna Pulpity wybierz pulpit, na którym chcesz wyświetlać wiadomości alarmowe – następnie zdefiniuj typ okna.

2 – Określa okna pomocnicze, które będą przypisane do Pulpitu alarmów:

- Wyświetl przy nowym alarmie (Display on new alarm): wyświetli automatycznie po alarmie.
- Ekran wiadomości (Message screen): ten ekran pozwala użytkownikowi pogląd oraz monitorowanie tych alarmów, które w parametrach mają ustawione wymaganie potwierdzenia.
- Ekran instrukcji (Instructions screen): okno wyświetla instrukcję przypisaną do zdarzenia (np. powiadomić policję, wyślij informację na aplikację klienta, etc.). Instrukcje są definiowane w System > Instrukcje (Instructions). Potem mogą zostać przypisane do zdarzeń.
- Ekran graficzny (Graphic screen): to okno wyświetli lokalizację, z której pochodzi zgłoszenie alarmu (jeżeli opcja jest udostępniona). Po więcej informacji sprawdź Definiowanie grafiki ([Graphics Definition](#)).

Notatka: Pulpit alarmów może zostać zdefiniowany, jako Okno wiadomości, Okno graficzne albo Okno instrukcji. Te właściwości odnoszą się do pojedynczego pulpitu. W momencie wybrania pulpitu określonego tymi trzema właściwościami, trzy okna zostaną wyświetlone jednocześnie. W celu lepszego wyświetlania może pojawić się potrzeba zmiany rozmiaru lub przemieszczenia okien.



Przeglądanie Systemowych Wiadomości Alarmowych (Viewing System Alarm Messages)

1 – Wybierz Pulpit alarmów. Zdarzenia alarmowe są wyświetlane według kryteriów wybranych w Sortuj wg (Sorted by field).

Notatka: wiadomości alarmowe są archiwizowane i mogą być sprawdzane w dowolnym momencie.

2 – Aby dodać komentarz kliknij podwójnie w pole logowania (środek ekranu). Okno Dodaj komentarz (Add a comment) zostanie otwarte. Po wpisaniu komentarza kliknij przycisk OK, aby zamknąć okno. Zdarzenie alarmowe będzie poprzedzane znakiem +, informującym o tym, że został do niego dodany komentarz.

Notatka: potwierdzenia oraz oznaczenia (oflagowanie) nie będą oznakowane znakiem „+”

3 – Możesz zmienić/zdefiniować kolejność sortowania:

- Kolejność zgłaszania (Trigger destination): alarmy są sortowane wg kolejności zgłaszania. Jest to ustawienie domyślne. Okno/lista przewija się za każdym razem do końca przy każdym zgłoszeniu.
- Stan (State): alarmy są sortowane wg statusu (odnotowane, do odnotowania, oznaczone). Używając tej opcji wpływa się na prawidłowe przewijanie zdarzeń. Wybierz Sekwencje (Sequence), aby wrócić do ustawień domyślnych.
- Data i czas (Date and time): alarmy są sortowane wg daty i czasu.
- Zdarzenie (Event): kolumna wiadomości zdarzeń jest sortowana alfabetycznie, grupując identyczne zdarzenia.
- Priorytet (Priority): zdarzenia są sortowane wg priorytetu.

4 – Możesz kliknąć prawym klawiszem myszy w dowolnym miejscu okna, aby wywołać okna Właściwości (Properties), skąd możesz aktywować przyciski statusu alarmu:

- Czerwony: do zatwierdzenia lub zawieszenia. W przypadku wybrania zawieszenia zostanie uruchomiony czas zawieszenia. Po jego upływie użytkownik jest zmuszony do zatwierdzenia. Użytkownik może zatwierdzić alarm w dowolnym momencie zawieszenia.
- Zielony: zatwierdzony.
- Żółty: oznaczony.
- Czarny: usunięty. Aby podejrzeć usunięte alarmy, wybierz Podgląd usuniętych logów (View deleted logs).
- Niebieski: wpis manualny.

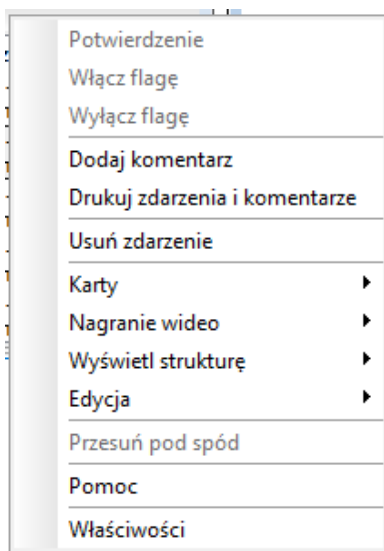
5 – Wybierz metodę zatwierdzenia: manualną lub automatyczną.

Notatka: opcja Zdalnego/Automatycznego potwierdzenia jest dostępna wyłącznie poprzez Pulpit alarmów. W momencie wylogowania się użytkownika, powróci do ustawień domyślnych, czyli „Zdalnego potwierdzenia”.



Pulpit alarmów

6 – Kliknij prawym przyciskiem myszy na wiadomości alarmowej w celu wyświetlenia nowych opcji w przypadku zdarzenia alarmowego:



- **Potwierdź (Acknowledge):** po wybraniu, obok alarmu, zostaje wyświetlony zielony punkt informujący o potwierdzeniu.
- **Sprawdź ponownie (Re-visit):** system oznacza wybrane zdarzenie. Żółty punkt wyświetla się przy zaznaczonym zdarzeniu.
- **Odznacz sprawdź ponownie (Clear re-visit):** usuwa identyfikator Sprawdź ponownie.
- **Dodaj komentarz (Add comment):** umożliwia wprowadzenie komentarzy do wybranego zdarzenia. Komentarze są wyświetlane w dolnej części ekranu alarmowego. Niebieski znaczek + oznacza dodany komentarz.
- **Drukuj zdarzenie wraz z komentarzem (Print event and comment):** po wybraniu system drukuje zdarzenie oraz związany z nim komentarz.
- **Usuń zdarzenie (Delete event):** po zaznaczeniu zdarzenie jest oznakowane do usunięcia (wskaźnik staje się "czarny"). Podgląd zdarzeń zaznaczonych do usunięcia jest możliwy przez kliknięcie prawym przyciskiem w dowolne miejsce okna, wybranie Właściwości (Properties) i wybranie Sprawdź usunięte logi (View deleted logs).



Automatyczne wyświetlanie Pulpitów alarmu (Alarm Desktops Automatically)

EntraPass umożliwia użytkownikom automatyczne wyświetlanie grafiki z poziomu pulpitu. Opcja pozwala automatyczny podgląd alarmu zaraz po zdarzeniu bez potrzeby otwierania okien pomocniczych. Jeżeli opcja Wyświetl przy nowym alarmie (Display on new alarm) jest zaznaczona pulpit alarmowy zostanie wyświetlony od razu po wystąpieniu alarmu.

1 – Zdefiniuj pulpit i ustaw go jako pulpit alarmu: w tym celu musisz zaznaczyć odpowiednie elementy w sekcji Pulpit alarmu.

2 – Zaznacz opcję Wyświetl przy nowym alarmie (Display on new alarm) dla automatycznego podglądu alarmu zaraz po zdarzeniu bez potrzeby otwierania okien pomocniczych

Notatka: jeżeli ta opcja jest wybrana – na przykład – w trakcie definiowania pulpitu Filtrowane wiadomości (Filtered message), a przycisk pulpitu jest zaznaczony, zostanie wyświetlony odpowiedni pulpit (kolor tła jego przycisków stanie się niebieski). Okna poniżej sekcji Wyświetl przy nowym alarmie (Display on new alarm) nie zostaną wyświetlone; zostaną wyświetlone wyłącznie w momencie wystąpienia alarmu. W przypadku wyświetlenia tych okien można je zamknąć znakiem X znajdującym się w prawym górnym rogu. Jeżeli opcja Wyświetl przy nowym alarmie nie jest zaznaczona, pulpit alarmów oraz wszystkie jego pomocnicze okna zostaną wyświetlone na żądanie.

3 – Kliknij OK and GO, aby ustawienia zaczęły działać.

Notatka: kiedy zdefiniujesz pulpit, jako pulpit alarmów tak, aby wyświetlał się przy nowym alarmie, zaleca się ponowne otworzenie pulpitu Automatyczne wyświetlanie alarmów (Automatic Alarm Display) w celu ułożenia okien tak, jak chcesz, aby były wyświetlane. Następnie kliknij OK i Działaj (OK. and GO). Dzięki temu zostanie on wyświetlony tak, jak to określiłeś.



Potwierdzanie Alarmów/Zdarzeń (Acknowledging Alarms/Events)

Zazwyczaj użytkownik musi potwierdzić zdarzenie alarmowe poprzez np. kliknięcie przycisku potwierdzenia. W EntraPass użytkownik potwierdza zdarzenia alarmowe z okna alarmów albo okna Pulpitu alarmów.

Notatka: kiedy wiadomość alarmowa jest potwierdzona przez użytkownika, wiadomość jest potwierdzona lub usunięta na wszystkich stacjach roboczych.

Notatka: do zdarzenia alarmowego można dodać sygnał dźwiękowy; zobacz Konfigurowanie urządzeń multimedialnych (Multimedia devices configuration)

Opcje zatwierdzania są ustawiane poprzez: Urządzenia > EntraPass > Zakładka Alarm, Parametry zatwierdzenia (Devices > EntraPass application > Alarm tab, Acknowledgement parameters). Zdarzenia, które potrzebują zatwierdzenia użytkownika są opisane w System > Parametry zdarzenia.

Notatka: jeżeli komponent, który jest w stanie alarmu jest przypisany do podglądu wideo, podgląd wideo albo nagranie wideo jest automatycznie wyświetlane w momencie alarmu.

Automatyczne potwierdzanie (Automatic Acknowledgement)

Alarmy mogą zostać automatycznie potwierdzone bez interwencji użytkownika. Ta opcja jest aktywowana w menu Użytkownika: System > Operatorzy > Upoważnienia, Automatyczne potwierdzanie (System > Operators > Privileges, Auto acknowledge).

Notatka: aby przycisk Zdalnie (Manual) wyświetlał się w oknie Pulpitu alarmów należy zakończyć sesję EntraPass, a następnie uruchomić ponownie po zaznaczeniu opcji Automatycznego potwierdzenia.

Notatka: tylko użytkownicy posiadający odpowiednie uprawnienia powinni korzystać z tej opcji. Jeśli opcja Automatycznego potwierdzenia (Automatic acknowledge) jest włączona, okienko wiadomości alarmowej nie jest wyświetlone; nie będzie możliwe zawieszenia alarmów. Jeśli ta opcja jest włączona w menu Definiowania operatora (Operator definition), przycisk Zdalnie (Manual) jest dodany do Pulpitu alarmów. Ten przycisk zmienia ustawienia powiadomień z automatycznych na zdalne.



Potwierdzenie wiadomości alarmowej (To Acknowledge an Alarm Message)

1 – Kiedy pojawia się pole potwierdzenia, możesz podjąć następujące akcje:

- Kliknij przycisk potwierdzenia, aby potwierdzić wyświetlone zdarzenie alarmowe. Po potwierdzeniu czerwony status zmienia się na zielony.
- Kliknij przycisk Wstrzymaj (Suspend), aby wykonać inne czynności w systemie. Alarm zostanie wstrzymany na czas określony w ustawieniach. Po jego upływie system poprosi użytkownika o potwierdzenie alarmu.
- Kliknij przycisk Sprawdź ponownie (Re-visit), aby potwierdzić zdarzenie i oznaczyć je do ponownego sprawdzenia. Żółty punkt wyświetla się przy oznaczonym zdarzeniu.
- Kliknij Wycisz (Mute), aby wyłączyć dźwięk alarmu.

Notatka: okienko wiadomości Potwierdzenia (Acknowledgement required) zostanie wyświetlone bez okna instrukcji, jeśli do wiadomości alarmowej nie ma przypisanych żadnych instrukcji.

Notatka: jeżeli komponent, który jest w stanie alarmu jest przypisany do podglądu wideo, podgląd wideo albo nagranie wideo jest automatycznie wyświetlane w momencie alarmu.

Potwierdzenie alarmów z Pulpitu alarmów (To Acknowledge Alarms from the Alarms Desktop)

Każda stacja robocza posiada własny pulpit alarmów, który wyświetla zdarzenia alarmowe otrzymywane z serwera. Po uruchomieniu stacji roboczej i nawiązaniu połączenia z serwerem, wszystkie zdarzenia na pulpicie alarmów zostaną zaktualizowane.

Notatka: ten proces zostanie aktywowany za każdym razem, gdy stacja robocza będzie miała problem z komunikacją z serwerem.

1 – Wybierz zdarzenie alarmowe, które chcesz potwierdzić i kliknij prawym przyciskiem myszy, aby otworzyć menu.

2 – Wybierz Potwierdź (Acknowledge). Oznaczenie statusu zmieni się na zielone.

Notatka: aby zaznaczyć wiadomość alarmową pod konkretny cel, wybierz zdarzenie alarmowe, które chcesz zidentyfikować; kliknij prawym przyciskiem i z menu wybierz Oznacz (Flag). Możesz również klikać na wiadomość alarmową, aż kolor jej statusu zmieni się na pożądanym.



Obowiązkowy komentarz do alarmów (Mandatory Alarm Comment)

Jeżeli do alarmu jest przypisana opcja Obowiązkowego komentarza do alarmów (Mandatory Alarm Comment), użytkownik będzie musiał wprowadzić komentarz, aby oznaczyć alarm, jako potwierdzony.

Notatka: dźwięk alarmu zostanie wyłączony po wprowadzeniu komentarza przez użytkownika.

Jeżeli zdarzenie alarmowe zostało już potwierdzone, wiadomość zostanie wyświetlona informująca o potrzebie dodania komentarza.

Zmiana zdarzeń na pulpicie (Changing Desktop Events)

Aby zmienić zdarzenia wyświetlane na liście komunikatów alarmowych, kliknij prawym przyciskiem myszy komunikat alarmowy listę i wybierz **Zdarzenia pulpitu**. Wybierz grupę zdarzeń, aby wyświetlić zdarzenia z tej grupy. Więcej informacji na temat grup zdarzeń znajduje się tutaj. Wybierz brak, aby zablokować wszystkie wiadomości.

Inne opcje dostępne w tym menu są następujące:

- Wybierz **Użyj wyboru pulpitu wiadomości**, aby wyświetlić te same zdarzenia zdefiniowane dla wybranego pulpitu.
- Wybierz **Wyświetl operatora**, aby wyświetlić wybór zdarzeń pulpitu dla zalogowanego operatora tryb tylko do odczytu.
- Wybierz **Edytuj operatora**, aby zmodyfikować wybór zdarzenia pulpitu dla zalogowanego operatora.
- Wybierz **Przypisz operatora**, aby przypisać jedno lub więcej zdarzeń pulpitu innemu operatorowi.

UWAGA: Zmiany wprowadzone w zdarzeniach na pulpicie dotyczą tylko nowych zdarzeń. Istniejące wydarzenia na stronie lista pozostanie niezmieniona.



Zmiana właściwości pulpitu (Changing the Display Properties)

1 – Kliknij prawym przyciskiem w dowolnym miejscu okna Pulpitu.

2 – Wybierz Właściwości (Properties) z menu.

3 – Następnie wybierz opcje wyświetlania (display), da to możliwość edycji następujących rzeczy:

- Małe przyciski (Small buttons): małe przyciski są wyświetlane poniżej elementów menu bez opisów.
- Duże przyciski z obrazami (Large buttons with images): ikony są wyświetlane z opisami.
- Duże przyciski bez obrazów (Large buttons without images): przyciski są wyświetlane bez opisów.
- Wyświetl menu (Display menu): pozwala obejrzeć menu systemu.
- Wyświetl pasek narzędzi (Display toolbar): pozwala obejrzeć pasek narzędzi systemu.
- Zmień czcionkę domyślną (Change system font): pozwala zmienić czcionkę oprogramowania dla wszystkich użytkowników.

Pulpit Raportów (Custom Report Desktop)

Pulpit Raportów na żądanie pozwala użytkownikowi na wyświetlenie zdarzeń pochodzących ze zdefiniowanych raportów, podejrzeć stan generowania raportów oraz, jeżeli jest taka możliwość, obejrzeć nagrania z EntraPass VideoVault. Poziomy bezpieczeństwa zdefiniują, które raporty są dostępne dla każdego użytkownika.

Lista wiadomości Raportów na żądanie działa w taki sam sposób jak wszystkie listy EntraPass, z jednym wyjątkiem: posiada dodatkowe pole, umożliwiające użytkownikowi wybieranie zdefiniowanego wcześniej raportu.

Notatka: Raporty na żądanie są definiowane w Raporty > Raporty na żądanie.

Notatka: Poziomy bezpieczeństwa dla raportów są definiowane w System > Poziomy bezpieczeństwa > zakładka Raporty.



Konfigurowanie Pulpitu Raportów na żądanie (Configuring a Custom Reports Desktop)

1 – Z głównego okna Pulpitu wybierz przyciskiem pulpit, który chcesz skonfigurować, jako Pulpit Raportów na żądanie.

2 – Przypisz nazwę do utworzonego pulpitu, następnie zdefiniuj typ pulpitu (okno wiadomości, okno obrazów, albo oba).

3 – Wybierz kryterium wg, którego chcesz wyświetlać dane (data i czas, zdarzenie, typ wiadomości)

Notatka: opcja segregowania sekwencyjnego nie jest dostępna dla zarchiwizowanych wiadomości.

4 – Możesz wprowadzić ciąg tekstowy, który zostanie wykorzystany do przeszukiwania wiadomości.

5 – W odpowiednich polach wybierz raport na żądania, który chcesz wygenerować. Lista dostępnych raportów jest zależna od twojego poziomu bezpieczeństwa.

6 – Po wybraniu raportu zostanie wyświetlone okno Daty i czasu (Date and Time).

7 – Wpisz datę i czas rozpoczęcia oraz zakończenia, albo kliknij na przycisk kalendarza i wybierz daty rozpoczęcia oraz zakończenia, a następnie wpisz ich czas.

8 – Przycisk Wyczyść przed następnym krokiem (Clear Screen Before Process) czyści wyniki poprzedniego wyszukiwania.

9 – Kliknij OK. Wskaźnik w lewym dolnym rogu ekranu zmieni się z zielonego na niebieski. Oznacza to generowania raportu. Po zakończonym transferze danych znowu zmieni się na zielony, a dane zostaną wyświetlone wg wybranych wcześniej kryteriów.

Tworzenie i edytowanie Raportów na żądanie z pulpitu (To Create and Edit Custom Reports from a Desktop)

- Jeżeli twój poziom bezpieczeństwa pozwala ci na generowanie nowych raportów, możesz uzyskać dostęp do pola tekstowego Raportu na żądanie. Aby dowiedzieć się więcej na temat Raportów na żądanie zobacz Definiowanie Raportów na żądanie (Custom Reports Definition).

- Jeżeli twój poziom bezpieczeństwa pozwala ci na edytowanie istniejących raportów, możesz uzyskać dostęp do pola tekstowego Raportu na żądanie. Aby dowiedzieć się więcej na temat Raportów na żądanie zobacz Definiowanie Raportów na żądanie (Custom Reports Definition).



Wyświetlanie stanu Raportu na żądanie w czasie rzeczywistym (To Display Custom Report State in Real-time)

Ta opcja pozwala na wyświetlanie postępu generowania raportu dla dowolnego raportu na żądanie.

- 1 – Kliknij prawym przyciskiem w dowolnym miejscu okna Pulpitu raportów na żądanie. Zostanie wyświetlone menu kontekstowe.
- 2 – Wybierz Stan raportu (Report State). Zostanie wyświetlone pole z informacjami na temat generowania raportu.
- 3 – Po zakończeniu generowania raportu, pole zostanie zamknięte. Kliknij Zamknij (Close)

Komentarze i wyświetlanie (Comment Entry and Display)

Komentarz może zostać dodany do dowolnego zdarzenia. W piątej kolumnie od lewej, znak „-” oznacza komentarz systemowy, a „+” komentarz dodany przez użytkownika. Z Pulpitu Raportów na żądanie można wyświetlić wszystkie komentarze.

Można to zrobić wybierając Wyświetl komentarze (View Comment) z menu kontekstowego (wywoływanego prawym przyciskiem myszy) wybranego zdarzenia. Komentarz można również dodać poprzez Dodaj nowy komentarz (Add a New Comment).

Podgląd nagrań wideo z Pulpitu wiadomości (Playing archived video recordings from a Desktop Message list)

- 1 – Kliknij prawym przyciskiem na wideo, które chcesz wyświetlić. Zostanie wyświetlone menu kontekstowe.
- 2 – Jeżeli nagranie jest zapisane w EntraPass Video Vault, opcja Odtwórz z Vault (Play from Vault) będzie dostępna. Po jej wybraniu, wybrane nagranie zostanie odtworzone w nowym oknie.



Personalizacja wyświetlania zdarzeń w oknie zdarzeń (Customizing Event Display in the Message Desktops)

1 – Wybierz Właściwości (Properties) z menu skrótu (Pulpit wiadomości > kliknij prawym w wiadomość)

2 – Z okna Właściwości (Properties), wybierz żadaną opcję wyświetlania.

- Multi-line: zazwyczaj zdarzenia są wyświetlane w osobnych liniach. Możesz zwiększyć odległość między liniami, wybierając odpowiednią opcję.
- Wyświetl kolumny (Show columns): Możesz wybrać różne rodzaje identyfikatorów do wyświetlania przy zdarzeniach.
 - Rodzaj wiadomości (Message type): identyfikator określający rodzaj zdarzenia zostanie wyświetlony przy każdym wylistowanym zdarzeniu.
 - Obraz (Picture): system umieszcza identyfikator karty przy zdarzeniach zawierających taką informację.
 - Wiadomości fail-soft (Fail-soft messages): znak “+” zostaje wyświetlony przy zdarzeniach, które miały miejsce w momencie, gdy kontrolery były offline.
 - Wideo (Video): wyświetla na wybranym ekranie nagranie z serwera podłączonego do systemu.
 - Wyświetl konto (Display account): okno pulpitów wyświetla teraz kolumnę Konto (Account), ze zdarzeniami powiązanymi z danym kontem.
- Sekcja Różne (Miscellaneous) pozwala na używanie następujących opcji:
 - Zachowaj obraz karty (Keep card picture): system zachowuje obraz karty, aż do wystąpienia następnego zdarzenia z kartą.
 - Wyświetl pasek narzędzi (Display toolbar): wyświetla/ukrywa pasek narzędzi na górze ekranu Wiadomości.
 - Zdalne zapisywanie właściwości (Manual properties save only): po wybraniu tej opcji trzeba kliknąć przycisk Zapisz (Save), aby zapisać ustawienia oraz pozycję okna.
 - Wyświetl zaznaczone wiadomości (w pełni) (Display selected messages (full)): opcja dodaje nowe okno w oknie Wiadomości. Wyświetla ono wybrane zdarzenia wraz z pełnym opisem.
 - Wyświetl zdarzenia – pogrubione (Display events in bold): zwiększa czytelność wiadomości wyświetlonych w pulpitych EntraPass (lista Wiadomości, wyfiltrowane Wiadomości, Pulpity alarmu).



- o Ostatnia wiadomość na górze (Last Message on Top): domyślnie wiadomości są wyświetlane wstępująco. Można to zmienić poprzez tą opcję.
- o Opóźnienie auto-przewijania (mm:ss) (Auto-scroll delay (mm:ss)): po upływie określonego czasu lista wiadomości zacznie być przewijana. Domyślnie ta opcja jest włączona ze ustawionym opóźnieniem. Wyłączenie tej opcji oznacza, że użytkownik będzie musiał kliknąć Zaczynij Przewijanie (Restart Scroll), aby lista zaczęła się przewijać sama.
- Kolor tła wiadomości (Message background colour): umożliwia modyfikowanie koloru tła.
- Wyświetl kolor zdarzenia w osobnej kolumnie (Display event colour in separate column): kolory zdarzeń są wyświetlane w osobnej kolumnie.

Notatka: aby zmienić kolor czcionki w wiadomościach systemowych: System > Parametry zdarzeń.

Filtrowany pulpit zdarzeń (Filtered Messages Desktop)

Filtrowany pulpit zdarzeń (The Filtered Messages desktop) pozwala wyświetlić konkretne zdarzenia. Można np. wyświetlać zdarzenia powiązane z konkretnym kontrolerem lub z konkretnej bramki systemu. W takim przypadku te zdarzenia zostaną wyświetlone w Pulpicie Wyfiltrowanych Wiadomości. Filtry są definiowane w menu System > Filtry wiadomości.

Notatka: kiedy korzystasz z filtrów, system pobiera zdarzenia, które są już wyświetlone na Pulpicie wiadomości i filtruje te zdarzenia według wybranych kryteriów.

Konfigurowanie Pulpitu Wyfiltrowanych Wiadomości (Configuring a Filtered Messages Desktop)

- 1 – Z głównego okna Pulpitu wybierz pulpit, który chcesz konfigurować jak Filtrowany pulpit zdarzeń.
- 2 – Wybierz jego nazwę oraz określ typ pulpitu.
- 3 – Możesz zmienić filtr Tekstu (Text filter), aby wyświetlić konkretne zdarzenie.



Okna map (Graphic Desktop)

Okna map wyświetla graficzną lokalizację zgłoszonego alarmu (w przypadku, gdy grafika jest określona w systemie). Grafika odnosi się do zabezpieczonego obszaru systemu, w którym składniki znajdują się na połączeniu. Dzięki grafice, użytkownik bez problemu może sprawdzić dokładną lokalizację zainstalowanego komponentu, albo jego status.

W przypadku sytuacji alarmowej odpowiednie identyfikatory wskażą, czy wszyscy pracownicy opuścili już teren. Użytkownicy mogą wykonać zdalnie operacje bezpośrednio z wyświetlonego komponentu (np. zarygluj/odrygluj drzwi).

Podglądanie Grafiki w Oknie map (Viewing Graphics in the Graphic Desktop)

- 1 – Kliknij prawym klawiszem na pulpit, który chcesz konfigurować, jako graficzny, nazwij go i określ jego typ.
- 2 – Kliknij OK and GO, aby wyświetlić Okna map.
- 3 – Kliknij prawym przyciskiem w dowolne miejsce Pulpitu grafiki, po czym z menu wybierz grafikę, którą chcesz wyświetlić.

Notatka: jeżeli okno jest mniejsze niż wyświetlana grafika, możesz kliknąć i przeciągnąć grafikę wewnątrz Okna grafiki.

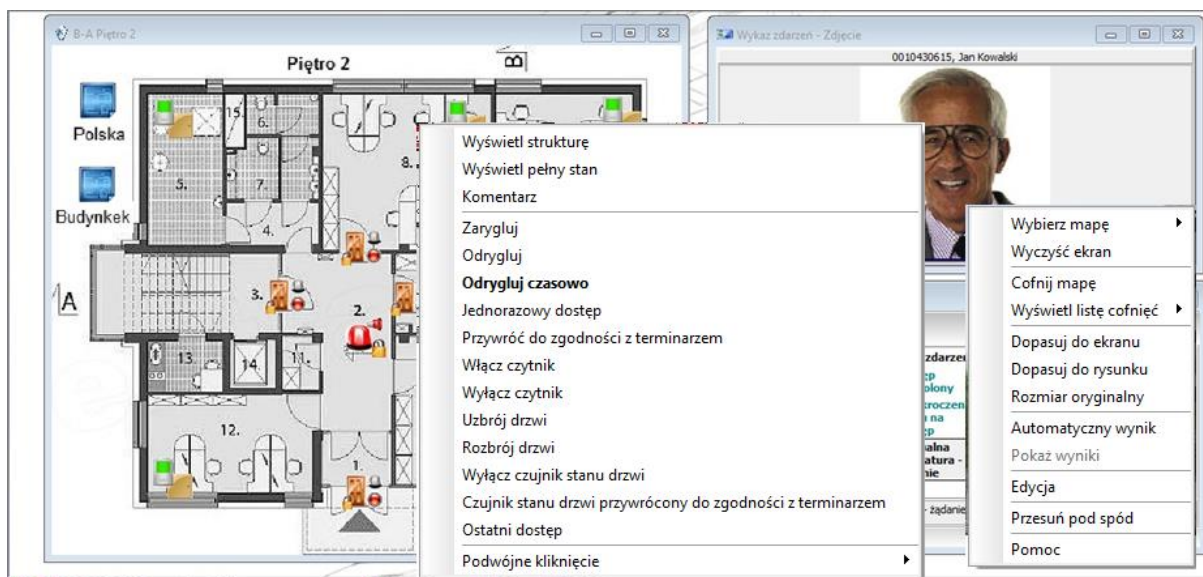
- 4 – Kliknij prawym przyciskiem w dowolne miejsce Pulpitu grafiki, aby wyświetlić menu do:

- zmienić rozmiar wyświetlonej grafiki
- wybrać Automatyczne wyświetlanie wyników (Auto result), aby system wyświetlił wiadomość wskazującą przyczynę utratę komunikacji w przypadku utraty komunikacji. Jeżeli opcja Automatycznego wyświetlania wyników nie jest wybrana, użytkownik musi zdalnie wydać polecenie wyświetlenia wyników poprzez Wyświetl wyniki (Show results)

- 5 – W przypadku zdarzenia kliknij prawym przyciskiem na komponent w celu wyświetlenia specjalnego menu.



EntraPass - Instrukcja instalacji i obsługi programu Pulpity



Notatka: Komponenty w stanie alarmu są reprezentowane przez animowane przyciski. Wybranie animowanego przycisku oraz podgląd komponentów pozwalają użytkownikowi na uzyskanie dodatkowych informacji na temat „przyczyn alarmu”.

6 – Wybierz Pełen status (Full status), aby wyświetlić pełną listę błędów powiązanych z jednym, lub ze wszystkimi komponentami.

7 – Wybierz Komentarz (Comment), aby wyświetlić komentarze przypisane do urządzenia.

8 – Wybierz (Double click), aby umożliwić użytkownikowi zmianę statusu komponentu w alarmie z poziomu Pulpitu grafiki. Na przykład, jeżeli podglądanym komponentem są drzwi, a w menu Double click była ustawiona opcja Odblokuj (Unlock), użytkownik może odblokować drzwi z Pulpitu grafiki.

Notatka: kiedy modyfikujesz opcję Podwójnego-kliknięcia poprzez Okna map system nie zachowuje modyfikacji. Modyfikuj domyślne ustawienia opcji Podwójnego-kliknięcia poprzez Definiowanie grafiki (Definiowanie > Grafika, Projektuj okno, kliknij prawym na komponent > obiekt menu Domyślnego podwójnego kliknięcia). W celu uzyskania informacji na temat tworzenia grafik oraz przypisywania komponentów do grafik zobacz Definiowanie grafiki.



Okno zdarzeń (Message List Desktop)

Domyślnie, pierwszy pulpit jest Oknem zdarzeń. Wyświetla wszystkie zdarzenia systemowe. Zdarzenia są wyświetlane za identyfikatorem, datą i czasem, opisem, składnikami (kontrolery, karty, etc.). Kiedy pojawia się nowe zdarzenie, okno przewija się do góry. Najnowsze zdarzenia są dodawane na dole okna.

Podgląd i sortowanie Zdarzeń Systemowych (Viewing and Sorting System Events)

Domyślnie, pierwszy pulpit jest przeznaczony do wyświetlania zdarzeń systemowych. Wybierając konkretne zdarzenie z listy, przerywasz sekwencje przychodzenia nowych zdarzeń (identyfikator statusu w dolnej lewej części ekranu zmienia kolor z zielonego na czerwony). Domyślnie, przewijanie rozpocznie się ponownie po określonym czasie, jeżeli auto przewijanie jest aktywne. W innym przypadku trzeba kliknąć Zaczynij Przewijanie (Restart Scroll).

Notatka: jeśli skonfigurujesz pulpit, jako ekran wiadomości oraz ekran obrazu, po wybraniu pulpitu zostaną wyświetlone dwa okna jednocześnie.

1 – Wybierz pierwszy pulpit. Domyślnie wszystkie zdarzenia są wyświetlone wstępująco.

Notatka: aby zmienić kolor czcionki w wiadomościach: System > Parametry zdarzeń.

2 – Z ekranu Okno zdarzeń możesz zmienić kryteria sortowania. Możesz wybrać z:

- Sekwencja (Sequence): domyślna. Nowe zdarzenia są dodawane na dole okna.
- Data i czas (Date and time): przerywa normalne przewijanie zdarzeń. To opcja jest przydatna, gdy chcesz wiedzieć, kiedy zdarzenie zostało wygenerowane. Czas może zmienić domyślną kolejność, np. w przypadku awarii prądu na stanowisku/obiekcie.
- Zdarzenie (Event): sortuje kolumnę Zdarzenia alfabetycznie, sortując ten sam typ zdarzeń ze sobą.
- Typ wiadomości (Message type): sortuje kolumnę Zdarzenia alfabetycznie, sortując podobny typ zdarzeń ze sobą.

Notatka: aby wrócić do domyślnego wyświetlania wybierz Sekwencja z rozwijanej listy Sekwencji.

3 – Klikając przycisk Filtr tekstu (Text filter) wyświetlisz pole Filtr tekstu. Możesz tam wprowadzić słowo klucz i tym samym wyświetlić wszystkie zdarzenia zawierające słowo klucz w Liście wiadomości. Aby uniknąć zbytniego obciążenia systemu zaznacz pole Zawieś odświeżanie (Suspend Refresh). Aby zamknąć pole Filtra tekstu, kliknij Anuluj (Cancel).

4 – Aby powrócić do normalnego wyświetlania zdarzeń na ekranie Okna zdarzeń kliknij przycisk Filtr tekstu.



Personalizacja wyświetlania zdarzeń w oknie zdarzeń (Customizing Event Display in the Message Desktops)

1 – Wybierz Właściwości (Properties) z menu skrótów (Pulpit wiadomości > kliknij prawym w wiadomość)

2 – Z okna Właściwości (Properties), wybierz żadaną opcję wyświetlania.

- Multi-line: zazwyczaj zdarzenia są wyświetlane w osobnych liniach. Możesz zwiększyć odległość między liniami, wybierając odpowiednią opcję.
- Wyświetl kolumny (Show columns): Możesz wybrać różne rodzaje identyfikatorów do wyświetlania przy zdarzeniach.
 - Rodzaj wiadomości (Message type): identyfikator określający rodzaj zdarzenia zostanie wyświetlony przy każdym wystawianym zdarzeniu.
 - Obraz (Picture): system umieszcza identyfikator karty przy zdarzeniach zawierających taką informację.
 - Wiadomości fail-soft (Fail-soft messages): znak “+” zostaje wyświetlony przy zdarzeniach, które miały miejsce w momencie, gdy kontrolery były offline.
 - Wideo (Video): wyświetla na wybranym ekranie nagranie z serwera podłączonego do systemu.
- Sekcja Różne (Miscellaneous) pozwala na używanie następujących opcji:
 - Zachowaj obraz karty (Keep card picture): system zachowuje obraz karty, aż do wystąpienia następnego zdarzenia z kartą.
 - Wyświetl pasek narzędzi (Display toolbar): wyświetla/ukrywa pasek narzędzi na górze ekranu Wiadomości.
 - Zdalne zapisywanie właściwości (Manual properties save only): po wybraniu tej opcji trzeba kliknąć przycisk Zapisz (Save), aby zapisać ustawienia oraz pozycję okna.
 - Wyświetl zaznaczone wiadomości (w pełni) (Display selected messages (full)): opcja dodaje nowe okno w oknie Wiadomości. Wyświetla ono wybrane zdarzenia wraz z pełnym opisem.
 - Wyświetl zdarzenia – pogrubione (Display events in bold): zwiększa czytelność wiadomości wyświetlonych w pulpitych EntraPass (lista Wiadomości, wyfiltrowane Wiadomości, Pulpity alarmu).
 - Ostatnia wiadomość na górze (Last Message on Top): domyślnie wiadomości są wyświetlane wstępująco. Można to zmienić poprzez tę opcję.
 - Opóźnienie auto-przewijania (mm:ss) (Auto-scroll delay (mm:ss)): po upływie określonego czasu lista wiadomości zacznie być przewijana. Domyślnie ta opcja jest włączona ze ustawionym opóźnieniem. Wyłączenie tej opcji oznacza, że użytkownik będzie musiał kliknąć Zaczynij Przewijanie (Restart Scroll), aby lista zaczęła się przewijać sama.
- Kolor tła wiadomości (Message background colour): umożliwia modyfikowanie koloru tła.

Notatka: aby zmienić kolor czcionki w wiadomościach: System > Parametry zdarzeń.



EntraPass - Instrukcja instalacji i obsługi programu Pulpity



Wiadomości Systemowe – zadania (Performing Tasks on System Messages)

EntraPass umożliwia wykonanie zadań na zdarzeniach systemowych. Np.:

- Usuwanie wiadomości
- Podgląd informacji karty
- Potwierdzanie status karty
- Modyfikowanie właściwości pulpitu
- Odtwarzanie, edytowanie oraz eksportowanie nagrań
- Odtwarzanie archiwalnych nagrań z EntraPass Video Vault

Notatka: niektóre zadania są przypisane do wybranego pulpitu. Na przykład, jeśli klikniesz prawym na zdarzenie alarmowe, menu skrótów wyświetli zadania, które są przypisane do zdarzeń alarmowych. Zobacz [Pulpit alarmów](#).

1 – Z Pulpitu wiadomości, kliknij prawym przyciskiem na zdarzenie, aby otworzyć menu.

2 – Wybierz jedną z opcji:

- Nowy filtr (New message filter): wyświetla pole Filtr wiadomości do zdefiniowania nowego filtra.
- Edytuj filtr (Edit message filter): wyświetla pole Filtr wiadomości do edytowania istniejących filtrów.
- Usuń wszystkie (Delete all): umożliwia usunięcie wszystkich wyświetlonych zdarzeń.
- Karta (Card): ta opcja przedstawia dwa wybory: Podgląd transakcji karty (View card transactions) oraz Wyszukiwanie karty (Search card). Wybranie pierwszego wyświetla wszystkie informacje związane z posiadaczem karty, który doprowadził do powstania zdarzenia. Druga opcja umożliwia przeszukiwanie bazy danych karty i wyświetlenia informacji o wszystkich numerach kart związanych z konkretnym posiadaczem karty. Z tego okna użytkownik może wykonać wiele operacji, np. podgląd i potwierdzenie informacji zawartych na karcie.
- Nagrania (Video recording): menu posiada trzy opcje: Odtwórz (Play), Odtwórz/Edytuj/Eksportuj (Play/Edit/Export) oraz Odtwórz z Video Vault (Play from Vault). Wybranie Odtwórz pozwala obejrzeć nagrane zdarzenie w oknie, umożliwiając wykonanie zrzutu i zachowanie go do wykorzystania w przyszłości. Wybranie Odtwórz/Edytuj/Eksportuj pozwala użytkownikowi na podobne czynności, jak w Liście Nagrań Zdarzeń (Video Event list). Wybranie Odtwórz z Video Vault odtwarza nagranie zapisane w EntraPass Video Vault.

Notatka: jeśli przyciski kamery nie są wyświetlone, po prostu kliknij prawym na wiadomości zdarzenia wideo. Z menu skrótów wybierz Właściwości i zaznacz Wideo w sekcji Pokaż przyciski.

- Pogląd Opiekuna (View parent): wyświetla opiekuna dla każdego komponentu powiązanego z wybranym zdarzeniem.



EntraPass - Instrukcja instalacji i obsługi programu Pulpity

- **Edytuj (edit):** Ta funkcja oferuje możliwość edycji każdego komponentu powiązanego z wybranym wydarzeniem. Jeśli Edycja jest zaznaczona, menu skrótów wyświetla komponenty powiązane z wybranym zdarzeniem. W tym przykład modyfikacja definicji połączenia dotyczy aplikacji EntraPass, operatora, który był na służbie, gdy wydarzenie zostało wygenerowane i połączenie związane z wydarzeniem. Teraz jest to możliwe aby edytować dowolny z trzech komponentów, wybierając go z menu skrótów. Jeśli wybrane zdarzenie jest zdarzenie dostępu i jeśli karta, która wyzwoliła zdarzenie, została już zarejestrowana w systemie, będzie być w stanie edytować kartę. Jeśli jednak karta jest powiązana z odmową dostępu - nieznana karta wydarzenie, karta zostanie utworzona i zarejestrowana w systemie.
- **Historia zmian**, wybierz jedną z następujących opcji:
 - o Aplikacja: wybierz tę opcję, aby otworzyć okno Historia zmian, aby zobaczyć, kto wprowadził zmiany i kiedy zmiany wystąpiły w komponencie.
 - o Operator: wybierz tę opcję, aby otworzyć okno kontroli, aby wyświetlić komponent operatora, który wygenerował zdarzenie wiadomości. Na przykład każda zmiana w systemie funkcji dla operatora, nazwy, bezpieczeństwa poziom i obszar roboczy. W przypadku braku modyfikacji wybranego komponentu opcja nie jest dostępny.
 - o Karta: wybierz tę opcję, aby otworzyć okno Audyt, aby zobaczyć, kto wprowadził zmiany i kiedy zmiany pojawiło się na karcie.
- **Odeślij do tyłu (Send to back):** opcja jest aktywna tylko w przypadku określenia typu okna, jako Ruchome (Floating). Przenosi ona aktywne okno za główne okno aplikacji. Aby przenieść Ruchome okno znowu na front, kliknij prawym przyciskiem na przycisk pulpitu i wybierz Przenieś na front (Bring to front).
- **Pomoc (Help):** wyświetla pomoc online.
- **Właściwości (Properties):** umożliwia użytkownikowi modyfikowanie właściwości wyświetlania dla wybranego pulpitu.



EntraPass - Instrukcja instalacji i obsługi programu Pulpity

Dodaj, Zmień albo Usuń oznaczone Zdarzenie (Add, Modify or Delete Tagged Events)

Możesz sprawdzić czy komponent został utworzony niedawno, zmieniany albo usunięty. Zdarzenia w bazie danych są oznakowane następująco:

- + Nowy (New)
- = Zmieniony (Modified)
- - Usunięty (Deleted)

	Data i czas	Opis zdarzenia	Szczegóły
	17.05.2017 14:16:40	Urządzenie IP - komunikacja przywrócona	KT-1, KT-1
	17.05.2017 14:14:51	Praca kontrolera w trybie autonomicznym	Kontrolery KT-1 #1
	17.05.2017 14:16:43	Praca kontrolera w trybie sieciowym	Kontrolery KT-1 #1
	17.05.2017 14:16:43	Kontroler - komunikacja przywrócona	Kontrolery KT-1 #1
	17.05.2017 14:16:43	Magistrala - komunikacja przywrócona	KT-1
	17.05.2017 14:15:07	Praca kontrolera w trybie autonomicznym	Kontrolery KT-400 #1
	17.05.2017 14:16:46	Praca kontrolera w trybie sieciowym	Kontrolery KT-400 #1
	17.05.2017 14:16:47	Kontroler - komunikacja przywrócona	Kontrolery KT-400 #1
	17.05.2017 14:16:47	Magistrala - problemy	KT-400
	17.05.2017 19:39:40	Start połączenia stacji operatora z serwerem	(1) Server Workstation
	17.05.2017 19:39:41	Start stacji operatora	(1) Server Workstation
	17.05.2017 19:42:07	Zalogowanie na stacji operatora	(1) Server Workstation, kantechpl, Currently login : 1
	17.05.2017 19:43:00	Server wideo - utrata komunikacji	REJ VIDEO #1

Zmiana zdarzeń na pulpicie (Changing Desktop Events)

Aby zmienić zdarzenia wyświetlane na liście komunikatów alarmowych, kliknij prawym przyciskiem myszy listę wiadomości i wybierz **Zdarzenia pulpitu**. Wybierz grupę zdarzeń, aby wyświetlić zdarzenia z tej grupy. Dla więcej informacji o grupach zdarzeń można znaleźć tutaj. Wybierz brak, aby zablokować wszystkie wiadomości. Inne opcje dostępne w tym menu są następujące:

- Wybierz **Wyświetl operatora**, aby wyświetlić wybór zdarzeń pulpitu dla zalogowanego operatora w tryb tylko do odczytu.
- Wybierz **Edytuj operatora**, aby zmodyfikować wybór zdarzenia pulpitu dla zalogowanego operatora.
- Wybierz **Przypisz operatora**, aby przypisać jedno lub więcej zdarzeń pulpitu innemu operatorowi.

UWAGA: Zmiany wprowadzone w zdarzeniach na pulpicie dotyczą tylko nowych zdarzeń. Istniejące wydarzenia na stronie lista pozostanie niezmieniona.



Okno zdjęć (Picture Desktop)

Jeżeli definiując Pulpit wiadomości (Message desktop) Ekran Obrazów (Picture Screen) zostanie on wyświetlony z oknem Obrazów. Zdarzenia dostępu (Access events) są wyświetlane wraz obrazem przedstawiającym kartę, jeżeli opcjach wyświetlania ustawiłeś odpowiednią właściwość (System > [Filtry wiadomości](#)).

Modyfikowanie opcji wyświetlania obrazów (Modifying Pictures Display Options)

1 – Z listy Wiadomości z Obrazami wybierz zdarzenie dostępu i kliknij prawym przyciskiem w obrazek karty.

Notatka: opcja Odeślij to tyłu (send to back) działa tylko wtedy, kiedy typ okna jest ustawiony na Ruchome. Wysyła aktywne okno (Okno obrazów) „za” główne okno Okna wiadomości. Aby przywrócić je na przód kliknij prawym na przycisk Wiadomości, a następnie wybierz Przenieś na przód z menu skrótów. Z Menu skrótów wybierz Właściwości.

2 – Z listy wybierz rozmiar wyświetlania obrazu:

- Rozmiar domyślny (Design size): obraz będzie wyświetlony w swoim oryginalnym rozmiarze.
- Rozciągnij (Stretch): obraz zostaje rozciągnięty bez zachowania proporcji.
- Współczynnik rozciągnięcia (Stretch ratio): obraz zostaje rozciągnięty do rozmiaru okna przy zachowaniu proporcji.

3 – Opcja Wyświetl wiele obrazów (Display multiple pictures) pozwala na jednoczesne wyświetlenie do czterech zdjęć.

4 – Wybierz Zastosuj dla wszystkich (Apply all the following items), aby przypisać parametry do wszystkich komórek.

5 – Wybierz informacje, która ma się wyświetlać wraz ze zdjęciem:

- Drzwi (Door): drzwi, przy których karta została pokazana, zostaną wyświetlone nad obrazem.
- Zdarzenie (Event): wiadomość powiązana ze zdarzeniem zostanie wyświetlona.
- Informacje o użytkowniku (User information): pole z informacjami o użytkowniku będzie wyświetlone nad obrazem.
- Komentarz (Comment): pod obrazem pojawia się pole komentarza (komentarz wprowadzony w trakcie definiowania karty pojawia się w tym polu).

Notatka: jeśli drzwi są przypisane do komórki (zdjęcia) oraz opcja Drzwi jest wybrana (Wyświetl zaznaczone pola) nazwa tych drzwi będzie wyświetlona na niebiesko, zamiast na czarno.



Personalizacja Pulpitu (Specific Desktop Customizing)

EntraPass umożliwia użytkownikowi z odpowiednimi uprawnieniami dostosowywanie swojego pulpitu. Ponadto, użytkownicy z pełnymi uprawnieniami mogą umożliwić takie dostosowywanie użytkownikom bez wymaganych uprawnień. Mogą dostosować dowolny pulpit i przetransferować go do innego użytkownika. Poniżej znajduje się wyjaśnienie jak dostosowywać pulpit.

- Dostosowanie pulpitu przez użytkownika z pełnymi uprawnieniami.
- Dostosowanie pulpitu przez użytkownika z ograniczonymi (tylko do odczytu) uprawnieniami.
- Transferowanie dostosowanego pulpitu.

Dostosowanie pulpitu przez operatora z pełnymi uprawnieniami (Customizing a Desktop for a "Full Access" Operator)

Operatorzy z pełnymi uprawnieniami mają możliwość dostosowywania pulpitu. Aby dać pełne uprawnienia operatorowi musisz (System > Poziom bezpieczeństwa):

1 – Wybierz pulpit do dostosowania, kliknij prawym i wybierz Właściwości (Properties).

2 – Nazwij wybrany przez siebie pulpit.

3 – Wybierz typ okna:

- Ruchome okno (Floating window): ruchome okno może mieć zmieniony rozmiar oraz być umieszczone w dowolnym obszarze ekranu roboczego. Można je wysłać do tyłu oraz przywrócić.
- Okno pulpitu (Desktop window): okno pulpitu jest przypisane do ekranu roboczego. Nie można go wysłać do tyłu, zawsze pozostaje w głównym obszarze roboczym.

4 – Aby zapisać zmiany:

- Kliknij OK: zapisuje bez wyświetlania okna.
- Kliknij OK and GO: zapisuje i wyświetla skonfigurowane okno.

Notatka: przy pierwszym otworzeniu okna pulpitu może zaistnieć potrzeba zmiany rozmiaru okna, aby wszystkie informacje wyświetliły się prawidłowo. Aby to zrobić najedź na krawędź ekranu i po zmianie ikony na podwójną strzałkę zwiększ rozmiar okna. Możesz przenieść okno w polu roboczym w dowolne miejsce.



Dostosowanie pulpitu przez operatora z ograniczonymi (tylko do odczytu) uprawnieniami (Customizing a Desktop for a "Read-Only" Operator)

Menadżer do spraw bezpieczeństwa, albo operator z odpowiednimi uprawnieniami, może dać operatorom z ograniczonymi uprawnieniami zgodę na personalizację pulpitu w trakcie danej sesji.

- 1 – Zaloguj się przy wykorzystaniu nazwy oraz hasła użytkownika z pełnymi uprawnieniami.
- 2 – Wybierz pulpit do dostosowania, kliknij prawym i wybierz Właściwości (Properties).

Notatka: przycisk Pozwól (Permit) wyświetla się, kiedy użytkownik, który jest zalogowany posiada dostęp „wyłącznie do odczytu”. Pozwolenie otrzymane w tej sesji będzie ważne aż do momentu wylogowania się użytkownika. Kliknij przycisk Pozwól (Permit). Pojawi się okno logowania. Wprowadź swoją nazwę użytkownika oraz hasło, następnie kliknij OK. Czasowy dostęp został przyznany.

Transfer ustawień pulpitu (Transferring a Customized Desktop)

Inną możliwością jest dostosowanie pulpitu przez użytkownika z pełnymi uprawnieniami, a następnie przesłanie go i przypisanie do użytkownika z ograniczonymi uprawnieniami.

- 1 – Klikając prawym przyciskiem wybierz pulpit, do którego chcesz przypisać ustawienia.
- 2 – Wybierz Przypisz (Assign) z menu.
- 3 – Z wyświetlonego okna wybierz użytkownika/użytkowników, do których chcesz przypisać nowe właściwości pulpitu.



Kolory Pulpitów (Desktops Colors)

Event colors can now be displayed in a separate column. Text and message background colors can also be selected.

1 – Z dowolnego pulpitu wiadomości, kliknij prawym przyciskiem na wiadomość i wybierz Właściwości (Properties).

2 – Z listy wybierz kolor.

3 – W razie potrzeby wybierz Wyświetl kolor w osobnej kolumnie (Display event color in separate column).

4 – Z drugiej listy wybierz kolor tekstu.



Transferowanie dostosowanego pulpitu (Transferring a Customized Desktop)

Inną możliwością jest dostosowanie pulpitu przez użytkownika z pełnymi uprawnieniami, a następnie przesłanie go i przypisanie do użytkownika z ograniczonymi uprawnieniami.

1 – Klikając prawym przyciskiem wybierz pulpit, do którego chcesz przypisać ustawienia.

2 – Wybierz Przypisz (Assign) z menu.

3 – Z wyświetlonego okna wybierz użytkownika/użytkowników, do których chcesz przypisać nowe właściwości pulpitu.

4 – Right-click the desktop you want to assign the settings.

5 – Wybierz Przypisz (Assign) z menu.

6 – Z wyświetlonego okna wybierz użytkownika/użytkowników, do których chcesz przypisać nowe właściwości pulpitu.



Status

Status aplikacji

Status aplikacji (Application Status)

Status aplikacji wyświetla informacje na temat wybranej aplikacji, takie jak: nazwa użytkownika, numer identyfikacyjny, etc. Jest również wykorzystywany do weryfikowania czy aplikacja EntraPass jest podłączona do serwera.

1 – W oknie Status, wybierz Aplikacja (Application). Okno Statusu aplikacji zostanie wyświetlone.

- Lista zawiera wszystkie aplikacje wylistowane razem lub oddzielnie. Możesz wybrać wszystkie połączenia (All connections), albo konkretną bramkę i sprawdzić szczegóły połączenia dla wybranej/wybranych aplikacji.

2 – Kliknij znak “+” aby zobaczyć szczegółowe informacje na temat aplikacji.

- Czerwony symbol oznacza, że aplikacja EntraPass nie jest podłączona do serwera.
- Zielony symbol oznacza, że aplikacja EntraPass jest podłączona do serwera
- Protokół (Protocol) – identyfikuje język wykorzystywany do komunikowania się z serwerem. Protokół informuje system w jaki sposób informacje są przekazywane pomiędzy komputerami.
- Identyfikacja sieci (Network identification) – zapewnia adres IP dla aplikacji w sieci albo nazwę NetBEUI.
- Nazwa operatora (Operator name) – wyświetla nazwę operatora obecnie zalogowanego do aplikacji. Nazwa użytkownika jest wykorzystywana w wielu celach, takich jak ustalenie, kto dokonał modyfikacji karty, kto potwierdził alarm, etc.
- Data ostatniego zapytania (Last query date) – wyświetla czas, kiedy aplikacja po raz ostatni komunikowała się z serwerem. Serwer i aplikacja wymieniają informacje regularnie.
- Data połączenia (Connected date) – wyświetla datę i czas, w których aplikacja połączyła się z serwerem. Ta data zostanie wykorzystana przy utworzeniu wydarzenia i zarchiwizowana.
- Transakcje (Transactions) – wyświetla liczbę zapytań od aplikacji (liczbę wymian z serwerem), np. zapytanie raportowe.
- Błędy (Errors) – wyświetla liczbę błędów na które natrafiła aplikacja. Pole zostanie zresetowane po wyłączeniu się aplikacji.
- Zbuforowane wiadomości / alarmy (0/1) (Messages/Alarms buffered (0/1))

o 0: liczba zbuforowanych wiadomości / alarmów dla aplikacji, kiedy aplikacja jest off-line. Liczba zostanie zresetowana do „0”, gdy aplikacja połączy się z serwerem.

o 1: liczba zbuforowanych wiadomości / alarmów, które zostały wysłane do aplikacji od momentu uruchomienia serwera. Liczba zostanie zresetowana w momencie wyłączenia serwera.

Notatka: serwer przechowuje maksimum 100,000 wiadomości oraz 100,000 alarmów na stację (domyślnie: 5000) w buforze. Możesz modyfikować te ustawienia przez menu Definiowanie stacji roboczej. Możesz również określić czy buforowane mają być starsze czy nowsze zdarzenia. Zdarzenia będą buforowane wyłączenie wtedy, kiedy stacja robocza jest offline (niepodłączona do serwera); oraz kiedy pola Wprowadź parametry operatora dla wiadomości (Apply operator parameters for messages) i Wprowadź parametry operatora dla alarmów (Apply operator parameters for alarms) nie są zaznaczone.



Status tekstowy (Text Status)

Pozwala użytkownikowi wyświetlić status wybranego komponentu oraz cechy powiązane z komponentem w formie tekstu. Okno zawiera dodatkowe przyciski, które pomagają użytkownikowi:

- Pierwsze siedem przycisków przedstawia urządzenia systemowe.
- Podsumowanie / Lista szczegółowa (Summary / Detailed list): przycisk Szklą powiększającego jest używany do wyświetlenia komponentów, które nie są w stanie normalnym. Wyświetla podsumowanie albo szczegółową listę.
 - o Podsumowanie (Summary): wyświetla komponenty, które nie są w stanie normalnym
 - o Szczegół (Detail): pokazuje wszystkie komponenty, niezależnie od stanu.
- Przerwij wyświetlanie (Stop display) – pozwala przerwać wyświetlanie, jeżeli proces pozyskania informacji trwa zbyt długo. Anuluje lub przerywa proces.
- Odśwież (Refresh) – odświeża status wybranego komponentu.
- Drukuj (Print) – drukuje wyświetlony status. Możliwe jest podejrzenie raportu przed wydrukiem.

Wyświetlanie statusu komponentu

- 1 - Na karcie Stan wybierz przycisk Status tekstu. Zostanie wyświetlone okno Tekst.
- 2 - W oknie Tekst wybierz przycisk komponentu, dla którego chcesz wyświetlić status. Jeśli ty wybierz przycisk Stacja robocza, system wyświetli listę aplikacji EntraPass zdefiniowanych w system
- 3 - Możesz sprawdzić aplikację EntraPass, której status chcesz wyświetlić, lub wprowadzić kilka znaków nazwa komponentu (pole u góry), aby system mógł wyszukiwać w bazie danych. Na przykład możesz wejść „Sec” dla Biura Bezpieczeństwa. System podświetli imię zawierające wprowadzone znaki. Ty może również kliknąć przycisk Wybierz wszystko, aby wybrać wszystkie aplikacje EntraPass; lub wybierz określone komponenty klikając pola wyboru obok nazwy każdego składnika. Przycisk Wyczyść wszystko usuwa czek
- znaki z wybranych komponentów. Kliknij Anuluj, aby powrócić do poprzedniego okna bez żadnego selekcje lub zmiany.
- 4 - Możesz zaznaczyć opcję Wyświetl podskładniki (dolna część okna), aby wyświetlić szczegóły informacje o podzespołach powiązanych z wybranym komponentem. Na przykład, jeśli wybrałeś akontroler, wszystkie jego komponenty (drzwi, przekaźniki, wejścia) o odpowiednim statusie będą wyświetlane na okno, jeśli ta opcja została zaznaczona. Aby uzyskać więcej ostrości w jednym oknie, filtruj drzwi, przekaźniki lub wejścia przez połączenie.
- 5 - Kliknij OK, aby powrócić do poprzedniego okna i zastosować wybrane opcje.

UWAGA: Przycisk lupy służy do wyświetlania elementów, które nie są w normalnym stanie.

Gdy znajduje się w pozycji „podsumowania”, będą tylko komponenty, które nie są w normalnym stanie wystawiany; pozycja „szczegółowa” wyświetla pełny status wszystkich komponentów.



Status liczbowy (numerical status)

To menu pozwala użytkownikowi sprawdzić liczbę komponentów w „nieprawidłowym” stanie dla wybranej bramki.

1 – W zakładce Status wybierz Status numeryczny. Okno Numeryczne zostanie wyświetlone.

2 – Z listy wybierz bramkę, dla której chcesz wyświetlić status. Okno wyświetli liczbę kart dla danej bramki, liczbę wejść w alarmie, liczbę przekaźników aktywowanych ręcznie, liczbę wymuszonego otwarcia drzwi, etc.



EntraPass - Instrukcja instalacji i obsługi programu Status

Status w postaci graficznej (Graphic Status)

Ta opcja jest wykorzystywana do wyświetlenia graficznego statusu kontrolera drzwi, jak i statusów wszystkich jego komponentów, poprzez kolorowe figury:

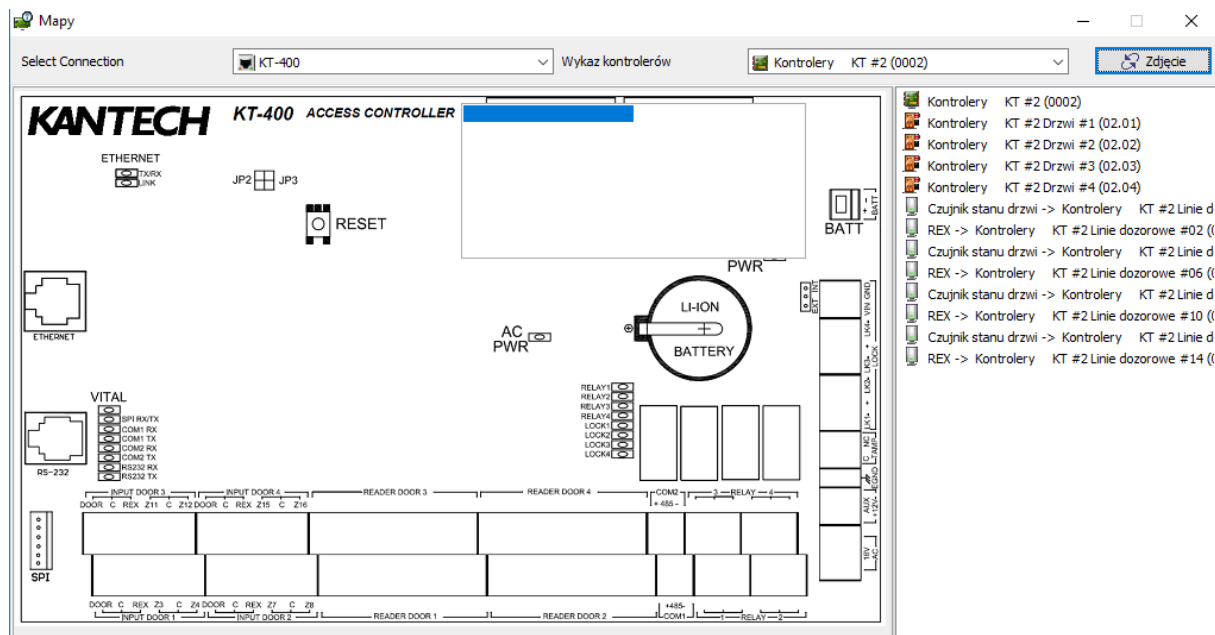
- Elipsa – kontroler.
- Okrąg – drzwi.
- Kwadrat – przekaźnik.
- Prostokąt – wejście. Mogą być poziome (KT-200, KT-300) lub pionowe (KT-100).

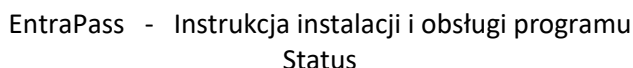
Pogląd Statusu kontrolera (Viewing a Controller Status)

1 – Z listy bramek wybierz bramkę, na której znajduje się kontroler. Możesz wybrać Wybierz wszystkie (All gateways), aby wyświetlić wszystkie kontrolery.

2 – Wybierz kontroler, dla którego chcesz wyświetlić status.

Przykład kontrolera KT-200 (Example with a KT-200 Controller)





The screenshot shows the KANTech software interface for configuring a KT-400 control unit. The main window displays a detailed wiring diagram of the device, including components like the Lithium Battery, Reset button, DC Power, AC Power, and various communication ports (RJ45, RS-485, RS-232). A central information box provides details for the selected unit (KT-400 (0001)), such as its serial number, version, MAC address, IP address, and memory usage.

KANTech	
Numer seryjny kontrolera	17299129
Kontroler - wersja	02.03.09
Kontroler - suma kontrolna program	0x06511111
Adres MAC	00:50:F9:56:A0:E2
IP adres - Ethernet 1	10.11.15.123
Maska podsieci Ethernet 1	255.255.0.0
Kontroler - karty razem	7
Pamięć używana	11,92 Magabajt
Pamięć całkowita	73,17 Magabajt

On the right side, a legend lists the connected devices:

- KT 400 (0001)
- KT 400 Drzwi #1 [01.01]
- KT 400 Drzwi #2 [01.02]
- KT 400 Drzwi #3 [01.03]
- KT 400 Drzwi #4 [01.04]
- kt-400 Przekaznik #1 [01.001]
- Awarijne otwieranie wszystkich drzwi [01.002]
- IoSmart -> KT 400 Drzwi #4 -> I2O Przekaznik [01.]
- IoSmart -> KT 400 Drzwi #1 -> I2O Przekaznik [01.]
- IoSmart -> KT 400 Drzwi #2 -> I2O Przekaznik [01.]
- Czujnik stanu drzwi -> Kontrolery KT #1 Linie d
- Czujnik stanu drzwi -> Kontrolery KT #1 Linie d

3 – Aby sprawdzić, które komponenty są przedstawione przez które kształty przesun kursor nad wybrany kształt. Komponent podświetlony po prawej stronie identyfikuje komponent.

- Czerwony – komponent jest “Nadzorowany” (Supervised) oraz “w stanie alarmowym” (in a trouble state).
- Zielony — komponent jest “Nadzorowany” (Supervised) oraz “w normalnym stanie” (in normal condition).
- Żółty — komponent jest “Nienadzorowany” (Not Supervised) oraz “w stanie alarmowym” (in a trouble state).
- Szary — komponent jest “Nienadzorowany” oraz “w normalnym stanie” (in normal condition).
- Niebieski — przekaźnik jest aktywny.

Notatka: jeśli występuje więcej niż jedno połączenie kontrolera na bramkę, cyfry pomiędzy wtrąceniami (xx) oznaczają numer kontrolera, a następne cyfry (xx) oznaczają numer komponentu.



Status bazy danych (Database Status)

Okno wyświetla status komponentów wewnątrz bazy danych w trakcie przeglądania struktur bazy danych. System wyświetla wszystkie aplikacje (połączone i nie), bramki, kontrolery, etc.

Możesz także przeprowadzać zdalne operacje bezpośrednio z okna i edytować komponenty w celu zmiany ich konfiguracji.

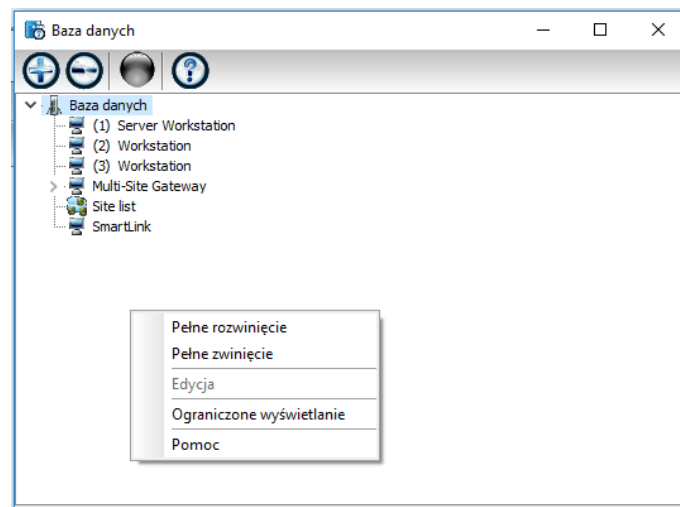
1 – Z okna Status kliknij przycisk Baza danych (Database). Pojawi się okno bazy danych.

Notatka: przycisk identyfikuje typ komponentu.

2 – W oknie bazy danych wybierz aplikację, której bazę chcesz sprawdzić. W dolnej części okna jest wyświetlany aktualny status wybranego komponentu oraz jego pełna nazwa.

3 – Wybierz komponent do modyfikowania bezpośrednio z Okna bazy danych klikając prawym przyciskiem, aby wyświetlić menu.

4 – Wybierz polecenie z menu.



Notatka: lista poleceń różni się zależnie od wybranego komponentu.

5 – Menu oferuje następujące opcje:



EntraPass - Instrukcja instalacji i obsługi programu Status

- Rozwiń wszystko (Full expand) – pozwala w pełni rozwinąć drzewo statusów i sprawdzić wszystkie komponenty. Tylko aplikacje podłączone do serwera będą miały znak „+”.
- Zwiń wszystko (Full collapse) – pozwala zwinąć drzewko statusów oraz ukryć wszystkie komponenty.
- Edytuj (Edit) – po wybraniu komponentu pojawi się okno definicji.
- Ograniczone / nieograniczone wyświetlanie (Limited display / No limited display) – dolna część okna wyświetla status.
- Po wybraniu Ograniczonego wyświetlania (Limited display) system usunie poprzedni status i wyświetli status następnego komponentu.

Notatka: przyciski po lewej stronie komponentów wskazują na typ komponentów

Stan serwera Video (Video Server Status)

EntraPass oferuje możliwość wyświetlania parametrów urządzeń wideo podłączonych do serwera wideo.

Operatorzy mogą na przykład przeglądać informacje związane z przesyłaniem danych sieciowych (obrazy i dźwięki cyfrowe).

UWAGA: Instalacja i korzystanie z funkcji wideo może wymagać dużej ilości sieci firmowej przepustowość (LAN lub WAN). Administrator sieci może kontrolować wykorzystanie przepustowości sieci do przesyłania wideo.

Wyświetlanie pełnego statusu serwera wideo

1 - W oknie Pulpit graficzny kliknij prawym przyciskiem myszy przycisk Serwer wideo, aby wyświetlić menu skrótów.

2 - Z menu skrótów wybierz Pełny status, aby wyświetlić informacje o stanie serwera wideo.

UWAGA: Zawartość okna pełnego stanu zależy od serwera wideo powiązanego z EntraPass.



EntraPass - Instrukcja instalacji i obsługi programu
Status

Poniższa lista zawiera krótki opis wyświetlanych pól.

Opis	
Nazwa jednostki	Nazwa sieciowa zdalnego systemu DVMS (w tym przykładzie Intellex). Po nazwie jednostki następuje adres IP rejestratora.
Typ jednostki	Typ urządzenia. może być Intellex, Iris (klient sieciowy) itp.
Tryb harmonogramu	Bieżący tryb harmonogramu zdalnego urządzenia DVMS. Wskazuje, jak obrazy są rejestrowane przez instalację DVR. Wartości dla tego pola mogą być: Regular (regularny rozkład) Pojedynczy (tylko jedna kamera) Niestandardowy (niestandardowy harmonogram został ustawiony przez operatora).
Postęp nagrywania	Aktywny stan nagrywania zdalnego urządzenia DVMS. Wartości mogą być: Prawda: nagrywa Fałsz: jest zatrzymane.
Okres czasu (h:mm)	Przedział czasu (w sekundach) między najstarszymi i najnowszymi obrazami w bazie danych.
Wersja jednostki	Oficjalna wersja jednostki DVMS.
Liczba kamer	Liczba kamer podłączonych do serwera wideo. Źródło danych wideo to zazwyczaj kamera, ale może to być także stacja telewizyjna lub inne źródło wideo. Wartość waha się od 0 do 16.
Tryb zapisu	Tryb zapisu może być liniowy lub ciągły (liniowy: jeśli wybierzesz to opcja, nagrywanie będzie kontynuowane nieprzerwanie aż skończy się miejsce; Ciągły: jeśli wybierzesz tę opcję, DVR powiadomi operatorów zanim przestrzeń nagrywania zostanie całkowicie wypełniona. Operator wybierze czy kontynuuje nagrywanie lub zatrzyma je. Domyślnie nagrywanie tryb jest ustawiony na Ciągły.
Tryb nagrywania	Standard nagrywania zdalnego urządzenia. Standard nagrywania zależy od obszaru. Wartości mogą być następujące: NTSC: standard NTSC jest głównie używane w Ameryce i wielu krajach azjatyckich, takich jak Japonia i Południowa Korea lub PAL: standard PAL jest stosowany głównie w Niemczech, Wielkiej Brytanii, Chiny, Australia i Brazylia.
Szacowany pozostały nagrywania	Szacowana liczba klatek, które mogą być jeszcze nagrane w bazie danych zanim przestrzeń jednostki DVMS zostanie całkowicie wypełniona. Ta opcja jest przydatna tylko wtedy, gdy tryb nagrywania jest liniowy.
Wersja interfejsu	Wskazuje wersję interfejsu aplikacji między EntraPass i wybranym serwerem wideo.
Liczba audio	Liczba dostępnych strumieni audio serwera wideo. Źródło danych audio jest zazwyczaj mikrofonem, ale może być innym dźwiękiem.
Liczba klatek	Wartość kodu stawki. Ta wartość wskazuje łączną szybkość rejestracji dla urządzenia DVR w liczbie klatek na sekundę. Wartość może wynosić: 1, 2,5, 7,5, 15, 30, 60, 120, inna wartość.
Liczba obrazów	Całkowita liczba obrazów w bazie danych jednostki zdalnej
Kompatybilność wersji	Kompatybilność między wersjami urządzenia DVR a aplikacją używanego interfejsu
Numer tekstów	Liczba strumieni danych tekstowych dostępnych w DVMS. Dane tekstowe źródłem może być kasa fiskalna lub inne urządzenie.



EntraPass - Instrukcja instalacji i obsługi programu Status



EntraPass - Instrukcja instalacji i obsługi programu Status

Stan serwera (Server State)

Stan serwera pozwala użytkownikowi sprawdzić szczegółowe informacje na serwerze, takie jak: informacje o systemie, pamięć ogólna systemu, pamięć operacyjna systemu, pojemność dyskowa systemu.

- Przycisk logów systemu (System log button): kliknij, aby wyświetlić logi systemu.

System
Liczba wątków : 49

Pamięć
Całkowita pamięć : 3,91 G
Dostępna pamięć : 1,50 G
Procent zajętości pamięci : 61,37%
Cała pamięć wirtualna : 4,0 G
Dostępna pamięć wirtualna : 1,50 G

Przetwarzanie
Strona licznika błędów : 77
Rozmiar roboczy maks. : 1,0 G
Bieżący ustawiony rozmiar : 1,0 G

Pojemność
Wolne miejsce na dysku : 9,0 G
Całkowita pojemn. dysku : 4,0 G

Zdarzenia w systemie

Archival report log

Filtr tekstowy Odśwież

Date requested	Na ządanie	Nazwa raportu	Date from	Do daty
28.11.2016 20:53:20	(kantech) Installer	All events	28.11.2016	28.11.2016 20:53:09
28.11.2016 20:55:59	(kantech) Installer	All events	28.11.2016	28.11.2016 20:55:36
01.02.2017 08:24:28	(kantech) Installer	All events	01.02.2017	01.02.2017 23:59:59
01.02.2017 08:25:56	(kantech) Installer	All events	01.02.2017	01.02.2017 23:59:59
01.02.2017 08:26:47	(kantech) Installer	All events	01.02.2017	01.02.2017 23:59:59
01.02.2017 08:34:01	(kantech) Installer	All events	01.02.2017	01.02.2017 23:59:59
01.02.2017 08:44:54	(kantech) Installer	All events	01.02.2017	01.02.2017 23:59:59
01.02.2017 08:46:40	(kantech) Installer	All events	01.02.2017	01.02.2017 23:59:59
15.02.2017 15:30:39	(kantechpl) kantechpl	Zdarzenia dot. dostępu	15.02.2017	15.02.2017 23:59:59
17.05.2017 12:43:54	(kantechpl) kantechpl	Wszytkie zdarzenia	17.05.2017	17.05.2017 23:59:59

Typ raportu: Szybki raport Requested date: 17.05.2017 12:43:54
Process by: Główny Serwer Queued date: 17.05.2017 12:43:54
Workspace applied: All Process date: 17.05.2017 12:43:54 (00:00:02)
Kierunek: (1) Server Workstation Delivery date: 17.05.2017 12:43:57
Used template: Wyświetl na ekranie Completion date: 17.05.2017 12:43:54
Pozycj w raporcie: 231 Completion state: Pomyślnie zakończone

- Przycisk Błędy w systemie (Error log button): kliknij, aby wyświetlić błędny log.

System
Liczba wątków : 49

Pamięć
Całkowita pamięć : 3,91 G
Dostępna pamięć : 1,50 G
Procent zajętości pamięci : 61,37%
Cała pamięć wirtualna : 4,0 G
Dostępna pamięć wirtualna : 1,50 G

Przetwarzanie
Strona licznika błędów : 77
Rozmiar roboczy maks. : 1,0 G
Bieżący ustawiony rozmiar : 1,0 G

Pojemność
Wolne miejsce na dysku : 9,0 G
Całkowita pojemn. dysku : 4,0 G

Zdarzenia w systemie

Błędy w systemie

Filtr tekstowy Odśwież

Data i czas	Konto	Kod	Stacja operatora	Błąd	Opis
29.11.2016 12:00:53			Multi-Site Gateway	Authentication denied - workstation locked	

View Comments View Error Log

Filtr tekstowy



Logowanie (Logins)

Ta opcja pozwala sprawdzić ilu operatorów jest aktualnie zalogowanych do systemu dla każdej aplikacji.

Aby uzyskać dostęp do Logowania, kliknij przycisk Logowania (Logins) na pasku narzędzi Status. Okno, które się wyświetli zawiera następujące kolumny:

- Aplikacja EntraPass: nazwa aplikacji, w której jest zalogowany użytkownik.
- SmartLink: nazwa aplikacji (EntraPass Web albo EntraPass Go), w której jest zalogowany użytkownik
- Nazwa operatora (Operator name)
- Login
- Zalogowany od (Login since): data oraz czas, od kiedy użytkownik jest zalogowany.

Notatka: możesz korzystać z filtrów dla kolumn: EntraPass, Konto, Smartlink; poprzez najechanie kursorem na tytuł kolumny i kliknięcie strzałki, która zostanie wtedy wyświetlona.

Notatka: na dole okna możesz sprawdzić łączną liczbę zalogowanych użytkowników.

Notatka: kiedy użytkownik się zaloguje, liczba określająca ilość użytkowników zalogowanych do systemu jest wyświetlona w kolumnie szczegółów zdarzenia (Pulpit wiadomości).

Notatka: Pod Poziom bezpieczeństwa/Stacja robocza/Status znajdziesz opcję, która pozwala przyznać/odebrać dostęp do przycisku Login.

Notatka: możesz zmusić innego użytkownika do wylogowania się. Kliknij prawym na użytkowniku i wybierz Wymuś logout. Aby nie pozwolić mu zalogować się od nowa, wybierz Wymuś logout i wyłącz operatora (Force logout and Disable operator)

Wyświetlania statusu komponentu (Displaying a Component Status)

1 – Z zakładki Status kliknij przycisk Status tekstowy. Pojawi się okno Tekst.

2 – W oknie Tekst wybierz przycisk komponentu, którego status chcesz wyświetlić. Jeżeli wybierzesz przycisk Stacji roboczej (Workstation), system wyświetli listę aplikacji EntraPass zdefiniowanych w systemie.

3 – Możesz zaznaczyć aplikację EntraPass, której status chcesz wyświetlić albo wprowadzić część nazwy komponentu (pole wyszukiwania znajduje się na górze), aby system sam przeszukał bazę danych. Dla przykładu wpisując „Sec” wyszuka się Security Office. System zaznaczy pierwszą nazwę zawierającą wyszukiwane hasło. Możesz również zaznaczyć wszystkie aplikacje Entrapass przy pomocy przycisku Select all; albo wybierać konkretne poprzez zaznaczanie pól przy nazwach komponentów. Przycisk Clear all odznacza wszystkie wybrane komponenty. Naciśnij Anuluj (Cancel), aby powrócić do wcześniejszego okna bez wprowadzenia żadnych zmian.

4 – Możesz wybrać opcję Podgląd podkomponentów, aby wyświetlić informacje o podkomponentach przypisanych do wybranego komponentu.

5 – Kliknij OK, aby powrócić do wcześniejszego okna i zapisać wprowadzone zmiany.

Notatka: przycisk Szklą powiększającego służy do wyświetlenia komponentów, które nie znajdują się w normalnym stanie. W pozycji „podsumowanie” zostaną wyświetlone tylko komponenty w stanie odbiegającym od normalnego; w pozycji „szczegół” wyświetlane są pełne statusy komponentów.



EntraPass - Instrukcja instalacji i obsługi programu Status



Operacje

Operacje dotyczące kontrolerów

Operacje na Bramce GSI (Manual Operations on Gateway)

Ręczne operacje na bramce umożliwiają operatorom komunikację z bramami w celu odświeżenia i przeładowania danych bramki.

Ikona	Definicja
	Zresetuj gniazda TCP i UDP: zwalnia gniazda komunikacyjne kontrolera TCP i UDP, a następnie odtwarza je.
	Przeładuj bramkę GSI: usuwa zawartość bazy danych bramki, ponownie uruchamia bramę i ponownie ładuje dane z bazy danych systemu. Przeładowanie jest dostępne na bramkach CE, GE i KT-NCC.

Uwaga...

Wskazówka jest wyświetlana po przesunięciu kursora nad przyciskiem. Podaje szczegółowe informacje na temat wykonywanej operacji.

Wybór bramki GSI

1 - Na stacji roboczej EntraPass kliknij kartę **Operacje**, a następnie kliknij opcję Bramka GSI z menu.

Zostanie wyświetlone okno bramki i lista wszystkich bram podłączonych do systemu.

2 - Aby wyświetlić statystyki bramki, wskaż żądaną bramę z wieloma lokalizacjami i kliknij dwukrotnie.

Wyświetlanie statystyk bramki GSI

Okno stanu bramki przedstawia bieżące statystyki bramki, w tym następujące szczegóły:

- Stan połączenia
- Liczba kart
- Liczba wątków
- Liczba oczekujących wiadomości
- Wersja
- Liczba lokalizacji
- Liczba lokalizacji Ok
- Liczba lokalizacji z usterkami
- Całkowita pamięć
- Dostępna pamięć
- Dostępna pamięć wirtualna
- Czas lokalny
- Ostatnie uruchomienie



Uwaga:

Kiedy definiujesz połączenia modemowe na bramie, musisz ręcznie sprawdzić ich status online jako EntraPass nie pokazuje połączeń modemowych w oknie stanu bramy w polu **Numer lokalizacji Ok** lub Liczba lokalizacji z usterkami. Liczba lokalizacji Ok oznacza liczbę, z którymi pomyślnie nawiązano połączenie szerokopasmowe na bramie, połączenia modemowe nie są liczone. Liczba lokalizacji z usterkami reprezentuje liczbę połączeń, których nie udało się połączyć za pomocą połączeń szerokopasmowych na bramie, modemie połączenia nie są liczone. Liczba lokalizacji reprezentuje liczbę połączeń zdefiniowanych w bramie.

Wykonywanie twardego resetu

Uwaga...

Wykonuj polecenia resetowania ostrożnie. Przed wykonaniem operacji resetowania sterownika zalecamy skontaktowanie się z naszym działem pomocy technicznej. Aby uzyskać więcej informacji, zobacz Pomoc techniczna.

- 1 - Wybierz bramę, dla której chcesz wykonać twardy reset.
- 2 - Kliknij przycisk **Twardy reset**. To polecenie usuwa istniejącą bazę danych bramy i ponownie ją przesyła nowa informacja.

Ponowne ładowanie danych bramy

EntraPass umożliwia operatorom przeładowanie danych w celu odświeżenia parametrów systemu nowymi danymi z bazy danych systemu. Kiedy należy przeładować bramę?

- Po większych zmianach w bazie danych systemu, takich jak nowe karty, nowe urządzenia, modyfikacja definicja komponentu, definicja nowych harmonogramów;
- Gdy jeden lub więcej kontrolerów działa nieprawidłowo (na przykład, gdy nie odbiera danych).

Po operacji przeładowania brama reorganizuje otrzymane dane i przekazuje nowe dane wszystkie witryny i kontrolery.

Uwaga...

Komunikacja z kontrolerami jest zawieszona podczas operacji przeładowania.

- 1 - Wybierz bramę, dla której chcesz ponownie załadować dane.
- 2 - Kliknij przycisk Przeładuj dane. Dane bramy zostaną zaktualizowane.



Operacje na Wirtualnych lokalizacjach i magistralach (Manual Operations on Sites)

Ręczne operacje na wirtualnych lokalizacjach i magistralach są wykorzystywane do odpytywania nieprzypisanych kontrolerów. Na przykład, kiedy kontroler został dodany do systemu bez numeru seryjnego, możesz użyć tego polecenia do uzyskania numeru seryjnego kontrolera.

Ikona	Definicja
	Połącz ze zdalną lokalizacją: Kliknij, aby połączyć się ze zdalną lokalizacją przy użyciu wstępnie skonfigurowanego połączenia telefonicznego.
	Odłącz zdalną lokalizację: Kliknij, aby zamknąć połączenie między tą stacją roboczą EntraPass i połączeniem zdalnym.
	Wymuś rozłączenie lokalizacji zdalej: Wymuś natychmiastowe rozłączenie połączenia zdalnego, nawet jeśli system przeładowuje. Ta opcja jest dostępna tylko w bramie z wieloma lokalizacjami.
	Wyłącz pozostały czas: kliknij, aby pozostać w kontakcie, aż do ponownego kliknięcia. Ta czynność wyłącza ustawienie wstępne pozostały czas połączenia. Ta akcja omija każdy czas bezczynności.
	Aktualizuj połączenie zdalne: Po wybraniu połączenia kliknij, aby połączyć i zaktualizować parametry połączenia
	Zaktualizuj wszystkie połączenia zdalne: Kliknij, aby połączyć i zaktualizować parametry wszystkich połączeń zaczynając od pierwszego połączenia na liście.
	Usuń połączenie z listy połączeń i oczekiwania: Wybierz połączenie, a następnie kliknij, aby zawiesić połączenie po ustawieniu wszystkich połączeń do aktualizacji.
	Przeładuj oprogramowanie firmowe IP Link: wymusi ponowne załadowanie firmware do wybranego urządzenia IP Link Kantech. UWAGA: Ze względów bezpieczeństwa administrator systemu może wyłączyć ten przycisk.
	Wymuś pakiet rozgłoszeniowy IP: wysyła sygnał do wybranego Kantech IP Link, KT-400 lub KT-1

Wskazówka jest wyświetlana po przesunięciu kursora nad przyciskiem. Podaje szczegółowe informacje na temat operacji wykonane.

Wykonywanie operacji ręcznych na stronie / połączeniu

1. W oknie Operacja kliknij przycisk Wirtualne lokalizacje i magistrale, aby otworzyć witrynę i połączenie okno, a następnie wybierz witrynę / bramę, z którą połączona jest witryna / połączenie.
2. Aby sondować kontroler, który nie jest przypisany, kliknij przycisk Kontroler. Wiadomość jest wysyłana do nieprzypisanego kontroler, prosząc go o identyfikację. Gdy kontroler odbierze połączenie z połączenia, wysyła komunikat potwierdzający na pulpicie wiadomości.
3. Możesz wybrać Pulpit wiadomości, aby wyświetlić numer seryjny kontrolera.



EntraPass - Instrukcja instalacji i obsługi programu Operacje

Kolumna% pokazuje wydajność komunikacji wybranego połączenia. Jeśli procent też jest niski (na przykład poniżej 75%), może to oznaczać, że połączenie nie komunikuje się wydajnie. Problemy z komunikacją itp.

Komunikaty stanu komunikacji dostępne na liście

Wiadomości na liście komunikacji. W następującym przykładzie, zobaczysz status wiadomości dla bramek GSI.

Wiadomość	Opis
Kontroler – komunikacja OK	Wszystkie kontrolery komunikują się z bramką
Kontroler – problemy z komunikacją	Przynajmniej jeden kontroler nie może skomunikować się z bramką
Urządzenie IP – utrata komunikacji	Brak komunikacji pomiędzy kontrolerami i aplikacja bramki
Komunikacja z bramką nie może zostać nawiązana	Bramka nie może otworzyć portu komunikacyjnego



Operacje na kontrolerach (Manual Operations on Controllers)

Poniższe opcje są używane do resetowania albo przeładowania kontrolera:

	Miękki reset (Soft reset): nie ma wpływu na bazę danych. Wysyła polecenie do kontrolera, aby zaktualizować komponenty o nowe informacje.
	Twardy reset (Hard reset): usuwa aktualną bazę danych i przeładowuje kontroler z nowymi informacjami w bazie danych. Przed użyciem tego polecenia zaleca się kontakt ze Wsparciem Technicznym.
	Przeładuj (Reload): przeładowuje bazę danych kontrolera.
	Przeładuj firmware (Reload controller firmware): przeładowuje firmware kontrolera (KT-100, KT-300)
	Wyczyść buforowane zdarzenia: kontrolery offline buforują zdarzenia do momentu ponownego połączenia z serwerem. Ta operacja odrzuci zapisane zdarzenia na kontrolerze. Ta operacja jest dostępna tylko dla KT-400 i KT-1
	Odblokuj klawiaturę czytnika (Unlock reader keypad): odblokowuj klawiaturę czytnika KT-100
	Resetuj zasilanie czytnika (Reset reader power): resetuje zasilanie czytnika KT-300
	Zapomnij (Forgive): resetuje licznik wczytywania kart.
	Lista anti-passback (Anti-passback cards list): wyświetla liczbę kart dla strefy, zbiera informacje o kartach w lokalnych kontrolerach oraz umożliwia zlokalizowanie karty.
	Przeładuj oprogramowanie modułu: przeładuje oprogramowanie układowe modułu ioSmart.

Notatka: wskazówka (informacja na temat operacji) jest wyświetlona, kiedy ustawisz kursor nad przyciskiem.

Wybieranie kontrolera (Selecting a Controller)

1 – Z okna Operacje kliknij na przycisk Kontroler, aby otworzyć okno Kontrolera skąd będziesz mógł zresetować kontroler.

2 – Z okna Bramka/Obiekt wybierz bramkę lub obiekt. Kontrolery przypisane do wybranej bramki/obiektu pojawią się w okienku po prawej.

- Z listy kontrolerów wybierz kontroler, na którym będą przeprowadzana operacje. Wybrany kontroler musi być podświetlony. Aby przeprowadzić operacje na grupie kontrolerów, wybierz Grupa Kontrolerów (Controller Group) (prawe, dolne okienko).

Notatka: jeśli w systemie jest określona tylko jedna bramka albo obiekt, Kontroler obiektów oraz Lista bramek nie zostaną wyświetlone w Oknie kontrolera.



Miękki reset kontrolera (Performing a Controller Soft Reset)

Miękki reset odświeża informacje w kontrolerze.

- 1 – W oknie Kontroler wybierz konkretny kontroler albo grupę kontrolerów.
- 2 – Kliknij przycisk Miękki reset (Soft reset) na pasku narzędzi. Ta operacja wysyła polecenie do kontrolera, aby zaktualizować komponenty o nowe informacje.

Twardy reset kontrolera (Performing a Controller Hard Reset)

Twardy reset usuwa aktualną bazę danych i przeładowuje kontroler z nowymi informacjami w bazie danych.

Notatka: polecenia resetowania powinny być wykonywane z uwagą. Przed przeprowadzeniem operacji resetowania polecamy kontakt z naszym Działem technicznym. Zobacz Wsparcie techniczne.

- 1 - W oknie Kontroler wybierz konkretny kontroler albo grupę kontrolerów.
- 2 – Kliknij przycisk Twardy reset (Hard reset) na pasku narzędzi. Ta operacja wysyła polecenie do kontrolera, aby zaktualizować komponenty o nowe informacje.

Zdalne przeładowanie kontrolera (Reloading a Controller Manually)

EntraPass umożliwia przeładowanie bazy danych kontrolera w przypadku, gdy baza danych nie załaduje się prawidłowo.

- 1 - W oknie Kontroler wybierz konkretny kontroler albo grupę kontrolerów.
- 2 – Kliknij przycisk Przeładuj (Reload) na pasku narzędzi. Baza danych zostanie przeładowana.

Zdalne przeładowanie firmware'u kontrolera (Manually Reloading a Firmware Controller)

EntraPass umożliwia przeładownia firmware'u kontrolera dla KT-100 oraz KT-300 po aktualizacji systemu albo firmware'u.

- 1 - W oknie Kontroler wybierz konkretny kontroler albo grupę kontrolerów.
- 2 – Kliknij przycisk Przeładuj firmware (Reload controller firmware) na pasku narzędzi.

Zdalne odblokowanie klawiatury czytnika (Manually Unlocking a Reader Keypad)

EntraPass umożliwia odblokowanie klawiatury czytnika dla KT-100 ze stacji roboczej.

- 1 - W oknie Kontroler wybierz konkretny kontroler albo grupę kontrolerów.
- 2 – Kliknij Odblokuj klawiaturę czytnika (Unlock reader keypa) na pasku narzędzi.

Resetowanie zliczania kart (Resetting Cards In and Cards Out Counters or all Controller local areas)

Ta operacja umożliwia resetowanie do zera zliczania kart.

- 1 - W oknie Kontroler wybierz konkretny kontroler albo grupę kontrolerów.
- 2 – Kliknij Zapomnij (Forgive) na pasku narzędzi.

Kalkulowanie liczby kart na wej./wyj. (Calculating Number of Cards In and Cards Out)

Jeżeli kontroler jest skonfigurowany z anti-passbackiem, możliwe jest zliczenie kart, które są w lub poza strefą. W tym celu opcja passback musi być aktywna na czytniku, a drzwi muszą być zdefiniowane jako drzwi wejściowe lub wyjściowe.

- 1 – W oknie Kontroler, w sekcji Bramka/Obiekt, wybierz KT-400-IP. Wyświetli się lista kontrolerów powiązanych z wybranym.
- 2 – Wybierz kontroler lub grupę kontrolerów.



EntraPass - Instrukcja instalacji i obsługi programu Operacje

3 – Kliknij przycisk Lista kart (Get card list) na pasku narzędzi. System wyświetli liczbę kart w lub poza strefą dla wybranego kontrolera lub grupy kontrolerów.

Notatka: ponieważ operacja jest czasochłonna, jest ona przeprowadzona w danym momencie wyłącznie na jednym kontrolerze. Opcja jest dostępna tylko dla Bramek multi-site.

Lokalizacja karty (Card Location)

- 1 – Kliknij prawym przyciskiem myszy na numer strefy, a następnie kliknij Znajdź kartę (Find card).
- 2 – W okienku Znajdź lokalizację karty (Get card position), kliknij Zaczynij od (Start with), Rozpocznij od (Begin with) albo Zawiera (Contains) w celu filtrowania poszukiwań.
- 3 – Z listy wybierz kartę i kliknij Pobierz lokalizację (Get position).

Resetowanie liczników kart i kart lub wszystkich lokalnych obszarów kontrolera

Opcja ta pozwala wyzerować karty i licznik kart.

1-w oknie dialogowym Kontroler wybierz żądany kontroler lub grupę kontrolerów.

2-kliknij przycisk przebacz na pasku narzędziowym. Posiadacze kart nie będą rozważani wewnątrz ani na zewnątrz, dopóki przy następnym użyciu karty w czytniku wjazdu lub wyjazdu.

Żądanie nieprzypisanych modułów

Ta funkcja zwraca numery seryjne wszystkich czytników ioSmart i ioModules podłączonych do kontrolera, ale nie zdefiniowanych w systemie. Użyj jednej z następujących metod, aby wyświetlić moduły nieprzypisane w komunikacji

Okno listy:

- Na karcie operacje wybierz kontroler, kliknij prawym przyciskiem myszy i wybierz polecenie Żądaj nieprzypisanych modułów.
- Na karcie operacje kliknij prawym przyciskiem myszy na pasku narzędzi i kliknij opcję Żądaj nieprzypisanych modułów.

Aby edytować moduł, kliknij prawym przyciskiem myszy zdarzenie, kliknij polecenie Edytuj, a następnie wybierz jedną z następujących opcji:

- Kontroler: służy do otwierania okna kontrolera i edytowania definicji kontrolera.
- Przypisz: wykonuje następujące czynności:
 - o Wypełnia dane na stronie konfiguracji kontrolera w ioSmart lub ioModule. W razie potrzeby zmień nazwę czytnika lub zmień szczegóły konfiguracji, a następnie kliknij przycisk Zapisz.

Pełny status

Aby przejrzeć ustawienia i konfigurację komunikacji kontrolera, użyj opcji pełny status.



Stan modułu

Stan modułu służy do przeglądania stanu modułu.

Uwaga...

Jeśli chcesz wyświetlić w tym samym czasie stan pełny i okno stanu modułu, kliknij przycisk pełny stan, a następnie w oknie kontrolera kliknij przycisk stan modułu.

Edytuj

Użyj **Edytuj**, Aby otworzyć okno **kontrolera** i edytować definicję kontrolera.

Operacje dotyczące drzwi (Manual Operations on Doors)

Ta operacja pozwala użytkownikowi z odpowiednimi upoważnieniami na modyfikowanie statusu drzwi oraz grup drzwi. Użytkownik może zdalnie zablokować/odblokować drzwi, czasowo zablokować/odblokować drzwi albo grupę drzwi oraz włączyć/wyłączyć czytniki na wybranych drzwiach.



Zarygluj drzwi albo grupę drzwi (Lock door or group of doors): zdalnie zarygluje wybrane drzwi lub grupę drzwi.



Odrygluj drzwi albo grupę drzwi (Unlock door or group of doors): zdalnie odblokowuje drzwi albo grupę drzwi. Pozostaną one odryglowane do następnej zmiany decyzji.



Czasowo zarygluj/odrygluj drzwi albo grupę drzwi (Temporarily lock/unlock door or group of doors): wykonuje operacje na zadany przedział czasu. Po jego upływie nastąpi automatyczne zamknięcie drzwi.



Powrót do terminarza (Return to schedule): ponownie wprowadzi terminarz zamykania drzwi lub grupy drzwi.



Włącz czytnik kart (Enable card reader): uruchomi wyłączony wcześniej czytnik.



Wyłącz czytnik kart (Disable card reader): wyłączy czytnik. Użytkownik nie będzie miał dostępu do drzwi nawet, jeżeli posiada prawa dostępu.



Uzbrój drzwi (Arm door) (tylko KT-400): uzbraja panel alarmowy.



Rozbrój drzwi (Disarm door) (tylko KT-400): rozbraja panel alarmowy.



Miękki reset czytnika: uruchomi ponownie czytnik, wyłączając go i włączając ponownie.

Notatka: wskazówka (informacja na temat operacji) jest wyświetlona, kiedy ustawisz kursor nad przyciskiem.



EntraPass - Instrukcja instalacji i obsługi programu Operacje

Istnieje kilka powodów, dla których można przeprowadzić powyższe operacje. Dla przykładu, może zająć potrzeba „wyłączenia czytnika” na krótki przedział czasu, aby zablokować dostęp do drzwi. Operacja umożliwia użytkownikowi zaryglowanie drzwi, które poprzednio zostały odryglowane przez użytkownika lub terminarz.

Jeżeli drzwi zostały zdalnie zaryglowane pozostaną zaryglowane aż:

- Zostanie zastosowana odpowiednia karta (po przejściu zostaną ponownie zaryglowane),
- Nastąpi automatyczne odryglowanie na skutek terminarza
- Użytkownik zdalnie odrygluje drzwi.

Wybieranie drzwi albo grup drzwi (Selecting a Door or a Door Group)

1 – Z okna Operacje wybierz przycisk Drzwi (Door). Wyświetli się okno Drzwi.

2 – Kliknij Włącz animacje (Enable animation), aby wyświetlić status drzwi w czasie rzeczywistym.

- Okienko z lewej strony wyświetla listę wszystkich obiektów/bramek. Możesz wybrać wszystkie albo jeden obiekt/bramkę.
- Drzwi powiązane z wybranym po lewej obiektem/bramką są wyświetlone w prawej, górnej części okienka. Jeżeli wybrałeś wszystkie, po prawej zostaną wyświetlone wszystkie drzwi w systemie. Możesz wybrać jedno, kilka albo wszystkie drzwi.

Notatka: jeśli w systemie jest określona tylko jedna bramka albo obiekt, okno listy bramek albo obiektów nie zostaną wyświetlone w Oknie kontrolera.

- Grupy drzwi powiązane z wybranym po lewej obiektem/bramką są wyświetlone w prawej, dolnej części okienka. Jeżeli wybrałeś wszystkie, po prawej zostaną wyświetlone wszystkie grupy drzwi w systemie. Możesz wybrać jedno, kilka albo wszystkie grupy drzwi.

Notatka: panel Grupy drzwi jest dostępny wyłącznie dla wybranego obiektu albo dla wybranego połączenia niepołączonego z obiektem.

Zdalne blokowanie drzwi (Locking a Door Manually)

1 – W oknie Drzwi wybierz konkretne drzwi albo grupę drzwi.

2 – Kliknij Zarygluj drzwi (Lock-door) na pasku narzędzi.

Zdalne odryglowanie drzwi (Unlocking a Door Manually)

1 - W oknie Drzwi wybierz konkretne drzwi albo grupę drzwi.

2 – Kliknij Odrygluj drzwi (Unlock-door) na pasku narzędzi. Drzwi zostaną odryglowane. System poprosi użytkownika o potwierdzenie. Drzwi z terminarzem odryglowania pozostaną odryglowane do:

- Następnej zmiany wynikającej z terminarza.
- Zdalnego zaryglowania drzwi przez operatora.

Czasowe odryglowanie drzwi (Unlocking a Door Temporarily)

EntraPass umożliwia czasowe odryglowanie drzwi na zadany przedział czasu. Po jego upływie nastąpi automatyczne zamknięcie drzwi.

Notatka: maksymalny czas odryglowania to 4:15 (255 sekund)

1 – Kliknij przycisk Czasowo odrygluj (Temporarily unlock). Pojawi się możliwość ustawienia/zmienienia zadanego przedziału czasu.

2 – Wprowadź Nowy czas opóźnienia (m:ss) i kliknij OK. Wybrane drzwi będą czasowo odryglowane.



Resetowanie terminarza drzwi (Resetting a Door Schedule)

EntraPass umożliwia zresetowanie terminarza drzwi po zdalnym wprowadzeniu zmian w komponencie.

- 1 - W oknie Drzwi wybierz konkretne drzwi albo grupę drzwi.
- 2 – Kliknij przycisk Wróć do terminarza (Return to Schedule).

Włączanie czytnika drzwi (Enabling a Door Reader)

- 1 - W oknie Drzwi wybierz konkretne drzwi albo grupę drzwi.
- 2 – Kliknij przycisk Włącz czytnik (Reader-enable).

Wyłączenie czytnika drzwi (Disabling a Door Reader)

- 1 - W oknie Drzwi wybierz konkretne drzwi albo grupę drzwi.
- 2 – Kliknij przycisk Wyłącz czytnik (Reader-disable). Ta opcja wyłączy czytnik. Użytkownik nie będzie miał dostępu do drzwi nawet, jeżeli posiada prawa dostępu.



Operacje dotyczące wind (Manual Operations on Elevator Doors)

Ta operacja pozwala operatorowi na zdalne zamknięcie, odblokowanie oraz czasowe odblokowanie pięter windy. Okno będzie również wyświetlać w czasie rzeczywistym status wybranych drzwi windy.

- Posiadacz karty wciska przycisk góry/dół, otwierają się drzwi windy
- Posiadacz karty przykładając kartę do czytnika (w kabinie)
- System sprawdza czy terminarz przypisany do drzwi jest prawidłowy. Jeżeli tak, system sprawdza, która grupa pięter jest przypisana do drzwi.
- Tylko piętra które są przypisane do terminarza będą dostępne do wyboru przez użytkownika.



Zablokuj piętro lub grupę pięter (Lock elevator floor or group of elevator floors): zdalnie zablokuje piętro lub grupę pięter



Odblokuj piętro i grupę pięter (Unlock elevator floor or group of elevator floors): zdalnie odblokuje piętro i grupę pięter. Pozostaną one odryglowane do następnej zmiany decyzji.



Czasowo blokuj/odblokuj piętra (Temporarily lock/unlock elevator floor or group of elevator floors): wykonuje operacje na zadany przedział czasu. Po jego upływie nastąpi automatyczne zablokowanie pięter.



Powrót do terminarza (Return to schedule): ponownie wprowadzi terminarz zamykania drzwi lub grupy drzwi.



Włącz czytnik kart (Enable card reader): uruchomi wyłączony wcześniej czytnik.



Wyłącz czytnik kart (Disable card reader): wyłączy czytnik. Użytkownik nie będzie miał dostępu do pięter, nawet, jeżeli posiada prawa dostępu.



Włącz piętro (Enable elevator floor): włączy wyłączone wcześniej piętro albo grupę pięter.



Wyłącz piętro (Disable elevator floor): wyłączy piętro. Użytkownik nie będzie miał dostępu do pięter, nawet, jeżeli posiada prawa dostępu.

Notatka: wskazówka (informacja na temat operacji) jest wyświetlona, kiedy ustawisz kursor nad przyciskiem.



Wybieranie drzwi windy (Selecting an Elevator Door)

1 – Z okna Operacje wybierz przycisk Drzwi windy (Elevator door).

2 – Kliknij Włącz animacje (Enable animation), aby wyświetlić status drzwi windy w czasie rzeczywistym.

- Okienko z lewej strony wyświetla listę wszystkich obiektów/bramek. Możesz wybrać wszystkie albo jeden obiekt/bramkę.

- Drzwi windy powiązane z wybranym po lewej obiektem/bramką są wyświetlone w prawej, górnej części okienka. Jeżeli wybrałeś wszystkie, po prawej zostaną wyświetlone wszystkie drzwi w systemie. Możesz wybrać jedno, kilka albo wszystkie drzwi.

- Grupy drzwi windy powiązane z wybranym po lewej obiektem/bramką są wyświetlone w prawej, dolnej części okienka. Jeżeli wybrałeś wszystkie, po prawej zostaną wyświetlone wszystkie grupy drzwi windy w systemie. Możesz wybrać jedno, kilka albo wszystkie grupy drzwi windy.

Notatka: panel Grupy drzwi jest dostępny wyłącznie dla wybranego obiektu albo dla wybranego połączenia niepołączonego z obiektem.

Blokowanie pięter (Locking Floors from Elevator Doors)

1 – Wybierz drzwi windy lub grupę drzwi windy.

2 – Kliknij Zarygluj (Lock) na pasku narzędzi.

Notatka: drzwi bez zdefiniowanego terminarza odryglowania zostaną zaryglowane wyłącznie przez zdalne polecenie. Aby zablokować wszystkie piętra, które były odryglowane skorzystaj z opcji Odblokuj w menu Zdalne operacje.

Odblokowanie pięter (Unlocking Floors from Elevator Doors)

1 – Wybierz drzwi windy lub grupę drzwi windy.

2 – Kliknij Odblokuj (Unlock elevator floors) na pasku narzędzi, aby odblokować uprzednio zaryglowane drzwi.

Notatka: dla drzwi, dla których zdefiniowany jest „terminarz automatycznego odblokowywania” piętra pozostaną dostępne aż do następnej zmiany terminarza, albo do zdalnego zablokowania przez użytkownika.



Czasowe odblokowanie pięter (Unlocking Floors from Elevator Doors Temporarily)

EntraPass umożliwia czasowe odblokowanie pięter. Po upływie czasu drzwi ponownie się zablokują. Maksymalny czas odblokowania to 4:15 (255 sekund)

1 – Kliknij przycisk Czasowo odblokuj (Temporarily unlock). Pojawi się możliwość ustawienia/zmienienia zadanego przedziału.

2 – Wprowadź Nowy czas opóźnienia (m:ss) i kliknij OK. Wybrane drzwi windy będą czasowo odryglowane.

Notatka: to polecenie czasowo odblokuje piętra, które są oznaczone „x” w kolumnie „” w menu Definiowanie Grup Pięter.

Nie istnieje „animacja” na tego rodzaju operacje

. Aby odblokować wszystkie piętra, użyj opcji „czasowe odblokuj piętra” (“temporarily unlock door”) z menu Zdalne operacje na drzwiach (manual operation on doors).

Resetowanie terminarza drzwi windy (Resetting an Elevator Door Schedule)

EntraPass pozwala zresetować terminarz drzwi windy po tym, jak zdalne operacje były przeprowadzone na danym komponencie.

1 - Wybierz drzwi windy lub grupę drzwi windy.

2 – Kliknij przycisk Powrót do terminarza (Return to schedule): Ta opcja ponownie wprowadzi terminarz zamykania drzwi lub grupy drzwi dla wybranych komponentów.

Włącz piętro (Enabling an Elevator Floor)

1 - Wybierz drzwi windy lub grupę drzwi windy.

2 – Kliknij przycisk Włącz piętro (Enable elevator floor). Ta opcja włączy wyłączone wcześniej piętro albo grupę pięter.

Wyłącz piętro (Disabling an Elevator Floor)

1 - Wybierz drzwi windy lub grupę drzwi windy.

2 - Kliknij przycisk Wyłącz piętro (Disable elevator floor). Ta opcja wyłączy piętro. Użytkownik nie będzie miał dostępu do pięter, nawet, jeżeli posiada prawa dostępu.



Operacje dotyczące przekaźników (Manual Operations on Relays)

Użyj tego menu, aby zdalnie zmienić stan przekaźnika albo grupy przekaźników. Możesz zdalnie włączyć/wyłączyć/czasowo włączyć przekaźnik lub grupę przekaźników. W oknie wyświetli się też, w czasie rzeczywistym, status wybranego przekaźnika (lub wybranych przekaźników).



Wyłącz przekaźnik (Deactivate relay): pozwala użytkownikowi wyłączyć włączony (przez użytkownika, zdarzenie, terminarz albo Wejście linii dozorowej) uprzednio przekaźnik.



Włącz przekaźnik (Activate relay): pozwala użytkownikowi włączyć wyłączony (przez użytkownika, zdarzenie, terminarz albo Wejście linii dozorowej) uprzednio przekaźnik.



Włącz czasowo przekaźnik (Temporarily activated relay): włącza przekaźnik albo grupę przekaźników na określony przedział czasu.



Powrót do terminarza (Return to schedule): ponownie wprowadzi terminarz po przeprowadzeniu zdalnej operacji na komponencie.

Notatka: wskazówka (informacja na temat operacji) jest wyświetlona, kiedy ustawisz kursor nad przyciskiem.

Wybieranie przekaźników (Selecting Relays)

1 – Z okna Operacje wybierz przycisk Przekaźnik (Relay).

2 – Kliknij Włącz animacje (Enable animation), aby wyświetlić status wejść w czasie rzeczywistym.

- Okienko z lewej strony wyświetla listę wszystkich obiektów/bramek. Możesz wybrać wszystkie albo jeden obiekt/bramkę.
- Przekaźniki powiązane z wybranym po lewej obiektem/bramką są wyświetlone w prawej, górnej części okienka. Jeżeli wybrałeś wszystkie, po prawej zostaną wyświetlone wszystkie przekaźniki w systemie. Możesz wybrać jeden, kilka albo wszystkie przekaźniki.
- Grupy przekaźników powiązane z wybranym po lewej obiektem/bramką są wyświetlone w prawej, dolnej części okienka. Jeżeli wybrałeś wszystkie, po prawej zostaną wyświetlone wszystkie grupy przekaźników w systemie. Możesz wybrać jedną, kilka albo wszystkie grupy wejść.

Notatka: panel Grupy przekaźników jest dostępny wyłącznie dla wybranego obiektu albo dla wybranego połączenia niepołączonego z obiektem.



Zdalne wyłączanie przekaźnika (Deactivating a Relay Manually)

- 1 – Wybierz przekaźnik lub grupę przekaźników.
- 2 – Kliknij przycisk Wyłącz przekaźnik (Deactivate Relay).

Notatka: jeśli zdalnie wyłączysz przekaźnik, który jest zazwyczaj aktywowany zgodnie z terminarzem, pozostanie on wyłączony do następnego uruchomienia według terminarza. Oznacza to, że jeżeli przekaźnik ma być uruchomiony według terminarza, a ty wyłączyłeś go, to musisz pamiętać o uruchomieniu go na pozostały czas trwania terminarza operacji, ponieważ jeden przekaźnik może być określany przez różne komponenty systemu – jego aktywacja/dezaktywacja będzie powiązana z jego konfiguracją w tych komponentach.

Zdalne włączanie przekaźnika (Activating a Relay Manually)

- 1 – Wybierz przekaźnik lub grupę przekaźników.
- 2 – Kliknij przycisk Włącz przekaźnik (Activate Relay). Ta opcja pozwala użytkownikowi włączyć wyłączony (przez użytkownika, zdarzenie, terminarz albo wejście) uprzednio przekaźnik.

Włączenie czasowe przekaźnika (Activating a Relay Temporarily)

- 1 – W okienku po prawej stronie możesz wybrać przełącznik w jego górnej części, albo wszystkie przekaźniki w dolnej.
- 2 – Kliknij Włącz czasowo przekaźnik (Activate relay temporarily). Pojawi się możliwość zdefiniowania czasu.
- 3 – Wprowadź Nowy czas opóźnienia (m:ss) i kliknij OK. Wybrany przekaźnik będzie czasowo aktywowany przez użytkownika.

Notatka: wybrany przekaźnik zostanie czasowo włączony. Jest to przydatna opcja dla użytkownika, który chciałby czasowo włączyć przekaźnik wyłączony uprzednio przez użytkownika, zdarzenie, terminarz. System prosi o wprowadzenie czasu aktywacji, po upływie którego przekaźnik automatycznie się wyłączy.

Resetowania terminarza przekaźnika (Resetting a Relay Schedule)

EntraPass pozwala ponownie wprowadzić terminarz po przeprowadzeniu zdalnej operacji na komponentcie.

- 1 – W okienku Przekaźnik drzwi (Relay door), wybierz przekaźnik albo grupę przekaźników.
- 2 – Kliknij Powrót do terminarza (Return to schedule). Ta operacja przywraca stany zaznaczonych elementów do zgodności z terminarzem.



Operacje na liniach dozorowych (Manual Operations on Inputs)

Ikona	Definicja
	Linia dozorowa - przywróć stan normalny: przywraca stan do zgodnego z ustawieniami urządzenia
	Włącz monitorowanie linii dozorowej: będzie monitorować wybrane linie cały czas
	Linia dozorowa – wyłącz monitorowanie: wyłącza monitorowanie linii dozorowej, nie zważając na jej harmonogram, i zacznie być monitorowana przy następnym harmonogramie
	Linia dozorowa – wyłącz monitorowanie czasowo: wyłączy monitorowanie na wybrany okres czasu.

Wykonywanie operacji na liniach dozorowych

1 – Z okna Operacje wybierz przycisk Linia dozorowa (Input).

2 – Kliknij Włącz animacje (Enable animation), aby wyświetlić status wejść w czasie rzeczywistym.

- Okienko z lewej strony wyświetla listę wszystkich obiektów/bramek. Możesz wybrać wszystkie albo jeden obiekt/bramkę.

- Wejścia linii dozorowej powiązane z wybranym po lewej obiektem/bramką są wyświetlone w prawej, górnej części okienka. Jeżeli wybrałeś wszystkie, po prawej zostaną wyświetlone Wejścia linii dozorowej w systemie. Możesz wybrać jedno, kilka albo wszystkie Wejścia linii dozorowej.

- Grupy wejść powiązane z wybranym po lewej obiektem/bramką są wyświetlone w prawej, dolnej części okienka. Jeżeli wybrałeś wszystkie, po prawej zostaną wyświetlone wszystkie grupy wejść w systemie. Możesz wybrać jedną, kilka albo wszystkie grupy wejść.

Notatka: panel Grupy wejść jest dostępny wyłącznie dla wybranego obiektu albo dla wybranego połączenia niepołączonego z obiektem.

Zdalne przywracanie linii dozorowej do normalnego stanu (Returning an Input to Its Normal State Manually)

Ta opcja jest wykorzystywana w sytuacjach, gdy status Wejścia linii dozorowej był modyfikowany przez użytkownika i chcesz przywrócić go do stanu normalnego.

1 - Wybierz Wejście linii dozorowej lub grupę wejść.

2 – Kliknij Linia dozorowa normalna (Input normal). Wybrana linia dozorowa wraca do normalnego stanu wg ustawień w menu Urządzenie (Device)

Przerwij monitorowanie linii dozorowej (Stopping Monitoring an Input)

Opcja przerywa monitorowanie linii dozorowej niezależnie od terminarza.

1 - Wybierz linię dozorową lub grupę linii dozorowych.

2 – Kliknij przycisk Linia dozorowa bez nadzoru (Input no supervision). Wybrana linia dozorowa nie będzie monitorowana.

Przerwij czasowo monitorowanie linii dozorowej (Stopping Input Supervision (Shunt) Temporarily)

Użyj tej opcji, jeżeli chcesz, aby system pominął wybraną Linię dozorową przez określony przedział czasu.

1 – Aby czasowo zablokować Linię dozorową, wybierz konkretną Linię dozorową, kliknij Czasowo ukryj (Temporarily shunt). Linia dozorowa nie będzie monitorowana przez przedział czasu.



EntraPass - Instrukcja instalacji i obsługi programu Operacje

2 – Kliknij Linia dozoruwa czasowo bez monitorowania (Input no supervision temporarily). Pojawi się możliwość zdefiniowania czasu.

3 – Wprowadź Nowy czas opóźnienia (m:ss) i kliknij OK. Obok Wejścia linii dozoruwej pojawi się przycisk oznaczający, że czasowo nie jest monitorowane. Jeśli wystąpi alarm, albo Wejście linii dozoruwej zostanie odłączone, nie pojawi się żadne informacje na ten temat na pulpicie Wiadomości.

Operacje

Operacje dotyczące systemów zintegrowanych

Operacje dotyczące raportu śledzącego (Manual Operations on View Roll Call)

Ta opcja umożliwia wizualizację czy użytkownik wchodzi na zdefiniowany obiekt. Kiedy użytkownik wejdzie w strefę, wyświetli się następujący raport:

Data i czas	Nazwisko użytkownika	Drzwi	Ostatni dostęp	Drzwi
Brak danych do wyświetlania				



Operacje dotyczące systemów zintegrowanych (Manual Operations on Integrated Panels)

- 1 – Z pasku narzędzi Operacje, wybierz Zintegrowane panele.
- 2 – W razie potrzeby z menu wybierz konkretny komponent.
- 3 – Wybierz panel z lewej kolumny i kliknij na niego prawym przyciskiem.
- 4 – Wybierz Pełen status (Full status), aby sprawdzić szczegóły panelu.
- 5 – Wybierz Panel wirtualnego alarmu (Virtual Alarm Panel), aby sprawdzić wirtualną klawiaturę.
- 6 – Wybierz partycję i prawym przyciskiem myszy uruchom menu.
- 7 – Wybierz Uzbrój/Rozbrój partycję (Arm/Disarm partition).



Operacje Harmonogramy akcji (Manual Operations on Action Scheduler)

Korzystaj z harmonogramu akcji, aby tworzyć akcje z opcją programowania jednorazowych lub powtarzających działań. Początkowym interfejsem wejściowym jest układ kalendarza, aby otworzyć nową akcję w oknie harmonogramu, kliknij dwukrotnie datę. Możesz przeglądać istniejące działania w formacie dziennym, tygodniowym, miesięcznym lub rocznym i korzystać z znacznik harmonogramu akcji do filtrowania typu wyświetlanych działań.

Widok początkowy zawiera listę zaprogramowanych działań i zawiera następujące szczegóły: kto go zażądał, datę i godzinę zaplanowania, co to jest działanie, pełny opis działania, czy jest to powtarzające się działanie lub nie, a licznik cykliczny używany i łączny.

Kontrolujesz uprawnienia do harmonogramu działań w Harmonogramie akcji w menu Operacje. Ikona to strona kalendarza z zegarem i jest automatycznie instalowana w aktualizacji systemu. Element bezpieczeństwa jest również dodano dla tej funkcji i znajduje się w menu Operacja, Harmonogram działań poziomu zabezpieczeń menu.

Notatka

Aby zaprogramować działania, domyślnym ustawieniem zabezpieczeń dla Instalatora i Administratorów jest, co jest wskazane zieloną ikoną domyślnym ustawieniem zabezpieczeń dla Operatorów jest, nie zezwalaj na to oznaczoną czerwoną ikoną. Zmienićrozwiń drzewo operacji i wybierz Harmonogram akcji.



Ikona	Opis
	Harmonogram akcji: Tworzy akcje, które są jednorazowymi cyklicznymi działaniami. Zapewnia widok kalendarza wszystkich zaprogramowane akcji z możliwością filtrowania, wyszukiwania i znaczników.

Programming the Action scheduler

The following table outlines the controller compatibility and firmware requirements for this feature.

Kontroler	Kompatybilność Assa Abloy	Bramki	Tryb autonomiczny
KT-1, firmware 2.00 i wyższy	tak	Multi-site, Global, KT-NCC	tak
KT-400, rev 1, firmware 1.29 i wyższe	tak	Multi-site, Global, KT-NCC	tak
KT-400, firmware 1.23 i wyższe	tak	Multi-site, Global, KT-NCC	tak
KT-300	nie	Global, KT-NCC	nie
KT-200	nie	Global, KT-NCC	nie

Aby zaprogramować harmonogram akcji, wykonaj następujące kroki:

- 1 - Kliknij zakładkę Operacja i wybierz z menu Harmonogram akcji.
- 2 - W interfejsie kalendarza kliknij dwukrotnie żądaną datę lub kliknij przycisk Dodaj w lewym górnym rogu płyta.
- 3 - W oknie Harmonogram akcji wprowadź nazwę akcji w polach podstawowych lub dodatkowych.
- 4 - Z listy Akcja wybierz odpowiednią akcję, domyślną akcją jest Odblokuj drzwi.

Notatka

Zadanie wykonywania jest nową akcją, która wybiera istniejący program budujący zadania jako komponent, opcję wyboru dostępna jest określona strefa czasowa, w której domyślną wartością jest lokalizacja lokalnego serwera. Kiedy ty utwórz nowy harmonogram działań, klikając prawym przyciskiem myszy komponent z menu Operacja, tylko menu wyświetla akcje odpowiednie dla tego komponentu. W przypadku bezprzewodowych połączeń drzwiowych użyj V3 oprogramowania układowego Assa-Abloy z dowolnym zgodnym kontrolerem wymienione w tabeli, Kompatybilność kontrolera i oprogramowania układowego.



5 - W polach Data i godzina harmonogramu wybierz odpowiednie wartości. Domyślnym dniem jest bieżący dzień, a domyślny czas to godzina później niż bieżący czas.

Notatka

Jeśli wybierzesz akcję tymczasową, pojawi się pole czasu zakończenia. Jeśli akcja ma podwójną funkcję, taką jak Pojawiają się pola Aktywuj i Dezaktywuj, Data i Czas.

6 - W polu Tag harmonogramu akcji utwórz nazwę, aby oznaczyć harmonogram działania. Tag wypełnia listę używane do filtrowania wszystkich akcji. Każda nowa nazwa generuje nowy tag, 50 tagów to maksymalna możliwa ilość. Jeśli żadna akcja nie używa tagu, jest automatycznie usuwana z listy.

7 - Opcjonalne: Zaznacz pole wyboru Cykliczne, jeśli chcesz, aby akcja się powtórzyła. Na liście częstotliwości wybierz od dziennego, tygodniowego, miesięcznego lub rocznego. Ustaw licznik, ile razy chcesz wykonać akcję powtarzając, jest to ustawienie statyczne, a 99 to maksymalna ilość dostępnych czasów. Licznik dynamiczny to widoczne w dolnej części widoku kalendarza.

8 - Zaznacz pole wyboru Usuń po wygaśnięciu, aby usunąć akcję po zaprogramowanej ilości nawrotów.

Notatka

Aby zapewnić przestrzeganie różnych stref czasowych, EntraPass usuwa działania 24 godziny po północy dzień egzekucji. Na przykład akcja zaprogramowana na poniedziałek 15:00 zostaje usunięta

Środa o godzinie 00:00.

9 - Musisz użyć jednego z ośmiu pól komponentu do akcji.

Notatka

Jeśli chcesz, aby działanie działało w trybie autonomicznym, używaj tylko kontrolerów nowej generacji, takich jak KT-1, KT-400, KT-400 rev1.

10 - Kliknij przycisk Zapisz.

KT-NCC, Global Gateway i harmonogram działania

Jeśli używany jest KT-NCC lub Global Gateway, harmonogram działania będzie działał ze wszystkimi typami kontrolerów, jak Globalna brama jest odpowiedzialna za wszystkie decyzje. Jeśli KT-1, KT-400 lub KT-400 rev 1 jest używany w trybie autonomicznym i traci połączenie z KT-NCC, KT-1 bierze odpowiedzialność za harmonogram działania. Jeśli korzystasz z kontrolera KT-100, KT-200 lub KT-300, a KT-NCC jest w trybie offline po uruchomieniu akcji, akcja nie zostanie uruchomiona, ponieważ harmonogram działania używa daty i godziny do wyzwolenia akcji oraz daty i czasu nie jest buforowany, gdy KT-NCC jest w trybie offline.



Programowanie harmonogramu akcji z okien drzwi lub przekaźnika

Poniższe kroki opisują, jak zaprogramować harmonogram działania z okna Drzwi, w tych samych krokach

zastosuj, jeśli zaprogramujesz harmonogram działania z okna Przełącznik:

- 1 - Kliknij kartę Operacja i kliknij polecenie Drzwi w menu.
- 2 - W panelu Drzwi wybierz odpowiednie drzwi i kliknij prawym przyciskiem myszy.
- 3 - Kliknij Harmonogram akcji, aby otworzyć okno Harmonogram akcji.
- 4 - Wykonaj kroki od 3 do 9 procedury programowania harmonogramu akcji.

Drukowanie kalendarza harmonogramu akcji

Dostępny jest raport o wszystkich działaniach harmonogramu akcji. Aby wydrukować raport, wykonaj następujące kroki:

- 1 - W oknie Harmonogram akcji kliknij przycisk Drukuj.
- 2 - Wybierz akcje, które chcesz uwzględnić w raporcie, użyj Zaznacz wszystko lub Odznacz wszystko, aby ułatwić wybór.
- 3 - Raport zawiera listę działań rozpoczynających się od najbliższej daty i godziny do najdalszego.
- 4 - Akcje obejmują następujące elementy:
 - Nazwa
 - Akcja
 - Które elementy
 - Data
 - Czas, godzina rozpoczęcia i godzina zakończenia
 - Cykliczny harmonogram z licznikiem
 - Strefa czasowa, jeśli dotyczy



Użytkownicy

Wyjątki dostępu

Poziom dostępu - wyjątki (Access Exception)

Użyj zakładki Wyjątki dostępu, aby przypisać konkretne działanie do drzwi.

1 – Z lewego panelu wybierz drzwi.

2 – Z prawego panelu wybierz działanie z listy. Użyj przycisków:  oraz  , aby dodać lub usunąć drzwi z listy po prawej.

3 – Pod kolumną Dostęp (Access), wybierz pomiędzy Dopuszcz (Allow) lub Zablockuj (Deny).

Notatka: zapisane zostaną tylko drzwi z przypisanymi terminarzami.

Uwaga: lista użytkowników nie uwzględnia wyjątków.

Aby aktywować Wyjątki, sprawdź [Parametry uwierzytelnienia](#).

Definiowanie poziomów dostępu (Access Levels Definition)

Poziomy dostępu określają gdzie i kiedy dana karta będzie działać. Grupy dostępu kart pozwalają na szybki wybór poziomów dostępu dla różnych bramek. Dla jednego połączenia można zaprogramować 248 poziomów dostępu. Aby przypisać poziom dostępu należy:

- Stworzyć terminarz, który będzie odzwierciedlać czas, w którym użytkownik ma dostęp do określonych drzwi.
- Przypisać stworzony terminarz do danych drzwi.
- Przypisać poziom dostępu do karty.

1 – Domyślnie ustawiony jest Pełny poziom dostępu do wszystkich drzwi: użytkownicy z takim poziomem dostępu mają dostęp do wszystkich drzwi o każdej porze dnia. Aby ograniczyć dostęp do konkretnych drzwi i konkretnego czasu musisz utworzyć konkretny poziom dostępu.

2 – Z paska narzędzi Użytkownicy (Users), kliknij przycisk Poziom dostępu (Access level). Wyświetli się okno Poziomu dostępu.

3 – Kliknij Nowy (New), a następnie przypisz nową nazwę dla poziomu dostępu, który tworzysz.



Użytkownicy

Projektowanie identyfikatorów

Notatka: komponenty, które są wyświetlone w kolumnach Drzwi oraz Terminarze albo Grupy pięter muszą zostać wcześniej zdefiniowane do wyboru. Aby zdefiniować drzwi: Urządzenia > Drzwi; terminarze: Definiowanie > Terminarze; grupy pięter: Grupy > Grupy pięter.

4 – Z listy Drzwi, wybierz drzwi, do których użytkownik karty ma dostęp.

5 – Z kolumny Terminarz (Schedule), wybierz terminarz, podczas którego użytkownik karty będzie miał dostęp do wybranych drzwi.

6 – Z kolumny Grupa pięter (Floor group), wybierz grupę pięter.

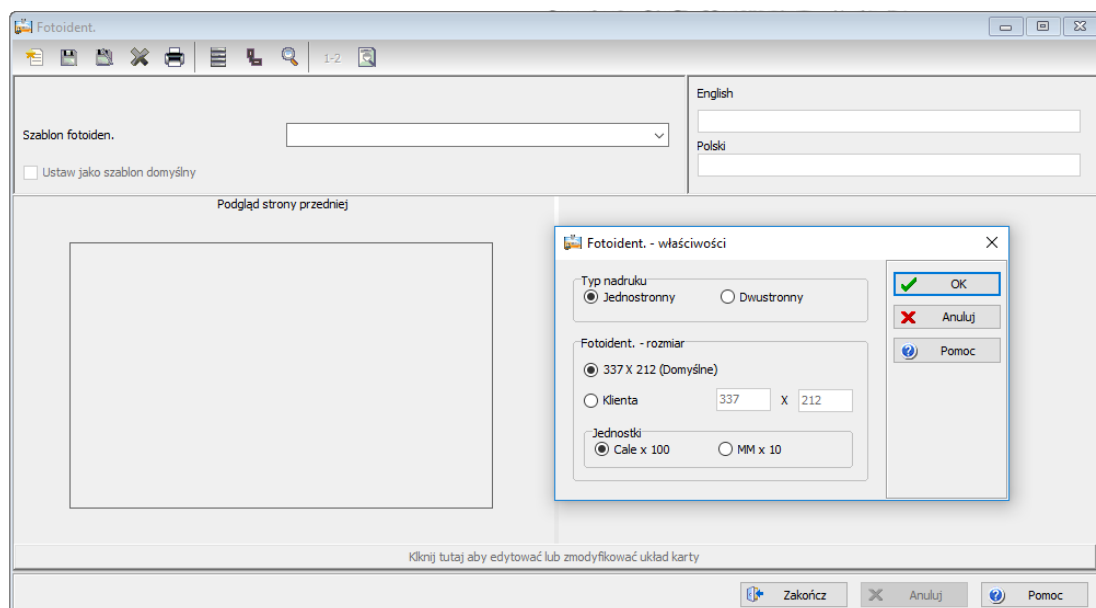
7 – Kliknij zakładkę Komentarz (Comment), aby umieścić komentarz do nowo utworzonego poziomu dostępu.

Projektowanie foto-identyfikatorów (Badges Designing)

EntraPass posiada edytor identyfikatorów, który pozwala na tworzenie, zapisywanie, edytowanie oraz usuwanie identyfikatorów, które mogą być wykorzystane przy kartach.

Tworzenie szablonu identyfikatora (Creating a Badge Template)

1 – Z menu Użytkownicy wybierz Identyfikator (Badge). Pojawi się okno Identyfikatora.



Notatka: Okno Identyfikatora zawiera wszystkie narzędzia dostępne w innych oknach EntraPass: nowy, zapisz, kopiuj, etc. Zawiera również dwa dodatkowe przyciski pozwalające modyfikować liczbę stron przypisanych do układu identyfikatora.

2 – Kliknij przycisk Nowy (New) na pasku narzędzi. Pojawi się okno Właściwości identyfikatora.



Właściwości szablonu identyfikatora (To Specify Properties for a Badge Layout)

1 – W oknie Właściwości identyfikatora określ liczbę stron identyfikatora, następnie wybierz wymiary identyfikatora i kliknij OK.

2 – Określ liczbę stron identyfikatora, następnie wybierz wymiary identyfikatora i kliknij OK.

Notatka: miary są wyrażone w calach lub milimetrach (setnych cala/dziesiętnych milimetra). Aby zmienić, miarę wybierz ją w sekcji Jednostki.

3 – Wprowadź nazwę dla szablonu identyfikatora w polu języków. Nazwa może składać się z 40 znaków.

4 – Możesz zaznaczyć Użyj szablon jako domyślny (Set as default card layout), aby nowy projekt był automatycznie wykorzystywany dla wszystkich nowych identyfikatorów.

Notatka: wyłącznie jeden domyślny szablon jest dostępny. Po wybraniu szablonu i kliknięciu Wybierz, jako domyślny szablon, obecny szablon zostanie zastąpiony.

5 – Kliknij Zapisz (Save), aby zapisać szablon.

Edytowanie szablonu identyfikatora (To Edit a Badge Layout)

Narzędzi projektowania identyfikatorów pozwala użytkownikom na edytowanie szablonu identyfikatora: na zmianę koloru tła, dodawanie grafiki, zmianę czcionki, etc.

Notatka: po stworzeniu szablonu nie możesz modyfikować jego rozmiarów; musisz utworzyć nowy szablon. Możesz natomiast edytować liczbę stron, klikając odpowiedni przycisk na pasku narzędzi okna Identyfikator.

Modyfikowanie liczby strony karty (To Modify the Number of Card Sides)

1 – Z okna Identyfikatora wybierz identyfikator, który chcesz edytować.

2 – Z paska narzędzi okna Identyfikatora kliknij 1-2.

3 - Kliknij Zapisz (Save), aby zapisać nowe informacje.



Modyfikowanie koloru tła (To Modify the Background colour)

1 – Z okna Identyfikatora wybierz identyfikator, który chcesz edytować.

2 – Kliknij przycisk [Kliknij tutaj](#), aby zmienić szablon karty (Click here to modify the card layout) (znajduje się w dolnej części okna), aby otworzyć okno Projektowania identyfikatora.

Notatka: po najechaniu kursorem na obiekt Projektowania identyfikatora pojawi się wskazówka dotyczące danego obiektu.

3 – Aby zmienić kolor tła, kliknij w dowolnym miejscu prawym przyciskiem myszy. Pojawi się menu Właściwości (Properties)

4 – Wybierz Właściwości (Properties). Pojawi się okno Właściwości tła.

5 – Wybierz pożądaną opcję dla szablonu:

- Brak tła (No background): domyślna.
- Użyj koloru, jako tła (Use colour as background): pozwala wybrać kolor tła.
- Użyj obraz, jako tło (Use image as background): pozwala dodać obraz/grafikę, która posłuży jako tło dla wszystkich identyfikatorów.
- Orientacja (Orientation): pozwala zdefiniować orientację na poziomą (horizontal) lub pionową (vertical).

Dodawanie obiektów do szablonu identyfikatora (To Add Objects to a Badge Layout)

Dzięki prostej opcji złap-przeciągnij-upuść, do szablonu identyfikatorów można dodawać inne obiekty:

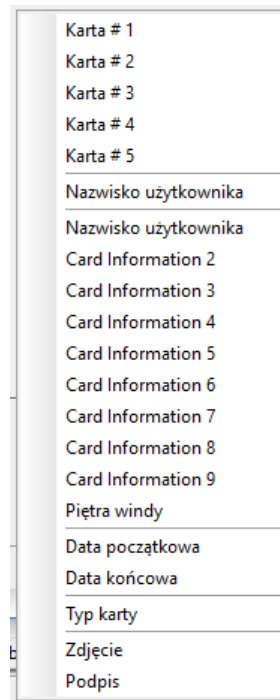
- Pola informacji o karcie
- Kody kreskowe
- Pola tekstowe
- Bieżącą datę
- Wcześniej zapisane obrazy lub logo (BMP, JPG, GIF, etc.)
- Ramki
- Linie, wypunktowania

Notatka: obiekty są wprowadzane z domyślnymi ustawieniami. Aby zmodyfikować te ustawienia kliknij prawym na obiekt, a następnie wybierz odpowiednie ustawienia z menu.



Wprowadzenie pól informacji o karcie (To Incorporate Card Information Fields)

1 – Aby dodać pole informacji o karcie do szablonu, kliknij przycisk Pola karty (Card fields). Pojawie się nowe menu.



2 – Aby zmodyfikować właściwości obiektu przed „upuszczeniem”, idź do Opcje (Options) w oknie Projektowanie identyfikatora, następnie wybierz Pokaż właściwości przy upuszczeniu (Show properties on drop). Jeśli tak zrobisz, okno Właściwości będzie się otwierać za każdym razem, gdy obiekt zostanie „upuszczony” w polu roboczym szablonu.

Notatka: aby umożliwić wybór Imienia i Nazwiska w menu Pola karty w oknie Projektowanie identyfikatora, przejdź do menu Opcje; następnie wybierz Parametry systemu > zakładkę Format nazwy użytkownika > zaznacz pole odnoszące się do analizowania nazwy użytkownika > wybierz nazwę (Imię albo Nazwisko), po której nazwy użytkowników będą sortowane.

3 – Z menu wybierz pole informacji o karcie, które chcesz dodać do układu szablonu.

Notatka: kiedy dodasz zdjęcie do układu projektowego identyfikatora, zdjęcie, które zostanie wyświetlone jest tylko znacznikiem. Wskazuje on, gdzie będzie wyświetlone zdjęcie użytkownika. Kiedy identyfikator zostanie przypisany do karty, odpowiednie zdjęcie zostanie wyświetlone.



Przypisywanie obiektu do układu szablonu (To Align Objects in the Template Layout)

Siatka układu pomaga w rozmieszczeniu obiektów na szablonie.

Dostępne są trzy opcje ułatwiające przypisywanie obiektów do szablonu identyfikatora:

- o Pokaż linie siatki (Show grid lines): wyświetla linie siatki.
- o Przypisz do siatki (Align to grid): ta opcja musi być włączona przed budowaniem szablonu. Po „upuszczeniu” obiektu w polu roboczym szablonu zostaną on „dosunięty” do najbliższej linii siatki.
- o Właściwości siatki (Grid settings): pozwala ustalić odstęp w siatce (w pikselach).

Notatka: aby wyłączyć siatkę odznacz Pokaż linie siatki.

Modyfikowanie właściwości pól (To Modify Card Fields Properties)

Obiekty są przypisywane do szablonu z ich domyślnymi ustawieniami (czcionka, kolor, etc.).

Możesz zmienić te ustawienia.

1 – Z szablonu Projektowanie identyfikatora, kliknij prawym przyciskiem myszy na obiekt umieszczony w szablonie.

2 – Z menu wybierz Właściwości pól karty (Card fields properties).

Notatka: Menu Właściwości zależy od wybranego obiektu. Na przykład, zmieni właściwości obrazu albo właściwości daty, zależnie od wybranego obiektu.

3 – Z nowego okna możesz zmienić następujące właściwości:

- Czcionkę (nazwę, kolor, styl (pogrubiona, kursywa, podkreślona)),
- Tło (przezroczyste lub wypełnione kolorem),
- Justowanie (poziome, pionowe)
- Orientacja,
- Właściwości (zawijaj tekst, etc.).

Notatka: pole Ustaw, jako domyślne pozwala wprowadzić wszystkie ustawienia tekstu do wszystkich obiektów tekstowych, które zostaną wprowadzone do szablonu.

Notatka: w momencie, kiedy Wyrównanie tekstu jest ustawione na „Inny” nie istnieje możliwość zmiany wielkości pola tekstowego.



Modyfikowanie właściwości obrazu (To Modify Picture Properties)

Odnosi się do dowolnego obiektu graficznego: zdjęcia, logo, etc.

1 – Z pola roboczego Projektowanie identyfikatora, kliknij prawym przyciskiem myszy na obraz umieszczony w szablonie, który chcesz modyfikować.

2 – Z menu wybierz Właściwości obrazu (Images properties).

3 – Możesz wybrać następny obraz z pliku albo modyfikować właściwości obrazu.

- Współczynnik rozciągania (Stretch ratio): pozwala na umieszczenie obrazu w środku, przy zachowaniu proporcji oryginalnego obrazu.
- Tryb transparentny (Transparent mode): przy wyborze tej opcji nie będzie ustawionego koloru tła.
- Narysuj ramę (Draw frame): ta opcja pozwala otoczyć obraz ramą.
- Kolor ramy (Frame colour): umożliwia ustawienie zmiany koloru ramy (możliwe tylko, gdy taka opcja Ramy (Frames) jest wybrana).

4 – Możesz zaznaczyć Ustaw, jako domyślne (Set as default), jeśli chcesz, aby ustawione właściwości były stosowane dla wszystkich obrazów do szablonu identyfikatorów.



Dodawanie obiektu tekstowego (To Add Static Text Objects)

Aby dodać obiekt tekstowy do identyfikatora, przeciągnij i upuść pole tekstowe, następnie wprowadź tekst w oknie Właściwości tekstu. Również w tym oknie zmieniasz właściwości samego tekstu.

1 – Z paska narzędzi Projektowanie identyfikatora, kliknij przycisk tekstu. Aby zmienić rozmiar pola tekstowego (wysokość, szerokość), wybierz je i przy pomocy strzałek określ nowy rozmiar.

2 – Aby przypisać pole tekstowe, sprawdź Przypisywanie obiektu do układu szablonu (To Align Objects in the Template Layout)

3 – Aby dodać tekst do pola tekstowego, kliknij prawym przyciskiem na pole tekstowe, następnie wybierz Właściwości tekstu (Static text properties) z menu.

4 – Wprowadź tekst w pole Wprowadź tekst (Enter text). Następnie możesz modyfikować tekst wedle wymagań. Możesz podejrzeć tekst przed zatwierdzeniem w sekcji Podgląd (Preview).

Dodawanie kodów kreskowych (To Add Bar Codes)

Możliwe jest dodanie kodów kreskowych do identyfikatorów. Domyślnie, kod kreskowy określa numer karty, o ile inne wartości nie zostaną określone.

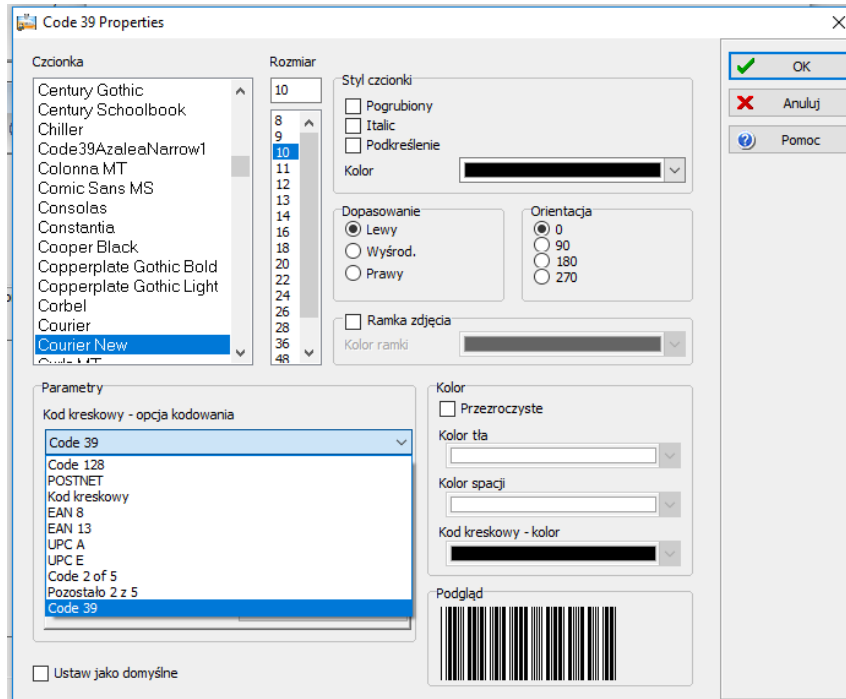
1 – Z okna Projektowanie identyfikatora, wybierz przycisk Kody kreskowe (Bar codes), następnie kliknij w pole robocze Projektowania identyfikatora.

2 – Aby przypisać kod kreskowy, sprawdź Przypisywanie obiektu do układu szablonu (To Align Objects in the Template Layout).



Ustawianie właściwości kodów kreskowych (To Set Up Bar code Properties)

1 – W oknie Projektowanie identyfikatora, kliknij prawym przyciskiem na kod kreskowy, aby otworzyć okno Właściwości kodu kreskowego.



2 – W oknie Właściwości kodu kreskowego możesz zdefiniować właściwości kodu kreskowego.

Notatka: jeśli istnieje potrzeba ustawienia kodowania Paska kodu na Code 390-Modulo 43, ustaw wartość Field Checksum na „prawda”.

Dodawanie bieżącej daty (To Add the Current Date)

Bieżącą datę dodajemy tak, jak każdy inny obiekt – wybierając obiekt z paska narzędzi, a następnie klikając w polu roboczym Projektowania identyfikatora.

1 – Z szablonu Projektowanie identyfikatora wybierz Bieżąca data (Current date), następnie kliknij w polu roboczym Projektowania identyfikatora.

2 – Kliknij prawym przyciskiem na bieżącej dacie, aby wyświetlić menu.

3 – Aby przypisać bieżącą datę, sprawdź Przypisywanie obiektu do układu szablonu (To Align Objects in the Template Layout).

4 – Wybierz Właściwości bieżącej daty z menu.

5 – Z okna Bieżąca data możesz:

- Wybrać format daty (górną część okna)
- Zmienić właściwości tekstu (czcionka, kolor, justowanie, orientacja, etc.)



Dodawanie obrazu (To Add an Image)

Obrazy (zeskanowane zdjęcia, zdjęcia wykonane aparatem cyfrowym, ilustracje wykonane w dowolnym programie graficznym) mogą być importowane z dowolnego katalogu.

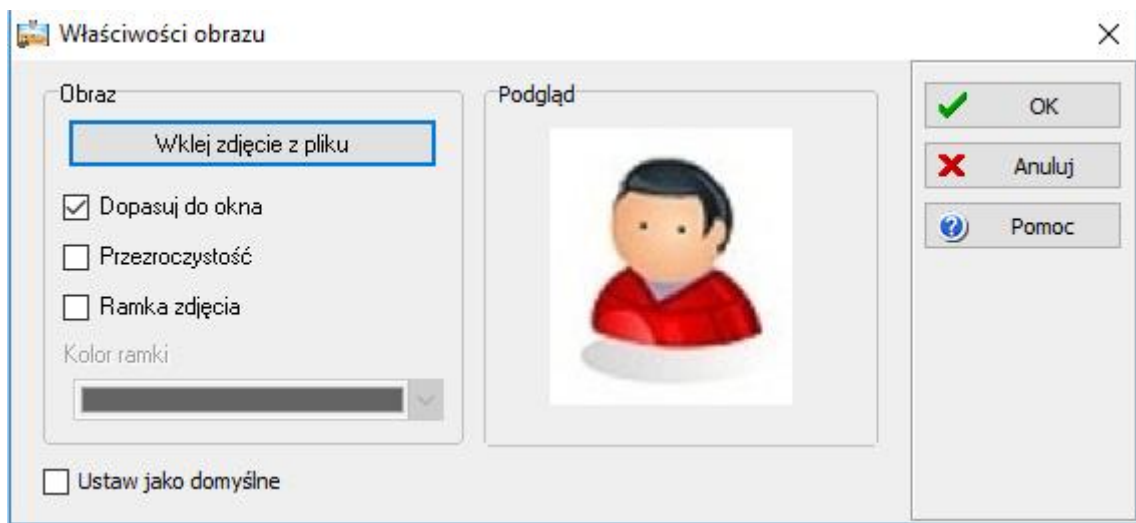
1 – Z okna Projektowanie identyfikatora, wybierz przycisk Obraz (Picture).

Notatka: opcja Identyfikowania obsługuje większość dostępnych formatów: BMP, JPG, EMF, WMF, GIF, PNG, PCD oraz TIF.

2 – Upuść przycisk w polu roboczym szablonu. Wyświetli się okno Właściwości obrazu.

3 – Kliknij przycisk Wybierz z pliku (Select image from file). Pojawi się okno umożliwiające wybór obrazu.

4 – Wyszukaj obraz, kliknij Otwórz (Open). Obraz pojawi się w polu roboczym szablonu.



Notatka: kiedy importujesz obraz, musisz zmienić rozmiary oryginalnego obrazu tak, jak jest to przedstawione na ilustracji.

5 – Możesz zmienić rozmiar obrazu oraz przesuwać go (przy pomocy linii siatki). Aby uzyskać więcej informacji, sprawdź Przypisywanie obiektu do układu szablonu (To Align Objects in the Template Layout).

6 – Kliknij prawym przyciskiem na obrazie, aby zmienić jego właściwości.

Dodawanie innych obiektów (To Place Other Design Objects)

Możliwe jest dodawanie ramek, granic, prostokątów (regularnych, zaokrąglonych, etc.), linii oraz punktów w taki sam sposób, jak innych obiektów – wybierając z paska narzędzi, a następnie „upuszczając” w polu roboczym Projektowania identyfikatora.

1 – Z okna Projektowanie identyfikatora, wybierz obiekt, który chcesz dodać (obok przycisku Dyskietki), a następnie kliknij w polu roboczym Projektowania identyfikatora. Okna Projektowania identyfikatora zostanie wyświetlone.



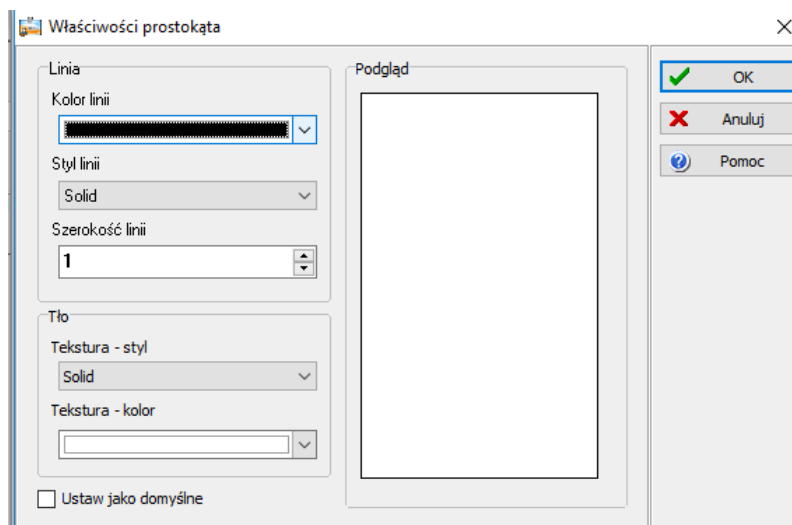
Użytkownicy

Modyfikacje grup kart

2 – Można zmienić kolor, styl i grubość ramki. Możesz zaznaczyć Użyj, jako domyślny (Set as default option), a następnie kliknąć OK, aby zamknąć.

Dodawanie prostokąta (To Place a Rectangle)

1 – Z okna Projektowanie identyfikatora, wybierz narzędzie prostokątów (rectangle tool), a następnie kliknij w polu roboczym.



Notatka: odnosi się to też do prostokątów, zaokrąglonych prostokątów oraz elips.

2 – W oknie Właściwości prostokątów możesz zdefiniować:

- Kolor linii,
- Styl linii,
- Grubość linii,
- Tło.

1 – Z menu Użytkownicy (Users), wybierz Identyfikator (Badge).

2 – Kliknij Drukuj próbkę (Print sample).

Notatka: jeśli Identyfikator jest dwustronny, słowo Próbka zostanie wydrukowane na obu stronach.



Operacje na grupach kart (Batch Operations on Cards)

To menu jest używane do modyfikowania grupy konkretnego typu kart. Możesz na przykład zmodyfikować „datę ważności” dla wszystkich kart typu „administrator”.

Przeprowadzanie działań na grupie kart (Performing Operations on a Group of Cards)

- 1 – Z paska narzędzi Użytkownicy wybierz przycisk Modyfikacje grup kart (Batch operations)
- 2 – Wybierz grupę użytkowników z listy Typy kart. Wszystkie karty z danej grupy zostaną zmodyfikowane.
- 3 – Wybierz odpowiedni filtr, aby sprecyzować Modyfikacje grup kart pośród konkretnych typów kart.

Notatka: lista filtrów kart jest dostępna tylko dla zarejestrowanych hattrix. Zobacz [Dodawanie komponentów systemu](#).

- 4 – Wybierz odpowiednią opcję z listy Operacji:

- Brak powiadomienia (No notification): system nie będzie informować o, ani nie będzie wymagać potwierdzenia od użytkownika.
- Powiadomienie (Notification): system wyświetli okno pokazujące postęp procesu.
- Powiadomienie i potwierdzenie (Notification and confirmation): system wyświetli okno pokazujące postęp procesu oraz będzie wymagać potwierdzenia operacji przez użytkownika dla każdego posiadacza konkretnego typu kart.

- 5 – Wybierz opcję, którą chcesz modyfikować dla wybranego typu.

- Karta (Card): jeżeli zostanie wybrany stan karty, system przypisze nowy stan karty do wszystkich użytkowników wybranego typu kart.
- Wartość zliczenia (Card count value): jeżeli zostanie wybrana wartość zliczania, system przypisze tą wartość do wszystkich użytkowników wybranego typu kart.
- Namierz (Trace): jeżeli wybrane zostało namierzanie, system będzie śledzić wszystkich użytkowników wybranego typu kart.
- Data rozpoczęcia (Start date): jeżeli została wybrana data rozpoczęcia, karty będą ważne dopiero od tej daty. Nowa data zostaje przypisana do wszystkich użytkowników wybranego typu kart.
- Data zakończenia (End date): jeżeli została wybrana data zakończenia, wszystkie karty przestaną działać po tej dacie. Nowa data zostaje przypisana do wszystkich użytkowników wybranego typu kart.



EntraPass - Instrukcja instalacji i obsługi programu Użytkownicy

- Usunąć po terminie ważności (Delete when expired): jeżeli wybrano tę opcję, karty zostaną usunięte w momencie przekroczenia Daty zakończenia (End date) określonej w Definicji Karty (Card Definition).
- Oczekiwanie na kod PIN z klawiatury (Wait for keypad) — jeżeli zostało wybrane, wszyscy użytkownicy wybranego typu kart będą musieli wprowadzić swój numer PIN przy pomocy klawiatury po wczytaniu karty.
- Grupa dostępu dla karty (Card access group): dwie listy, służące do modyfikowania grup dostępu dla karty dla wybranego typu karty, stają się dostępne. Pierwsza definiuje działania dla wybranego typu karty. Druga zawiera grupy dostępu dla karty (zdefiniowane w EntraPass), które zostaną wykorzystane do przeprowadzenia działania.
 - Zastąp grupę dostępu dla karty (Replace card access group (Replace)): zastępuje obecny poziom dostępu przez nowy, wybrany z listy.
 - Aktualizuj grupę dostępu dla karty (Update card access group (Update)): aktualizuje obecny poziom dostępu o nową, wybraną z listy. W przypadku, gdy poziom dostępu jest ustawiony na „żaden” (none), nowy poziom dostępu nie zostanie dodany.
 - Dodaj nowy poziom dostępu (Add new access level (Add)): ta opcja jest używana w przypadku dodania nowych obiektów i sytuacji, gdy poziomy dostępu na nowych obiektach muszą zostać dodane do listy poziomów dostępu.
 - Połącz poziomy dostępu (Merge): łączy poziomy z obu list. Nowe obiekty mają pierwszeństwo nad obecnymi.

Przykłady operacji wsadowych na poziomach dostępu (Examples of batch operations on card access levels)

Bieżący poziom dostępu	Nowy poziom dostępu	Zastąp	Aktualizuj	Dodaj	Połącz
Połączenie Y1	Połączenie X1	Połączenie X1	Połączenie X1	Połączenie Y1	Połączenie X1
Połączenie Y2	Połączenie X2	Połączenie X2	Połączenie X2	Połączenie Y2	Połączenie X2
Połączenie Y3	Brak połączenie	Brak połączenie	Połączenie Y3	Połączenie Y3	Połączenie Y3
Brak połączenia	Połączenie X4	Połączenie X4	Brak połączenie	Połączenie X4	Połączenie X4

- Szablon karty (Card layout): jeżeli wybrana, zostanie wyświetlona lista układów szablonów kart.
- Filtr karty (Card filter): użyj wybranego filtra dla wszystkich użytkowników wybranego typu kart.

6 – Kliknij przycisk Wykonaj (Execute), aby rozpocząć proces. System poprosi o potwierdzenie operacji.

7 – Kliknij Tak (Yest), aby kontynuować. W momencie rozpoczęcia procesu w dolnym, lewym okienku zostanie wyświetlony czerwony wskaźnik. Wskaźnik pozostanie czerwony aż do zakończenia procesu.



Definiowanie grup dostępu (Card Access Groups Definition)

Zdefiniowane wcześniej grupy dostępu dla karty umożliwiają szybki wybór poziomów dostępu dla różnych obiektów w systemie. Te grupy mogą zostać wykorzystane przy programowaniu kart w miejsce każdorazowego, osobnego wprowadzania poziomów dostępu dla każdego połączenia.

Notatka: w trakcie importowania kart, Grupa dostępu karty może zostać wykorzystana do przypisania poziomu dostępu do kart.

- 1 – Z paska narzędzi Użytkownicy, kliknij przycisk Grupa dostępu dla karty (Card access group)
- 2 – Aby zmodyfikować istniejącą grupę dostępu dla karty, wybierz ją z listy. Aby stworzyć nową grupę, kliknij przycisk Nowa (New) i wprowadź nazwę nowej grupy. Kolumna Połączenie (Connection) wyświetla połączenie/połączenia powiązane z grupą dostępu dla karty.
- 3 – Z listy Poziom dostępu, wybierz poziom, który określi dostęp wybranego połączenia do drzwi.



Definiowanie opcji kart (Card Options Definition)

Użyj zakładki Różne (Miscellaneous), aby określić i sprawdzić opcje karty.

1 – Wybierz numer karty przy pomocy strzałek góra/dół. Pole Data rozpoczęcia (Start date) wskazuje na datę utworzenia karty. Możesz zmienić tą datę wybierając inną z wyświetlonego kalendarza. Data rozpoczęcia musi być taka sama, albo wcześniejsza, w stosunku do bieżącej daty. W przeciwnym wypadku pole Stan karty (Card state) (w sekcji Różne (Miscellaneous)) będzie wyświetlać Oczekuje (Pending).

2 – Zaznacz Użyj daty zakończenia (Use end date), jeżeli jest taka możliwość. W przypadku zaznaczenia, system wyświetli kalendarz pozwalający wybrać datę zakończenia. Po przekroczeniu tej daty, pole Stan karty (Card state) wyświetli Wygasło (Expired).

Notatka: jeżeli firmware jest zaktualizowany przy określeniu godziny terminu ważności wykorzystywana jest bieżąca godzina połączenia. Dostępne wyłącznie dla kontrolerów KT-400 oraz KT-1.

3 – Zaznacz Usuń po terminie ważności (Delete when expired) (jeśli opcja jest dostępna). Ta opcja może być używana wyłącznie z opcją Użyj daty zakończenia (Use end date). W przypadku zaznaczenia, informacje na temat karty zostaną usunięte po przekroczeniu daty zakończenia (określonej wcześniej).

Notatka: usunięta karta to karta, która nie jest aktywna w bazie danych. Nawet, jeżeli karta została usunięta zdarzenia wygenerowane przez tą kartę są nadal przechowywane w archiwum.

4 – Zaznacz Oczekiwanie na kod PIN z klawiatury (Wait for keypad), aby wymusić na użytkowniku wprowadzenia numeru PIN. W pole Edycja numeru PIN (Editable PIN) wprowadź numer PIN, który będzie wymagany.

5 - Edycja numeru PIN (Editable PIN number): użytkownik może wprowadzić numer PIN wymagany przez czynnik/klawiaturę, aby uzyskać dostęp.

Notatka: wybranie Czekaj na klawiaturę opóźni dostęp do drzwi dla tej karty, aż do momentu wprowadzenia prawidłowego numeru PIN. Dotyczy to tylko drzwi z czytnikami oraz keypadami zdefiniowanymi w menu Definiowania drzwi (Urządzenia > Drzwi). Terminarz drzwi musi być ważny. Zobacz Konfigurowanie drzwi.

6 – Z listy Stan karty (Card state) wybierz stan dla zaznaczonej karty. Domyślnie: ważna (valid). Poniżej lista możliwości:

- Ważna (Valid): karta jest aktywna,
- Nieważna (Invalid): karta NIE jest aktywna,
- Zgubiona/Skradzione: karta NIE jest aktywna,
- Oczekująca (Pending) : karta nie jest jeszcze aktywna,
- Wygasła (Expired): karta przekroczyła datę zakończenia, nie jest już aktywna.

Notatka: nie można zmienić stanu karty na Oczekujący poprzez wybranie tego stanu z listy. Aby to zrobić, musisz zmienić Datę Początkową.

7 – Zaznacz Wyłącz passback (Disable passback), jeżeli chcesz, aby karta obesła passback.

Notatka: jeżeli przypisujesz kartę osobie z ograniczeniami ruchowymi zaznacz opcje Wydłużonego dostępu do drzwi. Aby włączyć tą opcję musisz określić odpowiednia opóźnienie w Definiowaniu drzwi.

Notatka: jeżeli przypisujesz kartę osobie z ograniczeniami ruchowymi zaznacz opcje Wydłużonego dostępu do drzwi. Aby włączyć tą opcję musisz określić odpowiednia opóźnienie w Definiowaniu drzwi. Ta opcja jest również dostępna przy definiowaniu karty gościa.

Notatka: jeżeli istnieje taka potrzeba zaznacz opcję Uprzywilejowane operacje, aby obejść dowolne zabezpieczenia drzwi.

8 – Dopuść Multi-odczyt karty (KT-400 oraz KT-1): umożliwia akcję Multi-odczytu karty.



EntraPass - Instrukcja instalacji i obsługi programu Użytkownicy



Nadruk na kartach (Card Printing)

Użyj opcji Drukuj (Print), aby wydrukować konkretny zakres kart ze wszystkich, które są przechowywane w bazie danych. Możesz skorzystać z wielu filtrów, aby zdefiniować listę do wydrukowania. Możesz podejrzeć listę przed wydrukiem, aby ją zmodyfikować albo zmienić ustawienia pól przed wydrukiem. Przy pomocy przycisku Czcionka (Font) możesz zmienić czcionkę i jej rozmiar dla drukowanego raportu.

Notatka: niezależnie od wyboru, nazwa użytkownika karty oraz numer karty zawsze będą wyświetlane. Domyślnie, tylko pola z informacjami będą drukowane. Jeżeli nie zostaną wybrane żadne pola, tylko pola z informacjami będą drukowane. Aby wydrukować puste pola, zaznacz pole Drukuj puste pola. Jeżeli chcesz wydrukować referencje komponentów, zaznacz pole Drukuj referencje komponentów. Jeżeli chcesz zrobić podgląd raportów kart przynajmniej jedna drukarka musi być zainstalowana.

1 – Z okienka Karta (Card), kliknij przycisk Drukarka (Printer).

Notatka: domyślnie puste pola nie są drukowane. Aby je wydrukować, zaznacz pole Drukuj puste pola.

2 – Wybierz kryterium sortowania z listy Indeks kart (Card Index).

3 – Jeżeli drukujesz konkretny zakres, zaznacz opcję Oznacz zakres (Specific range). Wybierz pole, które będzie używane do sortowania listy kart. Na przykład, jeżeli wybrałeś Numer karty, karty zostaną posortowane według kolejności numerów kart.

- Jeżeli chcesz wydrukować konkretny zakres, musisz określić numer początkowy w polu Dolna granica (Lower boundary).

- Jeżeli chcesz wydrukować konkretny zakres, i wprowadziłeś numer w polu Dolna granica (Lower boundary), wprowadź numer albo literę w polu Górna granica (Upper boundary).

Notatka: wydrukowane zostaną wyłącznie te karty, które pasują do WSZYSTKICH wybranych filtrów. Na przykład, jeżeli określisz sześć filtrów, sześć kryteriów musi zostać spełnione.

4 – Wybierz opcję Filtr (Filter), jeżeli nie chcesz, aby system przeszukiwał wszystkie karty w systemie. Filtry zawężą poszukiwania do potrzebnych kart.

- Data rozpoczęcia od/do (Start date between): system uwzględni karty, których data rozpoczęcia mieści się określonym przedziale (zakładka Różne).

- Data zakończenia od/do (End date between): system uwzględni karty, których data zakończenia mieści się określonym przedziale (zakładka Różne).



EntraPass - Instrukcja instalacji i obsługi programu Użytkownicy

- Karta (Card): wybierz tę opcję, aby wybrać określony stan. System uwzględni karty, których stan zgadza się z wybranym do filtrowania (zakładka Różne).
- Typ karty (Card type): wybierz tę opcję, aby wybrać określony typ karty. System uwzględni karty, których typ zgadza się z wybranym do filtrowania.
- Wybierz Namierzanie dla systemu (Exist trace for the system), aby uwzględnić karty, które posiadają opcje Namierz kartę (Card trace).
- Wybierz Opcja komentarzu (Exist comment option), aby uwzględnić karty, które posiadają pole Komentarz (Comment).
- Wybierz PIN (Exist PIN): system uwzględni karty, które posiadają numer PIN.
- Wybierz Usuń po terminie ważności (Exist delete when expired): aby uwzględnić karty, które posiadają opcję Usuń po terminie ważności.
- Wybierz Oczekiwanie na kod PIN z klawiatury (Exist wait for keypad), aby uwzględnić karty, które posiadają opcję Czekaj na klawiaturę.

5 – Możesz również wybrać Drukuj wybrane pola (Print selected fields), aby dodać konkretne dane.

6 – Kliknij filtr Wybierz dostęp do drzwi (Select door access), jeżeli chcesz dodać karty powiązane z drzwiami.

7 – Wybierz opcję Czas (Based on time), jeżeli chcesz wybrać karty według czasu, ale opcję Terminarz (Based on schedule), aby wybrać karty według zdefiniowanego terminarza.

Notatka: aby rozszerzyć wybór, kliknij prawym w oknie Wybierz drzwi do filtrowania.

8 – Zaznacz pole, które chcesz wydrukować. System doda zawartość pola, tak jak jest ono opisane w definicji karty.

9 – Możesz zapisać listę, jako plik .QRP (Quick Report), aby sprawdzić ją później przy pomocy opcji Quick Viewer.

10 – Możesz zmienić czcionkę i jej rozmiar przy pomocy przycisku Czcionka (Font). Ta zmiana zostanie przeprowadzona automatycznie w polu Próbką. Przycisk Podgląd (Preview) pozwoli na podgląd raportu.



Definiowanie typów kart (Card Type Definition)

Typ karty jest używany do grupowania użytkowników kart, a później również do modyfikowania istniejącej grupy kart albo tworzenia nowego raportu. Może również zostać wykorzystany do ograniczenia dostępu do informacji dla konkretnego użytkownika. Na przykład, możesz ograniczyć dostęp do wglądu oraz działań do konkretnej grupy kart dla konkretnego użytkownika. Czyli, jeżeli typ karty jest określony jako „Admin”, użytkownik nie posiadający odpowiedniego poziomu dostępu nie będzie mógł działać, podglądać, modyfikować, usuwać ani drukować tego typu karty.

Notatka: system ma zdefiniowane pięć typów kart, m.in. administratora, pracownika, ochrony, etc. Rodzaj karty może zostać przypisany do grupy dostępu kart.

Tworzenie nowego typu karty (Creating a New Card Type)

- 1 – Z paska narzędzi Użytkownicy (Users), kliknij przycisk Typ karty (Card type).
- 2 – W oknie Typ karty (Card type), kliknij przycisk Nowy (New) na pasku narzędzi, po czym wprowadź niezbędne informacje.
- 3 – Z listy Grupa dostępu do karty (Card access group) wybierz grupę albo utwórz jedną. Zobacz: Definiowanie grup dostępu dla karty (Card Access Groups Definition).
- 4 – Aby przypisać rodzaj karty do użytkownika, zobacz Definiowanie kart (Cards definition).



Przypisywanie poziomów dostępu (Cardholder Access Levels Assignment)

Poziom dostępu musi być przypisany do każdej karty. Poziom dostępu opisuje, gdzie i kiedy karta jest ważna. Pozwala użytkownikowi karty na dostęp do wybranych obiektów w czasie określonym przez terminarz. Zobacz: Definiowanie poziomów dostępu (Access Levels Definition).

Notatka: jeśli zmodyfikujesz poziom dostępu przypisany do karty modyfikujesz także pozwolenia danego użytkownika dotyczące dostępu do drzwi oraz terminarzy przypisanych do tego poziomu dostępu.

Aby przypisać poziom dostępu do karty:

- Stwórz terminarz,
- Przypisz terminarz do drzwi,
- Przypisz poziom dostępu do karty.

Przypisanie poziomów dostępu dla użytkowników (Assigning an Access Level to a Cardholder)

1 – Z okna Definiowanie karty (Card definition), wybierz zakładkę Poziom dostępu. Okno Poziomu dostępu zostanie wyświetlone, a w nim kolumna Bramka / połączenie (Gateway / connection) oraz lista poziomów dostępu.

2 – Kliknij przycisk Grupy dostępu do karty (Card access group), aby skopiować informacje z grupy do karty. Kolumna Bramka / połączenie (Gateway / connection) wyświetla obiekty oraz bramki, do których poziom dostępu zostanie przypisany.

3 – Z listy Poziom dostępu (access level), wybierz poziom dostępu do drzwi w wybranym połączeniu dla danego użytkownika. Jeżeli nie chcesz, aby dany użytkownika posiadał dostęp do drzwi w wybranym połączeniu, pozostaw pole puste (albo wybierz opcję Żaden (None)).

Notatka: musisz utworzyć Poziomy dostępu (Użytkownika > Poziom dostępu), aby były one dostępne na liście Poziomów dostępu.



Definiowanie kart (Card Options Definition)

Użyj zakładki Różne (Miscellaneous), aby określić i sprawdzić opcje karty.

1 – Wybierz numer karty przy pomocy strzałek góra/dół. Pole Data rozpoczęcia (Start date) wskazuje na datę utworzenia karty. Możesz zmienić tą datę wybierając inną z wyświetlonego kalendarza. Data rozpoczęcia musi być taka sama, albo wcześniejsza, w stosunku do bieżącej daty. W przeciwnym wypadku pole Stan karty (Card state) (w sekcji Różne (Miscellaneous)) będzie wyświetlać Oczekuje (Pending).

2 – Zaznacz Użyj daty zakończenia (Use end date), jeżeli jest taka możliwość. W przypadku zaznaczenia, system wyświetli kalendarz pozwalający wybrać datę zakończenia. Po przekroczeniu tej daty, pole Stan karty (Card state) wyświetli Wygasło (Expired).

3 – Zaznacz Usuń po terminie ważności (Delete when expired) (jeśli opcja jest dostępna). Ta opcja może być używana wyłącznie z opcją Użyj daty zakończenia (Use end date). W przypadku zaznaczenia, informacje na temat karty zostaną usunięte po przekroczeniu daty zakończenia (określonej wcześniej).

Notatka: usunięta karta to karta, która nie jest aktywna w bazie danych. Nawet, jeżeli karta została usunięta zdarzenia wygenerowane przez tą kartę są nadal przechowywane w archiwum.

4 – Zaznacz Oczekiwanie na kod PIN z klawiatury (Wait for keypad), aby wymusić na użytkowniku wprowadzenia numeru PIN. W pole Edycja numeru PIN (Editable PIN) wprowadź numer PIN, który będzie wymagany.

5 - Edycja numeru PIN (Editable PIN number): użytkownik może wprowadzić numer PIN wymagany przez czynniki/klawiaturę, aby uzyskać dostęp.

Notatka: wybranie Czekaj na klawiaturę opóźni dostęp do drzwi dla tej karty, aż do momentu wprowadzenia prawidłowego numeru PIN. Dotyczy to tylko drzwi z czytnikami oraz keypadami zdefiniowanymi w menu Definiowania drzwi (Urządzenia > Drzwi). Terminarz drzwi musi być ważny. Zobacz Konfigurowanie drzwi.

6 – Z listy Stan karty (Card state) wybierz stan dla zaznaczonej karty. Domyślnie: ważna (valid). Poniżej lista możliwości:

- Ważna (Valid): karta jest aktywna,
- Nieważna (Invalid): karta NIE jest aktywna,
- Zgubiona/Skradzione: karta NIE jest aktywna,
- Oczekująca (Pending) : karta nie jest jeszcze aktywna,
- Wygasła (Expired): karta przekroczyła datę zakończenia, nie jest już aktywna.

Notatka: nie można zmienić stanu karty na Oczekujący poprzez wybranie tego stanu z listy. Aby to zrobić, musisz zmienić Datę Początkową.

7 – Zaznacz Wyłącz passback (Disable passback), jeżeli chcesz, aby karta obeszła passback.

Notatka: jeżeli przypisujesz kartę osobie z ograniczeniami ruchowymi zaznacz opcje Wydłużonego dostępu do drzwi. Aby wyłączyć tą opcję musisz określić odpowiednia opóźnienie w Definiowaniu drzwi.

Notatka: jeżeli przypisujesz kartę osobie z ograniczeniami ruchowymi zaznacz opcje Wydłużonego dostępu do drzwi. Aby wyłączyć tą opcję musisz określić odpowiednia opóźnienie w Definiowaniu drzwi. Ta opcja jest również dostępna przy definiowaniu karty gościa.

Notatka: jeżeli istnieje taka potrzeba zaznacz opcję Uprzywilejowane operacje, aby obejść dowolne zabezpieczenia drzwi.



Dodawanie komentarza do karty (Adding Comments to a Card)

- 1 – Z okna Karta (Card), wybierz zakładkę Komentarz (Comment).
- 2 – Wpisz komentarz. Maksymalna liczba znaków: 241.
- 3 – Kliknij Zapisz (Save), a następnie Zamknij (Close).

Ograniczenie użycia karty (Limiting Card Usage)

EntraPass umożliwia wprowadzenie ograniczenia co do ilości razy użycia karty.

- 1 – Z okna Karta (Card), wybierz zakładkę Użycie (Usage).
- 2 – Zaznacz Włącz ograniczenie użycia (Enable usage restriction), aby aktywować funkcję.
- 3 – Z listy wybierz maksymalną liczbę określającą ilość użyci karty. Możesz wprowadzić wartość, albo wybrać przy pomocy strzałek.

Notatka: po określeniu Maksymalnej liczby wykorzystania karty, aktualny stan wykorzystania jest automatycznie aktualizowany po każdym użyciu karty. Istnieje możliwość zaznaczenia opcji Resetuj do zera, po zaznaczeniu której stan jest resetowany po przekroczeniu Maksymalnej liczby wykorzystania karty.



Przypisanie obrazu lub podpisu (Assigning Pictures and Signatures)

EntraPass umożliwia przypisywanie obrazów oraz podpisów do użytkowników, jak również szablonów identyfikatorów do kart. Obrazy oraz podpisy mogą być dodawane z pliku, wklejane, oraz przeklejane przy pomocy odpowiednich narzędzi. Zrzuty można wykonać przy pomocy urządzeń zgodnych z MCI albo TWAIN. Do wykonania zrzutów podpisów rekomendowane są pady, np. Topaz, Penware TTI500 albo Penware TT3100.

Przypisanie obrazu z pliku (Assigning a Picture from a File)

1 – Z okna Karta (Card), wybierz zakładkę Obraz (Picture)

Notatka: opcja Zapisywania wideo jest dostępna wyłącznie wtedy, kiedy zainstalowane urządzenie do zapisywania wideo.

2 – Kliknij prawym na obrazie. Z menu wybierz odpowiednią akcję:

- Pobierz obraz z pliku (Get picture from file): ta opcja pozwala wybrać obraz z posiadanych, zapisanych wcześniej obrazów:

3 – Z listy Typ plików (Files of type) wybierz typ, którego szukasz albo pozostaw na Wyświetl wszystkie (All), aby wyświetlić wszystkie pliki obrazów.

4 – Wybierz katalog, w którym przechowywane są obrazy. Wybierz obraz, a następnie kliknij Otwórz (Open), aby wprowadzić go w okno Karty (Card).

Notatka: obsługiwane są następujące formaty: BMP, EMF, WMF, JPG, GIF, PNG, PCD oraz TIF..

- Wstaw obraz (Paste picture): ta opcja pozwala wstawić skopiowany wcześniej obraz.

Notatka: aby usunąć zaimportowany obraz kliknij na niego prawym, a następnie wybierz Usuń obraz.



Przypisywanie obrazu przy pomocy kamery (Assigning a Picture Using a Video Camera)

Wykonywanie zrzutu obrazu jest możliwe tylko wtedy, gdy opcja Włącz zrzut ekranu (Enable video capture) jest aktywna: Opcje > Urządzenia multimedialne > Zrzut ekranu (Options > Multimedia devices > Video capture tab).

Notatka: zanim zapiszesz obraz przy pomocy kamery musisz upewnić się, że cały sprzęt jest odpowiednio skalibrowany. Dowiedz się więcej sprawdzając instrukcję obsługi danego urządzenia. Jeżeli posiadasz więcej niż jeden sterownik wideo określ, który sterownik będzie wykorzystany (Options > Urządzenia multimedialne > Zakładka wideo).

1 – Kliknij prawym przyciskiem na obrazie.

2 – Z menu wybierz Zrzut ekranu (Video capture).

Notatka: opcje mogą się różnić zależnie od programu. Jeżeli posiadasz więcej niż jeden sterownik wideo określ, który sterownik będzie wykorzystany. Zobacz Konfiguracja urządzeń multimedialnych.

3 – Kliknij przycisk Zatrzymaj (Freeze), kiedy znalazłeś odpowiedni obraz nagrania, następnie kliknij Zrzuć (Capture), aby zachować obraz.

4 – Aby przypisać szablon identyfikatora do wybranej karty, wybierz szablon z listy. Zobacz: Projektowanie Identyfikatorów (Badges designing).

Notatka: przyciski Drukuj identyfikator oraz Pogląd identyfikatora są dostępne w momencie, kiedy drukarka oraz układ identyfikatorów zostały wybrane, a opcja Użyj drukarki identyfikatorów została zaznaczona: Opcje > Opcje drukarki > Drukarka identyfikatorów. Dzięki tym przyciskom możesz podglądać i drukować identyfikatory.



Importowanie podpisu z pliku (Importing a signature from a file)

Możesz importować podpisy, tak jak importujesz inne obrazy na kartę.

1 – W oknie Karta (Card), kliknij prawym na podpisie.

2 – Z menu wybierz odpowiednią akcję:

- Pobierz podpis z pliku (Get signature from file): ta opcja pozwala wybrać podpis z posiadanych, zapisanych wcześniej obrazów.
- Wstaw obraz (Paste signature): ta opcja pozwala wstawić skopiowany wcześniej obraz.

Notatka: opcja Pad podpisów jest dostępna, jeżeli odpowiednie urządzenie jest udostępnione w menu Opcje.

3 – Wybierz podpis, a następnie kliknij Otwórz (Open).

Dodawanie podpisu ze Skanera do wzoru podpisu (Adding a Signature from a Signature Capture Device)

Ta opcja jest dostępna tylko w przypadku, gdy zainstalowane jest Skaner do wzoru podpisu (Signature Capture Device). Pad do podpisów musi być odblokowany w menu Opcji (Options) – Options > Multimedia devices > Signature (Options > Multimedia devices > Signature).

1 – W oknie Karta (Card), kliknij prawym na podpisie.

2 – Z menu wybierz Pad do podpisów (Signature pad). Pojawi się okno Podpis (Signature), w którym możesz podejrzeć podpis.

3 – Kliknij OK, aby wstawić podpis.

Edytowanie obrazów i podpisów (Working with Photos and Signatures)

Opcja EntraPass Definiowanie szablonów identyfikatorów (Integrated Badging) pozwala użytkownikowi na wycięcie fragmentu zdjęcia albo powiększenie obrazów, które są wgrane na karty.



Wycinanie fragmentu obrazu (Extracting Part of an Image)

Jeżeli wgrałeś duży obraz, a potrzebujesz tylko fragmentu, możesz wybrać i wyciąć ten fragment i przypisać go do karty.

1 – Kliknij prawym na obraz, który zaimportowałeś.

Notatka: opcja Wycinania jest włączona tylko po uruchomieniu trybu selekcji. Analogicznie, opcje Cofnij jest dostępna tylko po dodaniu obrazu.

2 – Wybierz Uruchom tryb wyboru (Start selection mode) z menu.

Notatka: możesz zwiększyć obszar selekcji przeciągając rogi oraz boki uprzednia zaznaczonego obszaru. Możesz również przenieść go w inny fragment obrazu.

3 – Po wybraniu fragmentu, który chcesz włączyć do karty, ponownie kliknij prawym na obraz.

Notatka: aby anulować selekcję kliknij prawym na na obrazie, a następnie wybierz Anuluj selekcję. Wybierz Cofnij, aby odrzucić zmiany. Opcja Cofnij jest dostępna tylko po dodaniu obrazu.

4 – Z menu wybierz Wytnij (Extract).

Edytowanie obrazu/podpisu (Editing a Picture/Signature)

1 – Kliknij prawym na obraz, który chcesz edytować.

Notatka: obszar Kodu pozwala przypisać kod do identyfikatora. Z listy wybierz obiekt, który będzie wykorzystany, jako wartość dla kodu. Możesz również wprowadzić własną wartość w polu Wartość. Jeżeli nie wprowadzisz własnej wartości Numer karty będzie wykorzystany, jako domyślna wartość.

2 - Z menu wybierz Edytuj (Edit).

3 – Ustaw właściwości obrazu. Przycisk Przywróć (Reset all) przywraca oryginalny obraz:

- Auto kontrast (Auto contrast),
- Ostrość (Sharpen),
- Jasność (Brightness),
- Przywróć (Reset all).

4 – Kliknij OK, aby zamknąć okno edycji.

5 – Z menu Szablon identyfikatora (Badge layout) wybierz szablon, który chcesz przypisać do definiowanej karty. Zobacz: Projektowanie identyfikatorów (Badges Designing).



Drukowanie identyfikatorów (Printing Badges)

Możesz wydrukować identyfikator, karty gości oraz przepustki z okien: Karta (Card) albo Podgląd identyfikatora (Badge preview). Oprogramowanie pozwala na wydruk jedno, jak i dwu stronnych identyfikatorów.

Przed wydrukiem musisz wybrać drukarkę. Może to być dowolna drukarka sieciowa, albo konkretna drukarka identyfikatorów.

Wybierania drukarki identyfikatorów (Selecting a Badge Printer)

1 – Z okna Stacji roboczej EntraPass (EntraPass Workstation) wybierz pasek narzędzi Opcje (Options), a następnie wybierz przycisk Opcje drukarki (Printer Options).

2 – Z okna Opcje drukarki wybierz zakładkę Drukarka identyfikatorów (Badge printer).

Notatka: możesz drukować identyfikatory na dowolnej drukarce sieciowej. Żeby wydrukować identyfikator na karcie potrzebna jest drukarka identyfikatorów.

3 – Zaznacz opcję Drukarka identyfikatorów, żeby poinformować system, że drukarka identyfikatorów została wybrana. W oknie, z której możesz wydrukować identyfikatory (karty, przepustki, etc.) zostaną wyświetlone polecenia: Drukuj identyfikator (Print badge) oraz Podgląd identyfikatora (Preview badge).

4 – Z listy Wybierz drukarkę identyfikatorów (Select badge printer) wybierz drukarkę przeznaczoną do drukowania identyfikatorów.

5 – Dopasuj marginesy,

- Oś X: oznacza lewy margines,
- Oś Y: oznacza górny margines.



Podgląd i wydruk identyfikatorów (Previewing and Printing Badges)

Okno pozwala na podgląd układu identyfikatora z informacjami karty (w przypadku, gdy układ identyfikatora jest przypisane do karty) albo z domyślnymi wartościami (w przypadku, gdy szablon nie jest jeszcze przypisany do konkretnej karty). Oprogramowanie pozwala na wydruk jedno, jak i dwu stronnych identyfikatorów.

1 – W oknie Karta, Przepustka (Card, Visitor or Daypass) kliknij na Podgląd identyfikatora (Preview badge).

Notatka: z okna Projektowanie identyfikatora opcja podgląd pozwala sprawdzić wygląd identyfikatora z domyślnymi wartościami.

2 – Z okna podglądu wybierz opcję drukowania:

- Drukuj frony (Print front side):
- Drukuj tył (Print back side): opcja jest dostępna wyłącznie w przypadku, gdy identyfikator ma dwie strony.
- Drukuj front i tył (Print both sides): opcja jest dostępna wyłącznie w przypadku, gdy identyfikator ma dwie strony.

Notatka: ważne! Aby wydrukować identyfikator z kodami należy prawidłowo skalibrować drukarkę. Musisz zaznaczyć opcję „black resin” (czarny), albo czytniki kodów mogą nie dać rady odczytać wydrukowanego kodu. Jeżeli masz problemy z drukowaniem kodów sprawdź instrukcję obsługi drukarki.



Definiowanie kart (Cards Definition)

Karty są opisane przez następujące właściwości: numer karty, nazwa użytkownika karty, typ karty, poziom dostępu oraz status (ważna, nieważna, oczekująca, zgubiona/skradziona, wygasła). Jeśli włączyłeś opcję Wykorzystaj multi format karty w oknie Format Karty (zobacz [Definiowanie formatu karty](#)), będziesz mógł zmieniać format karty dla każdej karty indywidualnie. Ta opcja umożliwia większą elastyczność przy przypisywaniu wielu kart do użytkownika albo przy przypisywaniu kart użytkowników do obiektów wyposażonych w różne technologie czytników. Innymi słowy, przy tworzeniu karty dla użytkownika, operator będzie mógł wybrać format karty bezpośrednio w okienku Karta, zgodnie z rodzajem czytnika użytym na obszarze, w którym użytkownik będzie wchodził do budynku. Jeśli włączyłeś opcję Zaawansowanego zarządzania w okienku Parametry systemu definicja karty będzie trochę inna. W tym środowisku, EntraPass pozwala na utworzenie karty użytkownika bez numeru przypisanego do niej. W obu przypadkach, karty zostaną zdefiniowane poprzez: nazwę użytkownika, rodzaj karty, poziom dostępu karty oraz status. Archiwa kart mogą być przeszukiwane, sortowane oraz usuwane.

Raport aktywności (Activity report)

Ikona raportu aktywności na pasku narzędzi staje się dostępna po wybraniu karty. Użyj tej ikony do generowania szybkiego raportu na podstawie parametrów czasu. Raport zawiera następujące informacje na user'scard: Data i godzina, komunikat zdarzenia, numer karty i wiele kolumn opis. Aby uzyskać więcej informacji opcji raportu, zobacz Wyświetlanie podglądu raportów.

Raport aktywności: generuje ostatni raport transakcji na podstawie parametrów czasowych, które należy wprowadzić. Po zakończeniu raportu, EntraPass generuje zdarzenie ze szczegółami, kto zażądał raportu i dla jakiego użytkownika.

Wprowadzanie nowej karty (Issuing a New Card)

1 – Z paska narzędzi Użytkownicy (Users), wybierz Karta (Card). Nowe okno Karty jest wykorzystane do wprowadzenia/zmiany informacji o użytkowniku karty.

Notatka: jeśli włączyłeś Zaawansowane zarządzanie (Enhanced User Management), przejdź do sekcji Wprowadzanie nowej karty w środowisku zaawansowanego zarządzania.

2 – Kliknij przycisk Nowy (New) na pasku narzędzi. Pole numeru karty jest dostępne.

3 – Wprowadź numer wydrukowany na karcie, następnie wciśnij Enter. Jeśli jest to nowa karta, w polu Nazwa użytkownika karty (Card user name) wyświetla się nazwa Nowy użytkownik (New user). Jeśli karta istniała wcześniej, system wyświetla informacje na temat karty.

4 – Wprowadź nazwę użytkownika karty w pole Nazwa użytkownika karty. Można użyć do 50 znaków.

5 – Zaznacz pole Skopiuj do karty gościa (Copy to visitor card). Dzięki temu informacje z karty są kopiowane do bazy danych szablonów gości (numer karty nie jest kopiowany). Ta opcja umożliwia archiwizowanie profili na wypadek potrzeby wystawienia karty tymczasowej.

6 – Zaznacz pole Typ karty (Card type), aby otworzyć menu Typ karty. Wybierz typ karty dla nowej karty. Typ karty jest używany do grupowania użytkowników kart, a później również do modyfikowania istniejącej grupy kart albo tworzenia nowego raportu. Zobacz: Definiowanie typów kart (Card Type Definition).

Notatka: w oknie Typ karty możesz kliknąć prawym na polu Typ karty i wybrać Nowy, aby stworzyć nowy typ karty. Kliknij Wybierz, aby wybrać istniejący typ karty albo Edytuj, aby edytować.

Notatka: system automatycznie wyświetla datę utworzenia, datę modyfikacji oraz liczbę modyfikacji w prawej-górnej części okna.



Użytkownicy

Definiowanie kart

7 – Wypełnij 1-20 pól z informacjami o karcie. Pola informacji gromadzą dodatkowe informacje na temat użytkownika karty. Na przykład, pole z informacjami nr 1 może zawierać numer pracownika, pole nr 2 informacje na temat działu, w którym pracuje, pole nr 3 adres zamieszkania, etc. Później te dane można wykorzystać do indeksowania raportów, tworzenia list, wyszukiwania, etc.

Notatka: te pola informacyjne są edytowalne. Aby zmienić nazwę pola kliknij na nie podwójnie, po czym wprowadź nową nazwę (do 50 znaków).

8 – Kliknij przycisk Zapisz (Save).

Wprowadzanie nowej karty w Zawansowanym zarządzaniu (Issuing a New Card in Enhanced User Management Environment)

1 – Z paska narzędzi Użytkownicy (Users), wybierz Kartę (Card). Nowe okno Karty jest wykorzystane do wprowadzenia/zmiany informacji o użytkowniku karty.

2 – Kliknij przycisk Nowy (New) na pasku narzędzi. Wprowadź nazwę użytkownika karty w pole Nazwa użytkownika karty. Można użyć do 50 znaków.

3 - Kliknij przycisk Zapisz (Save).

4 – Dwukrotnie kliknij na pole Typ karty (Card type), aby otworzyć okno Typ karty. Wybierz typ karty dla nowej karty. Typ karty jest używany do grupowania użytkowników kart, a później również do modyfikowania istniejącej grupy kart albo tworzenia nowego raportu. Zobacz: Definiowanie typów kart (Card Type Definition).

Notatka: w oknie Typ karty możesz kliknąć prawym na polu Typ karty i wybrać Nowy, aby stworzyć nowy typ karty. Kliknij Wybierz, aby wybrać istniejący typ karty albo Edytuj, aby edytować.

5 – Kliknij na zakładkę Numer karty (Card number), dwukrotnie kliknij na Karta #1 (Card #1), jeżeli chcesz zmienić nazwę.

6 - Wprowadź numer karty.

- Jeśli EntraPass był wcześniej skonfigurowany na wielokrotne formatowanie kart (Multiple Card Format), możesz zmienić format karty klikając prawym przyciskiem na pole Numeru Karty (Card number). Domyślny format karty to HH:DDDDD (Hexadecimal / decimal 24 bits).

Notatka: Poziom dostępu zostanie przypisany do użytkownika, czyli do pięciu kart.

- Kiedy Wielokrotne formatowanie kart jest aktywne: lista wszystkich formatów kart zostanie wyświetlona, gdy klikniesz prawym przyciskiem na pole numeru karty.

- Kiedy format karty zostanie określony przez administratora systemu, przy opisie formatu karty pojawia się znaczek potwierdzenia.



EntraPass - Instrukcja instalacji i obsługi programu Użytkownicy

Karty

Nazwisko użytkownika: Elizabeth Green

Typ karty: Administrator

E-Mail:

Data utworzenia: 01.12.2016 08:47:41

Data zmiany: 14.01.2017 22:16:37

Licznik zmian: 14

Numer karty | Informacja | Poziom dostępu | Poziomy dostępu - wyjątki | Parametry | Zdjęcie | Użycie | Komentarz

	Wyświetl numer karty	Ustaw datę ważności	Data końca ważności	Godzina końca	Karta śledzona	Skradziona/Zgubiona
Karta # 1	000000001237088	☐	☐	0	☐	☐
Karta # 2	00:00000	☒	☐	0	☐	☐
Karta # 3	00:00000	☒	☐	0	☐	☐
Karta # 4	00:00000	☒	☐	0	☐	☐
Karta # 5	00:00000	☒	☐	0	☐	☐

Zakończ Anuluj Pomoc

7 – Opcjonalnie, możesz natychmiastowo przypisać Numer karty (Card number).

8 – Jeśli pozwalają na to twoje uprawnienia, możesz wyświetlić numer karty, lub też nie.

Notatka: system automatycznie wyświetla datę utworzenia, datę modyfikacji oraz liczbę modyfikacji w prawej-górnej części okna.

9 – Zaznacz opcje Użyj daty zakończenia (Use expiration date) i wybierz datę.

10 – Zaznacz opcje Namierzaj (Trace), jeżeli chcesz monitorować użycie konkretnej karty. Zaznaczenie tej opcji sprawi, że zdarzenie „namierzania” będzie generowane za każdym razem, gdy karta zostanie użyta przy czytniku.

11 – Zaznacz opcję Skradziona/Zgubiona (Stolen/Lost), jeżeli karta została skradziona lub zgubiona. Karta przestanie być aktywna.

12 – Powtórz działania 5-11 dla kart #2-#5.



Historia zmian karty (Card audit trail)

Użyj ikony Historii zmian, aby zobaczyć, kto dokonał zmian oraz kiedy zmiany nastąpiły na karcie.

Aby zapewnić dostęp do funkcji śledzenia **Historii zmian**, należy zezwolić operatorowi na użycie funkcji Historii zmian grupy Systemie, aby uzyskać więcej informacji, zobacz [Poziom zabezpieczeń](#).

1 - Kliknij opcję Użytkownicy, kliknij kartę i wybierz posiadacza karty z listy Nazwa użytkownika karty.

2 - Aby otworzyć okno Audit, na pasku narzędzi kliknij ikonę Audit trail.

Okno kontroli zawiera dwie tabele, pierwsza tabela zawiera następujące informacje o karcie:

- Kolumna oznaczona kolorem: wskazuje, czy karta została utworzona, zmodyfikowana lub usunięta.

o Zielony: Utwórz

o Niebieski: Modyfikuj

o Czerwony: Usuń

- Data i godzina: data i godzina utworzenia, modyfikacji lub usunięcia karty przez operatora.

- Operator: nazwa operatora, który dokonał zmiany.

- Count: liczba zmienionych pól.

Druga tabela zawiera następujące informacje o karcie:

- Typ odniesienia: połączenie, witryna lub brama podłączone do karty, która uległa zmianie.

- Odniesienie: pozycja odniesienia do zmiany.

- Nazwa pola: nazwa pola GUI.

- Stara wartość: wartość przed wystąpieniem zmiany.

- Nowa wartość: wartość, gdy system zapisał zmianę.

- Opis pola: opis nazwy pola.

Aby uzyskać dostęp do następujących opcji kolumn, kliknij ikonę Filtr w lewym górnym rogu tabeli.

- Typ danych: typ danych bazy danych:

o Czas

Er Liczba całkowita

o Obiekt

o Komponenty

- Nazwa tabeli: nazwa tabeli bazy danych.

UWAGA: Zdefiniuj wyniki na podstawie ilości rekordów lub daty. Aby uzyskać więcej informacji, zobacz Serwer loguje się w parametrze System.



EntraPass - Instrukcja instalacji i obsługi programu Użytkownicy

Aby uzyskać dostęp do menu kontekstowego, wybierz wpis tabeli i kliknij prawym przyciskiem myszy. Dostępne są następujące opcje:

- Wybrano eksport CSV: wyeksportuj wybrany wpis ścieżki audytu karty do pliku w formacie CSV.
- Eksportuj wszystkie pliki CSV: wyeksportuj całą zawartość ścieżki audytu karty do pliku w formacie CSV.
- Wyświetl starą wartość: wyświetl okno z wartością przed zmianą.
- Wyświetl rodzic nadrzędny starej wartości: wyświetl okno nadrzędnego wybranego komponentu z wcześniejszą wartością
zmiana.
- Wyświetl łącze starej wartości: wyświetl okno reprezentujące łącze do komponentu z wartością przed
zmiana.
- Wyświetl nową wartość: wyświetl okno z wartością po zmianie.
- Wyświetl nową wartość nadrzędną: wyświetl okno nadrzędnego wybranego komponentu z wartością po
zmiana.
- Wyświetl łącze nowej wartości: wyświetl okno przedstawiające łącze do komponentu z wartością po
zmiana.



Szybki dostęp do listy drzwi dla karty (Quick Access to Door List per Card)

Ta opcja umożliwia szybkie wyświetlenie listy drzwi, wraz z przypisanymi terminarzami, dla wszystkich poziomów bezpieczeństwa wybranego użytkownika.

1 – Z menu Użytkownicy/Karta, kliknij przycisk Lista dostępu do drzwi (Door access list):



Informacje są wyświetlane w pięciu kolumnach:

- Przycisk bramka/połączenie
- Opis bramka/połączenie
- Opis drzwi
- Opis terminarza

Notatka: informacje mogą zostać wyeksportowane do pliki CSV w celach wydrukowania albo raportowania.

Tworzenie nowych kart przy pomocy funkcji „Zapisz jako” (Creating New Cards Using the “Save As” Feature)

Opcja Zapisz jako (Save as) umożliwia tworzenie nowej karty w oparciu o istniejącą już przy jednej zmianie informacji. Na przykład: zmieniając tylko nazwę użytkownika, ale pozostawiając wszystkie pozostałe informacje bez zmian.

1 – Wprowadź zmiany w dowolne pola w oknie Karty (Cards), a następnie kliknij Zapisz jako (Save as). Dzięki temu będziesz mógł utworzyć nową kartę, pod nową nazwą.

2 – Wprowadź nowy numer karty w pole Nowy numer karty (New card number).

3 – Wybierz opcję Zachowaj/Usuń (Kepp/Delete) dla oryginalnej karty, aby zachować albo usunąć (zazwyczaj zachować) zmienianą kartę. Kliknij OK, aby zachować nowe informacje.

Select the Keep/Delete original card options to specify if the original card should be kept or deleted (usually kept), then click OK to save the new information. The Card window is displayed.



Operacja przy pomocy opcji „Załaduj wsadowo” (Issuing Cards Using the “Batch Load” Feature)

Opcja Załaduj wsadowo (Batch Load) pozwala na działanie na karcie przy przyłożeniu karty do czytnika. Numer karty jest wyświetlony przy zdarzeniu „nieznana karta” albo „wstęp zabroniony”. Podczas działania operator może stworzyć nową kartę albo zmodyfikować już istniejącą.

1 – Z okna Karty (Card), kliknij przycisk Załaduj wsadowo (Batch Load)

2 – Z listy drzwi, wybierz drzwi, które będą odczytywać karty.

3 – Zaznacz którąś z opcji:

- Odśwież na wejściu (Refresh an access granted): przy każdym wejściu wyświetlane informacje będą aktualizowane.

- Zapisz na nowej karcie (Save on new card): jeśli ta opcja jest zaznaczona, przy zdarzeniu „nieznana karta”, nowa karta będzie zapisana w bazie danych.

Notatka: jeśli ta opcja jest wybrana pierwsza karta wykorzystana przy czytniku zostanie zapisana tylko wtedy, kiedy zostanie zaprezentowana również druga karta albo po przyciśnięciu przycisku Zapisz.

- Znajdź (Find): pozwala użytkownikowi szukać istniejącej karty, aby w oparciu o nią stworzyć nową.

Notatka: jeśli użytkownik kliknie przycisk Zamknij bez zapisywania, system poprosi o zapisanie ostatnio dodanych informacji.

Podgląd i weryfikacja numeru PIN (Viewing and Verifying PINs)

EntraPass pozwala użytkownikowi na podgląd i sprawdzenie każdego numeru PIN.

Podgląd kart z tym samym numerem PIN (Viewing Cards Assigned the Same PIN)

1 – Z okna Karta (Card), kliknij przycisk Lista numerów PIN (List of PIN owners).

2 - Z okna Karta (Card) albo okna Gość (Visitor), kliknij przycisk Lista numerów PIN (List of PIN owners).

3 – Wprowadź numer PIN, który chcesz sprawdzić i kliknij OK. Lista użytkowników, którzy mają taki numer PIN zostanie wyświetlona na ekranie.

Notatka: jeśli system umożliwia powtarzanie numerów PIN (Opcje > Parametry systemu), oraz PIN jest wykorzystany przez więcej niż jednego użytkownika, system wyświetli listę użytkowników posługujących się danym numerem PIN. Opcja jest przydatna, kiedy chcesz wyświetlić listę użytkowników posługujących się danym numerem PIN, albo chcesz zweryfikować, jakie numery PIN są wykorzystywane.



Edytowanie karty (Editing a Card)

- Wprowadź numer karty w pole Numer karty (Card number), następnie wciśnij Enter. System wyświetli kartę, którą możesz teraz modyfikować.
- Przeglądaj numery kart przy użyciu strzałek góra/dół i wybierz kartę do modyfikowania.
- Przeglądaj Nazwy użytkowników przy użyciu strzałek góra/dół.

Odnajdywanie karty (Finding a Card)

Z paska narzędzi okienka Karta (Card) możesz przeprowadzić poszukiwania karty na dwa sposoby.

- Znajdź informację o karcie 
- Znajdź zarchiwizowane informacje o karcie 

Notatka: możesz wprowadzić nazwę użytkownika w pole Nazwa użytkownika. Po rozpoczęciu wprowadzania autouzupełnianie zaproponuje nazwę.

Notatka: sprawdź Odnajdywanie komponentów, aby dowiedzieć się więcej o wyszukiwaniu informacji.



Usuwanie karty (Deleting a Card)

Opcja usuwania umożliwia użytkownikowi z odpowiednim poziomem dostępu na usunięcie karty z bazy danych. Karta usunięta z bazy danych musi zostać wprowadzona do niej na nowo, aby móc z niej znowu korzystać.

1 – Znajdź kartę, którą chcesz usunąć.

2 – Kliknij przycisk Usuń (Delete), a następnie Tak (Yes) w celu potwierdzenia operacji.

Notatka: chociaż usunięta karta jest usuwana z bazy danych, informacje na jej temat pozostają w historii karty; wszystkie zdarzenia związane z tą kartą pozostają w bazie danych. Raport zdarzeń zawierający zdarzenia powiązane z usuniętą kartą może zostać przygotowany.

Dostosowywanie pól z informacjami o karcie (Customizing Card Information Fields)

Możesz zmieniać nazwy pól informacyjnych w zakładce Ogólne (General) według własnych wymogów. Te pola mogą zawierać dowolne informacje.

1 – W okienku Definiowanie kart (Card definitione) wybierz kartę, a następnie dwukrotnie kliknij na nazwę/etykietę w zakładce Ogólne. System wyświetli okno Zmiana nazwy/etykiety (Change labels).

2 – Po lewej wybierz pole, które chcesz modyfikować, a po prawej wprowadź nazwę. Jeżeli system pracuje w dwóch językach, dostępne będą dwa pola do wprowadzania nazwy.

3 – Wybierz opcję Edytuj pole (Edit field), jeżeli informacja pojawia się jako pole do edycji (prosta informacja), albo opcję listy (Drop-down list). Kliknij OK, aby zapisać modyfikacje.

4 – Powtórz te kroki dla wszystkich pól, które chcesz modyfikować.

Notatka: Zaznacz Pole obowiązkowe, aby upewnić się, że pole zostanie uzupełnione.

Notatka: użytkownik musi posiadać pełne prawa dostępu, aby edytować pola informacji o karcie. Użytkownik bez takich praw może tylko odczytać te informacje.

Notatka: użytkownik może wyszukiwać informacje w oparciu o każde z 40 pól informacyjnych karty.



Przypisywanie poziomów dostępu dla użytkowników (Cardholder Access Levels Assignment)

Poziom dostępu musi być przypisany do każdej karty. Poziom dostępu opisuje, gdzie i kiedy karta jest ważna. Pozwala użytkownikowi karty na dostęp do wybranych obiektów w czasie określonym przez terminarz. Zobacz: Definiowanie poziomów dostępu ([Access Levels Definition](#)).

Notatka: kiedy modyfikujesz poziom dostępu przypisany do karty, modyfikujesz również pozwolenia dostępu użytkownika do drzwi oraz terminarzy powiązanych z tym poziomem dostępu.

Aby przypisać poziom dostępu do karty:

- Stwórz terminarz,
- Przypisz terminarz do drzwi,
- Przypisz poziom dostępu do karty.

Przypisywanie dodatkowych poziomów dostępu (tylko multi obiektowe bramki) (Assigning Additional Access Levels (Multi-site gateway only))

Przy wykorzystaniu KT-400, KT-400 rev1, oraz KT-1 łącznie do pięciu poziomów dostępu na użytkownika/połączenie jest możliwe.

1 – z okna Definiowanie karty, wybierz zakładkę Poziom dostępu. W wyświetlonym oknie zostaną wyświetlone: kolumna Bramka/Połączenia oraz lista Poziom dostępu.

Małe pole w prawej kolumnie wskazuje, że połączenie ma kontrolery, które akceptują wiele poziomów dostępu. Jeśli pole jest czarne oznacza to, że nie dodano żadnych poziomów dostępu. Jeśli jest zielone, dodano przynajmniej jeden dodatkowy poziom został przypisany. Jeśli pole jest żółte dodatkowe poziomy nie mogą zostać przypisane.

2 – wybierz Bramkę albo Połączenie klikając na nie w kolumnie po prawej stronie. Dodatkowe okienko poziomów dostępu z innymi Bramkami oraz Połączeniami zostanie wyświetlone.

3 – Z tego okna dodatkowe poziomy dostępu mogą zostać przypisane.

Notatka: jeśli przy Poziomie bezpieczeństwa w prawej kolumnie wyświetla się znak ostrzegawczy oznacza to, że istnieją kontrolery powiązane z poziomem bezpieczeństwa, które nie wspierają dodatkowych poziomów bezpieczeństwa, czyli KT-100, KT-200 oraz KT-300.



Przypisanie poziomów dostępu dla użytkowników (Assigning an Access Level to a Cardholder)

1 – Z okna Definiowanie karty (Card definition), wybierz zakładkę Poziom dostępu. Okno Poziomu dostępu zostanie wyświetlone, a w nim kolumna Bramka / połączenie (Gateway / connection) oraz lista poziomów dostępu.

2 – Kliknij przycisk Grupy dostępu do karty (Card access group), aby skopiować informacje z grupy do karty. Kolumna Bramka / połączenie (Gateway / connection) wyświetla obiekty oraz bramki, do których poziom dostępu zostanie przypisany.

3 – Z listy Poziom dostępu (access level), wybierz poziom dostępu do drzwi w wybranym połączeniu dla danego użytkownika. Jeżeli nie chcesz, aby dany użytkownika posiadał dostęp do drzwi w wybranym połączeniu, pozostaw pole puste (albo wybierz opcję Żaden (None)).

Notatka: musisz utworzyć Poziom dostępu, aby wyświetlił się na liście Poziomów dostępu.

Wyjątki dostępu (Access Exception)

Użyj zakładki Wyjątki dostępu, aby przypisać konkretną operację do drzwi.

1 – Z lewego panelu wybierz drzwi.

2 – Z prawego panelu wybierz operacje z listy. Użyj przycisków:  oraz , aby dodać lub usunąć drzwi z listy po prawej.

3 – Pod kolumną Dostęp (Access), wybierz pomiędzy Dopuszcz (Allow) lub Zablockuj (Deny).

Notatka: tylko drzwi z przypisanym terminarzem zostaną zapisane.

Uwaga: lista użytkowników nie uwzględnia wyjątków.

Aby aktywować Wyjątki, sprawdź Parametry uwierzytelnienia.



Definiowanie opcji karty (Card Options Definition)

Użyj zakładki Różne (Miscellaneous), aby określić i sprawdzić opcje karty.

1 – Wybierz numer karty przy pomocy strzałek góra/dół. Pole Data rozpoczęcia (Start date) wskazuje na datę utworzenia karty. Możesz zmienić tą datę wybierając inną z wyświetlonego kalendarza. Data rozpoczęcia musi być taka sama, albo wcześniejsza, w stosunku do bieżącej daty. W przeciwnym wypadku pole Stan karty (Card state) (w sekcji Różne (Miscellaneous)) będzie wyświetlać Oczekuje (Pending).

2 – Zaznacz Użyj daty zakończenia (Use end date), jeżeli jest taka możliwość. W przypadku zaznaczenia, system wyświetli kalendarz pozwalający wybrać datę zakończenia. Po przekroczeniu tej daty, pole Stan karty (Card state) wyświetli Wygasło (Expired).

3 – Zaznacz Usuń po terminie ważności (Delete when expired) (jeśli opcja jest dostępna). Ta opcja może być używana wyłącznie z opcją Użyj daty zakończenia (Use end date). W przypadku zaznaczenia, informacje na temat karty zostaną usunięte po przekroczeniu daty zakończenia (określonej wcześniej).

Notatka: usunięta karta to karta, która nie jest aktywna w bazie danych. Nawet, jeżeli karta została usunięta zdarzenia wygenerowane przez tą kartę są nadal przechowywane w archiwum.

4 – Zaznacz Oczekiwanie na kod PIN z klawiatury (Wait for keypad), aby wymusić na użytkowniku wprowadzenia numeru PIN. W pole Edycja numeru PIN (Editable PIN) wprowadź numer PIN, który będzie wymagany.

5 - Edycja numeru PIN (Editable PIN number): użytkownik może wprowadzić numer PIN wymagany przez czynnik/klawiaturę, aby uzyskać dostęp. (zobacz [Format wyświetlania numeru karty](#))

Notatka: wybranie Czekaj na klawiaturę opóźni dostęp do drzwi dla tej karty, aż do momentu wprowadzenia prawidłowego numeru PIN. Dotyczy to tylko drzwi z czytnikami oraz keypadami zdefiniowanymi w menu Definiowania drzwi (Urządzenia > Drzwi). Terminarz drzwi musi być ważny. Zobacz Konfigurowanie drzwi.

6 – Z listy Stan karty (Card state) wybierz stan dla zaznaczonej karty. Domyślnie: ważna (valid). Poniżej lista możliwości:

- Ważna (Valid): karta jest aktywna,
- Nieważna (Invalid): karta NIE jest aktywna,
- Zgubiona/Skradzione: karta NIE jest aktywna,
- Oczekująca (Pending) : karta nie jest jeszcze aktywna,
- Wygasła (Expired): karta przekroczyła datę zakończenia, nie jest już aktywna.

Notatka: nie można zmienić stanu karty na Oczekujący poprzez wybranie tego stanu z listy. Aby to zrobić, musisz zmienić Datę Początkową.

7 – Zaznacz Wyłącz passback (Disable passback), jeżeli chcesz, aby karta obeszła passback.

Notatka: jeżeli przypisujesz kartę osobie z ograniczeniami ruchowymi zaznacz opcje Wydłużonego dostępu do drzwi. Aby włączyć tą opcję musisz określić odpowiednia opóźnienie w [Konfiguracja drzwi](#).

Notatka: jeżeli przypisujesz kartę osobie z ograniczeniami ruchowymi zaznacz opcje Wydłużonego dostępu do drzwi. Aby włączyć tą opcję musisz określić odpowiednia opóźnienie w Definiowaniu drzwi. Ta opcja jest również dostępna przy definiowaniu karty gościa.

Notatka: jeżeli istnieje taka potrzeba zaznacz opcję Uprzywilejowane operacje, aby obejść dowolne zabezpieczenia drzwi.



Dodawanie komentarza do karty (Adding Comments to a Card)

- 1 – Z okna Karta (Card), wybierz zakładkę Komentarz (Comment).
- 2 – Wpisz komentarz. Maksymalna liczba znaków: 241.
- 3 – Kliknij Zapisz (Save), a następnie Zamknij (Close).

Ograniczenie użycia karty (Limiting Card Usage)

EntraPass umożliwia wprowadzenie ograniczenia co do ilości razy użycia karty.

- 1 – Z okna Karta (Card), wybierz zakładkę Użycie (Usage).
- 2 – Zaznacz Włącz ograniczenie użycia (Enable usage restriction), aby aktywować funkcję.
- 3 – Z listy wybierz maksymalną liczbę określającą ilość użyczeń karty. Możesz wprowadzić wartość, albo wybrać przy pomocy strzałek.

Notatka: po określeniu Maksymalnej liczby wykorzystania karty, aktualny stan wykorzystania jest automatycznie aktualizowany po każdym użyciu karty. Istnieje możliwość zaznaczenia opcji Resetuj do zera, po zaznaczeniu której stan jest resetowany po przekroczeniu Maksymalnej liczby wykorzystania karty.

Notatka: aby ta opcja była dostępna musi być włączony Smartlink.



Przypisanie obrazu lub podpisu (Assigning Pictures and Signatures)

EntraPass umożliwia przypisywanie obrazów oraz podpisów do użytkowników, jak również szablonów identyfikatorów do kart. Obrazy oraz podpisy mogą być dodawane z pliku, wklejane, oraz przeklejane przy pomocy odpowiednich narzędzi. Do wykonania zrzutów podpisów rekomendowane są pady, np. Topaz.

Przypisanie obrazu z pliku (Assigning a Picture from a File)

1 – Z okna Karta (Card), wybierz zakładkę Obraz (Picture)

Notatka: opcja Zapisywania wideo jest dostępna wyłącznie wtedy, kiedy zainstalowane urządzenie do zapisywania wideo.

2 – Kliknij prawym na obrazie. Z menu wybierz odpowiednią akcję:

- Pobierz obraz z pliku (Get picture from file): ta opcja pozwala wybrać obraz z posiadanych, zapisanych wcześniej obrazów:

3 – Z listy Typ plików (Files of type) wybierz typ, którego szukasz albo pozostaw na Wyświetl wszystkie (All), aby wyświetlić wszystkie pliki obrazów.

4 – Wybierz katalog, w którym przechowywane są obrazy. Wybierz obraz, a następnie kliknij Otwórz (Open), aby wprowadzić go w okno Karty (Card).

Notatka: obsługiwane są następujące formaty: BMP, EMF, WMF, JPG, GIF, PNG, PCD oraz TIF..

- Wstaw obraz (Paste picture): ta opcja pozwala wstawić skopiowany wcześniej obraz.

Notatka: aby usunąć zaimportowany obraz kliknij na niego prawym, a następnie wybierz Usuń obraz.



Przypisywanie obrazu przy pomocy kamery (Assigning a Picture Using a Video Camera)

Wykonywanie zrzutu obrazu jest możliwe tylko wtedy, gdy opcja Włącz zrzut ekranu (Enable video capture) jest aktywna: Opcje > Urządzenia multimedialne > Zrzut ekranu (Options > Multimedia devices > Video capture tab).

Notatka: zanim zapiszesz obraz przy pomocy kamery musisz upewnić się, że cały sprzęt jest odpowiednio skalibrowany. Dowiedz się więcej sprawdzając instrukcję obsługi danego urządzenia. Jeżeli posiadasz więcej niż jeden sterownik wideo określ, który sterownik będzie wykorzystany (Options > Urządzenia multimedialne > Zakładka wideo).

1 – Kliknij prawym przyciskiem na obrazie.

2 – Z menu wybierz Zrzut ekranu (Video capture).

Notatka: opcje mogą się różnić zależnie od programu. Jeżeli posiadasz więcej niż jeden sterownik wideo określ, który sterownik będzie wykorzystany. Zobacz Konfiguracja urządzeń multimedialnych.

3 – Kliknij przycisk Zatrzymaj (Freeze), kiedy znalazłeś odpowiedni obraz nagrania, następnie kliknij Zrzuć (Capture), aby zachować obraz.

4 – Aby przypisać szablon identyfikatora do wybranej karty, wybierz szablon z listy. Zobacz: Projektowanie identyfikatorów (Badges designing).

Notatka: przyciski Drukuj identyfikator oraz Pogląd identyfikatora są dostępne w momencie, kiedy drukarka oraz układ identyfikatorów zostały wybrane, a opcja Użyj drukarki identyfikatorów została zaznaczona: Opcje > Opcje drukarki > Drukarka identyfikatorów. Dzięki tym przyciskom możesz podglądać i drukować identyfikatory.



Importowanie podpisu z pliku (Importing a signature from a file)

Możesz importować podpisy, tak jak importujesz inne obrazy na kartę.

1 – W oknie Karta (Card), kliknij prawym na podpisie.

2 – Z menu wybierz odpowiednią akcję:

- Pobierz podpis z pliku (Get signature from file): ta opcja pozwala wybrać podpis z posiadanych, zapisanych wcześniej obrazów.
- Wstaw obraz (Paste signature): ta opcja pozwala wstawić skopiowany wcześniej obraz.

Notatka: opcja Pad podpisów jest dostępna, jeżeli odpowiednie urządzenie jest udostępnione w menu Opcje.

3 – Wybierz podpis, a następnie kliknij Otwórz (Open).

Dodawania Podpisu Skanera do wzoru podpisu (Adding a Signature from a Signature Capture Device)

Ta opcja jest dostępna tylko w przypadku, gdy zainstalowane jest Skaner do wzoru podpisu (Signature Capture Device). Pad do podpisów musi być odblokowany w menu Opcji (Options) – Options > Multimedia devices > Signature (Options > Multimedia devices > Signature).

1 – W oknie Karta (Card), kliknij prawym na podpisie.

2 – Z menu wybierz Pad do podpisów (Signature pad). Pojawi się okno Podpis (Signature), w którym możesz podejrzeć podpis.

3 – Kliknij OK, aby wstawić podpis.



Edytowanie obrazów i podpisów (Working with Photos and Signatures)

Opcja EntraPass Definiowanie szablonów identyfikatorów (Integrated Badging) pozwala użytkownikowi na wycięcie fragmentu zdjęcia albo powiększenie obrazów, które są wgrane na karty.

Wycinanie fragmentu obrazu (Extracting Part of an Image)

Jeżeli wgrałeś duży obraz, a potrzebujesz tylko fragmentu, możesz wybrać i wyciąć ten fragment i przypisać go do karty.

1 – Kliknij prawym na obraz, który zaimportowałeś.

Notatka: opcja Wycinania jest włączona tylko po uruchomieniu trybu selekcji. Analogicznie, opcje Cofnij jest dostępna tylko po dodaniu obrazu.

2 – Wybierz Uruchom tryb wyboru (Start selection mode) z menu.

Notatka: możesz zwiększyć obszar selekcji przeciągając rogi oraz boki uprzednia zaznaczonego obszaru. Możesz również przenieść go w inny fragment obrazu.

3 – Po wybraniu fragmentu, który chcesz włączyć do karty, ponownie kliknij prawym na obraz.

Notatka: aby anulować selekcję kliknij prawym na na obrazie, a następnie wybierz Anuluj selekcję. Wybierz Cofnij, aby odrzucić zmiany. Opcja Cofnij jest dostępna tylko po dodaniu obrazu.

4 – Z menu wybierz Wytnij (Extract).



Edytowanie obrazu/podpisu (Editing a Picture/Signature)

1 – Kliknij prawym na obraz, który chcesz edytować.

Notatka: obszar Kodu pozwala przypisać kod do identyfikatora. Z listy wybierz obiekt, który będzie wykorzystany, jako wartość dla kodu. Możesz również wprowadzić własną wartość w polu Wartość. Jeżeli nie wprowadzisz własnej wartości Numer karty będzie wykorzystany, jako domyślna wartość.

2 – Z menu wybierz Edytuj (Edit).

3 – Ustaw właściwości obrazu. Przycisk Przywróć (Reset all) przywraca oryginalny obraz:

- Auto kontrast (Auto contrast),
- Ostrość (Sharpen),
- Jasność (Brightness),
- Przywróć (Reset all).

4 – Kliknij OK, aby zamknąć okno edycji.

5 – Z menu Szablon identyfikatora (Badge layout) wybierz szablon, który chcesz przypisać do definiowanej karty. Zobacz: Projektowanie identyfikatorów ([Badges Designing](#)).

Drukowanie identyfikatorów (Printing Badges)

Możesz wydrukować identyfikatory, karty gości oraz przepustki z okien: Karta (Card) albo Podgląd identyfikatora (Badge preview). Oprogramowanie pozwala na wydruk jedno, jak i dwu stronnych identyfikatorów.

Przed wydrukiem musisz wybrać drukarkę. Może to być dowolna drukarka sieciowa, albo konkretna drukarka identyfikatorów.

Wybierania drukarki identyfikatorów (Selecting a Badge Printer)

1 – Z okna Stacji roboczej EntraPass (EntraPass Workstation) wybierz pasek narzędzi Opcje (Options), a następnie wybierz przycisk Opcje drukarki (Printer Options).

2 – Z okna Opcje drukarki wybierz zakładkę Drukarka identyfikatorów (Badge printer).

Notatka: możesz drukować identyfikatory na dowolnej drukarce sieciowej. Żeby wydrukować identyfikator na karcie potrzebna jest drukarka identyfikatorów.

3 – Zaznacz opcję Drukarka identyfikatorów, żeby poinformować system, że drukarka identyfikatorów została wybrana. W oknie, z której możesz wydrukować identyfikatory (karty, przepustki, etc.) zostaną wyświetlone polecenia: Drukuj identyfikator (Print badge) oraz Podgląd identyfikatora (Preview badge).

4 – Z listy Wybierz drukarkę identyfikatorów (Select badge printer) wybierz drukarkę przeznaczoną do drukowania identyfikatorów.

5 – Dopasuj marginesy,



- Oś X: oznacza lewy margines,
- Oś Y: oznacza górny margines.

Podgląd i wydruk identyfikatorów (Previewing and Printing Badges)

Okno pozwala na podgląd układu identyfikatora z informacjami karty (w przypadku, gdy układ identyfikatora jest przypisane do karty) albo z domyślnymi wartościami (w przypadku, gdy szablon nie jest jeszcze przypisany do konkretnej karty). Oprogramowanie pozwala na wydruk jedno, jak i dwu stronnych identyfikatorów.

1 – W oknie Karta, Przepustka (Card, Visitor or Daypass) kliknij na Podgląd identyfikatora (Preview badge).

Notatka: z okna Projektowanie identyfikatora opcja podgląd pozwala sprawdzić wygląd identyfikatora z domyślnymi wartościami.

2 – Z okna podglądu wybierz opcję drukowania:

- Drukuj frony (Print front side):
- Drukuj tył (Print back side): opcja jest dostępna wyłącznie w przypadku, gdy identyfikator ma dwie strony.
- Drukuj front i tył (Print both sides): opcja jest dostępna wyłącznie w przypadku, gdy identyfikator ma dwie strony.

Notatka: ważne! Aby wydrukować identyfikator z kodami należy prawidłowo skalibrować drukarkę. Musisz zaznaczyć opcję „black resin” (czarny), albo czytniki kodów mogą nie dać rady odczytać wydrukowanego kodu. Jeżeli masz problemy z drukowaniem kodów sprawdź instrukcję obsługi drukarki.



Tworzenie nowego szablonu do importu/eksportu kart (Creating a New Import/Export Pattern)

To menu pozwala stworzyć nowy szablon do importu /eksportu, który będzie wykorzystany do importowania/eksportowania plików CSV.

1 – Z paska narzędzi Użytkownicy (Users), wybierz Importuj/Eksportuj CSV (Import/Export CSV). System wyświetli okno Importuj/Eksportuj CSV.

2 – W oknie kliknij przycisk Nowy wzór (New pattern). W nowym oknie zostanie wyświetlona lista wszystkich pól dostępnych w bazie danych kart EntraPass. Pola posiadają własne oznaczenia, których należy przestrzegać. Na przykład, pole stan karty akceptuje wyłącznie wartości: 0=ważna; 1=nieważna; 2=skradziona/zgubiona).

3 – Kliknij podwójnie na dostępnych polach. Następnie, przy pomocy czerwonych strzałek Góra/dół, posegreguj informacje (w ten sam sposób informacje będą posegregowane w pliku CSV).

Notatka: numer karty musi zostać wybrany dla każdego szablonu. Na przykład, jeśli wybierzesz pole Karta#3 – Skradziona/Zgubiona, musisz również wybrać pole Karta#3 – Numer karty.

4 – Określ oznaczenie Dodaj (Add) oraz Modyfikacja (Modification). Te oznaczenia są wykorzystywane przez system, w momencie importowania pliku, do rozpoznania, które karty należy dodać do bazy danych albo modyfikować. Domyślnym oznaczeniem dla obydwu jest „+”.

5 – Określ oznaczenie Usuń (Delete). To oznaczenie jest wykorzystywane przez system, w momencie importowania pliku, do rozpoznania, które karty należy usunąć z bazy danych. Domyślnym oznaczeniem jest „-”.

6 – Wybierz separator. To oznaczenie jest wykorzystywane do oddzielenia pól przy importowaniu lub eksportowaniu danych. Zazwyczaj wybranym separatorem jest „,”.

7 – Wybierz format daty. Data będzie eksportowana / importowana zależnie od wybranego formatu. Najpopularniejszym formatem jest format YYYY/MM/DD. Pozostałe opcje to:

- miesiąc/dzień/rok (MM/DD/YYYY)
- dzień/miesiąc/rok (DD/MM/YYYY)
- rok/miesiąc/dzień (YY/MM/DD)
- miesiąc/dzień/rok określony dziesiętnie (MM/DD/YY)
- dzień/miesiąc/rok określony dziesiętnie (DD/MM/YY)

Notatka: opcja Użyj DLL pozwala uruchomić program, który przekonwertuje konkretny numer karty. Możesz użyć Usuń DLL jeśli nie chcesz, aby program konwertował numery kart.

8 – Kliknij OK, aby utworzyć wzór i określić jego nazwę.

9 – Wprowadź nazwę i kliknij OK. System automatycznie przejdzie do okna Importuj/Eksportuj CSV (Import/Export CSV). Utworzony wzór jest wyświetlony na liście Dostępnych wzorów (Available patterns).

10 – Jeżeli do wzoru chcesz dodać lub usunąć pola, kliknij dwukrotnie na nowym wzorze, aby go edytować.



Definiowanie karty gościa w szablonie definiowania nowej karty (Creating a Visitor Card When Creating a New Card)

- 1 – Z paska narzędzi Użytkownicy (Users), wybierz przycisk Karta (Card).
- 2 – Zaznacz opcję Kopiuj dla gościa (Copy to visitor). Informacja z karty zostaną wykorzystane przy tworzeniu nowych kart oraz wystawiania dziennych przepustek.

Import/eksport kart do pliku CSV (CSV Files Import and Export)

Ta opcja umożliwia importowania oraz eksportowanie plików kart zapisanych w formacie CSV (Comma Separated Value). Import/eksport pomiędzy dwoma aplikacjami umożliwia wymianę danych pomiędzy nimi. Pliki CSV mogą być edytowane przez większość aplikacji (Excel, NotePad, etc.). Możesz wykorzystać tę opcję, kiedy:

- Aktualizujesz EntraPass DOS albo WinPass 62 i chcesz zachować karty utworzone w poprzednich wersjach.
- Twoja firma chce zaimportować bazę danych kart do systemu płac.
- Twoja firma posiada nową bazę danych: wszystkie dane zawarte w bazie danych mogą być eksportowane do pliku CSV, a następnie zaimportowane do nowej bazy danych.

Notatka: opcja Importuj/Eksportuj CSV wprowadza kilka zasad: każde pole zawiera konkretny format wartości, który musi być zachowany. Na przykład, pole Status karty akceptuje tylko następujące wartości (0=prawidłowe; 1=nieprawidłowe; 2=skradziona/zgubiona).

Aby importować/eksportować informacje możesz użyć przygotowanych wzorów albo możesz stworzyć nowe.

Używanie przygotowanych wzorów (Using a Predefined Pattern)

Dostępne są dwa wzory: EntraPass (1,2,3) oraz model WinPass64. Możesz użyć szablonu „według wzoru”, albo go edytować.

- 1 – Z paska narzędzi Użytkownicy (Users), wybierz przycisk Importuj/Eksportuj CSV (Import/Export CSV file).
- 2 – Z listy wybierz Import albo Eksport.
- 3 – Wybierz wzór, który chcesz wykorzystać.
- 4 – Użyj przycisku Edytuj wzór (Edit pattern), jeżeli chcesz edytować wzór.

Tworzenie nowego szablonu do importu/eksportu kart (Creating a New Import/Export Pattern)

To menu pozwala stworzyć nowy szablon do importu /eksportu, który będzie wykorzystany do importowania/eksportowania plików CSV.

- 1 – Z paska narzędzi Użytkownicy (Users), wybierz Importuj/Eksportuj CSV (Import/Export CSV). System wyświetli okno Importuj/Eksportuj CSV.
- 2 – W oknie kliknij przycisk Nowy wzór (New pattern). W nowym oknie zostanie wyświetlona lista wszystkich pól dostępnych w bazie danych kart EntraPass. Pola posiadają własne oznaczenia, których należy przestrzegać. Na przykład, pole stan karty akceptuje wyłącznie wartości: 0=ważna; 1=nieważna; 2=skradziona/zgubiona).



Użytkownicy

Import/eksport plików CSV

3 – Kliknij podwójnie na dostępnych polach. Następnie, przy pomocy czerwonych strzałek Góra/dół, posegreguj informacje (w ten sam sposób informacje będą posegregowane w pliku CSV).

Notatka: numer karty musi zostać wybrany dla każdego szablonu. Na przykład, jeśli wybierzesz pole Karta#3 – Skradziona/Zgubiona, musisz również wybrać pole Karta#3 – Numer karty.

4 – Określ oznaczenie Dodaj (Add) oraz Modyfikacja (Modification). Te oznaczenia są wykorzystywane przez system, w momencie importowania pliku, do rozpoznania, które karty należy dodać do bazy danych albo modyfikować. Domyślnym oznaczeniem dla obydwu jest „+”.

5 – Określ oznaczenie Usuń (Delete). To oznaczenie jest wykorzystywane przez system, w momencie importowania pliku, do rozpoznania, które karty należy usunąć z bazy danych. Domyślnym oznaczeniem jest „-”.

6 – Wybierz separator. To oznaczenie jest wykorzystywane do oddzielenia pól przy importowaniu lub eksportowaniu danych. Zazwyczaj wybranym separatorem jest „,”.

7 – Wybierz format daty. Data będzie eksportowana / importowana zależnie od wybranego formatu. Najpopularniejszym formatem jest format YYYY/MM/DD. Pozostałe opcje to:

- miesiąc/dzień/rok (MM/DD/YYYY)
- dzień/miesiąc/rok (DD/MM/YYYY)
- rok/miesiąc/dzień (YY/MM/DD)
- miesiąc/dzień/rok określony dziesiętnie (MM/DD/YY)
- dzień/miesiąc/rok określony dziesiętnie (DD/MM/YY)

Notatka: opcja Użyj DLL pozwala uruchomić program, który przekonwertuje konkretny numer karty. Możesz użyć Usuń DLL jeśli nie chcesz, aby program konwertował numery kart.

8 – Kliknij OK, aby utworzyć wzór i określić jego nazwę.

9 – Wprowadź nazwę i kliknij OK. System automatycznie przejdzie do okna Importuj/Eksportuj CSV (Import/Export CSV). Utworzony wzór jest wyświetlony na liście Dostępnych wzorów (Available patterns).

10 – Jeżeli do wzoru chcesz dodać lub usunąć pola, kliknij dwukrotnie na nowym wzorze, aby go edytować.



EntraPass - Instrukcja instalacji i obsługi programu Użytkownicy



Eksportowanie kart (Exporting Cards)

Twoja firma może potrzebować eksportu bazy danych do innej aplikacji. Możesz użyć gotowego szablonu, albo stworzyć własny.

1 – Z paska narzędzi Użytkownicy wybierz przycisk Importuj/Eksportuj CSV (Import/Export CSV file). System wyświetli okno Importuj/Eksportuj CSV.

2 – Z listy wybierz Eksportuj (Export).

3 – Z listy Dostępne wzory (Available patterns) wybierz wzór, z którego chcesz skorzystać przy eksportowaniu kart. Możesz edytować istniejące wzory albo stworzyć nowy. Zobacz Tworzenie nowego szablonu do importu/eksportu kart ([Creating a New Import/Export Pattern](#))

4 – Kliknij ikoną trzech kropek (three-dot) i wybierz folder, w którym EntraPass zapisze zawartość bazy danych kart. Plik CSV możesz otworzyć m.in. w Excel, NotePad.

5 – Po wybraniu/stworzeniu folderu eksportowego, kliknij OK, aby powrócić do okna Importuj/Eksportuj CSV

6 – Kliknij przycisk Eksportuj (Export). Jest on dostępny po wybraniu pliku do transferu. System wyświetla okno, które pozwala filtrować karty, które chcesz eksportować.

Notatka: aby karty zostały włączone do twojego pliku, muszą odpowiadać wszystkim wybranym filtrom. Jeśli jeden z filtrów nie pasuje, karta nie zostanie włączona do pliku.

7 – W oknie wybierz karty, które chcesz eksportować. Po wybraniu, kliknij przycisk Eksportuj (Export). System wyświetli okno Importuj/Eksportuj CSV.

Notatka: pole Transaction field wskazuje lokalizację oraz nazwę wybranego pliku. Domyślnie, plik eksportowy jest zapisywany w określonym folderze (np. Exportadata). Pasek statusu pokazuje liczbę zaimportowanych kart (np. 1). Domyślna nazwa: YYYYMMDD.csv. Plik możesz otworzyć przy pomocy m.in. programu NotePad.



Importowanie kart (Importing Cards)

1 – Z paska narzędzi Użytkownicy wybierz przycisk Importuj/Eksportuj CSV (Import/Export CSV file). System wyświetli okno Importuj/Eksportuj CSV.

2 – Z listy wybierz Importuj (Import).

3 – Z listy Dostępne wzory (Available patterns) wybierz wzór, z którego chcesz skorzystać przy importowaniu kart. Zobacz **Tworzenie nowego szablonu do importu/eksportu kart** ([Creating a New Import/Export Pattern](#))

4 – Kliknij ikoną trzech kropek (three-dot) i przeszukaj dysk w poszukiwaniu plików CSV, które zawierają dane do zaimportowania do bazy danych.

5 – Po wybraniu pliku kliknij Otwórz (Open). System wyświetli okno Importuj/Eksportuj CSV.

6 – Jeżeli nie wystąpią żadne błędy (albo zostały już poprawione), kliknij Importuj (Import) aby zakończyć operację.

Notatka: system skanuje plik do zaimportowania; następnie wyświetla wyniki przy wykorzystaniu kolorów. Każde wprowadzenie jest identyfikowane innym kolorem (oflagowaniem). Żółte i czerwone oznaczenia określa nieprawidłowe wprowadzenie. Błędy są często generowane przez szablony. Musisz wybrać inny szablon albo edytować ten, z którego korzystasz, aby wprowadzenia pasowały do zawartości pliku źródłowego. Błędy mogą pojawiać się nawet wtedy, kiedy transakcja jest oznaczona zieloną flagą.



Poprawianie błędów Importuj/Eksportuj (Correcting Import/Export Errors)

Opcja Importuj/Eksportuj CSV (CSV Import/Export) wprowadza wiele zasad. Na przykład, pola posiadają własne oznaczenia, których należy przestrzegać. Na przykład, pole stan karty akceptuje wyłącznie wartości: 0=ważna; 1=nieważna; 2=skradziona/zgubiona). Wzór użyty musi być identyczny, jak wzór w pliku źródłowym. Poniżej znajdują się informacje, jak naprawiać błędy związane z importem/eksportem.

1 – Kliknij przycisk Importuj albo Eksportuj (poniższy przykład ilustruje przypadek importowania CSV). Dolna część okna wyświetla liczbą kart w liście.

Notatka: pomimo, że dane w kolumnie Kod transakcji (Transaction code) są oznaczone zieloną flagą, kolumna Numer karty jest pusta. Wskazuje to na problem w konwersji.

2 – Kliknij przycisk Importuj (Import).

Notatka: przycisk Błąd jest włączony, ponieważ system napotkał problemy podczas ważnej transakcji.

3 – Kliknij przycisk Błąd (Error), aby wyświetlić informacje o błędzie. Okna Błędu (Process error) pokazują, że użyty wzór jest nieprawidłowy.

4 - Kliknij Zamknij (Close), aby wrócić do okna Importuj/Eksportuj.

5 – W oknie Importuj/Eksportuj CSV, kliknij dwukrotnie na wykorzystany do operacji wzór.

6 – Z listy Separator (Field separator), wybierz „przecinek”, jako separator, a następnie kliknij OK.

Personalizacja pól informacyjnych karty (Customizing Card Information Fields)

Możesz zmieniać nazwy pól informacyjnych w zakładce Ogólne (General) według własnych wymogów. Te pola mogą zawierać dowolne informacje.

1 – W okienku Definiowanie kart (Card definitione) wybierz kartę, a następnie dwukrotnie kliknij na nazwę/etykietę w zakładce Ogólne. System wyświetli okno Zmiana nazwy/etykiety (Change labels).

2 – Po lewej wybierz pole, które chcesz modyfikować, a po prawej wprowadź nazwę. Jeżeli system pracuje w dwóch językach, dostępne będą dwa pola do wprowadzania nazwy.

3 – Wybierz opcję Edytuj pole (Edit field), jeżeli informacja pojawia się jako pole do edycji (prosta informacja), albo opcję listy (Drop-down list). Kliknij OK, aby zapisać modyfikacje.

4 – Powtórz te kroki dla wszystkich pól, które chcesz modyfikować.

Notatka: Zaznacz Pole obowiązkowe, aby upewnić się, że pole zostanie uzupełnione.

Notatka: użytkownik musi posiadać pełne prawa dostępu, aby edytować pola informacji o karcie. Użytkownik bez takich praw może tylko odczytać te informacje.



Definiowanie kart gości jednodniowych (Day Passes Definition)

Przepustki są przypisywane gościom, takim jak podwykonawcy, pracownikom z innych oddziałów, klienci, etc. Ta opcja pozwala w łatwy sposób przyznać dostęp dla „gościa” na jeden dzień. Nawet, jeżeli karta nie zostanie zwrócona, utraci ona ważność o 24:00 tego dnia. Możesz użyć profili przeniesionych do „Definiowania Gości” (Visitor definition) przy tworzeniu przepustek.

Tworzenie kart gości jednodniowych (Creating a Day Pass)

- 1 – Z paska narzędzi Użytkownicy wybierz przycisk Przepustka (Daypass). Pojawia się okna Przepustka.
- 2 – Możesz wypełnić pola samemu, albo przeszukać bazę danych i znaleźć potrzebną kartę.
- 3 – Zaznacz pole Skopiuj do karty gościa (Copy to visitor card). Dzięki temu informacje z karty są kopiowane do bazy danych gości.

Notatka: w celu uzyskania dodatkowych informacji odnośnie karta gości, zobacz Definiowanie karty gościa w szablonie definiowania nowej karty (Creating a Visitor Card When Creating a New Card). Zakładka Obraz pozwala wyświetlić m.in. zdjęcie użytkownika karty; jak również zrobić pogląd oraz wydrukować identyfikator.

Tworzenie karty gości jednodniowych przy pomocy opcji Zapisz jako (Creating a New Day Pass Using the “Save As” Feature)

Opcja Zapisz jako (Save as) umożliwia tworzenie nowej przepustki w oparciu o istniejącą już przy jednej zmianie informacji oraz przypisaniu nowego numeru karty. Na przykład: zmieniając tylko nazwę użytkownika, ale pozostawiając wszystkie pozostałe informacje bez zmian.

- 1 – Z paska narzędzi Użytkownicy wybierz przycisk Przepustka (Daypass). Pojawia się okna Przepustka.
- 2 – Aby zlokalizować istniejącą kartę kliknij ikonę lornetki, a następnie wybierz kartę, którą chcesz powielić.
- 3 – Wprowadź zmiany w dowolne pola, a następnie kliknij Zapisz jako (Save as).
- 4 – Zostaniesz poproszony o wprowadzenie nowego numeru karty.



Wprowadzanie nowej karty w Zaawansowanym zarządzaniu (Issuing a New Card in Enhanced User Management Environment)

Notatka: zobacz Parametry definiowania kart ([Credentials Parameters](#)), aby uzyskać więcej informacji jak włączyć Zaawansowane zarządzanie (Enhanced User Management).

1 – Z paska narzędzi Użytkownicy (Users), wybierz Karta (Card). Nowe okno Karty jest wykorzystane do wprowadzenia/zmiany informacji o użytkowniku karty.

2 – Kliknij przycisk Nowy (New) na pasku narzędzi. Wprowadź nazwę użytkownika karty w pole Nazwa użytkownika karty. Można użyć do 50 znaków.

3 - Kliknij przycisk Zapisz (Save).

4 – Dwukrotnie kliknij na pole Typ karty (Card type), aby otworzyć okno Typ karty. Wybierz typ karty dla nowej karty. Typ karty jest używany do grupowania użytkowników kart, a później również do modyfikowania istniejącej grupy kart albo tworzenia nowego raportu. Zobacz: Definiowanie typów kart (Card Type Definition).

Notatka: w polu Typ karty możesz kliknąć prawym na polu Typ karty i wybrać Nowy, aby stworzyć nowy typ karty. Kliknij Wybierz, aby wybrać istniejący typ karty albo Edytuj, aby edytować.

5 – Kliknij na zakładkę Numer karty (Card number), dwukrotnie kliknij na Karta #1 (Card #1), jeżeli chcesz zmienić nazwę.

6 - Wprowadź numer karty.

- Jeśli EntraPass był wcześniej skonfigurowany na wielokrotne formatowanie kart (Multiple Card Format), możesz zmienić format karty klikając prawym przyciskiem na pole Numeru Karty (Card number). Domyślny format karty to HH:DDDD (Hexadecimal / decimal 24 bits).

Notatka: Poziom dostęp zostanie przypisany do użytkownika, czyli do pięciu kart.

- Kiedy Wielokrotne formatowanie kart jest aktywne: lista wszystkich formatów kart zostanie wyświetlona, gdy klikniesz prawym przyciskiem na pole numeru karty.

- Kiedy format karty zostanie określony przez administratora systemu, przy opisie formatu karty pojawia się znaczek potwierdzenia.



Użytkownicy

Wprowadzanie nowej karty w trybie Zaawansowanego Zarządzania Użytkownikami

	Numer karty	Wyświetl numer karty	Ustaw datę ważności	Data końca ważności	Godzina końca	Karta śledzona	Skradziona Zgubiona
Karta # 1	000000001237088	☐	☐		0	☐	☐
Karta # 2	00:00000	☒	☐		0	☐	☐
Karta # 3	00:00000	☒	☐		0	☐	☐
Karta # 4	00:00000	☒	☐		0	☐	☐
Karta # 5	00:00000	☒	☐		0	☐	☐

7 – Opcjonalnie, możesz natychmiastowo przypisać Numer karty (Card number).

8 – Jeśli pozwalają na to twoje uprawnienia, możesz wyświetlić numer karty, lub też nie.

Notatka: system automatycznie wyświetla datę utworzenia, datę modyfikacji oraz liczbę modyfikacji w prawej-górnej części okna.

9 – Zaznacz opcje Użyj daty zakończenia (Use expiration date) i wybierz datę.

10 – Zaznacz opcje Namierzaj (Trace), jeżeli chcesz monitorować użycie konkretnej karty. Zaznaczenie tej opcji sprawi, że zdarzenie „namierzania” będzie generowane za każdym razem, gdy karta zostanie użyta przy czytniku.

11 – Zaznacz opcję Skradziona/Zgubiona (Stolen/Lost), jeżeli karta została skradziona lub zgubiona. Karta przestanie być aktywna.

12 – Powtórz działania 5-11 dla kart #2-#5.



EntraPass - Instrukcja instalacji i obsługi programu Użytkownicy

The screenshot shows the 'Karty' (Cards) window in the EntraPass application. The window has a menu bar and a toolbar. The main area is divided into several sections. On the left, there are input fields for 'Nazwisko użytkownika' (User Name), 'Typ karty' (Card Type), and 'E-Mail'. On the right, there are fields for 'Data utworzenia' (Creation Date), 'Data zmiany' (Change Date), and 'Liczba zmian' (Number of Changes). Below these is a tabbed interface with tabs for 'Numer karty' (Card Number), 'Informacja' (Information), 'Poziomy dostęp' (Horizontal Access), 'Poziomy dostęp - wyjątki' (Horizontal Access - Exceptions), 'Parametry' (Parameters), 'Zdjęcie' (Photo), 'Użycie' (Usage), and 'Komentarz' (Comment). The 'Numer karty' tab is active, showing a table of cards. The table has columns for 'Karta #', 'Wyświetl numer karty' (Display Card Number), 'Ustaw datę ważności' (Set Validity Date), 'Data końca ważności' (Expiration Date), 'Godzina końca' (End Time), 'Karta śladowa' (Trailing Card), and 'Skradziona/Zgubiona' (Stolen/Lost). The 'Skradziona/Zgubiona' column is highlighted with a red rectangle. At the bottom of the window are buttons for 'Zakończ' (Finish), 'Anuluj' (Cancel), and 'Pomoc' (Help).

Karta #	Wyświetl numer karty	Ustaw datę ważności	Data końca ważności	Godzina końca	Karta śladowa	Skradziona/Zgubiona
Karta # 1	0009381701	☒	18.05.2017	0	☒	☐
Karta # 2	00:00000	☒		0	☐	☐
Karta # 3	00:00000	☒		0	☐	☐
Karta # 4	00:00000	☒		0	☐	☐
Karta # 5	00:00000	☒		0	☐	☐

Dodawanie kart przez czytnik kontrolera (Issuing Cards Using the “Batch Load” Feature)

Opcja Załaduj wsadowo (Batch Load) pozwala na operację na karcie przy przyłożeniu karty do czytnika. Numer karty jest wyświetlony przy zdarzeniu „nieznana karta” albo „wstęp zabroniony”. Podczas działania operator może stworzyć nową kartę albo zmodyfikować już istniejącą.

1 – Z okna Karty (Card), kliknij przycisk Załaduj wsadowo (Batch Load)

2 – Z listy drzwi, wybierz drzwi, które będą odczytywać karty.

3 – Zaznacz którąś z opcji:

- Odśwież na wejściu (Refresh an access granted): przy każdym wejściu wyświetlane informacje będą aktualizowane.
- Zapisz na nowej karcie (Save on new card): jeśli ta opcja jest zaznaczona, przy zdarzeniu „nieznana karta”, nowa karta będzie zapisana w bazie danych.

Notatka: jeśli ta opcja jest wybrana pierwsza karta wykorzystana przy czytniku zostanie zapisana tylko wtedy, kiedy zostanie zaprezentowana również druga karta albo po przyciśnięciu przycisku Zapisz.

- Znajdź (Find): pozwala użytkownikowi szukać istniejącej karty, aby w oparciu o nią stworzyć nową.

Notatka: jeśli użytkownik kliknie przycisk Zamknij bez zapisywania, system poprosi o zapisanie ostatnio dodanych informacji.



Wyświetlanie listy ostatnich transakcji (Last Transactions Display)

Opcja pozwala sprawdzić ostatnią transakcję dla wybranego użytkownika karty. Na przykład, w oknie zostanie wyświetlona wiadomość „Brak dostępu”, jako typ zdarzenia, oraz informacje dotyczące daty i czasu, etc.

System wyświetli 15 ostatnich transakcji dla każdej kategorii:

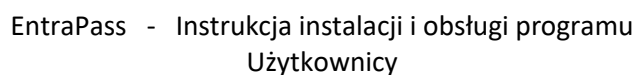
- Dostęp zabroniony (zła lokalizacja, zły poziom dostępu, zły status karty, etc.),
- Zdarzenia przyznania dostępu,
- Zdarzenia związane z bazą danych (mające wpływ na bazę danych: modyfikacje kart, modyfikacja połączeń, etc.)
- Inne/różne zdarzenia (zdarzenie wygenerowane przez użytkownika),
- Zdarzenia wejścia/wyjścia (entry/exit).

Notatka: aby wyświetlić więcej transakcji z wybranej kategorii, zobacz opcję Raport wykorzystania karty w menu Raporty historyczne.

Podgląd ostatniej transakcji (Viewing the Last Transaction)

1 – Z okna Definiowanie karty (Card definition), wybierz Podgląd ostatniej transakcji (View last transaction).

- Typ (Type): wyświetla kategorię zdarzenia.
- Data i czas (Date and time): wyświetla datę i czas zdarzenia/wiadomości o zdarzeniu.
- Zdarzenie (Even message): wyświetla wiadomość o zdarzeniu, która została wysłana do serwera (oraz do autoryzowanej stacji roboczej EntraPass) po zajściu zdarzenia. Jest to ta sama wiadomość, która pojawia się na Pulpicie Wiadomości (Message desktop).
- Szczegóły (Details): wyświetla dodatkowe szczegóły/informacja powiązane z typem transakcji.
- Odśwież (Refresh): odświeża okno wyświetlając zdarzenia, które właśnie miały miejsce.
- Opiekun (Parent): wyświetla komponent będący opiekunem dla wybranego komponentu. Zobacz: Funkcje główne (Basic functions).
- Drukuk (Print): drukuje kopie wyświetlonego okna. Zobacz: Funkcje główne (Basic functions).
- Podgląd (Preview): wyświetla okno przed wydrukiem.





Lista drzwi z dostępem wybranej karty (Quick Access to Door List per Card)

Ta opcja umożliwia szybkie wyświetlenie listy drzwi, wraz z przypisanymi terminarzami, dla wszystkich poziomów bezpieczeństwa wybranego użytkownika.

1 – Z menu Użytkownicy/Karta, kliknij przycisk Lista dostępu do drzwi (Door access list):



Informacje są wyświetlane w pięciu kolumnach:

- Przycisk bramka/połączenie
- Opis bramka/połączenie
- Opis drzwi
- Opis terminarza

Notatka: informacje mogą zostać wyeksportowane do pliki CSV w celach wydrukowania albo raportowania.

Informacje te są także dostępne w oknie Informacje o karcie (View card information).

Lista abonentów (Tenants List)

Abonentem nazywamy mieszkańca budynku albo pracownika firmy. Abonent może przyznać dostęp dla gościa. Lista abonentów może zostać stworzona w EntraPass przy pomocy KTES.

Tworzenie nowej listy Abonentów (Creating a New Tenants List)

1 – Z paska narzędzi Użytkowników wybierz przycisk Lista abonentów (Tenants list).

2 – Edytuj nazwę listy. Domyślna to: Nowa lista abonentów.

3 – Wybierz długość ID abonenta (1-5). Domyślna: 4.

4 – Wybierz długość PIN abonenta (1-5). Domyślna: 4.

5 – Wybierz format wyświetlania WIEGEND:

- Hexadecimal 24 bits
- Hexadecimal oraz decimal 24 bits
- Hexadecimal 32 bits
- Hexadecimal oraz decimal 32 bits
- Decimal ABA 8 digits
- Decimal ABA 10 digits

Domyślny: Hexadecimal 32 bits



Dodawanie nowy Abonentów do Listy (Adding New Tenants to the List)

1 – Wybierz zakładkę Ogólne (General).

2 – Kliknij przycisk Dodaj (+) (Add (+)). Przy pomocy przycisku Legenda (Legend) możesz wyświetlić aktualny status każdego abonenta.

3 – Ustaw parametry abonenta:

- Nazwa (Tenant name): wprowadź nazwę abonenta (max 20 znaków). Domyślna: Nowy abonent.
- ID Abonenta (Tenant ID): wprowadź ID abonenta. Jest to kod identyfikujący abonenta, którym goście mogą go wywołać. Długość kodu (1-5 znaków) została określona przy tworzeniu listy. Domyślna: 0000.
- Pierwszy numer telefonu (First phone number): wprowadź pierwszy numer telefonu. Ten numer jest wykorzystany, kiedy gość wybiera abonenta z katalogu KTES. Jeżeli numer nie został wprowadzony, abonent nie może zostać wywołany przez system KTES.
- Drugi numer telefonu (Second phone number): wprowadź drugi numer telefonu. Numer jest używany w przypadku, gdy nie było odpowiedzi na pierwszy.
- PIN Abonenta (PIN): numer skonfigurowany dla każdego abonenta. Długość kodu (4-6 znaków) została określona przy tworzeniu listy. Domyślna: 0000.
- Terminarz dostępu (Access schedule): łączy terminarz z prawami dostępu abonenta. Abonent ma dostęp do budynku w określonym czasie, w określone dni i święta, tak, jak to jest zdefiniowane w systemie. Domyślna: zawsze.
- Poziom administratora dla Abonenta (Tenant admin level): wybierz poziom administratora (instalator, właściciel, serwis, abonent). Domyślna: abonent.
- Język (Tenant language): wybierz język KTES dla abonenta (system, angielski, francuski, hiszpański, etc.).
- Wyłączony Abonent (Disabled Tenant): status umożliwia aktywowania połączenia lub generowania alarmu.
- Namierz (Trace): opcja umożliwia aktywowania połączenia lub generowania zdarzenia.
- Ukryj abonenta (Hide tenant): opcja umożliwia ukrycie nazwy abonenta.
- Przedłużone opóźnienie dostępu do drzwi (Extended door access delay): dodatkowy czas dostępu do drzwi (czasu, gdy drzwi pozostają niezablokowane i mogą być otwarte). Przydatne dla ułatwienia poruszania się osobom z ograniczoną sprawnością.
- Zwiększona ilość dzwonek (Extended ring): system może zwiększyć ilość dzwonek, aby dać abonentowi więcej czasu na odpowiedź.

4 – Wybierz zakładkę Opcje zaawansowane (Advanced options).



EntraPass - Instrukcja instalacji i obsługi programu Użytkownicy

5 – Ustaw datę walidacji dla abonenta:

- Data rozpoczęcia (Start date): data, od której abonent uzyskuje dostęp do systemu. Wprowadź datę (mm/dd/rrrr) albo wybierz datę z kalendarza.
- Data zakończenia (Use end date): data, po której abonent traci dostęp do systemu. Zaznacz odpowiednie pole, aby aktywować tą datę. Wprowadź datę (mm/dd/rrrr) albo wybierz datę z kalendarza.

6 – Ustaw opcję Nie przeszkadzać (Do not disturb). Ta funkcja ustawia dla abonenta status Nie przeszkadzać (DnD – Do not Disturb). Zaznacz opcję Ukryj Abonenta (Hide tenant), jeżeli chcesz aby abonent pozostał ukryty i nie był wyszukiwany na liście.

7 – Opcja Dzwon na drugi numer telefonu (The Call second phone number) pozwala dzwonić bezpośrednio na drugi numer, z pominięciem pierwszego.

8 – Ustaw protokół WIEGAND dla poziomu dostępu:

- Numer karty abonenta (Tenant card number): 64bitowy numer, wykorzystany przez abonenta, aby uzyskać dostęp do KTES.



EntraPass - Instrukcja instalacji i obsługi programu Użytkownicy

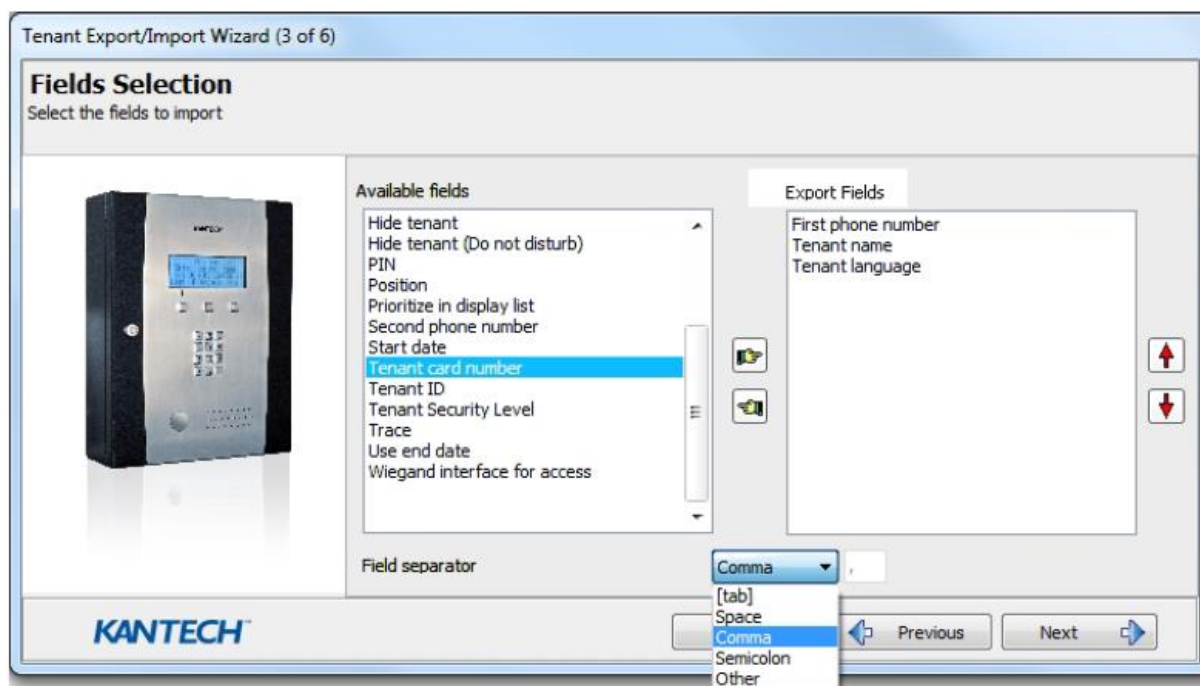
Importowanie listy abonentów (Importing a Tenant List)

Aby ułatwić proces importowania listy abonentów wprowadzono automatyczną procedurę.

Krok 1: kliknij przycisk Importuj (Import), aby uruchomić kreatora Eksportuj/Importuj Abonentów (Tenant Export/Import Wizard).

Krok 2: kliknij przycisk Następny (Next) i wybierz źródłowy plik CSV.

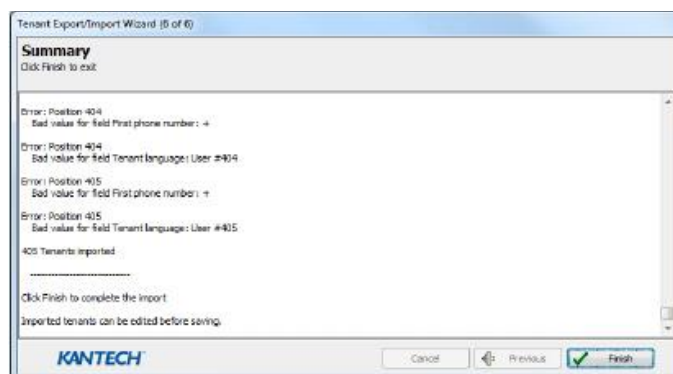
Step 3: kliknij przycisk Następny (Next) i wybierz pole do zaimportowania z listy po prawej stronie. Użyj przycisków prawo/lewo, aby dodać/usunąć pole. Możesz wybrać separator (domyślny: przecinek).



Krok 4: kliknij przycisk Następny (Next) i wybierz abonentów do zaimportowania.

Krok 5: kliknij przycisk Następny (Next), a następnie przycisk Importuj (Import), aby zakończyć operację.

Krok 6: kliknij przycisk Następny (Next), aby zobaczyć podsumowanie.





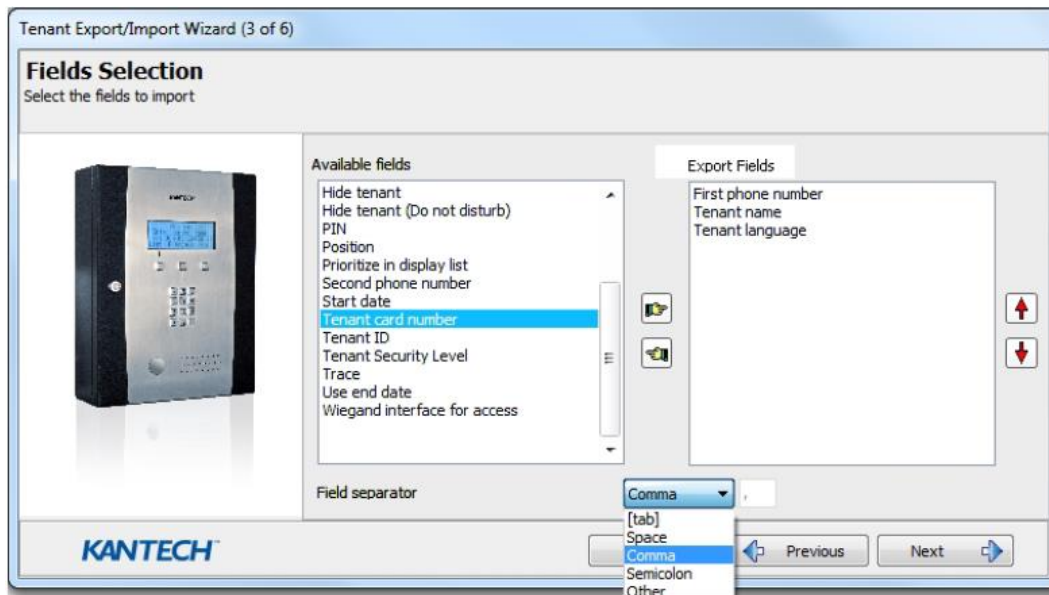
EntraPass - Instrukcja instalacji i obsługi programu Użytkownicy

Eksportowanie listy abonentów (Exporting a Tenant List)

Podobnie, jak w przypadku importowania, automatyczna procedura prowadzi użytkownika przez proces eksportowania listy abonentów.

Krok 1: kliknij przycisk Importuj (Import), aby uruchomić kreatora Eksportuj/Importuj Abonentów (Tenant Export/Import Wizard).

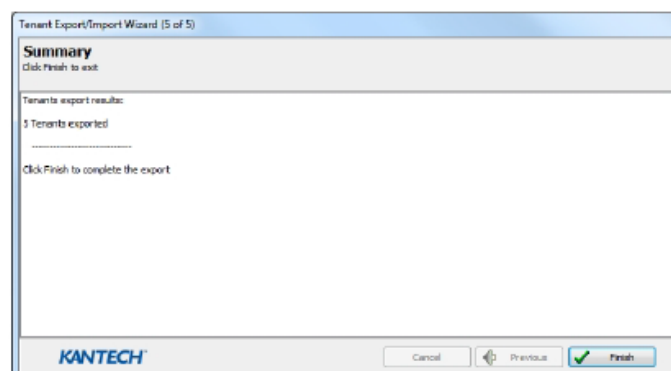
Krok 2: kliknij przycisk Następny (Next) i wybierz pole do eksportowania z listy po lewej stronie. Użyj przycisków prawo/lewo, aby dodać/usunąć pole. Możesz wybrać separator (domyślny: przecinek).



Krok 3: kliknij przycisk Następny (Next) i wybierz abonentów do eksportowania.

Krok 4: kliknij przycisk Następny (Next) i wybierz format zapisu pliku CSV. Kliknij przycisk Eksportuj (Export).

Krok 5: kliknij przycisk Następny (Next), aby zobaczyć podsumowanie.





Dodawania obiektów do szablonu foto-identyfikatora (To Add Objects to a Badge Layout)

Dzięki prostej opcji złap-przeciągnij-upuść, do szablonu identyfikatorów można dodawać inne obiekty:

- Pola informacji o karcie
- Kody kreskowe
- Pola tekstowe
- Bieżącą datę
- Wcześniej zapisane obrazy lub logo (BMP, JPG, GIF, etc.),
- Ramki
- Linie, wypunktowania

Notatka: obiekty są wprowadzane z domyślnymi ustawieniami. Aby zmodyfikować te ustawienia kliknij prawym na obiekt, a następnie wybierz odpowiednie ustawienia z menu.



Modyfikacja właściwości zdjęcia (To Modify Picture Properties)

Odnosi się do dowolnego obiektu graficznego: zdjęcia, logo, etc.

1 – Z pola roboczego Projektowanie identyfikatora, kliknij prawym przyciskiem myszy na obraz umieszczony w szablonie, który chcesz modyfikować.

2 – Z menu wybierz Właściwości obrazu (Images properties).

3 – Możesz wybrać następny obraz z pliku albo modyfikować właściwości obrazu.

- Współczynnik rozciągania (Stretch ratio): pozwala na umieszczenie obrazu w środku, przy zachowaniu proporcji oryginalnego obrazu.
- Tryb transparentny (Transparent mode): przy wyborze tej opcji nie będzie ustawionego koloru tła.
- Narysuj ramę (Draw frame): ta opcja pozwala otoczyć obraz ramą.
- Kolor ramy (Frame colour): umożliwia ustawienie zmiany koloru ramy (możliwe tylko, gdy taka opcja Ramy (Frames) jest wybrana).

4 – Możesz zaznaczyć Ustaw, jako domyślne (Set as default), jeśli chcesz, aby ustawione właściwości były stosowane dla wszystkich obrazów do szablonu identyfikatorów.



Weryfikacja poziomu dostępu wybranej karty (Validating Card Access)

Opcja Potwierdzenia dostępu dla karty pozwala sprawdzić poziomy dostęp, które są przypisane dla konkretnego posiadacza karty.

1 – Z okna Karta wybierz kartę.

2 – Z paska narzędzi okna Karta, kliknij Pogląd i Potwierdzenie Dostępu (View and Vaildate Access).

3 – Wybierz obiekt/bramkę/połączenie z listy Obiekt/Bramka/Połączenie.

4 – Z sekcji Wybierz konkretną wartość (Select specific value), wybierz datę, czas oraz drzwi, dla których wymagane jest potwierdzenie. System wyświetla poziom dostępu dla wybranych drzwi, oraz terminarze przypisane do wyświetlonego poziomu dostępu. Kolumna Poziom dostępu (Access Level) wyświetla poziom powiązane z wybranymi drzwiami. Kolumna Terminarz wyświetla terminarz przypisany do poziomu dostępu.

- Czerwony – brak dostępu (brak autoryzacji).
- Zielony – dostęp (autoryzowany).

Definiowania kart gości (Visitor Cards Definition)

Karta gościa jest wystawiana tymczasowo. Służy, jako szablon do wprowadzenia informacji o użytkowniku. Możesz ją stworzyć na dwa sposoby:

- Kopiując pola informacji do bazy danych Kart Gości (Visitor card database) w momencie tworzenia nowej karty albo przepustki,
- Tworząc nową kartę gościa.

Definiowanie karty gościa w szablonie definiowania nowej karty (Creating a Visitor Card When Creating a New Card)

1 – Wybierz przycisk Karta z paska narzędzi Użytkownicy. Okno Karta zostanie wyświetlone.

2 – Zaznacz opcje Kopiuj do gościa (Copy to visitor). Informacje zostaną wykorzystane później przy tworzeniu nowych kart i przepustek.

Tworzenie nowej karty gościa przy użyciu Szablonu karty (Creating a Visitor Card Using the Card Template)

1 – Wybierz przycisk Gość (Visitor) z paska narzędzi Użytkownicy.

2 – Wprowadź niezbędne informacje.

Notatka: aby uzyskać dodatkowe informacje na temat Przepustek dziennych oraz Kart gości zobacz Definiowanie kart. Zakładka Obraz pozwala wyświetlić m.in. zdjęcie użytkownika karty; jak również zrobić pogląd oraz wydrukować identyfikator.



Definiowanie

Definiowanie terminarzy (Schedules Definition)

Terminarz określa, kiedy system wykona daną operację, na przykład: automatyczne odryglowanie drzwi, przyznanie dostępu dla pracownika, monitorowanie wejść, etc. Określa również, kiedy zdarzenia muszą zostać zatwierdzone albo kiedy aktywować przekaźniki kontrolujące dodatkowe funkcje (oświetlenie, ogrzewanie, etc.). Możesz używać tego samego terminarza w różnych menu, ale rekomendowanym jest utworzenie osobnego terminarza dla każdej aplikacji.

Każdy terminarz składa się z czterech przedziałów. Każdy przedział ma swój czas rozpoczęcia i czas zakończenia. Każdy przedział może zostać wybrany dla siedmiu dni tygodnia, oraz czterech dni specjalnych. EntraPass daje użytkownikowi możliwość zaprogramowania 99 terminarzy na bramkę, i nieograniczoną ilość terminarzy na system. W tym celu musisz uruchomić Uruchom zaawansowane zasoby terminarza (Upgrade to advanced schedule capability) w okienku Parametry systemu (System parameters) (Options toolbar > System parameters > Server).

Notatka: Aby uzyskać więcej informacji zobacz Konfiguracja parametrów systemu ([System Parameters Configuration](#)).

EntraPass wspiera dwie grupy terminarzy:

- Terminarze systemowe: globalne funkcje – parametry zdarzeń, logowanie użytkowników, etc. Nie są wczytywane w kontrolerach.
- Terminarze między obiektowe: są definiowane na połączenie. Możesz zdefiniować 99 terminarzy na połączenie do następujących celów: nadzór zasilania, terminarz odblokowywania (drzwi), tryb aktywacji (przełączniki), etc. Jeżeli przypisujesz albo definiujesz terminarz, upewnij się, że wybierasz odpowiednią kategorię dla terminarza.



Definiowanie terminarza (Defining a Schedule)

1 – Z głównego okna EntraPass, wybierz zakładkę Definiowanie (Definition). Kliknij przycisk Terminarz (Schedule).

Notatka: jeśli zaznaczyłeś opcję Uaktualnienie możliwości terminarza do zaawansowanych (Upgrade to advanced schedule capability) (Parametry systemu > Serwer > Zakładka Terminarz), zostanie wyświetlona lista Bramek/Obiektów. Z listy wybierz terminarz dla Obiektu albo dla Systemu (stosowany dla komponentów).

2 – Z listy wybierz terminarz, który chcesz modyfikować albo wybierz terminarz do przypisania do kategorii wybranej w poprzednim kroku, albo wybierz Nowy (New), aby stworzyć nowy terminarz.

3 – Przypisz nazwę (albo zmodyfikuj).

4 – Klikając przycisk Dni specjalne (Holiday) na pasku narzędzi wyświetlisz listę dni specjalnych zdefiniowanych w systemie.

Notatka: EntraPass wspiera cztery typy dni wolnych.

5 – Określ czas rozpoczęcia (Start time): czas, w którym przedział staje się aktywny.

6 – Określ czas zakończenia (End time): czas, po którym przedział staje się nieaktywny.

Notatka: czas rozpoczęcia oraz czas zakończenia jest zapisany w 24 godzinnym formacie; oznacza to zakres czasu od 00:00 do 24:00. Dla każdego przedziału, czas zakończenia musi być wyższy niż czas rozpoczęcia.

7 – Wybierz dni tygodnia, w trakcie których przedział terminarza będzie aktywny zaznaczając pole pod każdym z dni.

8 – Zaznacz kolumnę Typ dnia specjalnego (Holiday type), jeżeli zdefiniowałeś cztery dni specjalne i chcesz aby przedział był aktywny podczas dnia specjalnego. Możesz również kliknąć przycisk + List (Holiday list), aby wyświetlić kalendarz na najbliższe 12 miesięcy z zaznaczonymi dniami specjalnymi (trzy kolorowa skala określona w legendzie).

Notatka: Legenda jest inna od tej, która jest wykorzystywana przy definiowaniu dni wolnych. Zobacz Definiowanie dni wolnych (Holiday definitione).



EntraPass - Instrukcja instalacji i obsługi programu Definiowanie

Tworzenie ciągłego, 2 dniowego przedziału (To Create a 2-day Continuous Interval)

Aby stworzyć przedział od poniedziałku (20:00) do wtorku (08:00), terminarz musi zostać podzielony na dwa przedziały:

To create an interval from Monday 20:00 (8:00 PM) to Tuesday 08:00 AM, the schedule must be divided into two intervals:

1 – Najpierw stwórz przedział dla poniedziałku, od 20:00 do 24:00;

	Godz. pocz.	Godz. koń.	Nie	Pon	Wto	Śro	Czw	Pią	Sob	Św 1	Św 2	Św 3	Św 4
1	20:00	00:08	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐
2	00:00	00:00	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐
3	00:00	00:00	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
4	00:00	00:00	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

2 – Następnie określ drugi przedział dla wtorku, od 00:00 do 08:00. System traktuje te dwa przedziały, jako jeden ciągły przedział.

Rozbudowane terminarze (Extended Schedule)

Ta opcja umożliwia zwiększenie ilości przedziałów do 20.

Notatka: terminarze z 20 interwałami w trybie stand-alone mogą być wykorzystane wyłącznie z kontrolerami KT-400 oraz KT-400 V1.



Definiowanie pięter (Floors Definition)

Opcja Piętra (Floor) jest wykorzystywana do tworzenia i edytowania pięter windy. Po ich stworzeniu, są grupowane i dostają przypisany terminarz, który określa, kiedy jest przyznany do nich dostęp.

- 1 – Z paska narzędzi Definiowanie (Definiotion), wybierz przycisk Piętro (Floor)
- 2 – Z listy Obiekt/Bramka/Połączenie wybierz obiekt/bramkę/połączenie dla którego definiujesz piętro.
- 3 – Wybierz piętro, albo kliknij Nowy (New), aby stworzyć nową grupę pięter.
- 4 – Przypisz odpowiednią nazwę dla piętra i kliknij przycisk Zamknij (Close). System poprosi o zapisanie danych.

Definiowanie map (Graphics Definition)

Mapa odpowiada strefie systemu, w której komponenty (aplikacje EntraPass, kontrolery, Wejścia linii dozorowej, przekaźniki, etc.) są zlokalizowane. Dzięki mapie, użytkownik może z łatwością sprawdzić dokładną lokalizację komponentu zainstalowanego na połączeniu, albo statusy komponentów i urządzeń takich, jak: drzwi, czujnik stanu drzwi, detektorów ruchu, kontrolerów, paneli, etc. Użytkownik może przeprowadzać zdalne operacje bezpośrednio z poziomu wyświetlonego komponentu (np. zablokować/odblokować drzwi), może bez potwierdzenia wykonywać zadania. Możesz utworzyć tak dużo map, jak potrzebujesz. Każda mapa może wyświetlić 250 komponentów. Możesz również importować mapę lub mapy z innych programów (formaty: BMP, EMF, WMF, JPEG, GIF, PCX, PNG, TIF albo PCD).

Notatka: EntraPass udostępnia użytkownikowi cztery przykładowe plany pięter. Możesz je edytować i zmieniać tak, aby pasowały do potrzeb twojego systemu. Przykładowe plany są zlokalizowane w: C:\Program Files\Kantech\Server_CE\Generaldata\Demobmp.

Definiowanie komponentów mapy (Defining Components of a Graphic)

- 1 – Z paska narzędzi Definiowanie (Definiotion), wybierz przycisk Grafika (Graphics)
- 2 – Z listy Grafik, wybierz mapę, którą chcesz modyfikować albo kliknij Nowy (New), aby stworzyć nową.
- 3 – Przypisz nazwę do mapy (albo zmień istniejącą nazwę).

Notatka: kiedy wybierzesz istniejącą mapę albo stworzysz nową wszystkie komponenty przypisane do twojej mapy zostaną wyświetlone w lewym panelu. Prawa część okna wyświetla samą mapę.

- 4 – Z okna Definiowanie mapy (Graphic definitione), kliknij utwórz, edytuj, zmień (create, edit, modify), aby wyświetlić okno Przypisz komponenty (Assign Components).

Notatka: Jeśli w twoim systemie opcja wideo jest włączona, komponenty wideo zostaną dodane do menu Grafika. Dostęp do tych komponentów jest możliwy z szablonu mapy. Przycisk może zostać umiejscowiony na szablonie mapy, a jego status może zostać uzyskany poprzez kliknięcie na przycisku wideo. Dodatkowo, następujące opcje statusów będą dostępne dla komponentów wideo: Serwer wideo online/offline, Parametry serwera wideo oraz Status kamery.

- 5 – Kliknij na menu Opcje, aby wyświetlić menu z opcjami rysowania. Znaczek potwierdzenia pojawia się przy każdej aktywnej opcji. Podpowiedzi związane z nazewnictwem komponentów są wyświetlane w momencie najechania kursorem na mapę.

- Rysuj przezroczyste (Draw transparent) – umieści przezroczysty przycisk na wierzchu tła.
- Rysuj ramę (Draw frame) – rysuje ramę dla komponentu. Możliwa jest zmiana koloru ramy.
- Auto wyświetlanie nagrania (Auto display video view) – pozwala dodać widok nagrania.
- Wybierz Edytuj tło (Edit background picture), aby edytować tło wybranej mapy. Z tego okna możesz zmienić ramę, kolor tła oraz dodawać przypisy.



EntraPass - Instrukcja instalacji i obsługi programu Definiowanie

- Wybierz Dodaj wideo na żywo, jako tło (Add live video as background), aby mieć wideo na żywo, jako tło.
- Wybierz Dodaj stronę www, jako tło (Add Web page as background), aby strona www była użyta, jako tło. Wprowadź adres URL połączenia i kliknij Enter, albo kliknij Test. Login i hasło nie są wymagane, chyba, że wymaga ich wybrana strona. Kliknij Test, żeby sprawdzić czy strona wczytuje się prawidłowo. Następnie kliknij Zapisz (Save).
- Wybierz Wyczyść tło (Clear background), aby wyczyścić obrazek z tła mapy pozostawiając przypisane komponenty. Możesz użyć tej opcji, jeżeli chcesz dodać nową mapę, albo pozostawić sam komponent.



Projektowania tła dla Okna Grafiki (Designing the Background for the Graphic Window)

1 – Kliknij podwójnie w dowolne miejsce tła okna Przypisz komponenty (Assign components), aby wyświetlić okienko Projektuj obrazek tła (Design background picture).

2 – Użyj tego okna, aby importować mapę stworzoną w innej aplikacji, albo stworzyć własne tło wykorzystując przyciski paska narzędzi rysowania.

-  Aby zaimportować mapę, kliknij przycisk dyskietki, po czym przeciągnij i upuść dyskietkę w wybranym obszarze pracy. Wyświetli się okienko właściwości obrazu. System wyświetli okno Otwórz (Open). Znajdź mapę i kliknij Otwórz.
-  Aby zaimportować dowolny obraz do tła, kliknij Obrazy niestandardowe (Custom images) na pasku narzędzi. Pojawi się okna Wybierz obraz (Select an image). Wybierz obraz, kliknij OK, aby zamknąć okno i zaimportować obraz.
- Aby wprowadzić dowolny kształt i tekst do tła, wybierz prostokąt, okrąg, elipsę, etc., z paska narzędzi i przeciągnij ją na pole tła.
- Aby zmodyfikować kształt, który właśnie umieściłeś w oknie, przy pomocy prawego przycisku myszy otwórz okienko Właściwości (Properties) i dokonaj zmian (kolor, pozycja, etc.).
- Możesz ustawić system tak, aby wyświetlał okienko Właściwości (Properties) zawsze, gdy umieszczasz „kształt” w okienku roboczym. W tym celu zaznacz Pokaż właściwości po upuszczeniu (Show properties on Drop) z menu Opcje (Options).
- Aby wykorzystać wcześniej zapisane kształty, wybierz opcję Wczytaj odniesienie (Load annotations) z menu Obrazy (Image).
- Aby zapisać odniesienia w osobnym pliku (nie w pliku z przygotowywaną mapą), wybierz opcję Zapisz odniesienie (Save annotations) z menu Obrazy (Image).
- Aby wyczyścić wszystkie kształty, wybierz opcję Wyczyść odniesienie (Clear annotations) z menu Obrazy (Image). Jeżeli zapiszesz mapę wraz z kształtami, kształt staje się permanentnym elementem mapy.
- Użyj menu Pogląd (View), aby sprawdzić, jak wyświetlana jest mapa.

Notatka: obramowanie (wyświetlone wzdłuż ścian wybranego obiektu) wskazuje, że obiekt jest wybrany.



Przypisywanie komponentów systemu do ikon mapy (Assigning System Components to Graphic Icons)

- 1 – Z paska narzędzi okna Przypisz komponent (Assign Components), kliknij i przeciągnij wybrany komponent na określoną pozycję.
- 2 – Po umiejscowieniu komponentu i „upuszczeniu”, pojawi się okienko Przypisz z (Assign From).
- 3 – Wybierz komponent systemu, który chcesz przypisać do przycisku na ekranie.
- 4 – Kliknij OK, aby wrócić do poprzedniego okna.

Notatka: jeśli nie przypiszesz przycisku do komponentu, przycisk nie zostanie zapisany w mapach. Tylko komponenty, które nie zostały wybrane w mapach będą dostępne do wyboru.

Drukowanie komponentów systemu oraz mapy (Printing System Components and Graphics)

- 1 – Z zakładki Definiowanie (Definition), wybierz przycisk Grafika (Graphic), a następnie wybierz mapę z listy.
 - 2 – Kliknij przycisk Drukuj (Print) z paska narzędzi.
- Wybierz mapy do druku za pomocą zaznaczenia. Możesz użyć przycisków Zaznacz wszystkie (Select all) albo Odznacz wszystkie (Clear all).
 - Wybierz Drukuj puste pola (Print empty fields), aby wydrukować nazwy pustych pól.
 - Wybierz Drukuj referencje komponentu (Print component references), aby wydrukować numery referencji.
 - Użyj przycisku Czcionka (Font), aby móc edytować właściwości czcionki.
 - Kliknij przycisk Pogląd (Preview), aby wyświetlić podgląd szablonu wydruku.



Definiowanie dni świątecznych (Holiday Definition)

Dzień specjalny (Holiday) jest traktowany inaczej od pozostałych dni. Rekomendowane jest zaprogramowanie dni specjalnych na początku roku. Pomaga to modyfikować święta ruchome (Wielkanoc, etc.). Dzień specjalny może być określony jako konkretny typ (Hol 1, 2, 3, 4). Ten sam dzień może być określony jako specjalny na jednym połączeniu, i jako dzień zwykły na innym.

1 – Z zakładki Definiowanie (Definition), wybierz przycisk Dzień specjalny (Holiday).

2 – Aby utworzyć nowy dzień specjalny, wybierz przycisk Nowy (New).

3 – Jeżeli chcesz utworzyć globalny dzień specjalny, kontynuuj z definiowaniem dnia specjalnego. Jeżeli chcesz przypisać dzień specjalny do konkretnej bramki/połączenia, wybierz bramkę/połączenie z listy.

4 – Przypisz nazwę dla dnia specjalnego.

5 – Z menu Data (Date), wybierz datę dnia specjalnego z kalendarza.

6 – Zaznacz opcję Powtarzające się (Recurring), jeżeli tak jest w przypadku definiowanego dnia specjalnego.

Notatka: jeśli dzień wolny nie jest „świętem powtarzalnym”, będziesz musiał przeprogramować go na następny rok. Możesz ustawiać dni wolne na rok z wyprzedzeniem; rekomendowane jest jednak, aby sprawdzać oznaczenie dni wolnych regularnie.

7 – W sekcji Typ dnia specjalnego (Holiday type), wybierz typ dnia specjalnego. Na przykład, możesz określić dany dzień, jako specjalny dla grupy użytkowników, a jako zwykły dla innej.

8 – Kliknij przycisk + List (Holiday list), aby wyświetlić kalendarz na najbliższe 12 miesięcy z zaznaczonymi dniami specjalnymi (trzy kolorowa skala określona w legendzie).

9 – Jeżeli dzień specjalny jest przypisany do konkretnego obiektu, Selektywny dzień specjalny (Selective Holiday) musi być zaznaczony.

10 – „Złap i upuść” odpowiedni system, obiekt albo bramkę przypisując go do konkretnego dnia specjalnego.

Możesz skorzystać z przycisków:  oraz , aby je przesunąć.

Notatka: Legenda jest inna od tej, która jest wykorzystywana przy definiowaniu terminarzy. Zobacz Definiowanie terminarzy (Schedules definitione).



Wyzwalacz i alarm, wcześniej Przełącznik makro SML (previously Event Trigger)

Tworzenie nowego przełącznika makro SML (Create a New Trigger)

- 1 – Z paska narzędzi Definiowanie (Definition), wybierz przycisk Przełącznik zdarzenia i kliknij zakładkę Ogólne (General)
- 2 – Kliknij Nowy (New) i wprowadź nazwę przełącznika.
- 3 – Wybierz komponent z listy komponentów.
- 4 – Wybierz pomiędzy Komponent (Single component), Grupa elementów (Trigger group) i Wszystkie elementy, jako źródło przełączników (All components as a trigger source).
- 5 – Kliknij na trzy-kropki, aby wybrać drzwi.
- 6 – Kliknij na trzy-kropki, aby wybrać terminarz przełącznika.
- 7 – Aby użyć rozbudowanego filtra, wybierz opcję Użyj rozbudowanego filtra (Use extended filter).
- 8 – Z listy Kategoria zdarzenia (Event category), wybierz typ zdarzenia.
- 9 – W sekcji Przeznaczenie przełącznika (Trigger destination), kliknij na trzy-kropki i wybierz SmartLink.
- 10 – Kliknij na trzy-kropki, aby wybrać zadanie
- 11 – Z zakładki Zdarzenia, wybierz zdarzenie.
- 12 – Kliknij na zakładkę Rozbudowany filtr (Extended filter).
- 13 – Kliknij na Dodaj (Add), aby dodać nowy filtr.
- 14 – Wybierz Typ filtra (Filter type) oraz Filtr komponentów (Component filter).
- 15 – Powtórz powyższy krok dla każdej karty.
- 16 – Kliknij na Zapisz i zamknij (Save and Close).



Wyłączenie przełącznika makro SML (Disable a Trigger)

- 1 – Z paska narzędzi Definiowanie (Definotion), wybierz przycisk Przełącznik zdarzenia
- 2 – Wybierz przełącznik z listy.
- 3 – Zaznacz Wyłącz **przełącznik makro SML** (Disable trigger)

Definiowanie nowych powiadomień o alarmie (Create a new Alarm notification)

- 1 - Kliknij kartę **Powiadomienie o alarmie**.
- 2 - Wybierz **harmonogram alarmów**, aby określić, kiedy traktować wyzwalacz jako alarm.
- 3 - Wybierz **harmonogram podręcznego pulpitu**, aby określić, kiedy na ekranie operatora pojawią się powiadomienia o alarmie pulpitu.
- 4 - Jeśli chcesz, aby operator potwierdził alarm, wybierz opcję potwierdzenia z listy rozwijanej lista.
 - a - **Brak potwierdzenia**. Nie pojawi się okienko potwierdzenia. Wiadomość jest wyświetlana w **alarmie Lista wiadomości**.
 - a - **Potwierdzenie dla wszystkich podłączonych stacji roboczych**. Wszystkie wyskakujące komunikaty potwierdzające są wyświetlane online i zalogowany na stacjach roboczych.
 - a - **Potwierdzenie dla wszystkich podłączonych i wybranych stacji roboczych**. Potwierdzające wiadomości wyskakujące to wyświetlane na wszystkich online i zalogowanych na **stacjach roboczych wybranych** na karcie Wybrane stacje robocze.
 - a - **Najpierw potwierdź, na podstawie poziomu operatora**. EntraPass określa najwyższe potwierdzenie priorytet wszystkich zalogowanych operatorów. Komunikat wyskakujący potwierdzenia jest najpierw wysyłany do tych operatorów. Jeśli wyskakujący komunikat nie zostanie potwierdzony w czasie określonym w potwierdzeniu przekroczenia limitu czasu opóźnienie, wyskakująca wiadomość jest wysyłana do wszystkich online i rejestrowana na stacjach roboczych.
 - a - **Najpierw potwierdź, na podstawie poziomu stacji roboczej**. EntraPass określa najwyższe potwierdzenie priorytet wszystkich zalogowanych stacji roboczych. Wyskakujący komunikat potwierdzenia jest najpierw wysyłany do nich
- stacje robocze. Jeśli wyskakujący komunikat nie zostanie potwierdzony w czasie określonym w Limit czasu
- potwierdź opóźnienie, wyskakujący komunikat zostanie wysłany do wszystkich online i zalogowany na stacjach roboczych.
- a - **Najpierw potwierdź, na podstawie poziomów operatora i stacji roboczej**. EntraPass określa najwyższą wartość potwierdź priorytet wszystkich zalogowanych operatorów i wszystkich stacji roboczych. Okno potwierdzenia wiadomość jest najpierw wysyłana do kandydata o najwyższym priorytecie. Jeśli wyskakujący komunikat nie zostanie potwierdzony w czasie określonym w Opóźnienie potwierdzenia przekroczenia czasu, wyskakująca wiadomość jest wysyłana do wszystkich online i zalogowany na stacjach roboczych.
- 5 - Jeśli operator wymaga dodania komentarza do alarmu, wybierz opcję Obowiązkowe sprawdzenie komentarza pudełko.
- 6 - Wybierz harmonogram wyskakującego interfejsu API, aby określić, kiedy wyskakujące okienka powiadomień o alarmach są aktywne dla osób trzecich Aplikacje.
- 7 - Wybierz opcję Instrukcja, aby skojarzyć instrukcję z alarmem.



EntraPass - Instrukcja instalacji i obsługi programu Definiowanie

8 - Wybierz harmonogram powiadomień e-mail, aby wysyłać wiadomości e-mail podczas alarmu. Adresatami poczty elektronicznej są

zdefiniowane w polu powiadomień e-mail.

9 - Wybierz pole Zezwól na potwierdzenie wiadomości e-mail, aby umożliwić potwierdzenie alarmów za pomocą poczty e-mail. Jeśli to

opcja jest wybrana, odbiorcy wiadomości e-mail zdefiniowani w polu Powiadomienia e-mail są wysyłani do łącza

potwierdź alarm. Adresy e-mail muszą być oddzielone średnikiem „;”. E-mail zawiera

data i godzina wydarzenia, nazwa wydarzenia, szczegóły wydarzenia i instrukcje powiązane z

wyzwalacz (jeśli został zdefiniowany).

UWAGA: Zezwól na potwierdzenie e-mailem wymaga usługi sieciowej zdefiniowanej pod co najmniej jednym łączem Smartlink.

10 - Wybierz język z listy rozwijanej.

11 - Kliknij Zapisz i zamknij.

Odbieranie wiadomości e-mail z powiadomieniem o wyzwalaczach wideo

Podczas konfigurowania powiadomienia o alarmie dla zdarzenia wideo należy skonfigurować powiadomienie e-mail

pole harmonogramu. Komponent, który wyzwala zdarzenie, musi mieć łącze widoku kamery lub wideo

otrzymasz powiadomienie e-mail zawierające miniatury. Gdy wystąpi wyzwolenie zdarzenia, EntraPass wysyła

e-mail zawierający cztery miniaturowe widoki wydarzenia. Jeśli urządzenie ma wiele kamer, podłącz

używana jest pierwsza kamera w widoku. Aby zapoznać się z czasem wyświetlania miniatur, zobacz następujące kroki:

1 - Pięć sekund przed wystąpieniem zdarzenia.

2 - W momencie wydarzenia.

3 - Dwie sekundy po zdarzeniu.

4 - Pięć sekund po wydarzeniu.



EntraPass - Instrukcja instalacji i obsługi programu Definiowanie

Kreator makro SML (Task Builder Definition)

Wymagania minimalne

Przyciski Makro-poleceń (Task builder) oraz Przełącznik zdarzeń (Event trigger) są dostępne tylko wtedy, kiedy komponent SmartLink został zainstalowany na stacji roboczej i zarejestrowany na serwerze EntraPass.

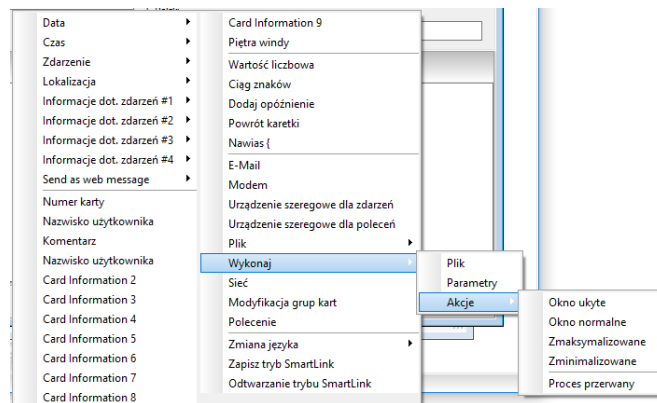
Opisywanie okienek makro-poleceń (Task Builder Dialogs Description)

1 – Z paska narzędzi Definiowanie (Definition), wybierz przycisk Makro-poleceń (Task Builder).

Menu Makro-poleceń umożliwia użytkownikowi tworzenie zadań SmartLink. Jeżeli masz zainstalowaną aplikację SmartLink, dla przycisku SmartLink dostępne jest menu Wstawienie zadania (Task insertion). Umożliwia użytkownikom wysyłanie wbudowanych poleceń do oprogramowania SmartLink.

Notatka: nowe polecenie zostało dodane do Smartlink (BATCHMODIFY). Jest teraz możliwe zmienianie parametrów dla grupy kart tego samego typu. Zmienione zostaną tylko pola z danymi wskazane przez polecenie. Aby dowiedzieć się więcej o poleceniach zadań sprawdź SmartLink Reference Manual, DN1327.

2 – Kliknij na menu Wstawienia zadania (Task insertion), aby wyświetlić menu.



Notatka: przy tworzeniu zadań Smartlink tylko polecenia pisane w głównym języku są traktowane, jako prawidłowe polecenia. Aby dowiedzieć się więcej o poleceniach zadań sprawdź SmartLink Reference Manual, DN1327.



EntraPass - Instrukcja instalacji i obsługi programu
Definiowanie

Opis parametru

Data (Date)	Wprowadź datę do zadania. Opcje: rok, miesiąc, dzień, RRRR/MM/DD albo MM/DD/RRRR
Czas (Time)	Wprowadź czas do zadania. Opcje: godzina, minuta, sekunda, HH:MM:SS albo HH:MM
Zdarzenie (Event)	Wprowadź opis zdarzenie w zadaniu. Możesz wyświetlić nazwę zdarzenia albo jego numer
Lokalizacja (Location)	Wprowadź lokalizację, w której zadania ma być zrealizowane. Opcje: aplikacja EntraPass, Bramka albo połączenie



Opis parametru

Informacja 1-4 (Info #1 to 4)	Wprowadź informacje o zdarzeniu. Opcje w bazie danych: numer indeksu, tekst indeksu, ID komponentu, tekst komponentu
Informacje o użytkowniku (User Information)	Wprowadź informację o karcie do zadania. Opcje: numer karty, nazwa użytkownika karty, informacje 1-10, komentarz
Numer (Numerical Value)	Wprowadź numer do zadania.
Dodatkowy opis (Character String)	Wprowadź ciąg znaków (wolny tekst) do zadania.
Dodaj opóźnienie (Add Delay)	Wprowadź opóźnienie w 1/10 sec do zadania.
Carriage Return	Wprowadź zwrot carriage do zadania.
Przytnij prawo (Trim Right)	Usuń ostatni znak po prawej od zadania.
Email	Wprowadź email do zadania, który zostanie wysłany automatycznie po zajściu zdarzenia.
Modem	Wprowadź wiadomość do zadania, która zostanie wysłana automatycznie przez pager po zajściu zdarzenia.



EntraPass - Instrukcja instalacji i obsługi programu Definiowanie

Urządzenie dla wiadomości (Serial Device for Messages)	Wybierz numer seryjny portu do komunikacji oraz szybkość transmisji do wysłania wiadomości.
Urządzenie dla poleceń (Serial Device for Commands)	Wybierz numer seryjny portu do komunikacji oraz szybkość transmisji do wysłania poleceń.
Plik (File)	Otwiera okienko Wybierz plik (Select a file), które pozwala zlokalizować plik (albo stworzyć nowy), do którego będą wprowadzone wszystkie informacje o zdarzeniu w momencie zajścia zdarzenia. Przycisk Zamknij (Close) zamknie plik. Przycisk Przypisz do dysku (Commit to disk) zapisze plik na dysku. To polecenie nie zamknie pliku.
Wykonaj (Execute)	Otwiera okienko Wybierz plik (Select a file), które pozwala zlokalizować plik wykonawczy, który będzie wykorzystany razem z poleceniem zadania. Przycisk Parametry (Parameters) otwiera okienko Wprowadź Dodatkowy Opis (Enter Character Strings), który pozwala wprowadzić ciąg znaków dodany później do polecenia zadania. Przycisk Akcja (Action) pozwala określić, jak chcesz uruchomić zadanie (normalnie, ukryte uruchomienie, zminimalizowane uruchomienie, etc.)
Sieć (Network)	Wprowadź oznaczenie sieci.
Polecenie (Command)	Wprowadź oznaczenie polecenia.



Opis parametru

Zmień język (Modify language)	Możesz zmienić język poleceń na angielski albo francuski.
Save SmartLink Mode	Wprowadza do SmartLink polecenie przerwanie i przeniesienie do tła obecnego trybu pracy SmartLink. Używane z Przywróć poprzedni tryb SmartLink (Restore Previous SmartLink mode)
Zmień język (Modify language)	Możesz zmienić język poleceń na angielski albo francuski.
Przywróć poprzedni tryb SmartLink (Restore Previous SmartLink mode)	Wprowadza do SmartLink polecenie przywrócenia poprzedniego ustawienia SmartLink. Używane z Save SmartLink Mode



EntraPass - Instrukcja instalacji i obsługi programu Definiowanie

Dodawanie wiadomości do zadania (Adding an Email to a Task)

1 – Po wybraniu istniejącego zadania albo utworzeniu nowego, kliknij na przycisk Skrzynki (Mailbox). Okienko Makro-poleceń: Wiadomość (Email Task Builder) zostanie wyświetlone.

2 – Wprowadź swój adres email w pole Od (From...)

3 – Wprowadź adresy email, na który wiadomość ma zostać wysłana w pole Do (To...). Każdy adres powinien być oddzielony średnikiem (;).

4 – Jeżeli chcesz wysłać kopię tej wiadomości do innych ludzi, wprowadź ich nazwę w pole Do wiadomości (CC...)

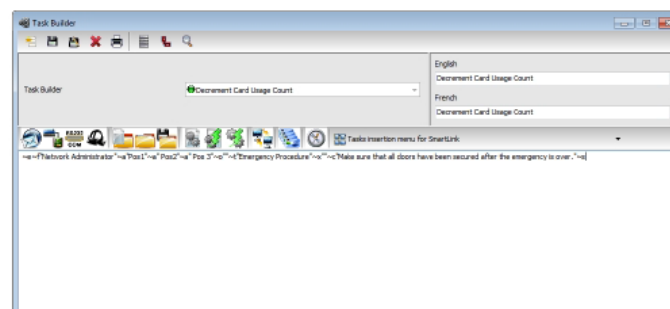
5 – Wprowadź temat.

6 – Jeżeli chcesz dodać załącznik do wiadomości, wprowadź adres załącznik pole Załącznik (Attachment). Każdy załącznik musi być oddzielony średnikiem (;).

7 – Wprowadź wiadomość w pole dla tekstu.

Notatka: Zmienne mogą być dodawane do tytułów wiadomości e-mail oraz ich treści.

8 – Kliknij OK, aby dodać wiadomość do zadania SmartLink. Wiadomość pojawi się w oknie.



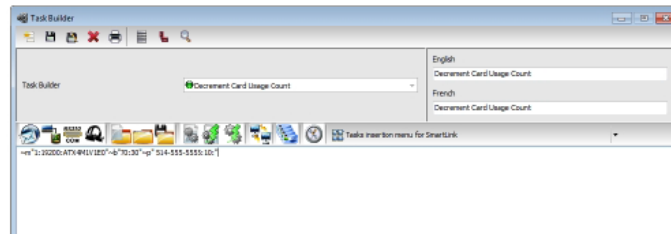


EntraPass - Instrukcja instalacji i obsługi programu Definiowanie

Wprowadzanie polecenia pagera w zadaniu (Inserting a Pager Command in a Task)

Tworząc zadanie przy wykorzystaniu SmartLink, EntraPass pozwala wprowadzić polecenie, które wyśle wiadomość do systemu powiadomień (paging system)

- 1 – Kliknij przycisk Modem (Modem). Wyświetli się okienko Parametrów zadania: Modem (Modem task parameters).
- 2 – Numer portu modemu powinien już być ustawiony.
- 3 – Wprowadź informacje o numerze telefonicznym pagera.
- 4 – Wprowadź wiadomość, która pojawi się na pagerze oraz opóźnienie (w sekundach), z jakim wiadomość zostanie wysłana. Przedział czasu: od 00:00 do 09:59 min.
- 5 – Kliknij OK. Numer telefonu oraz wiadomość pojawią się oknie.





Wprowadzanie urządzenia dla wiadomości (Inserting Serial Device for Messages)

- 1 – Kliknij **Urządzenie dla wiadomości (Serial device for messages)**.
- 2 – Wybierz numer seryjny portu oraz szybkość transmisji.
- 3 – Kliknij **OK**.

Wprowadzanie urządzenia dla poleceń (Inserting Serial Device for Commands)

- 1 – Kliknij przycisk **Urządzenie dla poleceń (Serial device for commands)**. Pojawi się okno **Wybierz numer seryjny portu do komunikacji (Serial com port)**.
- 2 – Wybierz **numer portu do komunikacji (Port Number)** oraz **szybkość transmisji do wysłania poleceń (Baud rate)**
- 3 – Kliknij **OK**.

Wprowadzanie Pliku (Inserting a File)

- 1 – Kliknij przycisk **Otwórz Plik (Open)**. Pojawi się okno **Wybierz plik (Select a file name)**.
- 2 – Wprowadź nazwę, albo wyszukaj plik.
- 3 – Kliknij **OK**.

Uruchamianie Pliku (Executing a File)

- 1 – Kliknij przycisk **Uruchom Plik (Execute)**. Pojawi się okno **Wybierz plik (Select a file name)**.
- 2 – Wprowadź nazwę, albo wyszukaj plik.
- 3 – Kliknij **OK**.



Uruchamianie Parametrów (Executing Parameters)

1 – Kliknij przycisk **Uruchom Parametr (Execute)**. Pojawi się okno **Wprowadź Dodatkowy Opis (Enter character string)**.

Wprowadzanie oznaczenia sieci (Entering a Network Tag)

1 – Kliknij przycisk Sieć (Network). Pojawi się okno **Wprowadź oznaczenie sieci (Enter network tag)**.

2 – Wprowadź oznaczenie sieci. Zakres od 0 do 999,999.

3 – Kliknij **OK**.

Wprowadzanie komend (Entering Commands)

1 – Kliknij przycisk **Polecenie (Command)**. Pojawi się okno **Makro-polecień SmartLink (SmartLink Task Builder)**

2 – Wybierz typ komponentu z listy.

3 – Wybierz polecenie listy.

Notatka: polecenie **Przełącz** jest dostępne wyłącznie przy niektórych komponentach, takich jak: Drzwi, Wejścia linii dozorowej, Przekazniki.

4 – Wybierz zmienną z listy. Są trzy rodzaje:

- Wartość (Message Value)
- Przełącznik (Trigger)
- Informacja o karcie: 1-10 (Card Information 1 to 10)

Przykłady tworzenie zadań (Task Building Examples)

Poniższe procedury uwzględniają wszystkie trzy rodzaje zmiennych, które mogą zostać przypisane do typu komponentu i polecenia.



Tworzenie zadania ze zmienną: wartość (Building a Task with a Message Value Variable)

- 1 – Z paska narzędzi **Definiowanie (Definition)**, wybierz **Makro-polecenia (Task Builder)**.
 - 2 – Kliknij **Nowy (New)** i wprowadź nazwę zadania: **Decrement Card Usage Count**
 - 3 – Kliknij przycisk **Polecenie (Command)**
 - 4 – Z okna **Makro-poleceń SmartLink (SmartLink Task Builder)**, wybierz **Karta (Card)** z listy **Typ komponentu (Component type)**.
 - 5 – Wybierz **Zmniejsz wykorzystanie zliczania (Decrement count usage)** z listy poleceń.
 - 6 – Wybierz **Wartość (Message value)** z listy. Zadanie wyświetla się na dole okienka. Kliknij **OK**.
 - 7 – Zadanie SmartLink wyświetla pole tekstowe.
 - 8 – Kliknij **Zapisz (Save)** i zamknij **Makro-polecenia (Task Builder)**.
 - 9 – Z paska narzędzi **Definiowanie (Definition)**, wybierz **Przełącznik zdarzenia (Event Trigger)**.
 - 10 – Kliknij **Nowy (New)** i wprowadź nazwę przełącznika zdarzenia: **Decrement Card Usage Count**
 - 11 – W sekcji **Źródło przełącznika (Trigger Source)**, wybierz **Drzwi (Door)** z listy komponentów.
 - 12 – Kliknij w **trzy-kropki**, aby wybrać komponent.
- Notatka: jako Źródło przełącznika (Trigger Source) możesz zaznaczyć również grupę komponentów albo wszystkie komponenty.
- 13 – W sekcji **Przeznaczenie przełącznika (Trigger destination)** kliknij w **trzy-kropki**, aby wybrać **SmartLink**.
 - 14 – Kliknij w **trzy-kropki**, aby wybrać zadania **Zmniejsz wykorzystanie zliczania karty (Decrement Card Usage Count)**.
 - 15 – Z zakładki **Zdarzenia (Events)**, wybierz zdarzenie.
 - 16 – Kliknij na **Zapisz (Save)** i **Zamknij (Close)**.

Tworzenie zadania ze zmienną: wartość przełącznika (Building a Task with a Trigger Value Variable)

- 1 – Z paska narzędzi **Definiowanie (Definition)**, wybierz **Makro-polecenia (Task Builder)**.
- 2 – Kliknij **Nowy (New)** i wprowadź nazwę zadania: **Wartość przełącznika (Trigger value)**
- 3 – Kliknij przycisk **Polecenie (Command)**
- 4 – Z okna **Makro-polecenia SmartLink (SmartLink Task Builder)**, wybierz **Przełącznik (Relay)** z listy **Typ komponentu (Component type)**.



- 5 – Wybierz **Opcje aktywowania przełącznika (Toggle relay activation)** z listy poleceń.
 - 6 – Wybierz **Przełącznik (Trigger #1)** z listy. Zadanie wyświetla się na dole okienka. Kliknij **OK**.
 - 7 – Zadanie SmartLink wyświetla pole tekstowe.
 - 8 – Kliknij **Zapisz (Save)** i zamknij **Makro-polecenia (Task Builder)**.
 - 9 – Z paska narzędzi **Definiowanie (Definition)**, wybierz **Przełącznik zdarzenia (Event Trigger)**.
 - 10 – Kliknij **Nowy (New)** i wprowadź nazwę przełącznika zdarzenia: **Wartość przełącznika**.
 - 11 – W sekcji **Źródło przełącznika (Trigger Source)**, wybierz **Drzwi (Door)** z listy komponentów.
 - 12 – Kliknij w **trzy-kropki**, aby wybrać komponent.
- Notatka: jako Źródło przełącznika (Trigger Source) możesz zaznaczyć również grupę komponentów albo wszystkie komponenty.
- 13 – Kliknij w **trzy-kropki** i wybierz **Zawsze ważne (Always valid)**, jako **Szablon przełącznika (Trigger schedule)**.
 - 14 – Zaznacz opcje **Użyj rozbudowanego filtra (Use extended filter)**.
 - 15 – W sekcji **Przeznaczenie przełącznika (Trigger destination)** kliknij w **trzy-kropki**, aby wybrać **SmartLink**.
 - 16 – Kliknij w **trzy-kropki**, aby wybrać zadania **Wartość przełącznika (Trigger value)**.
 - 17 – Zaznacz opcję **Użyj zmiennej zadania (Use task variable)**.
 - 18 – Z zakładki **Zdarzenia (Events)**, wybierz **Dostęp zezwolony (Access granted)**.
 - 19 – Kliknij na **Zapisz (Save)**.
 - 20 – Wybierz zakładkę **Zmienne (Variable)**.
 - 21 – Jako typ zmiennych wybierz **Przełącznik (Relay)** dla obydwu.
 - 22 – Wybierz zakładkę **Rozbudowany filtr (Extended filter)**.
 - 23 – Jako typ filtra wybierz **Karta (Card)**, następnie wybierz **filtr komponentów** i obie zmienne.
 - 24 – Powtórz punkt 23 dla każdej karty.
 - 25 - Kliknij na **Zapisz (Save)** i **Zamknij (Close)**.



Tworzenie zadania ze zmienną: Informacja o użytkowniku (Building a Task with a User Information Variable)

- 1 – Z paska narzędzi **Definiowanie (Definition)**, wybierz **Makro-polecenia (Task Builder)**.
- 2 – Kliknij **Nowy (New)** i wprowadź nazwę zadania: **Wybierz przekaźnik via Informacje o użytkowniku (Toggle Relay via User Information)**.
- 3 – Kliknij przycisk **Polecenie (Command)**.
- 4 – Z okna **Makro-polecenia SmartLink (SmartLink Task Builder)**, wybierz **Przekaźnik (Relay)** z listy **Typ komponentu (Component type)**.
- 5 – Wybierz **Opcje aktywowania przekaźnika (Toggle relay activation)** z listy poleceń.
- 6 – Wybierz **Informacja o użytkowniku 1 (User information 1)** z listy. Zadanie wyświetla się na dole okienka. Kliknij **OK**.
- 7 – Zadanie SmartLink wyświetla pole tekstowe.
- 8 – Kliknij **Zapisz (Save)** i zamknij **Makro-polecenia (Task Builder)**.
- 9 – Z paska narzędzi **Definiowanie (Definition)**, wybierz **Przełącznik zdarzenia (Event Trigger)**.
- 10 – Kliknij **Nowy (New)** i wprowadź nazwę przełącznika zdarzenia: **Informacja o użytkowniku**.
- 11 – W sekcji **Źródło przełącznika (Trigger Source)**, wybierz **Drzwi (Door)** z listy komponentów.

Notatka: jako Źródło przełącznika (Trigger Source) możesz zaznaczyć również grupę komponentów albo wszystkie komponenty.
- 12 – Kliknij w **trzy-kropki**, aby wybrać komponent.
- 13 – Kliknij w **trzy-kropki** i wybierz **Zawsze ważne (Always valid)**, jako **Szablon przełącznika (Trigger schedule)**.
- 14 – W sekcji **Przeznaczenie przełącznika (Trigger destination)** kliknij w **trzy-kropki**, aby wybrać **SmartLink**.
- 15 – Kliknij w **trzy-kropki**, aby wybrać zadania **Wybierz przekaźnik via Informacje o użytkowniku (Toggle Relay via User Information)**.
- 16 – Z zakładki **Zdarzenia (Events)**, wybierz **Dostęp zezwolony (Access granted)**.

Notatka: upewnij się, że Informacja o użytkowniku jest wprowadzona prawidłowo. Sprawdź poniżej, aby zobaczyć przykład z Paska narzędzi użytkowników > Okno karty > Zakładka Ogólne. Numer 1505 to ID (RELAYID) przekaźnika, który zostanie przełączony, kiedy zadanie zostanie przeprowadzone.
- 17 – Kliknij na **Zapisz (Save)** i **Zamknij (Close)**.



EntraPass - Instrukcja instalacji i obsługi programu Definiowanie



Grupy

Grupy Kontrolerów (Controller Group Creation)

Menu Grup kontrolerów jest wykorzystywane do grupowania kontrolerów tego samego połączenia.

- 1** – W oknie Grupy (Group), kliknij Kontroler (Controller).
- 2** – Wybierz Hierarchia (View hierarchy), aby wyświetlić wszystkie obiekty zdefiniowane w systemie.
- 3** – Z listy Bramka/Połączenie wybierz połączenie albo bramkę, dla których chcesz utworzyć grupę kontrolerów.
- 4** – Kliknij Nowy (New), aby utworzyć nową grupę, a następnie przypisz jej nazwę. Aby modyfikować istniejącą grupę, wybierz ją z listy i wprowadź wszystkie niezbędne informacje.
- 5** – Z listy kontrolerów przypisanych do wybranego połączenia zaznacz kontrolery, które chcesz przypisać do grupy.

Notatka: Zobacz Konfigurowanie kontrolerów.

Grupy Drzwi (Door Group Creation)

Menu Grup kontrolerów jest wykorzystywane do grupowania kontrolerów tego samego połączenia. Grupy drzwi mogą być następnie wykorzystywane do zdalnych działań, takich jak zablokowanie drzwi, etc.

- 1** – W oknie Grupy (Group), kliknij Drzwi (Door).
- 2** – Wybierz Hierarchia (View hierarchy), aby wyświetlić wszystkie obiekty zdefiniowane w systemie.
- 3** – Z listy Bramka/Połączenie wybierz połączenie albo bramkę, z których chcesz zgrupować drzwi.
- 4** – Kliknij Nowy (New), aby utworzyć nową grupę albo wybierz istniejącą grupę z listy, aby ją modyfikować.
- 5** – Z listy Drzwi, wybierz drzwi, które mają być przypisane do grupy.

Notatka: Zobacz Konfigurowanie drzwi.



Grup wyjść sterujących (Relay Group Creation)

Menu Grupa przekaźników jest wykorzystywane do grupowania przekaźników konkretnego połączenia. Grupy Przekaźników mogą być następnie wykorzystywane do działań zdalnych.

- 1 – W zakładki Grupy (Group), kliknij Przekaźnik (Relay).
- 2 – Wybierz Hierarchia (View hierarchy), aby wyświetlić wszystkie obiekty zdefiniowane w systemie.
- 3 – Z listy Bramka/Połączenie wybierz połączenie albo bramkę, z których chcesz zgrupować przekaźniki.
- 4 – Kliknij Nowy (New), aby utworzyć nową grupę albo wybierz istniejącą grupę z listy, aby ją modyfikować.
- 5 – Z listy Przekaźników, wybierz przekaźniki, które mają być przypisane do grupy.

Notatka: Zobacz Konfigurowanie przekaźników.

Grupy Linii dozorowych (Input Group Creation)

Menu Grupa Linii dozorowych jest wykorzystywane do grupowania Linii dozorowych połączenia kontrolera. Grupy Linii dozorowych mogą być następnie wykorzystywane do działań zdalnych.

- 1 – W zakładki Grupy (Group), kliknij Linia dozorowa (Input).
- 2 – Wybierz Hierarchia (View hierarchy), aby wyświetlić wszystkie obiekty zdefiniowane w systemie.
- 3 – Z listy Bramka/Połączenie wybierz połączenie albo bramkę, z których chcesz zgrupować Linie dozorowe.
- 4 – Kliknij Nowy (New), aby utworzyć nową grupę albo wybierz istniejącą grupę z listy, aby ją modyfikować.
- 5 – Z listy Linia dozorowa, wybierz Linie dozorowe, które mają być przypisane do grupy.

Notatka: Zobacz Konfigurowanie Linii dozorowych (Input).



Grupy poziomów dostępu (Access Level Groups Grouping)

Okno Grupy poziomu dostępu (Access level group) jest wykorzystywane do grupowania poziomów dostępu tego samego połączenia.

- 1 – Z okna Grupa (Group), wybierz przycisk Grupa poziom dostępu (Access level group)
- 2 – Wybierz Hierarchia (View hierarchy), aby wyświetlić wszystkie obiekty zdefiniowane w systemie.
- 3 – Z listy Bramka/Połączenie wybierz połączenie albo bramkę, dla których chcesz utworzyć grupę poziomów dostępu.
- 4 – Kliknij Nowy (New), aby utworzyć nową grupę, a następnie przypisz jej nazwę.
- 5 – Zaznacz pola odpowiadające grupie poziomu dostępu.

Grupy pięter (Floor Group Creation)

To menu służy do grupowania pięter stworzonych w menu definiowania pięter.

- 1 – W zakładki **Grupy (Group)**, kliknij **Grupy pięter (Floor group)**.
- 2 – Wybierz **Hierarchia (View hierarchy)**, aby wyświetlić wszystkie obiekty zdefiniowane w systemie. Następnie, z listy Bramka/Połączenie wybierz połączenie albo bramkę, z których chcesz zgrupować piętra.
- 3 – Kliknij Nowy (New), aby utworzyć nową grupę albo wybierz istniejącą grupę z listy, aby ją modyfikować.
- 4 – Z listy zdefiniowanych pięter, zaznacz kolumnę stanu dla pięter, które chcesz włączyć do grupy. Wyłącznie piętra, które mają wybrane pola stanu, będą dostępne, gdy:
 - ma miejsce operacja zdalnego odblokowania, albo
 - „Wejście linii dozorowej” jest zaprogramowane, na przykład, jako „przycisk” do udostępnienia pięter dla gości (Urządzenia > Menu definiowania Linii dozorowej > zakładka Windy) (Devices > Input definition menu > Elevator tab),
 - użytkownik karty użyje kartę na czytniku, aby odblokować wybór pięter (kontroler pracuje w trybie stand-alone (błąd komunikacji). Wyłącznie piętra oznaczone „X” są dostępne do wyboru.
- 5 – Z kolumny **Terminarz (Schedule)**, wybierz terminarz dla każdego piętra w grupie.
 - Kiedy przypisujesz grupę pięter i terminarz odryglowania do drzwi windy (zobacz: Definiowania drzwi windy), system skanuje kolumnę terminarz tej grupy i odpowiednio odblokowuje każde piętro.
 - Terminarz przypisany do grupy piętra będzie wykorzystany do potwierdzenia karty dostępu i jej terminarza odblokowania. W ten sposób piętro zostanie odblokowane tylko wtedy, gdy dwa terminarze (piętra i karty dostępu) będą się zgadzały.

Notatka: Terminarze są aktywne nawet wtedy, kiedy nastąpił błąd komunikacji z kontrolerem.



Grupy przełączników (Trigger Group Creation)

Grupy przełączników są wykorzystywane do konfigurowania elementów przełącznikowych.

1 – W zakładce Grupy (Group), kliknij **Grupa przełączników (Trigger group)**.

2 – Z listy **Grupa przełączników (Trigger group)**, wybierz istniejącą grupę, jeżeli chcesz ją modyfikować; albo kliknij **Nowy (New)**, aby stworzyć nową, a następnie przypisać jej nazwę.

3 – Z listy komponentów, wybierz jeden. Zaznacz pola odpowiadające pod-komponentom, które chcesz przypisać do grupy przełączników.

4 – Kliknij przycisk **Zapisz (Save)**.



Urządzenia

Aplikacja EntraPass

Aplikacja EntraPass (Application Configuration)

Minimalna konfiguracja oprogramowania EntraPass obejmuje serwer, aplikację stacji roboczej oraz aplikację bramki. Aplikacja bramki może zostać zintegrowana ze stacją roboczą EntraPass na tym samym komputerze. Zestaw oprogramowania posiada:

- aplikację stacji roboczej
- aplikację serwera
- aplikację wielo-obiektowej bramki
- oraz aplikacje użytkowe

Notatka: dla pojedynczej bramki limity są następujące: 2048 połączeń, 10000 drzwi, 100000 kart, 100000 Linii dozorowych (input) i wyjść (output).

Dla stabilności systemu rekomenduje się zainstalowanie Serwera EntraPass na przeznaczonym do tego komputerze. Okienko Aplikacja (Application) pozwala użytkownikom na konfigurowania komputerów, na których zainstalowany jest EntraPass. Aby konfigurować, musisz zdefiniować:

- ogólne parametry dla wszystkich komputerów, gdzie zainstalowany jest EntraPass.
- parametry bezpieczeństwa (dla wszystkich aplikacji EntraPass).
- filtry (aby określić, które bramki i aplikacje będą wysyłać wiadomości)
- polecenie zarządzania wiadomościami / alarmami.



Konfigurowanie aplikacji (Configuring an Application)

1 – Z głównego okna EntraPass, wybierz zakładkę **Urządzenia (Devices)**, i kliknij przycisk Aplikacja (Application). Pojawi się główne okno Aplikacji.

Notatka: obiekty wyświetlone w Oknie aplikacji różnią się, zależnie od wybranej aplikacji EntraPass. Na przykład, jeżeli wybrałeś aplikację stacji roboczej, zakładki takie jak: Stacja robocza, Bramka, Obiekt, etc., będą wyświetlone.

2 – Z listy **Aplikacja (Application)**, wybierz aplikację, którą chcesz konfigurować. Lista wyświetla wszystkie aplikacje, które zostały zainstalowane i zarejestrowane. Lista Typ aplikacji (Application type) wyświetla typ wybranej rzeczy. Może to być: stacja robocza, bramka, etc.

3 – Przypisz nazwę do wybranej aplikacji. Możesz ją przypisać w dwóch językach.

4 – Kliknij **Zapisz (Save)**, aby uruchomić nową aplikację.

Określanie ogólnych parametrów (Defining General Parameters)

Zakładka **Ogólne (General)** pozwala określić zachowanie systemu w momencie, kiedy użytkownik jest nieaktywny, czyli z klawiatury nie przychodzą żadne akcje (czas bezczynności).

1 – Wybierz **Wyślij na pasek przy bezczynności (Send to tray on idle)**, jeżeli chcesz, aby aplikacja została zminimalizowana przy bezczynności. W tym celu musisz określić czas bezczynności, po jakim aplikacja zostanie zminimalizowana.

2 – Wybierz **Automatyczny Logout przy bezczynności (Automatic Logout on idle)**, jeżeli chcesz, aby nastąpiło wylogowanie przy bezczynności. W tym celu musisz określić czas bezczynności, po jakim użytkownik zostanie wylogowany.

3 – Jeżeli opcja **Nagranie (Video)** jest dostępna, pojawi się pole **Pogląd nagrania (Video view)**. W tym przypadku wybierz podgląd nagrania, w którym chcesz, aby określony komponent się pojawił. Zobacz: Definiowanie Poglądu Nagrania Video Views Definition).

4 – Z listy **Grafika (Graphic)**, możesz wybrać grafikę do której aplikacja jest przypisana. Zobacz: Definiowanie grafiki (Graphics Definition).



Urządzenia

Konfiguracja aplikacji

5 – Dla aplikacji **Dublowanie bazy danych (Mirror database)**, wybierz **Automatyczna kopia zapasowa (Automatic backup)**, aby kopia zapasowa była tworzona automatycznie. Po kliknięciu przycisku **Konfiguruj automatyczną kopię zapasową (Configure Automatic backup)**, możesz określić właściwości i opcje kopii zapasowej.

Notatka: musisz oddzielnie skonfigurować Terminarz kopii zapasowej dla Dublowania bazy danych (Mirror database) oraz dla Serwera Redundantnego.

a – Możesz również uruchomić tworzenie kopii zapasowej natychmiast z aplikacji **Dublowanie bazy danych (Mirror database)** oraz **Serwer redundantny (Redundant Server)**, klikając **Kopia zapasowa teraz (Backup ALL NOW)**. Wykonana zostanie kopia dla wszystkich czterech baz danych: Danych, Archiwów, Czasu pracy oraz Nagrań. Możliwe jest także natychmiastowe wykonanie kopii zapasowej konkretnej bazy danych z okna Status:

- W oknie Status, wybierz przycisk Aplikacja (Application)
- Z menu, kliknij prawym na Dublowanie bazy danych (Mirror database)
- Kliknij na Kopia zapasowa teraz (backup now), a następnie wybierz typ bazy danych z następnego menu.

Notatka: aby uruchomić automatyczne tworzenie kopii zapasowych, aplikacja Dublowania bazy danych (Mirror database) musi być online oraz w trybie Aktualizacji.



Definiowanie parametrów (Defining Parameters)

Ta część odnosi się do wszystkich aplikacji EntraPass: stacji roboczych, bramek, SmartLink, serwerów redundantnych, etc.

1 – Z okna **Aplikacja (Application)** wybierz stację roboczą i przejdź do zakładki **Parametry (Parameters)**.

2 – Dokonaj wyboru:

- **Wyłącz aplikację (Disable application)**: użytkownik nie będzie w stanie włączyć aplikacji. Przy korzystaniu z tej opcji należy być ostrożnym.
- **Wyłącz autentyfikację dla serwera (Disable authentication to server)**: ta opcja uniemożliwia zarejestrowanie aplikacji dla serwera.
- **Automatyczne wyłączenie autentyfikacji (Auto disable authentication)**: system automatycznie wyłączy autentyfikację, kiedy aplikacja będzie autoryzować się po raz pierwszy.
- **Wyświetl listę logowania (Display Login List)**: ta opcja sprawia, że system zachowuje ostatnich pięć logowań, aby były możliwe do wyboru przy rozpoczęciu następnej sesji. Przyspiesz to rozpoczęcie nowej sesji, ponieważ użytkownik musi tylko wybrać nazwę użytkownika i wprowadzić hasło. Pozostawienie tej opcji wyłączonej zwiększa bezpieczeństwo – trzeba wprowadzić zarówno hasło, jak i prawidłową nazwę użytkownika.
- **Pojedyncze logowanie SSO (Single Sign On (SSO))**:
 - Jeżeli SSO jest włączone, przy następnym uruchomieniu aplikacji nie będzie proszony o wprowadzenie nazwy użytkownika, ani hasła.

Notatka: jeśli się wylogujesz, a aplikacja pozostanie włączona przy następnym logowaniu będziesz musiał wprowadzić swój login oraz hasło.

- Jeżeli SSO jest wyłączone, a użytkownika ma wyłączoną synchronizację, będziesz proszony o wprowadzenie nazwy użytkownika oraz hasła.
- Jeżeli SSO jest wyłączone, a użytkownik Active directory wprowadzi nazwę domeny albo użytkownika jako login, to jego upoważnienia zostaną sprawdzone pod kątem jego profilu.

Notatka: EntraPass obsługuje logowanie między-domenowe (cross-domain), ale najpierw użytkownik musi utworzyć oraz zapisać loginy, hasła oraz domeny w EntraPass (zobacz Tworzenie/Edytowanie użytkownika). Nazwa takich użytkowników jest zapisywana według formatu: domena\nazwa użytkownika. Dzięki temu EntraPass nie musi działać na platformie opartej na środowisku Windows.



Urządzenia

Konfiguracja aplikacji

- **Zaloguj przed wyjściem (Must be login to close application):** użytkownik musi być zalogowany, zanim wyjdzie z programu EntraPass.
- **Wstrzymaj wiadomości (Suspend messages):** wszystkie przychodzące wiadomości zostaną wstrzymane. Zastosuj tę opcję dla stacji roboczych, które są wykorzystywane tylko do konfigurowania komponentów, albo w przypadku, gdy wiadomości nie są wymagane.
- **Operator musi się zalogować, aby przejrzeć wydarzenia (Operator must login to view events):** operator musi się zalogować, zanim wiadomości zdarzeniowe będą mogły być sprawdzone.
- **Wyłącz nagrania (Disable video):** ukrywa opcje poglądu nagrań z konkretnej stacji roboczej EntraPass. Użytkownicy z odpowiednim poziomem dostępu będą mogli konfigurować opcje nagrań, ale nie będą mogli robić podglądu na żywo, ani odtwarzać nagranych fragmentów.
- **Powiadom w przypadku aktualizacji obiektu (Notify when remote sites must be updated):** system wyśle powiadomienie w przypadku potrzeby aktualizacji obiektu. Za każdym razem, gdy zmieniane będą dane związane z obiektem (terminarz, kontroler, etc.) powiadomienie zostanie wysłane. Użytkownik będzie miał wybór, aby przeprowadzić aktualizację, albo nie.



Definiowanie obszaru roboczego (Defining Workspaces)

Notatka: Definiowanie obszaru roboczego jest dostępne tylko przy włączonych Zdarzeniach Zarządzanych przez Operatora

Zakładka Obszar roboczy (Workspace) pozwala wybrać, która konfiguracja obszaru i które parametry zdarzenia będą wprowadzone do konkretnej stacji roboczej. Ta opcja pozwala określić zachowanie stacji roboczej.

- **Wprowadź obszar roboczy oraz parametry zdarzenia dla stacji roboczej (Apply workstation workspace and event parameters):** pozwoli na zdefiniowanie obszaru roboczego stacji dla stacji roboczej pod kątem wiadomości o zdarzeniach.
 - **Podczas wylogowania (When logged out):** określi zasady/zadania, kiedy nikt nie jest zalogowany do stacji roboczej.
 - **Podczas zalogowania (When logged in):** określi zasady/zadania, kiedy użytkownik jest zalogowany do stacji roboczej, nadpisując zdefiniowany obszar roboczy użytkownika.
 - **Podczas wyłączenia (When shutdown):** określi zasady/zadania, kiedy stacja robocza jest wyłączona.
- **Przypisz obszar roboczy operatora do filtrowania wiadomości (Apply operator workspace to filter messages):** po zalogowaniu, stacja robocza wprowadzi zasady obszaru roboczego.
 - Sekcja **Działaj, gdy oba obszary robocze są wybrane (Process when both workspaces are selected)** wyświetla opcje, które są dostępne wyłącznie, gdy **Wprowadź obszar roboczy oraz parametry zdarzenia dla stacji roboczej (Apply workstation workspace and event parameters)** oraz **Przypisz obszar roboczy operatora do filtrowania wiadomości (Apply operator workspace to filter messages)** są aktywne.
 - **Obszar roboczy stacji roboczej ORAZ obszar roboczy operatora (Workstation workspace AND Operator workspace):** zdarzenia będą filtrowane zgodnie z konfiguracją obszaru roboczego stacji roboczej, a następnie filtrowane ponownie zgodnie z konfiguracją obszaru roboczego operatora, który jest obecnie zalogowany na stacji roboczej.
 - **Obszar roboczy stacji roboczej ALBO obszar roboczy operatora (Workstation workspace OR Operator workspace):** wybierze obszar roboczy o wyższym poziomie w hierarchii.
 - **Wyłącznie obszar roboczy operatora (Operator workspace ONLY):** obszar roboczy operatora będzie miał pierwszeństwo nad obszarem roboczym stacji roboczej.



Definiowanie kontroli wiadomości (Defining Message Controls)

1 – Kliknij zakładkę **Wiadomości (Messages)**, aby określić, jak wiadomości powinny być procesowane, w momencie, gdy stacja robocza EntraPass jest podłączona (albo nie) do serwera.

Notatka: Pulpity wiadomości są konfigurowane w menu Definiowanie Pulpitów.

2 – W sekcji **Kontrola wiadomości (Message control)**:

- określ liczbę wiadomości, które będą zachowywane na serwerze, kiedy stacja robocza będzie offline (max. 10,000 wiadomości na stację roboczą; domyślnie: 500).
- określ liczbę wiadomości, które będą zachowywane na stacji roboczej (max. 100,000 wiadomości na stację roboczą; domyślnie: 5,000).

Notatka: Stacja robocza EntraPass zawsze zachowa najnowsze zdarzenia. Aby sprawdzić starsze zdarzenia, musisz sprawdzić raporty historyczne. Zobacz Żądanie raportów (Requesting reports).

3 – Określ, czy serwer ma zatrzymywać najnowsze, czy najstarsze wiadomości w momencie osiągnięcia maksymalnej liczby zapisanych wiadomości (pozostałe zostaną zarchiwizowane):

- **Zatrzymaj najstarsze (Keep older messages)**
- **Zatrzymaj najnowsze (Keep newer messages)**

4 – W sekcji **Wyczyść pulpit wiadomości (Clear Message Desktops)** określ, kiedy wiadomości mają być usunięte z pulpitu:

- **Przy wylogowaniu (On logout).**
- **Przy wyłączeniu stacji roboczej (On workstation shutdown).**

5 – W sekcji **Informacje o obrazie (Picture information)** wybierz zawartość pola, która będzie wyświetlana pod obrazem.

Notatka: domyślnie pola wyświetlają od Informacja #1 do Informacja #10. Tytuły mogą być edytowane. Aby dowiedzieć się więcej o zmianie tytułów oznaczeń informacji zobacz Dostosowywanie pól z informacjami o karcie (Customizing Card Information Fields).



Urządzenia

Konfiguracja aplikacji

6 – W sekcji **Opóźnienie odświeżania przycisku Status (Status button refresh delay)** określ przedział czasu, w jakim aplikacja odświeża status zgłoszony przez przycisk Status. Przedział czasu: od 0.01 do 5.00 min. (krok 0.01 sek.).

7 – Możesz określić **Maksymalną liczbę rekordów (Maximum number of records)**, które mogą być pobrane ze zarchiwizowanych plików. Maksimum: 200,000.



Definiowanie kontroli alarmów (Defining Alarm Controls)

1 – Kliknij zakładkę **Alarmy (Alarms)**, aby określić, jak alarmy powinny być procesowane, w momencie, gdy stacja robocza EntraPass jest podłączona (albo nie) do serwera.

Notatka: Pulpity alarmów są konfigurowane w menu Definiowanie pulpitu (Desktop definition). Zobacz Pulpity alarmów.

2 – W sekcji **Kontrola alarmów (Alarm control)**:

- określ liczbę alarmów, które będą zachowywane na serwerze, kiedy stacja robocza będzie offline (max. 100,000 wiadomości na stację roboczą; domyślnie: 500).
- określ liczbę alarmów, które będą zachowywane na stacji roboczej (max. 100,000 wiadomości na stację roboczą; domyślnie: 5,000).

Notatka: Stacja robocza EntraPass zawsze zachowa najnowsze zdarzenia. Aby sprawdzić starsze zdarzenia, musisz sprawdzić raporty historyczne. Zobacz Żądanie raportów (Requesting reports).

3 – Określ, czy serwer ma zatrzymywać najnowsze, czy najstarsze alarmy w momencie osiągnięcia maksymalnej liczby zapisanych alarmów (pozostałe zostaną zarchiwizowane):

- **Zatrzymaj najstarsze (Keep older messages)**
- **Zatrzymaj najnowsze (Keep newer messages)**

4 – W sekcji **Wyczyść pulpit alarmów (Clear Alarm Desktops)** określ, kiedy alarmy mają być usunięte z pulpitu:

- **Przy wylogowaniu (On logout).**
- **Przy wyłączeniu stacji roboczej (On workstation shutdown).**

5 – Możesz określić parametry potwierdzenia. Zaznaczenie **Wyświetl wiadomość alarmową (Display alarm message)** wyśle prośbę o potwierdzenie, nawet, jeśli operator pracuje w innej aplikacji. Musisz określić przedział czasu wyświetlania wiadomości.

6 – Możesz zaznaczyć **Wyłącz automatyczne wyświetlanie nagrań (Disable auto display of video views)**, aby nagrania nie były automatycznie wyświetlane przez stację roboczą.

7 – Możesz włączyć opcję Wyślij po potwierdzeniu time-out, aby wygenerować zdarzenie „potwierdź time-out” w momencie, kiedy operator nie potwierdzi zdarzenia podczas opóźnienia time-out, określonego w polu Opóźnienie potwierdzenia time-out. Wiadomość zostanie wysłana na Pulpit wiadomości oraz na Pulpit alarmów. Zobacz Pulpit alarmów, aby dowiedzieć się więcej.

Definiowanie opcji raportów email (Defining Email Report Options)

EntraPass oraz EntraPass Web umożliwiają wysyłanie raportów przy pomocy wiadomości email.

Notatka: połączenia z certyfikatem SSL nie są wspierane.



Urządzenia

Konfiguracja aplikacji

1 – Z okna **Aplikacja (Application)**, wybierz zakładkę **Raporty Email (Email reports)**.

2 – W polu **Serwer Email (Email Server)**: SMTP albo Serwer Zamienny; wprowadź adres IP serwera, który będzie wykorzystywany do wysyłania wiadomości email.

3 – W polu **Port Email (Email Port)**, wprowadź numer portu, który będzie wykorzystywany do wysyłania wiadomości email (zazwyczaj: 25).

4 – Wprowadź adres email w pole **Nadawca (Email sender)**. Ten adres będzie wykorzystywany do autentyfikacji serwera email.

5 – **Autentyfikacja (Authentication)**: te opcje mogą być wykorzystane do konfigurowania metody autentyfikacji.

- **Brak autentyfikacji (No authentication)**

- **Autentyfikacja SMTP (SMTP authentication)**: autentyfikacja, wysłana na port SMTP, musi zostać potwierdzona zanim wiadomość zostanie wysłana.

- **Autentyfikacja POP3 (POP3 authentication)**: autentyfikacja, wysłana na port POP3, musi zostać potwierdzona zanim wiadomość zostanie wysłana.

6 – **Nazwa użytkownika (User name)** : wprowadź nazwę użytkownika dla procesu autentyfikacji.

7 – **Hasło (Password)**: wprowadź hasło dla użytkownika.

8 – **Serwer POP3 (E-mail server (POP3))**: wprowadź adres serwera POP3 dla autentyfikacji POP3.

9 – **Port POP3 (E-mail port (POP3))**: wprowadź numer portu POP3 dla autentyfikacji POP3.

10 – **Wyślij do (Send to)**: adres odbiorcy.

11 – **Test (Test button)**: wysyła wiadomość testową z wybranymi parametrami.

Komentarz (Comment)

Sprawdź: Pole komentarza.

Konfigurowanie aplikacji bramki (Configuring a Gateway Application)

EntraPass Gateway konwertuje informacje otrzymane z kontrolera albo obiektu i przesyła przekonwertowane dane do serwera, który następnie przesyła je do odpowiedniej aplikacji. Konwertuje również informacje otrzymane ze stacji roboczej EntraPass i przesyła je do kontrolerów. Aplikacja bramki pozwala monitorować obiekty kontrolerów przyłączonych do bramki. Możesz dodać do 40 wiele obiektowych bramek.

Konfigurowanie ogólnych parametrów dla bramki (Configuring General Parameters for a Gateway)

Z listu Aplikacja wybierz aplikację bramki, którą chcesz konfigurować.



Konfigurowanie Oracle/MS-SQL (Configuring an Oracle/MS-SQL Interface (CardGateway))

Interface Oracle/MS-SQL tworzy kopię bazy danych kart EntraPass w bazie danych MS-SQL albo Oracle. Dodatkowo pozwala użytkownikowi działać na bazie danych kart systemu z programów MS-SQL albo Oracle. Użytkownik może dodać, modyfikować albo usuwać karty. Może również otrzymywać informacje na temat kart z bazy danych kart EntraPass. Informacje o karcie są aktualizowane w każdej bazie danych za każdym razem, gdy program modyfikuje albo aktualizuje bazę danych. Interface MS-SQL zapewnia, że modyfikacje są przeniesione na serwer, a następnie na stacje robocze.

Notatka: interface Oracle/MS-SQL wymaga dodatkowej licencji.

Upewnij się, że oprogramowanie klienckie MS-SQL oraz Oracle jest zainstalowane na tym samym komputerze, co Oracle/MS-SQL Interface. Instalowanie Oracle/MS-SQL Interface na tym samym komputerze, co EntraPass, nie jest rekomendowane. Instalowanie na tym samym komputerze dwóch aplikacji może powodować problemy podczas wymiany danych pomiędzy EntraPass, a serwerem Oracle oraz MS-SQL. Aby skonfigurować bazę danych Oracle/MS-SQL Interface musisz określić:

- ogólne parametry, w tym parametry bezpieczeństwa aplikacji,
- parametry bazy danych, w tym prawa dostępu bazy danych.

1 – Z listy Aplikacja wybierz **Oracle/MS-SQL Interface**.

2 – Określ, na której aplikacji zainstalowałeś Oracle/MS-SQL Interface.

3 – Wybierz zakładkę Parametry (Parameters), aby określić parametry bezpieczeństwa dla Oracle/MS-SQL Interface. Zobacz: Definiowanie parametrów bezpieczeństwa ([Defining Security Parameters](#))

4 – Wybierz zakładkę ORACLE/MS-SQL Interface, aby określić, jak EntraPass będzie się komunikować z bazą danych klienta oraz, aby określić prawa dostępu do bazy danych.

5 – Z listy Typ bazy danych (Database type), wybierz serwer bazy danych: Oracle 8.0, Oracle 7.3 albo SQL. Upewnij się, że wybrałeś prawidłową wersję serwera ponieważ konfiguracja bazy danych jest inna dla każdej.

Notatka: jeśli zostanie wybrana zła wersja, interface Oracle/MS-SQL nie będzie się komunikował i nie będzie w stanie nawiązać połączenia z serwerem.

6 – Wprowadź nazwę serwera bazy danych.

7 – Wprowadź nazwę wybranej bazy danych Oracle albo SQL.

8 – Jeżeli korzystasz z serwera Oracle, wprowadź nazwę pliku z danymi Oracle, która określi dane, do których uzyskać dostęp.



Urządzenia

Konfiguracja aplikacji

Notatka: serwery Oracle oraz SQL mogą zostać tak skonfigurowane, że będą zawierać więcej niż jedną bazę danych. Dostęp do bazy danych SQL wymaga wskazania jej nazwy, podczas gdy dostęp do bazy danych Oracle wymaga podania jej nazwy oraz konkretnego pliku. W celu uzyskania informacji na temat parametrów dostępu do bazy danych skontaktuj się z administratorem sieciowym.

9 – Zaznacz *Użyj dostępu administratora do rozpoczęcia (Use administrator Access for Initialization)*, co umożliwi wprowadzenie nazwy administratora oraz hasła.

Notatka: zaznaczenie tego pola jest bardzo istotne. Jeśli tego nie zrobisz będziesz musiał zdalnie stworzyć bazę danych, nazwę użytkownika oraz hasło w serwerze.

10 – Wprowadź nazwę administratora oraz jego hasło. Program automatycznie stworzy bazę danych, nazwę użytkownika oraz hasło w bazie danych serwera.

11 – W obszarze *Dostęp do bazy danych (Database access)*, wprowadź nazwę użytkownika oraz hasło, które będą wykorzystane przez Kartę/Bramkę do połączenia się bazą danych Oracle/SQL.

Notatka: procedura dostępu do bazy danych nie pozwala CardGateway na tworzenie ani modyfikowanie istniejących profili użytkowników na serwerze Oracle/SQL.

12 – Zaznacz *Zachowaj usunięte rekordy (Keep deleted records)*, jeżeli chcesz zachować zapis karty, nawet jeżeli karta została usunięta z bazy danych EntraPass. Zapis będzie zachowany w bazie danych Oracle/MS-SQL Interface.



Notatka: jeśli nie wybierzesz tej opcji usunięte zapisy zostaną fizycznie oraz permanentnie usunięte z bazy danych Oracle/MS-SQL. Kiedy EntraPass tworzy automatycznie bazę danych na serwerze SQL albo Oracle udostępnia 50MB na bazę danych kart. Jeśli chcesz zwiększyć ilość udostępnionego miejsca, musisz stworzyć bazę danych zdalnie. Zobacz Zdalne tworzenie bazy danych serwera (Creating Server Databases Manually).

13 – Kliknij zakładkę Serwis (Service), aby określić informacje, kiedy Oracle/MS/SQL działa, jako usługa i trzeba wydrukować raport.

- Musi być zaznaczone pole Zaloguj do aplikacji serwisowej EntraPass, aby włączyć tę opcję.
- Wprowadź nazwę domeny oraz login dla Oracle/MS-SQL Interface.
- Wprowadź hasło i potwierdzenie hasła.

Zdalne tworzenie bazy danych serwera (Creating Server Databases Manually)

Aby zintegrować bazę danych z EntraPass, najpierw trzeba stworzyć bazę danych, która będzie wykorzystana, a następnie utworzyć użytkownika Kantech'a w bazie danych. Jeżeli twój system korzysta z serwera MS-SQL, postępuj następująco.

Zdalne tworzenie Operatora dla serwera ORACLE/MS-SQL (Creating an Operator Manually in the ORACLE/MS-SQL Server)

Pierwszym krokiem w integracji ORACLE/MS-SQL z EntraPass jest stworzenie bazy danych, która będzie wykorzystana.

- 1** – Kliknij prawym folder Baza danych (Database) i wybierz **Nowa baza danych (New Database)**.
- 2** – Wprowadź nazwę bazy danych w polu **Nazwa bazy danych (Database name)**.
- 3** – Kliknij OK po wprowadzenia nazwy bazy danych.



Tworzenie Operatora Kantech dla serwera MS-SQL (Creating a Kantech Operator for an MS-SQL Server)

Musisz stworzyć operatora, z którego Oracle/MS-SQL Interface będzie logować się do serwera MS-SQL.

- 1** – Kliknij prawym na Login i wybierz **Nowy Login (New Login)**.
- 2** – Wprowadź w pole **Nazwa (Name)**: kantech.
- 3** – Upewnij się, że opcja **Autentyfikacji Serwera SQL (SQL Server Authentication)** jest włączona.
- 4** – Wprowadź w pole **Hasło (Password)**: kantech.
- 5** – Wybierz zakładkę **Dostęp do bazy danych (Database Access)**
- 6** – Zaznacz nazwę bazy danych utworzonej w punkcie 2.
- 7** – W celu modyfikowania bazy danych, zaznacz opcję **Public and db_owner**, a następnie kliknij OK, aby zapisać i wyjść. Zostaniesz poproszony o potwierdzenie hasłem.
- 8** – Wprowadź kantech i kliknij **OK**, żeby wyjść.



Tworzenie operatora Kantech dla serwera Oracle (Creating a KANTECH Operator for an Oracle Server)

- 1** – Zaloguj się do serwera Oracle, jako administrator. Domyślna nazwa operatora: kantech; może zostać użyta.
- 2** – Stwórz bazę danych. Domyślna nazwa bazy danych: kantech; może zostać użyta.
- 3** – Utwórz profil do logowania. Domyślna nazwa operatora i hasło: kantech; może zostać użyta.
- 4** – Przypisz do operatora kantech pozwolenie „Właściciel”.

Notatka: jeśli zmienione zostały jakieś ustawienia domyślne zgadzać się musi Nazwa bazy danych, Nazwa użytkownika oraz Hasło pomiędzy bazą danych oraz oprogramowaniem EntraPass.

Komentarz (Comment)

Sprawdź: Pole komentarza.



Konfigurowanie duplikatu bazy danych oraz serwera redundantnego (Configuring the Mirror Database and Redundant Server)

Monitory dublowania bazy danych mogą komunikować się pomiędzy sobą oraz głównym serwerem. Duplikat bazy danych jest kopia systemowej bazy danych oraz wpisów rejestrowych systemu Windows, za wyjątkiem bazy danych kart Oracle/MS-SQL.

Synchronizacja pomiędzy systemową bazą danych, a duplikatem, może być synchroniczna albo asynchroniczna. Synchroniczna oznacza, że synchronizowania odbywa się w czasie rzeczywistym. Asynchroniczna oznacza, że synchronizacja odbywa się przedziałach określonych przez użytkownika (5 minut, 15 minut, 30 minut, 60 minut, 2 godziny oraz 4 godziny). Dublowania asynchroniczne może poprawić wydajność systemu poprzez zredukowanie liczby transakcji serwera.

Notatka: asynchroniczne dublowanie jest dostępne wyłącznie dla Archiwum, Wej./Wyj. oraz Zdarzeń wideo. Synchroniczne jest wykorzystywane przy pozostałych rodzajach danych.

Gdy komunikacja pomiędzy duplikatem bazy danych, a głównym serwerem, zawiedzie, duplikat automatycznie uruchamia opóźnienie, po którym serwer redundantny jest automatycznie włączony i zastępuje serwer główny. Duplikat bazy danych oraz serwer redundantny nie mogą działać na tym samym komputerze, co serwer EntraPass. Powinny być zainstalowane na dedykowanym dla nich komputerze.

Notatka: możesz działać na systemie posiadającym więcej niż jedną zdublowaną bazę danych (mirror database) oraz serwer redundantny. Obie opcje wymagają dodatkowej licencji.

Aby skonfigurować stację roboczą **duplikatu bazy danych oraz serwera redundantnego**, musisz określić:

- Ogólne parametry dla duplikatu bazy danych oraz serwera redundantnego oraz parametry zabezpieczeń.
- Parametry serwera redundantnego.
- Parametry zabezpieczeń.

1 – Z listy Aplikacja, wybierz **Duplikat bazy danych oraz Serwera Redundantnego (Mirror Database and Redundant Server)**

2 – Aby określić parametry z zakładki Ogólne (General), zobacz: Definiowanie Ogólnych Parametrów ([Defining General Parameters](#)).

3 – Wybierz zakładkę Parametry (Parameters), aby określić parametry zabezpieczeń; zobacz: Definiowanie Parametrów Zabezpieczeń ([Defining Security Parameters](#)).

4 – Przejdź do zakładki Serwer Redundantny (Redundant Server), aby określić parametry komunikacji dla Duplikatu bazy danych oraz Serwera Redundantnego.

5 – Wybierz protokół, który będzie wykorzystywany do komunikacji z komputerem, gdzie zainstalowany jest duplikat bazy danych: **Brak**, **TCP/IP** albo **Automatyczny**.



Urządzenia

Konfiguracja aplikacji

Notatka: kiedy wybierzesz pole Adres serwera możliwe jest wprowadzenie adresu TCP/IP komputera hostującego zdublowaną bazę danych oraz serwer redundantny. Jeśli zaznaczone jest pole Automatycznie, adres IP komputera zostanie wysłany do serwera w celu rozesłania go do wszystkich stacji roboczych w sieci. Ta opcja jest przydatna wtedy, kiedy nie znasz adresu IP lub kiedy komputer posiada zmienne IP lub jest podłączony do serwera DHCP.

6 – Wprowadź adres IP serwera redundantnego.

7 – Określ działania, które serwer redundantny poweźmie, w przypadku uruchomienia bez komunikacji z serwerem.

8 – Określ opcje dla uruchamiania serwera redundantnego w momencie, gdy główny serwer się wyłącza: automatyczna, przy normalnym wyłączeniu (kiedy użytkownik wyłącza serwer EntraPass), albo przy wyłączeniu „wymuszonym”. Duplikat bazy danych uruchomi serwer redundantny, kiedy opóźnienie określone w polu **Czekaj, przed rozpoczęciem (Wait before start)** upłynie.

Notatka: jeśli nie zaznaczysz opcji Uruchom serwer automatycznie, serwer redundantny nie uruchomi się w momencie, kiedy główny serwer zostanie wyłączony (w warunkach normalnych). Oznacza to, że trzeba go będzie uruchomić zdalnie.

9 – Określ działania systemu w momencie, kiedy serwer powróci do działania: określ opóźnienie, po jakim serwer redundantny przestanie pracować po powrocie serwera głównego do prawidłowego działania.

10 – Przejdź do zakładki Przywróć parametry (Restore Parameters), aby określić działania serwera redundantnego w momencie, kiedy główny serwer zostanie włączony:

- Aby zautomatyzować proces przywracania zaznacz **Proces automatyczny przy przywracaniu (Automatic process on restore)**. Pozostałe opcje stają się dostępne.
- Zaznacz odpowiednie pola, zależnie od zainstalowanych opcji oraz procesu przywracania, który chcesz uruchomić:



Urządzenia

Konfiguracja aplikacji

o **Przywróć (Restore)**: przeniesie całą bazę danych zawierającą wszystkie transakcje z serwera redundantnego to głównego, nadpisując dane na serwerze głównym.

o **Połącz (Merge)**: przeniesie tylko te dane, których nie można znaleźć na serwerze głównym.

Notatka: w przypadku korzystania z funkcji Połącz, dane nie zostaną przeniesione, jeśli karta została zmodyfikowana jednocześnie na serwerze redundantnym oraz serwerze głównym, a serwer główny nie był online.

11 – Kliknij zakładkę **Asynchroniczne aktualizowanie (Async updates)**, aby określić właściwości synchronizacji duplikatu bazy danych. Może być synchroniczna (na żywo) albo asynchroniczna (co: 5 minut, 15 minut, 30 minut, 60 minut, 2 godziny oraz 4 godziny)

Notatka: aby sprawdzić status asynchronicznego transferu możesz sprawdzić połączenie w Zakładce Status (Aplikacja).

12 – Kliknij zakładkę **Serwis (Service)**, aby określić informacje do logowania, kiedy **Duplikat bazy danych oraz Serwer Redundantny** działają, jako usługa i trzeba wydrukować raport.

- Musi być zaznaczone pole **Zaloguj do aplikacji serwisowej EntraPass (Login to EntraPass service application)**, aby włączyć tą opcję.
- Wprowadź nazwę domeny oraz login Duplikatu bazy danych oraz Serwera Redundantnego.
- Wprowadź hasło i potwierdzenie hasła.

Komentarz (Comment)

Sprawdź: Pole komentarza



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia



Konfigurowanie aplikacji SmartLink (Configuring the SmartLink Application)

Aplikacja SmartLink umożliwia użytkownikowi zaprogramowanie oprogramowania kontroli dostępu EntraPass z dowolnym „inteligentnym” urządzeniem, jak np. krosownice wideo, systemy powiadomień, aplikacje email, etc.; przy wykorzystaniu połączenia RS-232 pomiędzy jedną ze stacji roboczych EntraPass, a urządzeniem zewnętrznym. Integracja z innymi systemami może również zostać osiągnięta poprzez oprogramowanie DLL. SmartLink może zostać wykorzystany do podłączenia się do innego komputera i do przeprowadzenia wymiany informacji oraz aktualizacji w czasie rzeczywistym. Umożliwia również EntraPass otrzymywanie i wysyłanie wiadomości, raportów oraz poleceń, jak również komunikowanie się z aplikacjami klienckimi.

Notatka: opcja SmartLink nie wymaga dodatkowej licencji.

1 – Z listy Aplikacja wybierz **SmartLink**.

2 – Określ stację roboczą, na której zainstalowałeś **SmartLink**. Zobacz: **Definiowanie Ogólnych Parametrów** ([Defining General Parameters](#)).

3 – Skonfiguruj parametry zabezpieczeń stacji roboczej SmartLink. Zobacz: **Definiowanie Parametrów Zabezpieczeń** ([Defining Security Parameters](#)).

4 – Skonfiguruj wiadomości stacji roboczej SmartLink. Zobacz: **Definiowanie Wiadomości** ([Defining Message Controls](#)).

5 – Skonfiguruj raporty email stacji roboczej SmartLink. Zobacz: **Definiowanie Opcji Raportów Email** ([Defining Email Report Options](#)).

6 – Kliknij zakładkę SmartLink, aby wyświetlić i ustawić parametry połączenia SmartLink.



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia

7 – Z listy Dostępny tryb (Mode enabled) (z sekcji Seryjne połączenia SmartLink oraz z sekcji Sieciowe połączenie SmartLink), wybierz tryb transmisji:

- **Tylko wiadomości (Messages only):** SmartLink będzie tylko odbierać wiadomości.
- **Tylko polecenia (Commands only):** SmartLink będzie tylko uruchamiać polecenia (zadania)
- **Wiadomości i polecenia (Messages and commands):** SmartLink będzie otrzymywać wiadomości i uruchamiać polecenia.

Notatka: kiedy uruchamiasz aplikację SmartLink opcje połączenia dla portu oraz trybów sieciowych są pobierane z Serwera EntraPass. Jeśli tryb połączenia sieciowego jest inny niż „brak”, aplikacja SmartLink zostanie uruchomiona, aby umożliwić aplikacji klienckiej połączenie z aplikacją SmartLink.

8 – Zaznacz opcję **Pomiń ustawienia parametrów zdarzenia (Bypass event parameter preset)**, jeżeli chcesz zignorować wszystkie domyślne ustawienia menu Definiowania Parametrów Zdarzeń (Event Parameter definition). Domyślnie, wszystkie zdarzenia mają być wysyłane do wszystkich stacji roboczych (wliczając stacje robocze SmartLink). Zaznacz tę opcję, aby uniknąć otrzymywania niepotrzebnych wiadomości.

Notatka: będziesz musiał zdalnie stworzyć połączenia zdarzeń oraz zadań w menu Definiowanie parametrów zdarzeń. Na przykład, możesz powiązać zdarzenie Wymuszone otwarcie drzwi i wybrać tylko specyficzne zadanie, który wyśle emaile z informacją.

9 – W sekcji Zadania SmartLink (SmartLink tasks), możesz określić zadania startowe albo domyślne. Przypisane zadania zostaną przeprowadzone automatycznie po uruchomieniu aplikacji SmartLink. Zobacz: **Definiowanie Konfiguratora Zadań (Task Builder Definition)**.

10 – Kliknij zakładkę **Wiadomości Email SmartLink (SmartLink email)**, aby wyświetlić i ustawić parametry połączenia SmartLink.

11 – W polu Serwer wiadomości Email (Email server) wprowadź adres IP serwera, który będzie wykorzystywany do wysyłania wiadomości email.



Urządzenia

Konfiguracja aplikacji

12 - W polu **Port Email (Email Port)**, wprowadź numer portu, który będzie wykorzystywany do wysyłania wiadomości email (zazwyczaj: 25).

Select the encryption method.

- Unsecured (No SSL/TLS)
- Gmail(SSL/TLS)
- Secured (SSL/TLS)
- Office 365 (STARTTLS)

13 - Wprowadź adres email w pole **Nadawca (Email sender)**. Ten adres będzie wykorzystywany do autentyfikacji serwera email.

14 - **Autentyfikacja (Authentication)**: te opcje mogą być wykorzystane do konfigurowania metody autentyfikacji.

• **Brak autentyfikacji (No authentication)**

• **Autentyfikacja SMTP (SMTP authentication)**: autentyfikacja, wysłana na port SMTP, musi zostać potwierdzona zanim wiadomość zostanie wysłana.

• **Autentyfikacja POP3 (POP3 authentication)**: autentyfikacja, wysłana na port POP3, musi zostać potwierdzona zanim wiadomość zostanie wysłana.

15 - **Nazwa użytkownika (User name)** : wprowadź nazwę użytkownika dla procesu autentyfikacji.

16 - **Hasło (Password)**: wprowadź hasło dla użytkownika.

17 - **Serwer POP3 (E-mail server (POP3))**: wprowadź adres serwera POP3 dla autentyfikacji POP3.

18 - **Port POP3 (E-mail port (POP3))**: wprowadź numer portu POP3 dla autentyfikacji POP3.

19 – **Usuń wiadomości email, kiedy skrzynka się zapełni (Delete e-mail(s) when maximum reached)**: przy włączonej funkcji, maksymalna liczba wiadomości email, które będą zachowane wynosi 9999. Minimum (oraz wartość domyślna): 1000.

20 – **Usuń wiadomości email starsze niż (hh:mm) (Delete e-mail(s) when older than (hh:mm))**: przy włączonej funkcji, maksymalny przedział czasu, przez jaki wiadomości email będą przechowywane to 24:00. Minimum: 02:00; domyślna: 05:00.

21 - **Wyślij do (Send to)**: adres odbiorcy.

22 - **Test (Test button)**: wysyła wiadomość testową z wybranymi parametrami.

Notatka: domyślna wartość portu email jest ustawiona na 25. Możesz zmienić tą wartość (dostępne wartości: 0-65.535). Aby uzyskać więcej informacji skontaktuj się z administratorem sieci.



Urządzenia

Konfiguracja aplikacji

23 – Aby określić parametry EntraPass Web wybierz zakładkę **SmartLink Web i API (SmartLink Web and API)**

24 – Określ czas dla **Przerwij połączenia przy bezczynności (mm:ss) (Connection timeout on idle (mm:ss))**: kiedy czas bezczynności połączenia zostanie osiągnięty, użytkownik będzie musiał się ponownie zalogować. Wszystkie zmiany po ostatnim zapisaniu zostaną utracone. Domyślna wartość okresu bezczynności: 05:00. Zakres czasu: 00:30 do 20:00.

Notatka: jeśli zaktualizowałeś system EntraPass, wartość przerwania połączenia nie została zmodyfikowana automatycznie – pozostanie bez zmian. Sprawdź jej wartość.

25 - Kliknij zakładkę **Serwis (Service)**, aby określić informacje do logowania, kiedy serwer **SmartLink** działa, jako usługa i trzeba wydrukować raport.

26 – Kliknij zakładkę **Serwis (Service)**, aby określić informacje do logowania, kiedy serwer **SmartLink** działa, jako usługa i trzeba wydrukować raport zbiorczy.

- Musi być zaznaczone pole **Zaloguj do aplikacji serwisowej EntraPass (Login to EntraPass service application)**, aby włączyć tę opcję.
- Wprowadź nazwę domeny oraz login SmartLink.
- Wprowadź hasło i potwierdzenie hasła.

Komentarz (Comment)

Sprawdź: Pole komentarza



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia



Konfigurowanie aplikacji EntraPass Video Vault (Configuring the EntraPass Video Vault Application)

Aplikacja EntraPass Video Vault jest odpowiedzią na zapotrzebowania na lepsze archiwizowanie danych wideo. Aplikacja pobiera fragmenty nagrań z serwerów wideo podłączonych do EntraPass i zachowuje je do przyszłego użycia. W rzeczywistości, segmenty nagrań mogą być przechowywane na serwerze przez ograniczony przedział czasu. Zależy on od pojemności dysku i ustawień. Aby w pełni wykorzystać możliwości integracji, użytkownicy EntraPass, którzy operują monitoringiem muszą umożliwić EntraPass Video Vault zarządzanie bazą danych archiwalnych nagrań.

Po zainstalowaniu i rejestracji aplikacji EntraPass Video Vault musisz określić jej środowisko. Zobacz: **Dodawanie komponentów systemu (Adding System Components)**. Po szczegóły odnośnie użytkowania EntraPass Video Vault, zobacz: **EntraPass Video Vault**.

1 – Z listy Aplikacja wybierz EntraPass Video Vault.

2 – Aby określić Ogólne parametry dla aplikacji EntraPass Video Vault, zobacz: **Definiowanie Ogólnych Parametrów (Defining General Parameters)**.

3 – Aby określić parametry zabezpieczeń dla aplikacji EntraPass Video Vault, zobacz: **Definiowanie parametrów zabezpieczeń (Defining Security Parameters)**.

4 – Wybierz zakładkę Folder, aby określić lokalizację pliku i strukturę nazewnictwa. Ustawienia określone w tym oknie będą miały wpływ na to, jak pliki wideo będą wyświetlane w oknie Przeglądaj Video Vault (Browse Video Vault).

- **Dysk(i) do zapisu (Destination drive(s))**: określ listę dysków, na których segmenty będą archiwizowane. Segmenty będą zachowywane według dostępności miejsca w kolejności określonej podczas wybierania dysków.

Notatka: dyski, które są dostępne do wyboru odpowiadają sieci dysków w twoim komputerze. Różni się ona zależnie od komputera. Domyślnie dyski są wylistowane alfabetycznie. Możesz zmienić kolejność, ustawiając je według dostępnego wolnego miejsca. Możesz zmieniać ich kolejność (górze/dół) również dzięki zielonym strzałkom.

- **Minimalna wolna przestrzeń dyskowa (Minimum free disk space (MB))**: określ minimalną wolną przestrzeń dyskową, zanim system wyśle wiadomość, że kończy się miejsce w EntraPass Video Vault i archiwizowanie zostanie przerwane. Maksymalna wartość: 99,999 MB.



Urządzenia

Konfiguracja aplikacji

- **Próg wolnej przestrzeni dyskowej (MB) (Disk free space threshold (MB)):** określ maksymalny próg pojemności, zanim system wyśle wiadomość, że EntraPass Video Vault osiągnął próg swojej pojemności, ale będzie nadal archiwizował, aż osiągnie **Minimalną wolną przestrzeń dyskową (Minimum free disk space)**. Maksymalna wartość: 99,999 MB.

- **Separator pól dat (Date field separator):** określa separator pól dat.

- **Folder do zapisu (Destination folder):** wybierz folder, który będzie służył do archiwizowania danych wideo. Jeżeli nie wybierzesz folderu do zapisu, żaden fragment wideo nie zostanie zarchiwizowany. Domyślnie, segmenty będą archiwizowane w folderze: C:\KantechVideoArchive

- **Struktura pod-folderów (Sub-folder structure):** istnieją kryteria wykorzystywane do tworzenia pod-folderów w miejscu archiwizowania danych. Na przykład, wybranie **Nazwa serwera wideo (Video Server Name)** stworzy pod-folder dla każdego serwera wideo, na którym zachowywane są fragmenty nagrań. Można stworzyć 5 poziomów pod folderów.

5 – Wybierz zakładkę Plik (File), aby określić zasadę nazewnictwa plików.

- **Struktura nazewnictwa plików (File name structure):** zaznacz pola, które odpowiadają informacjom, które chcesz uwzględnić w nazwie pliku.

- **Separatory (Separators):** możesz określić separatory pola dla nazwy pliku, jak również i daty i czasu.

6 – Wybierz zakładkę Procesowanie (Process), aby poinstruować system, jak zarchiwizowane segmenty będą procesowane.

- **Domyślny format pliku dla archiwum (Default Video file format for your video archives):** możesz archiwizować segmenty korzystając z formatów: KVI, KVA, AVI, IMG oraz PS.

- **KVI (Kantech Video Intellex).** KVI zawiera miniaturę, kontekstową informację wideo oraz umieszcza cyfrowy znak wodny na obrazie. Musi być odtwarzany przy pomocy Intellex Video Player, który korzysta z American Dynamics API. Musisz być pewny, że API zostało zainstalowane na klienckim komputerze.

- **KVA (Kantech Video AVI).** KVA zawiera miniaturę, kontekstową informację wideo oraz nie umieszcza cyfrowego znaku wodnego na obrazie. Pliki wideo mogą być odtworzone przy pomocy Windows Media Player albo innego odtwarzacza plików AVI.

- **AVI (Audio Video Interlaced).** Pliki AVI mogą być odtworzone przy pomocy Windows Media Player.

- **IMG,** format Intellex. Pliki są przechowywane w formacie .img i mogą być odtworzone przy pomocy Intellex Video Player.

- **PS:** skompresowany format wideo HDVR.



Urządzenia

Konfiguracja aplikacji

Notatka: formaty KVI oraz KVA pozwalają chronić pliki wideo hasłem oraz pozwalają wybrać kluczowe fragmenty dla wybranego zdarzenia wideo. Kluczowe fragmenty umożliwiają szybki sposób odnajdywania segmentów wideo w oparciu o obraz (bmp) reprezentujący całą sekwencję wideo.

- **Symultaniczny transfer segmentów wideo (Simultaneous video segment transfers):** określ liczbę symultanicznych pobrań. Nie można pobierać więcej niż jednego segmentu z jednego serwera na raz. Ale można pobierać segmenty z kilku serwerów jednocześnie. Minimalna wartość: 1; maksymalna: 8.

Notatka: duża liczba pobrań wymaga dużej przepustowości sieci. Skontaktuj się z administratorem sieci.

- **Czas trwania segmentu wideo (Video segment duration limit):** określ minimalny i maksymalny czas trwania segmentu, który ma zostać zarchiwizowany. Maksymalny czas trwania: 59min59sek. Najechnie kursorem nad edytowalne pole uruchomi wskazówkę wyświetlającą minimalny i maksymalny czas trwania. Ułatwia to nadzorowanie plików archiwizowanych. Możesz polecić systemowi ignorowanie wszystkich nagrań krótszych niż 10 sekund.

- **Hasło dla plików w formacie KVI oraz KVA (Default password for KVI and KVA file formats):** zaznacz to pole, jeżeli chcesz, aby segmenty były chronione hasłem. Pliki w formacie KVI oraz KVA chronią twoje zarchiwizowane dane hasłem. Upewnij się, że pola Hasło oraz Potwierdź hasło, są uzupełnione prawidłowo. Użytkownicy z odpowiednimi pozwoleniami będą mogli oglądać zarchiwizowane nagrania po uprzednim wprowadzeniu hasła.

- **Częstotliwość odpytywania serwera Kantech (m:ss) (Kantech server polling frequency (m:ss)):** przy pomocy paska można określić, jak często EntraPass Video Vault będzie sprawdzać serwer EntraPass.

Notatka: pamiętaj, że częstotliwość odpytywania pomiędzy serwerem EntraPass, stacjami roboczymi, bramkami oraz serwerami wideo będzie miała wpływ na przepustowość. Częstsze odpytywanie oznacza zwiększenie obciążenia sieci.



Urządzenia

Konfiguracja aplikacji

7 – Kliknij na **Główny kadr (Significant Frame)**, aby określić główny obraz, który będzie służył, jako miniatura nagrania w katalogach.

- Musisz wybrać typ ustawienia:

- **Główny kadr (Significant Frame)**: najbardziej reprezentatywny kadr z nagrania segmentu. Ten kluczowy obraz służy, jako podsumowanie całego segmentu.

- **Główny kadr sekwencji (Significant Frame on Sequence)**: ta opcja jest wykorzystywana tylko w kamerach kopułkowych, w których ustalono trasę. Najbardziej reprezentatywny kadr z nagrania segmentu ze zdefiniowanej trasy służy, jako podsumowanie całego segmentu.

- **Główny kadr na ustawieniu (Significant Frame on Preset)**: ta opcja jest wykorzystywana tylko w kamerach kopułkowych, w których ustalono preset. Najbardziej reprezentatywny kadr z nagrania segmentu od pierwszej klatki do przejścia do pozycji presetu służy, jako podsumowanie całego segmentu.

- Możesz wybrać jeden z **Domyślnych typów kadrów (Default Key Frame types)**:

- **Brak obrazu (No image)**: nie będzie żadnej miniatury dla segmentu wideo.

- **Pierwszy kadr (First frame)**: segment będzie reprezentowany przez obraz wykonany przed alarmem.

- **Kadr zdarzenia (Event Frame)**: segment będzie reprezentowany przez obraz wykonany w momencie wystąpienia alarmu.

8 - Kliknij zakładkę **Serwis (Service)**, aby określić informacje do logowania, kiedy serwer EntraPass Video Vault działa, jako usługa i trzeba wydrukować raport.

9 - Kliknij zakładkę **Serwis (Service)**, aby określić informacje do logowania, kiedy serwer EntraPass Video Vault działa, jako usługa i trzeba wydrukować raport zbiorczy.

- Musi być zaznaczone pole **Zaloguj do aplikacji serwisowej EntraPass (Login to EntraPass service application)**, aby włączyć tę opcję.



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia

- Wprowadź nazwę domeny oraz login EntraPass Video Vault.
- Wprowadź hasło i potwierdzenie hasła.

Komentarz (Comment)

Sprawdź: Pole komentarza



Konfiguracja bramek EntraPass (EntraPass Gateways Configuration)

Bramka EntraPass konwertuje informacje otrzymywane od kontrolera albo połączenia, a następnie transmituje przekonwertowane dane do serwera. Bramka konwertując również informacje otrzymywane od serwera i transmitują je do kontrolera. Bramki mogą być zainstalowane na dedykowanym do tego komputerze albo zintegrowane z inną stacją roboczą EntraPass.

Notatka: dla pojedynczej bramki limity są następujące: 2048 połączeń, 10000 drzwi, 100000 kart, 100000 Linii dozorowych (input) i wyjść (output).

Właściwości bramek multi-obiektowych (Multi-site Gateway features)

Pojemności	Multi-obiektowe bramki
Ilość bramek	41
Lokalne połączenie	32 obiektów (z numerem seryjnym i USB)
Zdalne połączenia online	512 obiektów (z Kantech IP Link* i KT-400)
Modemy dial-up na połączenia hosta	32 na bramkę
Zdalne połączenia dial-up	512 na bramkę
Kontrolery na bramkę	17,408 (32 na połączenie)
Czytniki/klawiatury na bramkę	34,816
Zdarzenia na regulator wł./wył.	34

* Wymagania systemowe mogą się różnić zależnie od wielkości połączeń i liczby zdarzeń generowanych na dzień



Konfigurowanie bramki multi-obiektowych (Configuring a multi-site Gateway)

1 – Z zakładki **Definiowanie urządzeń (Devices definitione)**, kliknij przycisk **Bramka**.

2 – Z listy **Bramka**, wybierz bramkę, którą chcesz konfigurować.

3 – W zakładce **Ogólne (General)**:

- Wybierz **Pogląd Grafiki i Wideo (Graphic and Video view)**, do którego przypisana jest bramka.
- Jeżeli twoja multi-obiektowa bramka jest podłączona do pierwszego kontrolera przez modem, kliknij **Definiowanie Modemu Host (Host Modem Definition)**, aby skonfigurować komunikację modemem.
 - o Kliknij przycisk **Nowy**, aby dodać modem do listy wyboru modemów.
 - o Skonfiguruj modem, jak to było przykładowo pokazane w poprzednim oknie i kliknij **OK**, aby powrócić do okna **Definiowanie Urządzenia Device definitione**.

Notatka: dla zachowania ciągłości ustawień oraz niezawodności Kantech wspiera wyłącznie modemy US Robotics Sportster. Dodatkowo, rodzaj połączenia modemu powinien być ustawiony na **Wysyłaj i odbieraj**, podczas gdy Ustawienia modemu nie powinny być zmieniane. Jeżeli nie jesteś pewien, czy wybrane parametry są prawidłowe, skontaktuj się z administratorem sieci.

4 – W zakładce **Bramki multi-obiektowe (Multi-Site Gateway)**, wprowadź **Adres IP** oraz **Nazwę domeny** dla bramki. Bramka jest skonfigurowana, aby obsługiwać zdarzenia powiązane z KT-100, KT-200 oraz KT-300.

5 – W zakładce **Zdarzenia KT-100/KT-200/KT-300 (KT-100/KT-200/KT-300 Events)**, określ czas włączenia i wyłączenia licznika czasu LED (LED Timer on/LED Timer off) dla każdego zdarzenia. Bramka jest skonfigurowana, aby obsługiwać zdarzenia powiązane z KT-100, KT-200 oraz KT-300.

6 – W zakładce **Zdarzenia KT-400/KT-1 (KT-400/KT-1 Events)**, określ wł./wył. pulsowanie LED (LED Pulse on/LED Pulse off) dla każdego zdarzenia. Bramka jest skonfigurowana, aby obsługiwać zdarzenia powiązane z KT-400.

7 – W zakładce **Zdarzenia KTES (KTES Events)**, określ wł./wył. pulsowanie LED (LED Pulse on/LED Pulse off) dla każdego zdarzenia.

Notatka: EntraPass wspiera do 41 multi obiektowych bramek.



Lista zdarzeń dostępnych w bramkach multi-obiektowych.

Przyznanie dostępu	Prośba o uzbrojenie odmowa	Czas oczekiwania na drugą kartę minął
Dostęp zabroniony	Wstrzymanie przyznano	Dostęp zabroniony – oczekiwanie na drugą kartę
Czas dostępu wygaś	Wstrzymanie odmowa	Dostęp zabroniony – czytnik zablokowany
Oczekiwanie na klawiaturę	Drzwi otwarte	Opóźnienie wyjścia
Czas dostępu do klawiatury wygaś	Wymuszone otwarcie drzwi	Opóźnienie wejścia
Kod kreskowy na klawiaturze	Drzwi przed-alarmem otwarte za długo	Dostęp zezwolony przez abonenta
Prawidłowy wybór piętra	Drzwi otwarte za długo	Dostęp zabroniony przez abonenta
Nieprawidłowy wybór piętra	Alarm na ponownym zablokowaniu	Przełącznik pomocniczy aktywowany przez abonenta
Czas wyboru piętra upłynął	Drzwi odryglowane	Prośba o uzgodnienie zamka – przyznano (Postal lock request granted)
Prośba do wyjścia przyznano	Czytnik wyłączony	Prośba o uzgodnienie zamka – odmowa (Postal lock request denied)
Prośba do wyjścia odmowa	Drzwi uzbrojone	
Prośba o uzbrojenie przyznano	Oczekiwanie na drugą kartę	

Notatka: czas aktywacji dla zdarzenia Czekaj na klawiaturę jest określany w zakładce Opóźnienia klawiatury.

8 – W zakładce Opóźnienia klawiatury (Keypad delays) określ opcje klawiatury.

- W sekcji Opóźnienia klawiatury (Keypad delays), wprowadź **Ukryty-cyfrowy czas opóźnienia (m:ss) (Inter-Digit Delay time (m:ss))**. Przedstawia on maksymalny dopuszczalny czas opóźnienia pomiędzy wyborem przez użytkownika przycisku na klawiaturze.
- Wprowadź **Czas przekroczenia czasu opóźnienia na klawiaturze (m:ss) (Time-out on keypad delay time (m:ss))**. Wartość jest ustawiana w sekundach. Przedstawia maksymalny czas, jakim dysponuje użytkownik, na rozpoczęcie wprowadzania swojego numeru identyfikacyjnego na klawiaturze.

Notatka: maksymalny czas dla opóźnienia wprowadzenia cyfr oraz wyłączenia klawiatury to 2 minuty i 7 sekund; a dla KT-400 to 4 minuty i 15 sekund.

- W sekcji **Opóźnienia (Delays)** (nie dla KT-200), przy pomocy strzałek góra/dół, można określić liczbę **Błędnych prób (Invalid attempts)**, po której nastąpi blokada klawiatury. Użytkownik ma maksymalnie 255 błędnych prób przed zablokowaniem klawiatury.
- Wprowadź **Opóźnienie blokady klawiatury (h:mm) (Keypad disabled duration delay (h:mm))**. Maksimum to 4 godziny i 15 minut. Kiedy ten czas zostanie osiągnięty, klawiatura zostanie zablokowana dla wszystkich kart. Jest zablokowana na czas określony w polu **Czas zablokowania klawiatury (Keypad disabled duration)**.



- Wprowadź **Opóźnienie resetowania zliczania (m:ss) (Reset attempt counter delay (m:ss))**. Kiedy opóźnienie ustawione w polu Resetuj zliczanie prób (**Reset attempt counter**) upłynie, system zresetuje zliczanie do zera. Maksymalne opóźnienie to 4 minuty i 15 sekund.

Komentarz (Comment)

Sprawdź: Pole komentarza

Konfiguracja wirtualnych magistrali (Site configuration)

Obiekt, w przeciwieństwie do fizycznego komponentu, składa się z jednego albo wielu połączeń (zobacz [Konfigurowanie połączenia](#), aby dowiedzieć się więcej).

Dzięki temu wiele „kontrolerów”, komunikujących się po IP w systemie EntraPass, może być połączonych razem w „wirtualny obiekt” niezależnie od ich fizycznych połączeń.

Notatka: połączenie dial-up nie są wspierane przez wirtualne obiekty.

1 – z okna **Urządzenia**, kliknij **Obiekt**.

2 – jeśli definiujesz **Obiekt**, kliknij przycisk **Nowy**, przypisz nazwę do nowego obiektu i kliknij **Zapisz**. Punkt przy nazwie obiektu stanie się zielony.

3 – wprowadź albo edytuj opis w obu językach.

Ogólne parametry

1 – kliknij zakładkę **Ogólne**.

2 – w sekcji **Lista połączeń** znajdziesz wszystkie połączenia dla tego obiektu. Kliknij prawym na połączeniu, aby je wyświetlić albo edytować.

3 – jeśli jest to możliwe, wybierz **Grafikę** oraz **Podgląd** wideo do którego przypisana jest bramka. Podgląd będzie włączony wtedy, jeśli opcja wideo jest włączona w EntraPass.

Informacje

1 – kliknij zakładkę **Informacje**.

- wprowadź informacje w odpowiednie pola (do 20).
- pierwsze 10 pól jest już wypełnione. Kliknij na dowolnym z nich, aby je edytować.

Komentarz (Comment)

1 – kliknij zakładkę **Komentarz (Comment)**:

- Aby dowiedzieć się więcej na temat Komentarza, zobacz Pole komentarza.

Opcje łączenia połączeń (Merge Connection Options)

Zakładka Połącz istniejące połączenia pozwala na dodanie istniejących połączeń do obiektu. W ten sposób wszystkie logiczne oraz fizyczne komponenty podłączone do połączenia zostaną przeniesione do obiektu. Podczas procesu połączenia, system złączy wszystkie poziomy dostępu z obiektu oraz złączonych połączeń. Proces utworzy nowe poziomy dostępu i przypisze je do użytkowników. Nowe poziomy dostępu zostaną przemianowane przy pomocy prefiksu „Kombinacja:”, po którym zostanie dodana nazwa złączonych poziomów dostępu.

Notatka: upewnij się, że łączna liczba logicznych komponentów na obiekcie oraz połączeń nie przekroczy limitu: 100 grup (kontrolerów, przekaźników, etc.), 250 poziomów dostępu, 100 harmonogramów, 256 pięter, 250 grup pięter; albo komponenty zostaną utracone.

Aby połączyć połączenie (-a) w obiekt,



1 – kliknij zakładkę **Połącz istniejące połączenia**.

2 – wybierz połączenia, które mają być zintegrowane z obiektem.

3 – kliknij przycisk **Zapisz**. System wyświetli wtedy okienko Opcje połączenia połączeń (**Merge connection options**) (wszystkie są domyślnie wybrane)

- **Połącz identyczne harmonogramy (Merge Identical Schedules)**: ta opcja pozwala systemowi odnaleźć zduplikowane połączenia pomiędzy obiektem oraz połączeniem (połączeniami) i złączyć je w jedno. Jeśli opcja nie jest wybrana wszystkie harmonogramy z połączenia (połączeń) zostaną przeniesione do obiektu, nawet, jeśli są istnieje duplikat.

- **Dodaj Nazwę Obiektu do Nazwy Komponentu (Add Site Name as Prefix to Component's Name)**: ta opcja pozwala dodać nazwę, jako prefix, do wszystkich nazw fizycznych komponentów (kontrolerów, drzwi, etc.). Na przykład, dla obiektu „Biuro Montreal”, drzwi nazwa „Główne drzwi” będą nazywać się „Biuro Montreal, Główne drzwi”.

4 – kliknij **OK**, aby kontynuować.

5 – w razie potrzeby edytuj nazwę poziomu dostępu w obu językach. Kliknij **OK**.

6 – okienko **Wyniki połączenia (Merge results)** zostanie wyświetlone. Sprawdź, czy w trakcie procesu połączenia nie powstały jakieś błędy. Kliknij przycisk **Zamknij**.

7 – aby zakończyć proces połączenia musisz zamknąć okno Definiowanie obiektu. Rozpocznie się wtedy przeładowanie bramki (bramek) / konta.



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia



Zmiana nazwy/opisu (Change Site Labels)

- 1 – Wybierz pole informacji o obiekcie z listy po lewej.
- 2 – Edytuj pole informacji. Możesz wprowadzić dwa różne opisy i zmieniać je przy pomocy przycisku **Zmień (Swap)**.
- 3 – Kliknij **OK**, aby zachować zmiany albo **Anuluj (Cancel)**, żeby wrócić.

Konfiguracja magistrali (Connection Configuration)

Połączenie jest utworzone, kiedy kontrolery są połączone do tego samego portu komunikacyjnego. System jest w stanie obsłużyć do 32 połączeń na multi-obiektową bramkę. EntraPass umożliwia użytkownikom dodanie do 2048 połączeń na multi-obiektową bramkę. Połączenia multi-obiektowe składają się z kontrolerów: KT-100, KT-200, KT-300, KT-400 oraz KT-1.

Obiekty wyświetlone w oknie Połączenia EntraPass różnią się i są zależny od wybranego typu połączenia. Na przykład, jeżeli wybranym typem połączenia jest RS-232, zakładka RS-232 zostanie wyświetlona do konfigurowania odpowiedniego portu i odpowiedniej szybkości transmisji.

Notatka: dla pojedynczej bramki limity są następujące: 2048 połączeń, 10000 drzwi, 100000 kart, 100000 Linii dozorowych (input) i wyjść (output).

Dostępne jest siedem typów połączeń: Direct (RS-232 albo USB), Secure IP (KT-400), Secure IP (KTES), Secure IP (IP Link), Secure IP KT-1, Ethernet and Dial-Up (RS-232).

Poniższa tabela obrazuje typ połączenia vs bramka.

Typ połączenia	Multi-obiektowa bramka	Bramka globalna	KT-NCC
Direct (RS-232 albo USB)	Tak	Tak	Tak
Ethernet	Tak	Tak	Tak
Secure IP (KT-1)	Tak	Tak	Tak
Secure IP (KT-400)	Tak	Tak	Tak
Secure IP (KTES)	Tak	-	-
Secure IP (IP Link)	Tak	-	-
Dial-up (RS-232)	Tak	-	-

- 1 – Z okna Urządzenia, wybierz **Połączenie (Connection)**.
- 2 – Z listy wybierz **Filtr obiektu (Site filter)**.
- 3 – Wybierz **Bramkę (Gateway)**
- 4 – Z listy **Połączenie (Connection)**, wybierz połączenie, na którym znajduje się kontroler.



5 – Jeżeli określasz nowe Połączenie, kliknij **Nowe**. Określ nazwę dla nowego połączenia i kliknij przycisk **Zapisz (Save)**.

6 – W zakładce **Ogólne (General)**:

Notatka: jeśli typ połączenia to Zabezpieczone IP (KTES), liczba KTES jest automatycznie ograniczone do jednego KTES na połączenie.

- W sekcji **Definiowania sprzętu (Hardware definitione)** określ ilość kontrolerów dla połączenia. Można ustawić 32 kontrolery na połączenie. Jeżeli zostanie wprowadzona większa liczba, system automatycznie ustawi 32.
- Ustaw Strefę czasową (Time zone): dzięki tej opcji, zdarzenia z obiektów będą mogły być wyświetlane według strefy czasowej bramki, na stacjach roboczych EntraPass w innych strefach czasowych.
- Wybierz Grafikę i Podgląd nagrania, do których przypisana jest bramka.
- Z listy wybierz **Typ połączenia pomiędzy komputerem, a bramką (Connection type between the computer and the Gateway)**.



Ustawianie koordynacji czasowej komunikacji (Setting up Communication Timing)

Uwaga: nie korzystaj z opcji **Koordinacja czasowa komunikacji (Communication timing)**. Jeżeli musisz ustawić opóźnienie komunikacji i frekwencje odpytywania, zadzwoń do Pomocy technicznej Kantech. Nieodpowiednie użycie tej opcji może spowodować poważne problemy z systemem. Okno **Koordinacja czasowa komunikacji (Communication timings)** pokazuje aktualne ustawienia domyślne. Muszą pozostać bez zmian, chyba, że Kantech zasugeruje zmianę.

Konfigurowanie połączenia RS-232 (Configuring a Direct RS-232 Connection Type)

Ten typ połączenia może być konfigurowany w EntraPass Corporate Edition, aby multi-obiektowych bramki komunikowały się przez RS-232.

Aby odblokować zakładkę RS-232, wybierz **Połączenie RS-232 (Direct RS-232 connection type)** w zakładce **Ogólne (General)**.

- Wybierz **Port komunikacji COM (Communication Port COM)**
- Wybierz **Szybkość transmisji pętli kontrolera (Controller's loop baud rate)**. Domyślna: 19200.



Konfigurowanie rodzaju połączenia urządzenia IP (Configuring an IP Device Connection Type)

Ten typ połączenia może być konfigurowany dla multi-obiektowych bramek w EntraPass Corporate Edition do komunikacji przez Kantech IP Link, KT-400, KT-1 oraz KTES.

Notatka:

Informacje na temat konfiguracji Kantech IP Link znajdziesz w Kantech IP Link Installation Manual, DN1670.

Informacje na temat KT-400 znajdziesz w KT-400 Installation Manual, DN1726.

Informacje na temat KT-1 znajdziesz w KT-1 Installation Guide.

Jeśli wybierzesz Zabezpieczone (IP KT-400), jako typ połączenia, głównym kontrolerem musi być KT-400.

Dla KTES, jedynym kontrolerem w pętli musi być KTES. Informacje na temat KTES znajdziesz w KTES Installation Manual, DN1769.

1 – Kiedy określisz **Bezpieczne IP (Secure IP)**: IP Link, KT-400, KT-1 albo KTES z listy **Typ połączenia (Connection type)** w zakładce **Ogólne (General)**, będziesz miał dostęp do trzech nowych zakładek: **Konfiguracja IP urządzenia IP (IP Device IP configuration)**, **Automatyczna konfiguracja urządzenia IP (IP Device Automated Connection)** oraz **Parametry urządzenia IP (IP Device Parameters)**.

- **Adres MAC (MAC address)**: wprowadź adres MAC urządzenia. Pierwsze sześć znaków w adresie MAC (00-50-F9) nie mogą być modyfikowane.

- Pole **Online** jest domyślnie zaznaczone.

- **Automatycznie pobierz adres IP (Obtain IP address automatically)**: zaznacz tą opcję, jeżeli konfigurujesz urządzenie z zastrzeżonym adresem **DHCP IP (Reserved DHCP IP)**.

- **Użyj następującego adres IP (Use the following IP Address)**: zaznacz tą opcję, jeżeli chcesz przypisać stały adres IP dla urządzenia. Po zaznaczeniu pojawią się trzy następne parametry.

- **Adres IP (IP Address)**: stały adres IP powinien być dostarczony przez Administratora Systemu.

- **Maska podsieci (Subnet Mask)**: ten adres powinien być dostarczony przez Administratora Systemu



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia

- **Bramka (Router) (Gateway (Router))**: adres powinien być dostarczony przez Administratora Systemu.
- **Adres serwera DNS (DNS server address)**: adres powinien być dostarczony przez Administratora Systemu (dla Kantech IP Link, KT-400 oraz KT-1).
- **Protokół (Protocol)**: wykorzystany do określenia protokołu komunikacji, UDP albo TCP.
- **Port (Port)**:
 - **TCP (For TCP)**: port 18802 dla strony gospodarza. Nie jest wymagany dla pozostałych stron.
 - **UDP (For UDP)**: port 18802 jest przypisywany, jako domyślny. Nie powinien być zmieniany, chyba, że urządzenie IP znajduje się w innej lokacji.

Notatka: port 18802 powinien być wykorzystany dla KT-400, KTES, KT-1 oraz IP Link.

- Adres multi-obiektowych bramek IP będzie wykorzystany albo pominięty, po wybraniu **Pomiń adres bramki IP (Override Gateway IP Address)**

Notatka: pole Auto wykrywanie IP – nawet, jeśli nie jest wybrane, zawsze jest aktualizowane i posiada adresem IP. Dla nowej bramki opcja nie ta nie jest wybrana domyślnie. Pole Adres IP jest domyślnie wybraną opcją.

- **Automatycznie wykryte IP (Auto Discovered IP)**: pole tylko do odczytu, wyświetla automatycznie adres IP bramki. Jeżeli wybrana jest opcja radio (radio), system nadpisuje adres IP oraz przeładowuje połączenie z nowymi informacjami.
- **Adres IP (IP address)**: wprowadź adres IP bramki.
- **Nazwa domeny (Domain name)**: jeżeli nie posiadasz adresu IP bramki, możesz wprowadzić nazwę domeny, którą dostarcza Administrator Systemu (dla Kantech IP Link, KTES, KT-400 oraz KT-1).

Notatka: musisz wprowadzić adres IP albo nazwę domeny. Nie możesz wprowadzić obu jednocześnie (wyłącznie dla Kantech IP Link, KTES, KT-1 oraz KT-400).



- **Testuj DNS (Test DNS):** kiedy wprowadzisz nazwę domeny, kliknij przycisk Testuj DNS. Powinien zostać wyświetlony odpowiedni adres IP (dla Kantech IP Link, KTES, KT-400 oraz KT-1).

2 – Przejdź do zakładki **Automatyczne połączenia urządzenia IP (IP Device Automated Connection)**, jeżeli pracujesz w środowisku **WAN**.

- Pole **Konfiguracja transmisji (Broadcast configuration)** musi być wybrana!

- **Prywatny adres IP (Private IP Address (LAN)):** automatycznie przypisze adres IP.

- **Publiczny adres IP (Public IP Address (WAN)):** adres IP dostarczony przez dostawcę Internetu.

- **Nazwa domeny (Domain Name (WAN)):** ta informacja powinna być dostarczona przez Administratora Systemu.

- **Pozwól na diagnostykę KT-Finder dla urządzenia IP (Enable KT-Finder diagnostic for IP device):** zaznacz to pole, jeżeli chcesz, aby KT-Finder był wykorzystany, jako narzędzie konfiguracyjne i pomocnicze.

3 – Przejdź do zakładki Parametry urządzeń IP, aby skonfigurować parametry bezpieczeństwa i połączenia.

- **Klucz szyfrujący (Encryption key):** 16 znakowy kod szesnastkowy.

- **Szybkość transmisji pętli kontrolera (Controller's loop baud rate):** wprowadź szybkość transmisji pętli kontrolera

Notatka: dla KT-200, max. 19200.

- W sekcji Opóźnienia (**Delays**):



- **Częstotliwość „pulsu” (mm:ss) (Heartbeat frequency (mm:ss))**: wprowadź częstotliwość z jaką chcesz, aby urządzenie IP wysyłało sygnał do bramki o tym, że jest online (00:15 do 10:00).
- **Błąd w komunikacji (mm:ss) (Fail to report after (mm:ss))**: wprowadź opóźnienie po którym uznaje się zerwanie komunikacji (01:30 do 59:59).
- **Opóźnienie fail-soft dla błędu w komunikacji bramki (mm:ss) (Fail-soft delay on gateway communication failure (mm:ss))**: wprowadź opóźnienie po którym urządzenie IP przyjmie, że komunikacja z kontrolerem została utracona i kontroler jest w stanie asekuracji.
- **Ilość prób (Retry Count)**: wprowadź ile razy urządzenie IP będzie próbowało skomunikować się z kontrolerem przed uznaniem utracenia komunikacji (1 do 15).
- **Maksymalny czas oczekiwania na wysłanie polecenia (s.cc) (Maximum wait on send command (s.cc))**: wprowadź maksymalne opóźnienie, na jakie pozwoli bramka w stosunku do urządzenia IP w sprawie potwierdzenia otrzymania polecenia ze stacji roboczej EntraPass (1.00 do 9.99).

Konfigurowanie typu połączenia odpytywania Ethernet (Configuring an Ethernet Polling Connection Type)

Ten typ połączenia może być konfigurowany na bramce przez sieć (Lantronix).

Zakładka Urządzenie IP będzie dostępna po wybraniu opcji **Ethernet (Odpytywanie) (Polling)** w zakładce **Ogólne (General)**.

- Wprowadź **adres IP** oraz **Numer portu**.
- Wybierz protokół komunikacji:
 - **TCP**, jeżeli komunikacja jest prowadzona z bramką przez serwer terminalu (terminal server) korzystający z protokołu TCP. W tym przypadku musisz skonfigurować serwer (skorzystaj np. z instrukcji producenta)
 - **UDP (User Datagram Protocol)**, wykorzystuje protokół IP do wysyłania datagramów z jednej aplikacji do drugiej. Nazywane jest także „bezpoleceniowe”, ponieważ nadawca i odbiorca nie muszą nawiązywać połączenia przed przesłaniem danych.



Konfigurowanie typu połączenia modemowego (RS-232) (Configuring a Dial-Up (RS-232) Modem Connection Type)

Jeżeli z zakładki Ogólne (General), a następnie z listy Typ połączenia, określisz modem RS-232, będziesz miał do dyspozycji trzy dodatkowe zakładki: opcje modemu, parametry terminarza modemu, różne.

Notatka: opcja Dial-up jest dostępna wyłącznie dla multi-obiektowych bramek.

1 – Wybierz zakładkę **Opcje modemu (Modem options)**, aby ustawić opcję połączeń wychodzących do modemu.

Notatka: ustawienia modemu nie powinny być zmieniane. Jeżeli nie jesteś pewien, czy wybrane parametry są prawidłowe, skontaktuj się z administratorem sieci.

- Wprowadź **Kod dostępu to linii zewnętrznej (Code to access an outside line)**
- Wprowadź **Numer telefonu (Remote phone number)**

Notatka: dla zachowania ciągłości ustawień oraz niezawodności Kantech wspiera wyłącznie modemy US Robotics Sportster. Ustawienia wewnętrzne modemu nie mogą zostać zmienione.

- Wybierz **typ linii telefonicznej (Phone line type)**: tonowa lub impulsowa.



- nastaw Liczbę sygnałów przed odpowiedzią (**Number of rings before answer**), która określi liczbę sygnałów, zanim modem odbierze połączenie. Ta opcja jest ważna wtedy, kiedy terminarz dzwonienia nie jest włączony.
- nastaw Odpowiedz po pierwszym sygnale (**Answer on first ring schedule**), aby skonfigurować interwał w trakcie którego modem będzie mógł odebrać połączenie po pierwszym sygnale.
- nastaw Liczbę powtórzeń (**Number of retries**), która określi liczbę podejść modemu do połączenia przed zawieszeniem prób.

2 – przejdź do zakładki Parametry terminarza modemu (**Modem Schedule parameters**), aby ustawić interwały, podczas których bramki albo obiekty łączą się z obiektami albo bramkami (przez połączenia modemowe) w celu przeprowadzenia określonych zadań.

- kliknij przycisk Odzyskaj zdarzenia obiektu (**Retrieve site events**), aby wyświetlić okno wyboru terminarza. Wybierz terminarz najbardziej pasujący ramom czasowym wyznaczonym dla konkretnego zadania. Zobacz Definiowanie terminarzy, aby dowiedzieć się więcej.
- powtórz te kroki dla: Dane zmodyfikowane od ostatniego, Raportuj zdarzenia po rodzaju połączenia priorytetowego, Raportuj zdarzenia automatycznie (**If data is modified since last, Report events under prioritycall type, Report events automatically**).
- określ opóźnienie zanim system nie przyjmie, że Nie zaraportowano po (**Fail to report after (mm:ss)**) .

Notatka: aby ustawić terminarz raportowania zdarzeń pod kątem priorytetów zgłoszeń najpierw określ Priorytety zgłoszeń (Priority call types) dla takich obiektów, jak drzwi, Linie dozоровe (inputs) oraz kontrolery.

3 – kliknij zakładkę Różne, aby skonfigurować, jak modemy traktują połączenia przychodzące/wychodzące.

- zaznacz opcję Wykorzystaj połączenie oddzwaniania (**Use a callback connection**), aby zmusić modem bramki do rozłączenia się po połączeniu i przejście w tryb oczekiwania na połączenie z potwierdzeniem ze zdalnego modemu.
- tylko KTES. Zaznacz Włącz podział linii KTES (**Enable multiple KTES line sharing**), aby zmienić Opóźnienie identyfikacji (**Identification delay**) pomiędzy każdym KTES. Przedział czasowy: 00 do 20 sekund.
- wybierz Główny modem (**Primary host modem**) z listy. Jeśli możliwe, wybierz Pomocniczy modem (**Secondary host modem**). Ta opcja jest przydatna, jeżeli modem główny jest zbyt obciążony.
- zaznacz Po odebraniu pozostań online (**After reception stay online**), jeśli chcesz ograniczyć czas połączenia do określonej wartości. Przedział czasowy: 00.03.00 do 23.59.59.



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia

- Zaznacz **Natychmiastowe powiadomienie, kiedy zawodzi komunikacja z kontrolerem podległym (Call immediately when slave controller communication failure)**, aby zostać powiadomionym w przypadku, gdy podległy kontroler nie przesyła danych do głównego kontrolera.
- Zaznacz **Natychmiastowe powiadomienie, kiedy bufor będzie wypełniony w 70% (Call immediately when buffer 70% full)**, aby wymusić pobranie bufora w momencie osiągnięcia 70% pojemności.

Notatka: nie wybieraj przycisku Zdalne opóźnienie modemu. Wszystkie ustawienia są domyślne skalibrowane pod kątem optymalnego działania z modemami US Robotics. Ustawienia NIE POWINNY być zmieniane, chyba, że Kantech rekomenduje inaczej.

Komentarz (Comment)

Sprawdź: Pole komentarza



Migrowanie kopii zapasowej KT-Standalone do serwera EntraPass (Migrating KT-Standalone Back-up Data to an EntraPass Server)

Możesz przenieść dane kopii zapasowej z kontrolera KT-Standalone do serwera EntraPass; zgodny kontrolery obejmują KT-1, firmware v2.01 i nowsze oraz KT-401, oprogramowanie firmowe v2.00 i nowsze. The kopia zapasowa zawiera następujące dane:

- Definicje kontrolerów
- Definicje drzwi
- Definicje przekaźników
- Definicje harmonogramów
- Definicje świąt
- Definicje użytkowników
- Harmonogram działań

Uwaga...

Następujące funkcje nie są uwzględniane w migracji:

- Strefa czasowa
- Integracja z panelem alarmowym
- Ustawienia wielokrotnego przesuwania na drzwiach wyjściowych.

Ikona	Opis
	KT-Standalone: wybiera pliki kopii zapasowej z KT-1, firmware v2.01 i nowszych oraz kontrolery KT-401, firmware v2.00 i wyższe.

Przed migracją danych należy skonfigurować EntraPass, aby używał tego samego formatu karty, karty globalnej Format i długość kodu PIN jako samodzielne ustawienia:

- 1 - Przejdź do karty Konto i wybierz z menu System.
- 2 - Aby otworzyć okno Format wyświetlania, kliknij
- 3 - W obszarze Domyślny format karty wybierz format karty nr 1, aby dopasować format karty nr 1 w polu samodzielny kontroler, powtórz dla karty # 2 do karty # 5.

UWAGA: Jeśli karta # 1 i karta # 2 używają innego formatu wyświetlania, EntraPass migruje na kartę # 4 lub kartę

5.

- 4 - W obszarze Globalny format karty wybierz odpowiedni format karty globalnej.

- 5 - Wybierz odpowiednią długość kodu PIN z listy Liczba cyfr PIN (KT-400 i KT-1).

Aby przeprowadzić migrację danych kopii zapasowej, wykonaj następujące kroki:

- 1 - Na karcie Urządzenia wybierz Połączenie z menu.

- Kliknij samodzielny przycisk KT na pasku menu, aby wyświetlić autonomiczne pliki CFG kopii zapasowej KT



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia

KT-1, oprogramowanie sprzętowe w wersji 2.01 i wyższej oraz KT-401, oprogramowanie sprzętowe w wersji 2.00 i wyższej.

3 - Wybierz plik, aby wyświetlić informacje o kopii zapasowej:

- a - Data i godzina utworzenia kopii zapasowej
- b - Typ sterownika
- c - MAC kontrolera / numer seryjny
- a - Wersja oprogramowania układowego sterownika
- b - Ilość użytkowników
- c - Ilość harmonogramów
- d - Ilość świąt
- e - Ilość harmonogramu akcji
- f - Ilość drzwi
- g - Ilość przekaźników
- h - Ilość danych wejściowych

4 - Wyświetlone zostanie okno z komunikatem „Czy na pewno chcesz zaimportować następujące dane?” Jeśli klikniesz

Tak: importuj dane, pojawi się następujący komunikat: „Migracja zakończona”, kliknij OK. Jeśli klikniesz Nie, okno wiadomości zostanie zamknięte.

Lista nieprzypisanych kontrolerów (The Unassigned Controllers List)

Gdy EntraPass otrzymuje dane z procesu rejestracji KT-1, dodaje kontroler do kontrolerów nieprzypisana lista. „Kontroler został dodany do listy nieprzypisanych” jest następnie generowany za pomocą następujące parametry:

- Opis bramy
- Adres MAC
- Rodzaj urządzenia

Wyświetlana jest nieprzypisana lista kontrolerów:

- Data i godzina (kiedy została dodana do listy) bramy
- Model kontrolera
- Adres MAC
- Numer seryjny
- Nadaj odebrany adres IP

Uwaga

Nieprzypisana lista kontrolerów może mieć ograniczoną liczbę 100 wpisów.



Konfiguracja parametrów czasowych komunikacji (Setting up Communication Timing)

Uwaga: nie korzystaj z opcji **Ustawiania czasu połączenia (Setting up Communication Timing)**. Jeśli musisz ustawić opóźnienia komunikacji, skontaktuj się z Obsługą techniczną Kantech. Złe zastosowanie tej opcji może doprowadzić do poważnych problemów z systemem. Okno **Ustawiania czasu połączenia (Setting up Communication Timing)** wyświetla wartości domyślne. Należy je zachować, chyba, że Obsługa techniczna Kantech zarekomenduje inaczej.

Konfiguracja kontrolerów (Controllers Configuration)

Kontrolery zapewniają informację audiowizualną odnośnie decyzji dostępu. Czerwone/zielone światło (LED) ze wskaźnika na czytniku informuje posiadacza karty, że drzwi są odryglowane albo zaryglowane. Lokalny alarm może zostać zainstalowany na drzwiach, aby ostrzeżenie dźwiękowe zostało uruchomione w przypadku wymuszonego otwarcia lub pozostawienia drzwi bez zamknięcia.

Definiowanie kontrolera informuje system o tym, jak kontroler będzie wykorzystywany oraz jakie urządzenia są z nim powiązane: drzwi, strefy wejść, przekaźniki, etc.). Kontrolery mogą być zdefiniowane podczas konfiguracji bramki albo połączenia; albo w menu definiowania kontrolerów, przez wybranie przycisku kontroler (Devices > Controller) lub przez użycie programu **Aplikacja Instalacja ekspresowa (Express Setup program)**. EntraPass wspiera pięć typów kontrolerów: KT-100, KT-200, KT-300, KT-400 oraz KT-1. Poniższa tabela podsumowuje podstawowe komponenty powiązane z każdym typem kontrolera Kantech:

Typ	Drzwi	Bezprzewodowe drzwi Aperio (licencja)	Przekaźniki	Strefy wejść	Pomocnicze wyjścia
KT-100	1	Brak wsparcia	4	4	2
KT-200	2	Brak wsparcia	2	16	4
KT-300	2	Brak wsparcia	2	8	4
KT-400	4	8	4	16	16
KT-1	1	2	2	5	5

Żądanie nieprzypisanych modułów (Unassigned modules)

Aby znaleźć listę modułów komunikujących się z kontrolerem, ale nieprzypisanych, kliknij opcję **Żądanie nieprzypisanych modułów** Ikona. Wyświetlone zostanie okno z następującymi informacjami:

Typ modułu: ioSmart lub ioModule.

Numer seryjny modułu: modułu.

Aby zdefiniować nieprzypisany moduł, kliknij moduł prawym przyciskiem myszy, a następnie kliknij polecenie **Przypisz moduł**, automatycznie wypełnia dane modułu na stronie konfiguracji kontrolera w zakładce **ioModule** lub **ioSmart** patka. W razie potrzeby zmień nazwę modułu lub zmień szczegóły konfiguracji i kliknij **Zapisz**. Kiedy definiujesz moduł, system usuwa go z listy.



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia



Konfigurowanie parametrów ogólnych dla kontrolerów Kantech (Configuring General Parameters for Kantech Controllers)

1 – Z okna **Urządzenia/Kontroler (Devices/Controller)** z listy wybierz **Filtr obiektu (Site filter)**

2 – Wybierz Bramkę (zobacz: **Konfigurowanie bramki (Gateway Configuration)**), aby dowiedzieć się więcej o konfigurowaniu bramki)

3 – Z listy Połączenie (Connection) wybierz połączenie, na którym znajduje się kontroler (zobacz: **Konfigurowanie połączenia (Connection Configuration)**), aby dowiedzieć się więcej o konfigurowaniu połączenia)

4 – Z listy Kontroler (Controller) wybierz kontroler, który chcesz określić. Następnie możesz nazwać wybrany kontroler.

5 – Z listy Typy kontrolerów KT (**KT controller type**), wybierz typ kontrolera. Następnie możesz nazwać wybrany kontroler.

- Przypisz odpowiednią nazwę do kontrolera w sekcji Języki (angielski i francuski, etc.), a następnie kliknij przycisk **Zapisz (Save)**. Po zapisaniu, lista Typ kontrolera przestaje być dostępna.

- System poprosi o użycie programu **Aplikacja Instalacja ekspresowa (Express Setup program)**. Kliknij TAK, aby kontynuować. Jeżeli klikniesz NIE, będziesz musiał konfigurować zdalnie te urządzenia w ich menu (drzwi, przekaźniki, Wejścia linii dozorowej i pomocnicze wyjścia).

Notatka: EntraPass oferuje możliwość zainstalowania dwóch rodzajów czytników na jednym kontrolerze (główny i pomocniczy). Opcja dostępna tylko dla KT-100 oraz KT-300. Dla KT-400 oraz KT-1 instalowane mogą być różne typy czytników (opcja dostępna wraz z firmware 1.06 oraz późniejszym).

Na danym kontrolerze rodzaj wszystkich czytników musi być taki sam (Wiegand albo ABA).

6 – Wybierz z listy Typ Czytnika (Reader type) czytnik zainstalowany na twoim kontrolerze. Sprawdź poniższą tabelę, aby sprawdzić typy kontrolerów vs typy czytników.

Notatka: przycisk  pozwala zainstalować dowolny sterownik dla konkretnego kontrolera. Dodatkowo pozwala na dodanie sterownika do Reader+ Driver, co sprawia, że sterownik będzie dostępny do wyboru przy następnym konfigurowaniu kontrolera.



Tabela 1: Typy czytników

Typy czytników	KT-100	KT-200	KT-300	KT-400/KT-1
ABA z kartami typu CNPID	Tak	Tak	Tak	
BC-201 - CF100	Tak	Tak	Tak	
Kody kreskowe BC-201 z kartami Polaris	Tak	Tak	Tak	Tak
CARDKEY	Tak	Tak	Tak	
CASI-RUSCO	Tak	Tak	Tak	
CHECKPOINT format Sielox	Tak	Tak	Tak	



EntraPass - Instrukcja instalacji i obsługi programu
Urządzenia

Typy czytników	KT-100	KT-200	KT-300	KT-400/KT-1
CHUBB	Tak	Tak	Tak	
DORADO ABA	Tak	Tak	Tak	
DORADO ABA Wiegand	Tak	Tak	Tak	
DORADO EMPI 26-Bit	Tak		Tak	
DORADO EMPI 34-Bit	Tak	Tak	Tak	
FIPS 201 75-bit bez daty końcowej				Tak
FIPS 201 75-bit z datą końcową				Tak
h20302, 37-Bit	Tak	Tak	Tak	Tak
HID CORPORATE 1000 Generic	Tak	Tak	Tak	Tak
HID iClass 37-Bit No Party				Tak
HID KSF (Kantech Secure Format)	Tak	Tak	Tak	Tak
HUGHES 36-Bit - CF104	Tak	Tak	Tak	
INDALA old 27-Bit Format	Tak	Tak	Tak	
INTERCON	Tak	Tak	Tak	
ioProx Dual Driver (26-Bit oraz XSF)	Tak	Tak	Tak	Tak
ioProx Kantech 26-Bit Wiegand	Tak	Tak	Tak	Tak
ioProx Kantech XSF Format	Tak	Tak	Tak	Tak
ioProx UK 31-Bit Wiegand				Tak
KRONOS Card z czytnikiem kodów kreskowych	Tak	Tak	Tak	
Mifare 32-Bit CSN	Tak	Tak	Tak	Tak
Mifare 34-Bit AID 517A	Tak	Tak	Tak	
Mirage 135	Tak	Tak	Tak	
NCS	Tak	Tak	Tak	
Northern 32-Bit with NR1 Reader	Tak	Tak	Tak	



EntraPass - Instrukcja instalacji i obsługi programu
Urządzenia

Typy czytników	KT-100	KT-200	KT-300	KT-400/KT-1
Northern 34-Bit z czytnikiem Hughes	Tak	Tak	Tak	
Paramount Farm 32-Bit Wiegand	Tak	Tak	Tak	Tak
Polaris 1 - CF101	Tak	Tak	Tak	
Polaris 1 z kartami 10-Digit	Tak	Tak	Tak	
Polaris 1 z kartami 16-Digit	Tak	Tak	Tak	
Polaris 1 z kartami Polaris	Tak	Tak	Tak	Tak
Polaris 2 ABA z kartami 10-Digit	Tak	Tak	Tak	
Polaris 2 ABA z kartami 16-Digit	Tak	Tak	Tak	
Polaris 2 ABA z kartami Polaris	Tak	Tak	Tak	Tak
Polaris 2KP ABA z kartami 10-Digit	Tak	Tak	Tak	
Polaris 2KP ABA z kartami 16-Digit	Tak	Tak	Tak	
Polaris 2KP ABA z kartami Polaris	Tak	Tak	Tak	Tak
Polaris 32/35/37 CHRS - CF103	Tak	Tak	Tak	
RBH 50-Bit Card Driver				Tak
SCHLAGE 1030 oraz 1040 Card Format	Tak	Tak	Tak	
Sensor 26-Bit Wiegand Standard	Tak	Tak	Tak	Tak
Sensor 34-Bit Wiegand	Tak	Tak	Tak	Tak
SFT-R50 26-Bit	Tak	Tak	Tak	
Shadow PROX	Tak	Tak	Tak	Tak
Siteguard Format	Tak	Tak	Tak	
Wiegand 26/28-Bit - CF102	Tak	Tak	Tak	
WLS Wireless 26-Bit	Tak	Tak	Tak	
WLS Wireless Shadow Prox and HID	Tak	Tak	Tak	

7 – Wybierz klawiaturę zainstalowaną na twoim kontrolerze z listy **Typ klawiatury (Keypad type)**. Sprawdź poniższą tabelę, aby sprawdzić typy kontrolerów vs typy klawiatur.



Tabela 2: Typy klawiatur

Typy klawiatur	KT-100	KT-200	KT-300	KT-400/KT-1
KP-1003H	Tak	Tak	Tak	
KP-500, KP-2000, KP-2500, KP-3000	Tak	Tak	Tak	
ioProx with Integrated Keypad (8-Bit Burst)	Tak	Tak	Tak	Tak
POL-2KP - 5-Digit Integrated Keypad	Tak	Tak	Tak	Tak

8 – Zaznacz pole opcji **Wyłącz odpytywanie kontrolera (Disable controller polling)**, kiedy musisz odłączyć kontroler od systemu w celach serwisowych. W tym trybie kontroler nie będzie odpytywany, a żądanie wyświetlenia jego statusu spowodują wyświetlenie komunikatu, że odpytywanie kontrolera zostało wyłączone.

9 – Wybierz tryb **Vital LED** (tylko dla KT-1). Zobacz: Instrukcja obsługi KT-1 D29008966.

Notatka: ta opcja może zostać wykorzystana, kiedy kontroler jest czasowo usunięty, ale nie może zostać skasowany (na przykład w czasie naprawy). Pozwala także użytkownikom na łatwe ustawienie oprogramowania przed zakończeniem instalacji.

10 – Wybierz **Na żądanie (On demand)** albo **Zawsze (Always)** dla Status LED (tylko dla KT-1). Zobacz: Instrukcja obsługi KT-1 D29008966.

11 – Wybierz **Grafika (Graphic)** albo **Podgląd wideo (Video view)**, do którego przypisana jest bramka. Podgląd wideo będzie dostępny tylko wtedy, gdy opcja ta jest udostępniona w EntraPass.

Konfigurowanie konkretnych parametrów kontrolera (Configuring Specific Controller Parameters)

1 – Z okna Kontroler (Controller) wybierz zakładkę kontroler (KT-100, KT-200, KT-300, KT-400 albo KT-1).



Zmiana typu kontrolera (Changing controller type)

Rodzaj kontrolera może zostać zaktualizowany do nowszego bez resetowania ustawień kontrolera. Aby dokonać zmiany wykonaj następując czynności:

1 – Z zakładki **Urządzenia** wybierz **Kontroler**. Następnie z listy wybierz kontroler.

2 – z listy Rodzaj kontrolera KT wybierz nowy rodzaj kontrolera.

3 – kliknij przycisk Zapisz. Pojawi się wiadomość z zapytaniem czy chcesz kontynuować. Kliknij Tak. Otworzy się okno Ustawień ekspresowych.

4 – każdy niezidentyfikowany komponenty może zostać skonfigurowany przy pomocy okna Ustawień ekspresowych. Na przykład, przy zmianie z KT-1 na KT-400, niezidentyfikowane drzwi mogą zostać skonfigurowane.

5 – kliknij OK, aby zakończyć proces.

6 – podczas procesu opcja Wyłącz odpytywanie kontrolera (Disable controller polling) jest automatycznie włączona. Upewnij się, że ta opcja zostanie wyłączona. Ta opcja wspiera tylko aktualizowanie kontrolerów do nowszych kontrolerów. Zasady aktualizowania rodzajów kontrolerów znajdują się w poniższym zestawieniu.

KT-100 → KT-300, KT-1, KT-400

KT-200 → KT-300, KT-400

KT-300 → KT-400

KT-1 → KT-400

Notatka: przy konwertowaniu z KT-100 albo KT-1 do KT-400 czytniki wyjścia są konwertowane, jako drugie drzwi.

Notatka: nie jest możliwa zmiana typu kontrolera, jeżeli wykorzystano KT-IP.

Notatka: moduły Cambus oraz SPI połączone z kontrolerem nie mogą zostać przetransferowane. Aby zmienić typ kontrolera, definicje modułów Cambus oraz SPI muszą najpierw zostać usunięte.



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia

1 – Wybierz zakładkę kontrolera (KT-100, KT-200, KT-300, KT-400 albo KT-1) z okna Kontrolera.

2 – Wprowadź numer seryjny kontrolera w pole Numer seryjny (Serial number). Numer jest na etykiecie kontrolera. Pole przyjmuje tylko znaki numeryczne, za wyjątkiem pierwszego znaku, którym może być „a” albo „A”. Jeżeli wprowadzone małą literę, system poprawi ją na wielką.

3 – Wyłącznie dla KT-400:

- Aby skonfigurować moduły SPI, zobacz **Ustawienia modułów rozszerzeń** ([Expansion Modules Setup](#)).
- Aby skonfigurować przypisanie pięter, zobacz **Definiowanie przypisania pięter dla KT-400 (Defining the KT-400 Elevator Floor Associations)**.

4 - Wyłącznie dla KT-300:

- Aby skonfigurować moduły Combus, zobacz **Moduły Combus KT-300 (KT-300 Combus Modules)**.
- Aby skonfigurować przypisanie pięter, zobacz **Definiowanie przypisania pięter dla KT-300 (Defining the KT-300 Elevator Floor Associations)**.



5 - Wyłączenie dla KT-200:

- Aby skonfigurować urządzenia pomocnicze KT-200, zobacz **Konfigurowanie urządzeń pomocniczych KT-200 (Configuring KT-200 Auxiliary Devices)**.
- Aby zdefiniować przekaźniki REB-8, zobacz **Definiowanie przekaźników REB-8 (Defining REB-8 Relays)**
- Aby skonfigurować kontrolery windy REB-8, zobacz **Programowanie kontrolerów windy REB-8 (Programming REB-8 Elevator Controllers)**.
- Aby skonfigurować kontrolery windy KT-2252, zobacz **Programowanie kontrolerów windy KT-2252 (Programming KT-2252 Elevator Controllers)**.

6 – Wprowadź Opóźnienie oczekiwania na drugą kartę dostępu (Wait for second access card delay). Ta opcja jest przydatna w strefach, gdzie wymagane są dwie karty, aby uzyskać dostęp do drzwi. Dopuszczalny czas: 2 minuty 7 sekund.

7 – Z listy Przycisk Escape/Powtórz (Keypad escape key), wybierz przycisk Escape/Powtórz. Ta funkcja jest powiązana z numerem PIN. Kiedy użytkownik wprowadzi zły numer, może przy pomocy przycisku Escape/Powtórz ponownie wprowadzić numer PIN bez tracenia szansy na prawidłowe wprowadzenie kodu.

8 – Z listy Opornik EOL (5.6K) (EOL resistor), wybierz typ opornika wykorzystany w twoim systemie. Domyślnie: brak. Ta opcja jest wykorzystywana, jako urządzenie nadzorcze dla wszystkich wejść. Jeżeli ta opcja jest aktywna, a wejście zostanie odłączone, wiadomość alarmowa zostanie wygenerowana i wysłana do pulpitu Wiadomości alarmowe.

9 – Kliknij przycisk Zapisz (Save).



Konfigurowanie aktywowania statusu przekaźnika (Configuring the Status Relay Activations)

Wybierz zakładkę **Status przekaźnika (Status relay)**, aby zaprogramować przekaźnik albo grupę przekaźników, które zostaną aktywowane w momencie zajścia zdarzenia.

Konfigurowanie „licencjonowanych” drzwi bezprzewodowych Aperio (Configuring Licensed Wireless Doors)

Ta opcja wspiera „licencjonowane” drzwi Assa Abloy w EntraPass. Aby uzyskać więcej informacji na temat konfiguracji zarządzania Assa Abloy, zobacz *ASSA ABLOY Wireless Locks integration (AH30 hub, serial)*. Aby skonfigurować aplikację EntraPass dla „licencjonowanych” drzwi bezprzewodowych, postępuj następująco:

- Z okna **Urządzenia/Kontroler (Devices/Controller)** wybierz kontroler, który chcesz konfigurować. Jeżeli kontroler wspiera „licencjonowane” drzwi bezprzewodowe ikona „licencjonowanych” drzwi będzie dostępna na pasku menu Kontrolera.
- Wybierz symbol Drzwi „licencjonowanych”.
- Jeżeli żaden zintegrowany panel nie został wcześniej przypisany do tego kontrolera, EntraPass automatycznie stworzy nowy zintegrowany panel.
 - Wybierz **Konfiguracja (Configuration)**, aby otworzyć okno **Drzwi „licencjonowanych” (Licensed Doors)**. Wyświetli się liczba **Zakupionych (Purchased)** oraz **Dostępnych (Available)** licencji.
 - Aby dodać drzwi, wybierz „+”.
 - Musisz wprowadzić opis drzwi oraz adres urządzenia. Adres urządzenia (EAC) został skonfigurowany podczas konfiguracji bezprzewodowego zamka. Aby uzyskać więcej informacji na temat konfiguracji zarządzania Assa Abloy, zobacz *ASSA ABLOY Wireless Locks integration (AH30 hub, serial)*.
 - Zaznacz pole, aby określić czy drzwi posiadają funkcję **czujnika stanu drzwi (contact)** – otwarte albo zamknięte; czy **REX (Request To Exit – prośba o wyjście)**
 - Aby usunąć drzwi wybierz **Usuń (Delete)** i kliknij **OK**.
- Jeżeli zintegrowany panel został wcześniej przypisany do wybranego kontrolera wyświetli się okno **„Licencjonowanych” drzwi (Licensed Doors)**. Można w nim edytować istniejące drzwi bezprzewodowe.



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia

- Aby sprawdzić status zamka bezprzewodowego wybierz zamek bezprzewodowy z panelu **Operacja/Zintegrowany panel (Operation/Integrated Panel)**. Aby zobaczyć szczegóły kliknij dwukrotnie na urządzeniu. Możliwe stany znajdują się w tabeli poniżej.

Parametr	Stany
Liczba drzwi (Door Number):	
Czujnika antysabotażowy (Tamper):	Czujnik antysabotażowy w stanie alarmu Czujnik antysabotażowy w normalnym stanie [Stan nieznany: BRAK INFORMACJI]
Status komunikacji urządzenia (Device communication status):	Urządzenie Online Urządzenie Offline [Stan nieznany: BRAK INFORMACJI]
Strona drzwi (Door side):	Strona drzwi: do środka Strona drzwi: na zewnątrz Strona drzwi: obie [Stan nieznany: BRAK INFORMACJI]
Stan klamki (Handle State):	Klamka nieużywana Klamka używana [Stan nieznany: BRAK INFORMACJI]
Stan cylindra klucza (Key Cylinder State):	Cylinder klucza nieużywany Cylinder klucza używany Cylinder klucza w konkretnej pozycji: 1/2/3 [Stan nieznany: BRAK INFORMACJI]
Stan zamka (Lock State):	Drzwi odryglowane Drzwi zaryglowane Zamek zabezpieczony Zamek uszkodzony-zacięty [Stan nieznany: BRAK INFORMACJI]
Stan drzwi (Door State):	Drzwi otwarte Drzwi zamknięte [Stan nieznany: BRAK INFORMACJI]
Wersja protokołu	
Numer wersji	
ID sprzedawcy (Vendor ID):	
Adres MAC (Mac Address):	
Centrum adresów MAC (Hub Mac Address):	
Przy podejrzanym zachowaniu (On abnormal behaviour):	Oprogramowanie kontrolera nie wspiera integracji Brak sterownika czytnika Drzwi nieskonfigurowane Wejście nieskonfigurowane

Notatka: bezprzewodowe drzwi mogą zostać zidentyfikowane poprzez niebieską ikonę. Pozostałe przez zieloną.

Dla drzwi bezprzewodowych występuje mniej konfigurowalnych parametrów. Występują także różnice w działaniach na tych drzwiach.

- Niektóre opcje, takie jak **Uzbrój drzwi, Rozbrój drzwi, Powrót czujnika stanu drzwi do terminarza** oraz **Wyłącz czujnik stanu drzwi (Arm Door, Disarm Door, Door contact back to schedule oraz Disable Door Contact)** nie są dostępne dla zamków bezprzewodowych.
- Zamki bezprzewodowe przejdą w tryb uśpienia, aby oszczędzać moc. Jeżeli chcesz wysłać polecenie do zamka, najpierw trzeba go „wybudzić” (poprzez interakcję z zamkiem). Tak samo sprawa wygląda z terminarzem odblokowywania. Aby „wybudzić” zamek trzeba dwukrotnie użyć karty.
- Przy pierwszym uruchomieniu **Stan Czujnika antysabotażowego (Tamper State)** będzie **Nieznany (Unknown)**.



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia

- Jeżeli bezprzewodowe centrum utraci zasilanie nie zachowa ostatnich statusów zamków bezprzewodowych.
- **Syrena (Buzzer)** oraz LED nie mogą być kontrolowane przez EntraPass.
- Przy zmianie długości kodu PIN, zamek bezprzewodowy musi zostać zdalnie przekonfigurowany.
- Status zamka jest aktualizowany tylko przy zdarzeniu.
- Zamek bezprzewodowy nie może być sterowany przy utracie połączenia z kontrolerem.
- Obecnie zamki bezprzewodowe mają tylko wsparcie sterowników 26-bit.

Notatka: kiedy wybierzesz Urządzenia/Panele zintegrowane... Drukuj (Devices / Integrated Panel...Print) możesz sprawdzić liczbę licencjonowanych drzwi połączonych z tym zintegrowanym panelem.

Notatka: obecnie, drzwi bezprzewodowe są wspierane przez kontrolery KT-1 oraz KT-400.



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia



Definiowanie opcji kontrolera (Defining Controller Options)

Zakładka Opcje (Option) umożliwia konfigurację:

- Anty-passback: dla zsynchronizowania czytników wejść/wyjść
- Funkcje wymuszeń (Duress function): dla określenia przycisku alarmowego
- Opcje zliczania kart: dla określenia ilości kart w strefie, etc.

Notatka: opcja anti-passback działa z czytnikami wejść/wyjść. Pozwala kontrolować administratorowi bezpieczeństwa liczbę użytkowników kart w obszarze. Przekaznik może zostać aktywowany w momencie, kiedy licznik osiągnie wartość określoną, jako maksymalną ilość kart w obszarze.

1 – Z okna Kontroler (Controller), kliknij zakładkę Opcje, aby określić opcje anty-passback, wymuszeń oraz zliczania kart.

2 – Określ opcje Wymuszeń (Duress). Po wybraniu tej opcji musisz określić przycisk, który będzie działać, jako przycisk alarmowy.

- Wymuszenie na przyznaniu dostępu (**Duress on access granted**): ta opcja włącza dostępność do przycisku alarmowego przy przyznaniu dostępu.
- Wymuszenie na odmowie dostępu (**Duress on access denied**): ta opcja włącza dostępność do przycisku alarmowego przy odmowie dostępu.

3 – Wybierz przycisk alarmowy z listy.

Notatka: dla zwiększenia bezpieczeństwa możesz wybrać obie opcje. Programowanie anti-passback jest dostępne przy multi-obiektowej bramce.

4 – Z opcji **Anty-passback (Anti-passback)**, wybierz opcję **anty-passback (anti-passback)** z listy **Typ (Type)**: kiedy opcja anti-passback jest wybrana, karta nie może być użyta na drzwiach wyjścia, o ile nie została wcześniej użyta na odpowiadającym im drzwiom wejścia.

- **Brak (None)**: opcja **anty-passback (anti-passback)** jest wyłączona.
- **„Miękki” anty-passback (Soft anti-passback)**: ta opcja pozwala użytkownikowi karty na użycie czytnika wejścia (albo wyjścia) więcej niż jeden raz, bez użycia korespondującego czytnika wyjścia (albo wejścia). Do Pulpitu Wiadomości (**Message desktop**) jest wysłane zdarzenie „Dostęp zezwolony – Zła lokalizacja passback” (**“Access granted - Passback bad location”**)
- **„Twardy” anty-passback (Hard anti-passback)**: karta wykorzystana przy czytniku wejścia nie będzie mogła zostać użyta przy tym samym czytniku, o ile nie zostanie wcześniej użyta przy odpowiednim czytniku wyjścia. Do Pulpitu Wiadomości (**Message desktop**) jest wysłane zdarzenie „Odmowa dostęp – Zła lokalizacja passback” (**“Access denied - Passback bad location”**)
- **Strefa lokalna kontrolera (Controller local area)**: ta opcja jest tylko dostępna dla KT-400. Zobacz: **Definiowanie stref lokalnych dla KT-400 (Defining the KT-400 Controller Local Areas)**.

5 – W sekcji **Zapomnij terminarz (Forgive schedule)**, kliknij na przycisk **trzech kropek (three-dot)**, aby nastawić terminarz resetowania opcji **anty-passback (anti-passback)** dla wszystkich kart.

Notatka: sekcja Zapomnij terminarz jest dostępna wyłącznie wtedy, kiedy „Miękki” anti-passback albo „Twardy” anti-passback są wybrane.



6 – W sekcji Różne (Miscellaneous) wskaż opcję dla **Uruchomienia opóźnienia fail-soft (Enable fail-soft delay)** (10-255 sec). W tym trybie komunikacja z kontrolerem została utracona i kontroler działa w trybie samodzielnym.

7 – Wprowadź kod (32-bit) dla rodziny kart (opcjonalnie). Kod znajduje się na karcie dostępu.

8 – W opcjach **Zliczania kart (Card count)**, użyj kontrolerek góra/dół, aby ustawić maksymalną liczbę kart. Maksimum: 2, 147, 483, 647. System nadzoruje karty, które znajdują się w monitorowanej strefie i aktywuje przełącznik, gdy limit zostanie osiągnięty. Kiedy użytkownik opuści obszar, licznik się zmniejsza, a przełącznik się ostatecznie zresetuje.

9 – Możesz skonfigurować system tak, aby aktywował jeden przełącznik albo grupę przełączników, kiedy zostanie osiągnięty limit zliczania. Kliknij na przycisk trzech kropek (three-dot), aby wybrać przełącznik albo grupę przełączników, które zostaną aktywowane, kiedy limit zostanie osiągnięty.



Terminarz nadzoru (Supervision Schedule)

1 – Wybierz terminarz dla **Nadzoru zasilania (Power supervision)** (nieдоступne dla KT-1)

2 – Wybierz terminarz dla **Przełączniki Czujnika antysabotażowego (Tamper switch)** (nieдоступny dla KT-100 oraz KT-300).

Notatka: zobacz Definiowanie terminarzy, aby dowiedzieć się więcej.

KT-200

Definiowanie urządzeń pomocniczych KT-200 (Defining KT-200 Auxiliary Devices)

1 – Z okna **Definiowanie kontrolera (Controller definitione)**, wybierz zakładkę KT-200.

2 – W sekcji **Urządzenia pomocnicze (Auxiliary devices)**, wybierz typ urządzeń wykorzystanych przy KT-200.

- Zaznacz opcję **Przełącznik REB-8**, jeżeli REB-8 jest wykorzystany, jako przełącznik. Tylko 16 przełączników może być określonych. Jeżeli dodane są REB-8, dwa ostatnie przełączniki (siedemnasty i osiemnasty) mogą zostać wykorzystane do przeprowadzenia innych działań. Musisz określić te dodatkowe akcje na liście **Dodatkowe przełączniki (Extra relay)**.

- Zaznacz **Kontroler windy KT-2252** oraz **Przełącznik REB-8**, jeżeli KT-2252 są wykorzystane, jako kontrolery windy, a REB-8, jako przełączniki tych samych kontrolerów drzwi. Maksymalnie cztery KT-2252 mogą być podłączone do kontroli windy.

- Zaznacz Kontroler windy REB-8, jeżeli REB-8 są wykorzystane, jako kontroler windy. Maksymalnie cztery REB-8 mogą być podłączone do kontroli windy.

Notatka: jeśli opcja kontrolera windy jest zaznaczona, zakładka Winda pojawi się obok zakładki KT-200.



Programowanie kontrolerów windy KT-2252 (Programming KT-2252 Elevator Controllers)

Zakładka Winda (Elevator) pozwala określić, które urządzenia pomocnicze są wykorzystane razem z KT-200 do kontroli windy, oraz to, jak są wykorzystane. Zainstalowane mogą być: REB-8 albo KR-2252 (zależnie od wybranej opcji oraz od zainstalowanej karty rozszerzenia).

1 – Z okna **Definiowanie kontrolera (Controller definition)** wybierz zakładkę KT-200.

2 – W sekcji **Urządzenia pomocnicze (Auxiliary devices)**, wybierz KT-2252 albo KT-2252 i REB-8. Wyświetli się zakładka Winda (Elevator).

3 – Aby skonfigurować kontrolery windy, wybierz zakładkę Winda (Elevator). Kiedy w użyciu są KT-2252, **Tryb windy (Elevator mode)** jest włączony.

4 – W sekcji **Tryb windy (Elevator mode)**, zaznacz odpowiednią ilość pięter.

- Wybierz 16 pięter, jeżeli KT-2252 przypada na dwie kabiny przypisane do tych samych pięter.
- Wybierz 32 piętra, jeżeli KT-2252 przypada na jedną kabinę.

Notatka: kolumna Linia dozorowa (input) odnosi się do terminali KT-2252. Jeśli piętra zostaną zdefiniowane (w menu Piętra), kolumna Piętra zawiera piętra powiązane z Liniami dozorowymi (inputs).

• W sekcji zainstalowane KT-2252 określ liczbę zainstalowanych KT-2252. Opcja jest kumulacyjna: jeżeli zaznaczony jest KT-2252 #3, KT-2252 #1 oraz # 2 też muszą być zaznaczone. Poniższa tabela przedstawia, jak KT-2252 są wykorzystywane:

Ilość kabin	Ilość pięter	Ilość KT-2252
1	8	1
1	16	1
1	32	1
1	64	2
2	8	1
2	16	1
2	32	2
2	64	4

5 – W kolumnie Piętra (Floors), wybierz piętra powiązane z terminalami KT-2252.

Notatka: kolumna Linia dozorowa (input) odnosi się do terminali KT-2252. Jeśli piętra zostaną zdefiniowane (w menu Piętra), kolumna Piętra zawiera piętra powiązane z Liniami dozorowymi (inputs).



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia



Programowanie kontrolerów windy REB-8 (Programming REB-8 Elevator Controllers)

Karty rozszerzenia przekaźnika REB-8 może być wykorzystana, jako alternatywna oraz ekonomiczna kontrola windy. Po przyłączeniu REB-8 do KT-200, oprogramowanie może kontrolować do dwóch kabin na kontroler.

1 – W oknie definiowania KT-200, wybierz opcję **Kontroler windy REB-8 (REB-8 elevator controller)**. Zakładka **Winda (Elevator)**, pojawi się obok zakładki KT-200. Sekcja definiowania REB-8 jest aktywna tylko wtedy, gdy REB-8 są wykorzystywane, jako przekaźniki.

2 – Wybierz zakładkę **Winda (Elevator)**, aby skonfigurować REB-8.

3 – Określ liczbę REB-8, które są zainstalowane na kontrolerze. Opcja jest kumulacyjna. Poniższa tabela przedstawia, jak REB-8 są przypisane do pięter i do kabin windy:

Ilość REB-8	Ilość pięter	Ilość kabin
1	1 do 8	Cab 1
2	9 do 16	Cab 1
3	1 do 8	Cab 2
4	9 do 16	Cab 2

Notatka: kolumna Linia dozorowa (input) odnosi się do terminali REB-8. Jeśli piętra zostaną zdefiniowane (w menu Piętra), kolumna Piętra zawiera piętra powiązane z Liniami dozorowymi (inputs).

4 – W kolumnie Piętra (Floors), wybierz piętra powiązane z terminalami REB-8. Zobacz: **Konfigurowanie drzwi (Doors Configuration)**, aby dowiedzieć się o definiowaniu pięter i grup drzwi.

Notatka: jeśli REB-8 jest wykorzystany jako kontroler windy nie występuje potwierdzenie pięter.



Definiowanie przekaźników REB-8 (Defining REB-8 Relays)

Kiedy REB-8 są wykorzystane, jako przekaźniki, musisz określić ile przekaźników jest zainstalowanych na KT-200. Kontroler może obsłużyć do 16 przekaźników i jednocześnie sam posiada 2 przekaźniki.

1 – W zakładce KT-200, wybierz opcję **Przekaźnik REB-8 (REB-8 relay)**.

2 – Jeżeli są wykorzystywane razem z kontrolerem KT-2252, wybierz **Kontroler KT-2252 oraz przekaźnik REB-8 (KT-2252 elevator controller and REB-8 relay)**.

3 – W sekcji **Definiowanie REB-8 (REB-8 Definition)**, wybierz opcje: **Bez REB-8**, **Jeden REB-8** lub **Dwa REB-8**.

4 – Jeżeli dodane są dwa REB-8, dwa ostatnie przekaźniki mogą zostać wykorzystane do przeprowadzenia innych działań. Musisz określić te dodatkowe akcje na liście **Dodatkowe przekaźniki (Extra relay)**.

5 – Wybierz zakładkę Status przekaźnika (**Status relay**), aby zaprogramować przekaźnik albo grupę przekaźników, które zostaną aktywowane w przypadku zajścia zdarzenia.



Definiowanie powiązań piętra KT-300 (Defining the KT-300 Elevator Floor Associations)

Notatka: zakładka Windy wyświetla się, jeśli moduły Combis zostały zdefiniowane w zakładce KT-300, jako windy.

Przypisywanie numerów pięter (Associating Floor Numbers)

- 1 – W oknie **Kontroler (Controller)**, kliknij na zakładkę windy, aby określić powiązania piętra.
- 2 – Z menu **Piętra (Floors)**, do każdego numeru wybierz piętro.
- 3 – Kliknij **Zapisz (Save)**.

Notatka: aby zdefiniować piętra, zobacz Definiowanie pięter.



Konfigurowanie modułów rozszerzeń KT-400 (Configuring the KT-400 Expansion Modules)

KT-400 wspiera moduły rozszerzające przez swoje porty rozszerzające SPI. SPI jest portem, do którego można dołączać łańcuchowo moduły rozszerzeń linii dozorowych, wyjść sterujących za pomocą 6-żyłowego przewodu.

Notatka: maksymalny pobór prądu dla portu KT-400 SPI to 500mA (terminale 12V AUX nie są wykorzystywane). Dodatkowe źródło zasilania (12 VDC, 2 Amp) jest niezbędne, jeżeli łączyn pobór prądu przekroczy 500mA. Po dodatkowe informacje sprawdź the KT-400 Installation Manual, DN1726.

Dostępne są trzy typy modułów rozszerzających:

- **KT-MOD-INP16:** moduł wejść, który dodaje 240 stref do kontrolera KT-400. Do 15 modułów wejść (16 jest użytych do konfiguracji wind) może być podłączone do KT-400, co daje łącznie 240 zewnętrznych wejść. Dodając do tego 16 wejść wewnętrznych otrzymujemy 256 wejść na KT-400. Zobacz: *KT-MOD-INP16 KT-400 Expansion Module 16-Zone Input with SPI Cable, Install Sheet, DN1776.*
- **KT-MOD-OUT16:** 16-wyjściowy moduł. Do 16 modułów wyjść może być podłączone do KT-400, do łącznej liczby 256 wyjść. Zobacz: *KT-MOD-OUT16 KT-400 Expansion Module 16-Output with SPI Cable, Install Sheet, DN1781.*
- **KT-MOD-REL8:** 8-przełącznikowy moduł rozszerzający. Do 32 modułów przełącznika może być podłączone do KT-400, do łącznej liczby 256 przełączników. Zobacz: *KT-MOD-REL8 KT-400 Expansion Module 8-Relay Output with SPI Cable, Install Sheet, DN1786.*

Poniżej znajdują się opcje powiązane z każdym modułem:

- KT-MOD-INP16: Wejścia linii dozorowej kontrolera (do 256) oraz/lub Wejścia linii dozorowej windy (do 64 na drzwi windy)
- KT-MOD-OUT16: wyjścia kontrolera (do 256) oraz/lub wyjścia windy (do 64 na drzwi windy)
- KT-MOD-REL8: przełączniki (do 256) oraz/lub wyjście windy (do 64 na drzwi windy)

Notatka: dostępne są 4 przełączniki na KT-400. Sprawdź numery przełączników, aby uniknąć redundancji, chyba, że została zaplanowana. Ustawienie przełączników 9-16 jest domyślne.

1 – Jeżeli moduł(y) jest podłączony do KT-400, kliknij **Konfiguruj moduł SPI (SPI module configuration)**. Pojawi się menu **Ustawienia modułów rozszerzających (The Expansion modules setup)**.



Jeśli chcesz...	... to przejdź do
Skonfigurować moduł wejść KT-MOD-INP16	Krok 2
Skonfigurować moduł wyjść KT-MOD-OUT16	Krok 5
Skonfigurować moduł wyjścia KT-MOD-REL8	Krok 6
Zmodyfikować konfigurację istniejącego modułu rozszerzającego	Krok 7

2 – Aby dodać **KT-MOD-INP16**, wybierz zakładkę **Moduł Linii dozorowej (Input Module)** i kliknij **Dodaj (Add)**. Jeżeli wylistowany jest więcej niż jeden moduł, upewnij się, że wybrałeś prawidłowy. Przypisz nazwy do modułów oraz wybierz opcje.

3 – Zaznacz pole **Włącz: Podwójny końcowy opornik JP4 (DEOL: Double end-of-line resistor JP4 On)**, aby określić moduł KT-MOD-INP16 w DEOL.

Notatka: cała płyta rozszerzeń jest wykorzystana do dostarczenia 8 Linii dozorowych (inputs) z DEOL. Te 8 Linii dozorowych (inputs) jest dodane do następnej grupy 8 Linii dozorowych (inputs). Na przykład, jeśli Linie dozorowe (inputs) #33-40 są podłączone do modułu DEOL, Linie dozorowe (inputs) #33-40 oraz #41-48 nie będą dostępne dla innych modułów.

Linie dozorowe (inputs) 1-16 są zarezerwowane dla Linii dozorowyc (inputs) KT-400.

4 – Wybór liczby wejść może zostać zrobiony na dwa sposoby: przy pomocy menu albo poprzez **Pole rozszerzonego wyboru (Extended selection box)**. Kliknij prawym na selekcji menu wejść i wybierz **Pole rozszerzonego wyboru (Extended selection box)**.

Notatka: jest to wyjątkowy warunek. Nie możesz wybrać tego samego obiektu z menu Linie dozorowe (Inputs) oraz z menu Linie dozorowe windy, ponieważ będzie on zdublowany, a system nie akceptuje żadnych duplikatów. Na przykład, Wejścia linii dozorowej #17-24 nie mogą być wybrane dwa razy.



5 – Aby dodać **KT-MOD-OUT16**, wybierz zakładkę **Moduł Wyjść (Output Module)** i kliknij **Dodaj (Add)**. Pojawi się menu, w którym zaznaczysz moduły, które chcesz dodać. Przypisz nazwy do modułów oraz wybierz opcje.

6 – Aby dodać **KT-MOD-REL8**, wybierz zakładkę **Moduł Wyjść (Output Module)** i kliknij **Dodaj (Add)**. Pojawi się menu, w którym zaznaczysz moduły, które chcesz dodać. Przypisz nazwy do modułów oraz wybierz opcje.

Ostrzeżenie: dostępne są 4 przekaźniki na KT-400. Sprawdź przypisane numery do przekaźników, aby nie dopuścić do redundancji, chyba, że była zaplanowana.

7 – Z zakładki **Podsumowanie (Summary)**, możesz modyfikować wszystkie moduły. Upewnij się, że prawidłowy moduł jest zaznaczony w lewej kolumnie, zanim zaczniesz przeprowadzać modyfikacje po prawej stronie.

8 – Kiedy skończysz konfigurowanie modułów rozszerzenia, kliknij **OK**, aby wrócić do okna konfiguracji KT-400.

Notatka: zobacz Konfigurowanie połączenia.



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia



Moduł wejść wyjść (ioModule)

Aby zdefiniować KT-MOD-IO16 dla KT-400 lub kontrolera KT-1, kliknij zakładkę ioModule i uzupełnij następujące kroki:

- 1 - Wybierz kontroler z listy Controller i kliknij przycisk ADD.
- 2 - W obszarze ioModule wpisz nazwę ioModule w polu językowym.
- 3 - W polu Numer seryjny wpisz numer seryjny.
- 4 - Wybierz jeden z następujących banków terminali:
 - Terminale 1 - 4
 - Terminale 5 - 8
 - Terminale 9 - 12
 - Terminale 13 - 16

Dla każdego terminala wybierz jedną z następujących opcji akcji:

- o **Nieużywany:** jest to ustawienie domyślne. Wybierz, aby wskazać, że terminale nie są używane.
- o **Użyj jako Linii dozorowej:** wybierz, aby użyć zacisków jako wejść. EntraPass używa tego samego ustawienia dla EOL jako ustawienia kontrolera. Jeśli chcesz zmienić ustawienia EOL, użyj menu Linie Dozorowe. Więcej informacji patrz Konfigurowanie określonych parametrów kontrolera (Configuring Specific Controller Parameters) W polu Linie dozorowe wybierz z listy.

Uwaga:

Nie można używać wyjść sterujących dla tych samych pięter na różnych urządzeniach. Gdy używasz go na jednym urządzeniu, nie jest już dostępne, dopóki nie usuniesz konfiguracji.

- o **Użyj jako przekaźnika:** wybierz, aby użyć zacisków wejść / wyjść jako przekaźników. W polu Przekazniki wybierz przekaźnik z listy.

Uwaga:

Możesz zdefiniować bank przekaźników na wielu urządzeniach, które wzajemnie się odzwierciedlają.

As Użyj jako windy: wybierz, jako wyjście sterujące / Użyj jako Przyciski wyboru piętra. Dwie dodatkowe opcje stać się dostępnym:

- Użyj jako wyjścia
- Użyj jako potwierdzenia piętra (dane wejściowe)

Użyj jako wyjście sterujące

a - W polu Winda wybierz czytnik z listy.

b - W polu Windy wyj. Ster. Przypisz wyjścia do do terminali.

Można zdefiniować bank wyjściowy windy na wielu windach, które odzwierciedlają się wzajemnie.



Użyj jako przyciski wyboru piętra (dane wejściowe)

a - W polu Winda wybierz czytnik z listy.

b - W polu Wejścia linii doz. przypisz linie doz. do terminali.

Uwaga:

Nie można używać banku wejściowego na wielu urządzeniach. Kiedy używasz go na jednej windzie, nie jest już dostępne, dopóki nie usuniesz konfiguracji.

Terminale 9 - 12

Oprócz opcji **Nie używane**, **Użyj jako Linii doz.owej**, **Użyj jako przekaźnika** i **Użyj dla windy** jest dostępne dla terminali 9 - 12.

Użyj jako SPI: wybierz, aby użyć zacisków 9-12 jako przekaźników SPI. Oprócz zdefiniowanych 32 modułów przekaźnikowych SPI bezpośrednio na porcie SPI można dodać kolejne 32 moduły SPI za pomocą karty ioModule.

Aby kontynuować konfigurację, wykonaj następujące kroki:

- a - Kliknij kartę **SPI** i kliknij **moduł Wyjście** na karcie **ioModule**.
- b - Jeśli zdefiniowałeś więcej niż jeden **ioModule**, wybierz ten, który chcesz z listy **ioModule**.
- c - W zakładce **Przekaźnik 1 - 8** wybierz jedną z następujących opcji:
 - **Nie używany**
 - **Używane jako przekaźniki**
 - **Używaj jako wyposażenia windy**

Uwaga:

Można zdefiniować przekaźniki w module rozszerzenia SPI i w module ioModule. Na przykład dla KT-1 kontroler, jeśli zdefiniujesz przekaźniki 1-4 na ioModule, a moduł rozszerzenia SPI, zapali się na kontroler, ioModule i moduł rozszerzenia SPI.

5 - Aby usunąć moduł, kliknij przycisk **USUŃ**.



Włącz czytnik Wyjścia (Enable Exit Reader)

Ta opcja zwiększa liczbę czytników do 8 (na 4 drzwiach) dla kontrolerów KT-400 oraz KT-401, kiedy korzystają z 31 bitowych czytników ioProx XSF oraz ioProx UK. W ten sposób drugi czytnik może być podłączony do kontrolera. Drugi czytnik zachowa takie same wartości, jak pierwszy:

- Tryb zaryglowania drzwi (Door lock mode)
- Czas odryglowania (Unlock time)
- Czas otwarcia (Open time)
- Rozszerzony czas odryglowania (Extended Unlock time)
- Rozszerzony czas otwarcia (Extended Open time)
- Terminarz odryglowania (Unlock Schedule)
- Podgląd wideo (Video View)
- Grafika (Graphic)
- Wszystkie opcje Czujnika stanu drzwi (All "Door Contact" features)

- Aktywacja przekaźnika dla zdarzeń Drzwi, za wyjątkiem „Wymuszenie otwarcia”.

Drugi drzwi zostaną automatycznie oznakowane z pierwszymi oraz dodatkowym słowem **WYJŚCIE (EXIT)** na końcu.

1 – Z zakładki KT-400, pod **Włącz czynn timer wyjścia (Enable exit reader)**, wybierz drzwi, dla których czytnik ma zostać włączony.

2 – Kliknij **Zapisz (Save)**.

Notatka:

- Opcja jest dostępna wyłącznie, gdy czytniki ioProx XSF oraz ioProx UK są wykorzystane pod **Ogólne/Czytnik i klawiatura (General/Reader and keypad)**. Jeżeli wybrany jest inny rodzaj czytnika, opcja nie jest dostępna.
- Pewne opcje nie są dostępne dla drugiego czytnika, ponieważ są one już zaprogramowane dla pierwszego.
- Jeżeli odznaczysz czytnik wyjścia pod kontrolerem, czytnik wyjścia zostanie wyłączony. Nie jest możliwe usunięcia czytnika wyjścia.



Definiowanie stref lokalnych kontrolera KT-400 (Defining the KT-400 Controller Local Areas)

Notatka: opcja Strefa lokalna kontrolera (Controller local area) jest dostępna tylko dla kontrolera KT-400 dla multi obiektowej bramki. Zobacz Definiowanie kontrolera.

- 1 – Kliknij zakładkę Strefa lokalna kontrolera (**Controller local area**), aby określić do 4 stref lokalnych.
- 2 – Przypisz nazwę dla obu języków dla strefy lokalnej pierwszego kontrolera.
- 3 – Wybierz **Zapomnij terminarz (Forgive schedule)** z menu.
- 4 – Wprowadź maksymalną ilość kart w polu **Próg (Cards threshold)**.
- 5 – Zaznacz pole Dostęp zabroniony przy pełnej strefie (**Deny access on area full**), aby uniemożliwić wejście do strefy nowym użytkownikom po przekroczeniu progu.
- 6 – Kliknij na przycisku trzech kropek, aby wybrać przekaźnik albo grupę przekaźników do aktywacji w momencie, gdy próg zostanie osiągnięty.
- 7 – Powtórz kroki 2-6 dla każdego kontrolera strefy lokalnej.



Definiowanie powiązań piętra KT-400 (Defining the KT-400 Elevator Floor Associations)

Notatka: zakładka Winda wyświetla się tylko wtedy, kiedy moduły rozszerzeń zostały zdefiniowane, jako Wejścia linii dozorowej (inputs) oraz wyjścia (outputs) dla wind w zakładce KT-400.

Dla kontrolera KT-400 istnieje możliwość wybrania do czterech wzorców do określenia drzwi i numerów pięter, które będą powiązane z każdym wzorcem. Domyslnie, wzorzec 1 określa wszystkie numery drzwi.

- 1 – W oknie **Kontroler (Controller)**, kliknij na zakładkę windy, aby określić powiązania piętra.
- 2 – W zakładce Winda, kliknij **Wzorzec #2 (Pattern #2)**, a następnie zaznacz odpowiedni numer Drzwi.
- 3 – Z menu Piętra (Floors) wybierz odpowiedni numer piętra, który zostanie przypisany do numeru drzwi i numeru wzorca.
- 4 – Powtórz kroki 2-3 dla każdego wzorca.
- 5 – Kliknij **Zapisz (Save)**.

Notatka: aby zdefiniować piętro, zobacz Definiowanie pięter.



KT-1

Przycisk zarejestrowania (Enrollment Button)

Przycisk zarejestrowania jest wykorzystany do wysłania do EntraPass prośby „zarejestruj mnie”, zawierającej status kontrolera z:

- Adresem IP (IP address)
- Informacją o zasilaniu (PoE albo 12 VDC)
- Pełnym statusem

1 – Instalator naciska **Przycisk zarejestrowania (enrollment button)**.

2 – Kontroler wysyła informację przez okres 10 minut, w 30 sekundowych odstępach.

3 – Po upływie 10 minut kontroler przestaje wysyłać informacje.

Notatka: aby proces rejestrowania był dostępny dla każdego operatora, musi zostać najpierw włączony w System/Poziom bezpieczeństwa/Urządzenia/Połączenie/Rejestracja.

Po otrzymaniu zgłoszenia prośby o zarejestrowanie, w prawej-dolnej części głównego okna stacji roboczej wyświetli się oznaczona cyfra. Określa ona liczbę nieprzypisanych kontrolerów. Kiedy występuje tylko jeden nieprzypisany kontroler, kliknij dwukrotnie na oznaczonej liczbie, aby otworzyć Kreator Rejestrowania (**Enrollment Wizard**). Postępuj według instrukcji wyświetlanych na ekranie. Możesz również kliknąć prawym przyciskiem myszy na oznaczonej liczbie, aby wyświetlić menu z następującymi opcjami:

- **Zdefiniuj (Define)**: wyświetli Kreatora Rejestrowania (Enrollment Wizard).
- **Full status (Full Status)**: wyświetla okno pełnego statusu. Wyświetla również adres IP, rodzaj zasilania oraz pełne informacje statusowe.
- **Usuń (Delete)**: usuwa wybrany kontroler z listy.
- **Przypisz do konta (Assign to an account)**.



Lista nieprzypisanych kontrolerów (The Unassigned Controllers List)

Kiedy EntraPass otrzymuje dane od KT-1 odnośnie procesu zarejestrowania dodaje on kontroler do listy nieprzypisanych kontrolerów. Generowane jest wtedy zdarzenie „**Dodano kontroler do listy nieprzypisanych kontrolerów**” ("Controller was added to the unassigned list") z następującymi parametrami:

- Opis bramki
- Adres MAC
- Typ urządzenia

Lista nieprzypisanych kontrolerów wyświetla:

- Datę i czas dodania bramki do listy
- Model kontrolera
- Adres MAC
- Numer seryjny
- Odbierany adres IP

Notatka: lista nieprzypisanych kontrolerów może mieć 100 pozycji.

Rejestrowanie Bramki Viedo lub Video Vault (Video Gateway or Video Vault enrolment)

Gdy bramka wideo lub Viedo Vault odbiera połączenie wychodzące, odbiera następujące elementy informacji przychodzące z rejestratorów:

- Nazwa
- Numer seryjny
- Adres IP

Powyższa lista pozostaje w trybie oczekiwania, gotowa do przypisania do konta hattrix lub zdefiniowanego Corporate Edition lub Global Edition. Na stacji roboczej liczba oczekujących rejestracji jest wyświetlana w dolnej prawej sekcji paska stanu. Kliknij dwukrotnie etykietę rejestracji oczekującej, aby otworzyć następujący raport:

Kolumna	Opis
Żądanie daty	Data otrzymania żądania
Konto	Identyfikuje czy konto jest wybrane lub przypisane
Ikona	Serwer Video
Model	Exacq model
Adres MAC	Adres MAC rejestratora
Żądanie od	Adres IP rejestratora, który wysłał żądanie



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia

Po wybraniu rejestracji kliknij dwukrotnie rejestrację, aby wyświetlić menu kontekstowe. The dostępne są następujące opcje:

Kolumna	Opis
Definiuj	Otwiera okno serwera wideo, które EntraPass wypełnia wstępnie informacjami odebrane z połączenia wychodzącego, które jest aktywnym kontem. Zmień nazwę DVR i zapisz go.
Usuń	monituje o potwierdzenie i usunięcie jednostki z listy.

Po zdefiniowaniu rejestratora DVR za pomocą rejestracji otworzy się okno Serwer wideo z wypełnionymi polami informacje otrzymane z połączenia wychodzącego. Po zdefiniowaniu jednostki DVR EntraPass ją usuwa z listy.

Jeśli wprowadzisz nieprawidłowe dane logowania, zostanie wyświetlony komunikat o błędzie. Jeśli import się powiedzie, a zostanie wyświetlone okno potwierdzenia. Po kliknięciu przycisku Zapisz szczegóły kamery są automatycznie wyświetlane nazywa. Następnie możesz zmienić nazwę rejestratora na karcie Parametry serwera. Aby zachować nazwę zaimportowane kamery, zaznacz pole wyboru Zastąp nazwę kamery z DVR, jeśli wyczyścisz to pole wyboru, operatorzy mogą zmienić nazwę importowanej kamery.



Dodawanie czytnika ioSmart

Wykonaj czynności opisane w [Jak skonfigurować czytniki ioSmart](#), aby dodać czytnik ioSmart.



Wiadomość o przepełnieniu bufora zdarzeń kontrolera (Controller Event Buffer Overflow Message)

Kiedy kontroler zostanie odłączony od serwera, bufor kontrolera zaczyna zbierać zdarzenia kontrolera. Kiedy bufor zostanie zapełniony, przesyła najstarsze zdarzenia do pobocznego bufora (50 do 100 bitów), który zawsze mieści 50 zdarzeń. Kiedy komunikacja zostanie przywrócona, system zaczyna wiadomości na Pulpi Wiadomości, aby wskazać, że bufor jest pełny i zdarzenia są z niego usuwane.

- Kontroler usuwa wiadomości w kolejności PDPU (Pierwsza Dodana, Pierwsza Usunięta). Tym samym, najstarsze wiadomości będą usunięte pierwsze.
- Kiedy kontroler zostanie ponownie podłączony do serwera, zdarzenia kontrolera zostaną przesłane na Listę Wiadomości wszystkie naraz, według kolejności: zdarzenia z pobocznego bufora; informacja o przepełnieniu bufora; lista zdarzeń wygenerowanych podczas czasu, gdy kontroler był odłączony od serwera.

Konfiguracja modułów Combust KT-300 (KT-300 Combust modules)

Pięć modułów Combust może zostać podłączone do KT-300:

- **KT-PC4108** (8-strefowy moduł rozszerzeniowy). Ten moduł posiada wejście czujnika antysabotażowego.
- **KT-PC4116** (16-strefowy moduł rozszerzeniowy). Ten moduł posiada wejście czujnika antysabotażowego.
- **KT-PC4204** (4-przełącznikowy moduł rozszerzeniowy z zasilaczem). Ten moduł posiada wejście czujnika antysabotażowego oraz wbudowany zasilacz 12VDC, 1A.
- **KT-PC4216** (16-strefowy wyjściowy moduł rozszerzeniowy). Może być wykorzystywany przy windach, chociaż może pojawić się potrzeba zainstalowania dodatkowego sprzętu.
- **KT-LCD3** (32-znakowy LCD Kantech). LCD zielone (stan normalny), czerwone (awaria zasilania), żółte (problem).

1 – jeśli moduł Combust jest zainstalowany na kontrolerze KT-300, kliknij przycisk konfiguracji modułu Combust. Niezidentyfikowane terminale Combust są oznaczone na czerwono (flagi/punkty). Po zdefiniowaniu modułu zostaje on oznaczony na zielono.

2 – aby zdefiniować moduł wybierz go, a następnie kliknij przycisk Definiuj. Pojawi się komunikat Wprowadź numer seryjny modułu Combust.

3 – wprowadź numer seryjny i kliknij OK.

Notatka: aby otrzymać ten numer musisz uruchomić Przełącznik Tamper albo nacisnąć dowolny klawisz na klawiaturze. Numer seryjny Combust jest wyświetlony na Pulpicie wiadomości.

4 – przypisz nazwy dla modułów.

5 – sprawdź opcje powiązane z modułem, który chcesz skonfigurować.

Notatka: opcje wykorzystania modułu różnią się zależnie od wybranego modułu Combust. Na przykład, zainstalowanie KT3-LCD oraz zaznaczenie opcji Combust niski pobór mocy, przy jednoczesnym wybraniu Wyświetl datę i godzinę pozwoli KT-300 raportować niski pobór mocy oraz wyświetlić datę oraz godzinę.

Rodzaj Combust	Opcje	Opcje dodatkowe
KT3-LCD	Słabe zasilanie Combust, wyświetl datę i czas	Brak
KT-PC4108	Alarm czujnika antysabotażowego, Słabe zasilanie Combust	Moduł 8-wejściowy
KT-PC4116	Alarm czujnika antysabotażowego, Słabe zasilanie Combust	Moduł 16-wejściowy
KT-PC4204	Alarm czujnika antysabotażowego, Słabe zasilanie Combust, Słaba bateria, Awaria zasilania	Wykorzystany, jako przełącznik 1-4
KT-PC4216	Alarm czujnika antysabotażowego, Słabe zasilanie Combust	Wykorzystany, jako wyjścia



6 – zaznacz opcję Słabe zasilanie Combust (**Combust low power**), aby KT-300 raportował problemu ze słabym zasilaniem.

7 – zaznacz Wyświetl datę i czas, aby LCD mogło wyświetlić datę i czas.

8 – kiedy zakończysz konfigurowanie modułu Combust, kliknij OK i wróć do zakładki Status przekaźnika.

9 – powiąż Lokalny przekaźnik aktywacji z Awarią zasilania, Awarią Combust oraz Słabym zasilaniem Combust (bramki multi obiektowe). Jeśli chcesz przypisać do tego konkretny przekaźnik możesz kliknąć na przycisk trzech kropek i wybrać konkretny przekaźnik albo grupę przekaźników.

Notatka: aby skonfigurować przekaźnik lokalnej aktywacji musisz skonfigurować przekaźniki (Urządzenia > Przekaźniki), a następnie wybrać konkretny przekaźnik do lokalnej aktywacji.

10 – pod Rodzajem powiadomień priorytetowych (**Priority call type**) przypisz rodzaj powiadomienia, który najlepiej odpowiada raportowaniu awarii. Aby mieć dostęp do tej opcji połączenie musi być modemowe.

Notatka: aby dowiedzieć się więcej, zobacz Konfigurowanie połączenia.



Konfiguracja modułów rozszerzeń (Expansion Modules Setup)

Konfiguracja Modułu Wejścia linii dozorowej KT-MOD-INP16 (Input Module KT-MOD-INP16 Configuration)

1 – Aby dodać **KT-MOD-INP16**, wybierz zakładkę **Moduł Wejścia linii dozorowej (Input Module)** i kliknij **Dodaj (Add)**. Nadaj nazwę modułom i wybierz odpowiednie opcje.

2 – Zaznacz pole **Włącz: Podwójny końcowy opornik JP4 (DEOL: Double end-of-line resistor JP4 On)**, aby określić moduł KT-MOD-INP16 w DEOL.

Notatka: cała płyta rozszerzeń jest wykorzystana do dostarczenia 8 Wejść linii dozorowej (inputs) z DEOL. Te 8 Wejść linii dozorowej (inputs) jest dodane do następnej grupy 8 Wejść linii dozorowej (inputs). Na przykład, jeśli Wejścia linii dozorowej (inputs) #33-40 są podłączone do modułu DEOL, Wejścia linii dozorowej (inputs) #33-40 oraz #41-48 nie będą dostępne dla innych modułów.

Wejścia linii dozorowej (inputs) 1-16 są zarezerwowane dla Wejścia linii dozorowej (inputs) KT-400.

3 – Wybór liczby wejść może zostać zrobiony na dwa sposoby: przy pomocy menu albo poprzez **Pole rozszerzonego wyboru (Extended selection box)**. Kliknij prawym na selekcji menu wejść i wybierz **Pole rozszerzonego wyboru (Extended selection box)**.

Notatka: jest to wyjątkowy warunek. Nie możesz wybrać tego samego obiektu z menu Wejścia linii dozorowej (Inputs) oraz z menu Wejścia linii dozorowej windy, ponieważ będzie on zdublowany, a system nie akceptuje żadnych duplikatów. Na przykład, Wejścia linii dozorowej #17-24 nie mogą być wybrane dwa razy.

Konfigurowanie modułu wyjścia KT-MOD-OUT16

Aby dodać **KT-MOD-OUT16**, wybierz zakładkę **Moduł Wyjść (Output Module)** i kliknij **Dodaj (Add)**. Pojawi się menu, w którym zaznaczysz moduły, które chcesz dodać. Przypisz nazwy do modułów oraz wybierz opcje.

Konfigurowanie modułu wyjścia KT-MOD-REL8

Aby dodać **KT-MOD-REL8**, wybierz zakładkę **Moduł Wyjść (Output Module)** i kliknij **Dodaj (Add)**. Pojawi się menu, w którym zaznaczysz moduły, które chcesz dodać. Przypisz nazwy do modułów oraz wybierz opcje.

Ostrzeżenie: dostępne są 4 przekaźniki na KT-400. Sprawdź przypisane numery do przekaźników, aby nie dopuścić do redundancji, chyba, że była zaplanowana.

Konfigurowanie opcji modyfikowania istniejącego modułu rozszerzenia (Modify an Existing Expansion Module Configuration)

1 - Z zakładki **Podsumowanie (Summary)**, możesz modyfikować wszystkie moduły. Upewnij się, że prawidłowy moduł jest zaznaczony w lewej kolumnie, zanim zaczniesz przeprowadzać modyfikacje po prawej stronie.

2 - Kiedy skończysz konfigurowanie modułów rozszerzenia, kliknij **OK**, aby wrócić do okna konfiguracji KT-400.



Konfiguracja Kantech Telephone Entry System (KTES) (Kantech Telephone Entry System (KTES) Configuration)

Kantech Telephone Entry System (KTES), jest systemem telefonicznym odpowiednim dla małych i dużych aplikacji z osobnymi systemami kontroli dostępu, albo dla aplikacji, które wymagają tylko wejścia telefonicznego. System przydziela gościom kontrolę dostępu do różnych aplikacji: apartamentów, ogrodzonych osiedli, mieszkań, biur, fabryk, etc. Goście korzystają z KTES, aby komunikować się bezpośrednio z abonentem i są w łatwy sposób zidentyfikowani przez komunikację głosową. Abonent może udzielić lub odmówić dostępu bezpośrednio z linii telefonicznej (stacjonarnej lub komórkowej).

KTES został zaprojektowany, jako jednostka samodzielna system kontroluje jedne drzwi, pomocnicze przekaźniki oraz zamki. Przy większych obiektach, KTES jest zintegrowany z EntraPass poprzez multi-obiektową bramkę i kontrolery KT, aby zapewnić pełną kontrolę nad dostępem. Całe programowanie systemu może zostać wykonane bezpośrednio z klawiatury albo zdalnie z PC przez modem, połączenie Ethernet albo RS-485.

System raportuje wszystkie zdarzenie bezpośrednio do EntraPass, skąd możesz pełen wykaz zdarzeń. Aby dowiedzieć się więcej na temat instalacji i programowania KTES sprawdź *KTES Installation Manual*, DN1769 oraz *KTES Programming Manual*, DN1770.

Notatka: dla zachowania ciągłości ustawień oraz niezawodności Kantech wspiera obecnie modemy US Robotics Sportster. Nawet, jeżeli inne typy modemów są dostępne, rekomendujemy stosowanie modemów US Robotics.



Definiowanie parametrów ogólnych dla KTES (Defining General Parameters for the KTES)

1 – Na pasku narzędzi **Urządzenia**, wybierz przycisk **KTES**.

Notatka: przy konfigurowaniu KTES musisz wybrać multi obiektową bramkę.

Notatka: zobacz Konfiguracja kontrolerów pomocą Instalacji ekspresowej (Configuring a KTES Using Express Setup), aby dowiedzieć się więcej.

2 – Wybierz **Filtr obiektu (Site filter)** z pierwszej listy.

3 – Wybierz **Bramkę**.

4 – Z listy **Połączenie**, wybierz połączenie, na którym zainstalowany jest kontroler.

5 – Z listy KTES wybierz KTES, który chcesz definiować. Po wybraniu pojawi się pole, w którym możesz zmienić nazwę wybranego KTES.

Notatka: zobacz Konfigurowanie połączenia, aby dowiedzieć się więcej.

6 – Z zakładki Ogólne (General), określ ustawienia połączenia dla gościa:

- **Czas rozmowy (Talk time):** maksymalny czas, w sekundach, na połączenie pomiędzy gościem a abonentem (od 10 sekund do 59 minut 59 sekund). Domyślnie: 40 sekund.
- **Rozszerzony czas rozmowy (Extended talk time):** maksymalny czas, w sekundach, na rozszerzone połączenie pomiędzy gościem a abonentem (od 10 sekund do 59 minut 59 sekund). Domyślnie: 60 sekund.
- **Ostrzeżenie przed końcem czasu rozmowy (Talk time remaining warning):** system wysyła ostrzegawczy dźwięk w określonym momencie, aby poinformować o kończącym się czasie rozmowy (od 10 sekund do 59 minut 59 sekund przed końcem rozmowy). Domyślnie: 10 sekund.
- **Ilość dzwonek przed odebraniem (Number of rings before answer):** maksymalna liczba dzwonek przed odebraniem (od 4 do 16). Domyślnie: 5.
- **Rozszerzona ilość dzwonek przed odebraniem (Extended number of rings before answer):** maksymalna liczba dzwonek w opcji rozszerzonej przed odebraniem (od 4 do 16). Domyślnie: 10.



7 – Określ opcje Zamka (Postal Lock):

Notatka: zobacz Konfigurowanie Wejścia linii dozorowej (Input), aby dowiedzieć się więcej.

- **Czujnik stanu zamka (Postal lock contact):** to jest Wejście linii dozorowej odpowiadające zamkowi (od 0 do 4). Wybierz Wejście linii dozorowej i kliknij **OK**.

Notatka: zobacz Konfigurowanie terminarzy, aby dowiedzieć się więcej.

8 – wyłącz opcję Odpytywania KTES: zaznacz to pole, jeśli chcesz wyłączyć KTES. KTES nie będzie wtedy odpytywany. Domyślnie: wybrana.

9 – Określ opcje Listy abonentów:

- **Pojemność listy abonentów (Tenants list capacity):** domyślnie 250, chyba że zarejestrowanych jest 500, 1000 albo 3000 abonentów w sumie.

Notatka: pamiętaj, że jesteś ograniczony opcjami zakupionymi wraz z oprogramowaniem. Jeżeli zarejestrowałeś wiele opcji KTES pamiętaj, aby przypisać je do odpowiednich obiektów KTES.

- **List abonentów (Tenants list):** wybierz listę. Domyślnie: brak.

Notatka: zobacz Lista abonentów, aby dowiedzieć się więcej.

- **Użyj wszystkich abonentów z listy (Use all tenants from list):** zaznacz to pole, aby uwzględnić wszystkich abonentów z listy. Ewentualnie, przy pomocy przycisku **Wybierz (Customize)**, możesz wybierać abonentów.
- Przycisk **Drukuj (Print)** wysyła listę do wydruku do drukarki wybranej przez użytkownika.
- Wybierz **Grafikę** albo **Podgląd wideo**, do których przypisana jest bramka.



Definiowanie parametrów KTES (Defining the Kantech Telephone Entry System parameters)

1 – Z okna **KTES**, wybierz zakładkę **KTES**.

2 – Określ Ogólne opcje:

- **Numer seryjny (Serial number)**: numer ten jest unikatowy dla każdego **KTES**. Jest wykorzystywany do komunikacji pomiędzy **KTES** oraz oprogramowaniem EntraPass. Domyślnie: 00000000.
- **Włącz opóźnienie fail-soft (Enable fail-soft delay)**: określ opóźnienie zanim EntraPass wejdzie w tryb asekuracyjny i uzna komunikację z KTES za przerwana. Przedział od 10 sekund do 4 minut 15 sekund. Domyślnie: 45 sekund.
- **Opornik EOL**: ten parametr określa przerwanie wejścia, jako: **Brak (None)** dla braku końcowego opornika, **Pojedynczy (Single)** dla pojedynczego **końcowego opornika (5.6K)**, albo **Podwójny (Double)** dla podwójnego końcowego opornika (2 x 5.6K). Domyślnie: **Brak**.

3 – Określ parametry **Konfiguracji regionalnej (Regional configuration)**:

- **Typ linii (Line Type)**: określ ten parametr, aby wybrać typ linii telefonicznej wykorzystanej przez system. Możliwe jest: **Tonowe** lub **Impulsowe**. Domyślnie: Tonowe.

Notatka: wybieranie Impulsowe jest niedostępne dla Nowej Zelandii.

- **Ustawienia regionalne linii telefonicznej (Telephone line regional setting)**: ta opcja musi być ustawiona, aby określić kod kraju, który powinien być używane przez KTES. Domyślnie: USA/Kanada (0). Lista wyświetli dostępne kraje:



- **Podstawa czasu (Time base):** główna podstawa czasu pochodzi z wejścia zasilania AC (50Hz, 60Hz). Podstawa czasu zostanie automatycznie zamieniona na wewnętrzną **Xtal** w przypadku awarii zasilania. Domyślnie: 60Hz.
- **Monitoring linii (Line monitoring):** linia jest monitorowana, kiedy jest zajęta albo rozłączona w momencie, gdy opcja jest zaznaczona. Domyślnie: zaznaczona.

4 – Określ ustawienia Odpowiedzi abonentów:

- **Przycisk klawiatur: Przyznanie dostępu przez abonenta (Keypad key for access granted by tenant):** domyślnie: 9.
- **Przycisk klawiatur: Dostęp zabroniony przez abonenta (Keypad key for access denied by tenant):** domyślnie: *.
- **Przycisk klawiatur: Aktywuj pomocniczy przekaźnik (Keypad key for auxiliary relay activated by tenant):** przyznanie dostępu dla gościa, gdy ten korzysta z drugiego wejścia. Domyślnie: puste.

5 – Określ opcja Interfejsu Wiegand:

- **Typ czytnika:** format wyjścia interfejsu Wiegand, który jest wysłany do KTES. Domyślnie: **Kantech XSF**.
- **Pobranie sterownika czytnika (Reader's Driver download):** kliknij, aby otworzyć okno wyboru i wybrać sterownik do pobrania.
- **Integracja Wiegand z kontrolerem dostępu (Wiegand integration with an access controller):** wybrania tej opcji wskazuje, że KTES jest podłączony do kontrolera dostępu. W innym przypadku działa w trybie Samodzielnym.



Definiowanie parametrów języka oraz wiadomości powitania (Defining the Language and Welcome Message Parameters)

1 – Z okna KTES, wybierz **Języki i wiadomości powitania (Languages and Welcome messages)**.

2 – Określ **Dostępne języki (Enabled languages)**: wybierz języki, które są udostępnione. Domyślnie: brak wybranych.

3 – Określ **Wybrane języki (Custom languages)**: wybierz języki, które są dostępne dla użytkownika dodatkowo do **Dostępnych języków**. Użyj przycisku „+”, aby dodać następny język. Domyślnie: **Brak**.

Notatka: zobacz Edytor słownika (Vocabulary Editor), aby dowiedzieć się więcej.

4 – Określ **Domyślny język KTES (Default KTES language)**: wybierz język domyślny dla KTES. Domyślnie: **Brak**.

5 – Określ **Wiadomości powitania (Welcome Messages)**:

- Wprowadź wiadomość, która ma być wyświetlona dla każdego udostępnionego języka. Domyślnie: puste.
- Wprowadź opóźnienie wyświetlania (od 0 sekund do 4 minut 15 sekund). Domyślnie: 2 sekundy.
- Powtórz oba kroki dla drugiej wiadomości.

6 – Kliknij przycisk **Zapisz (Save)**.

Znaki specjalne (Special Characters)

Poprzez połączenie poleceń znajdujących się w tabelce poniżej, może wyświetlić bieżącą godzinę i datę **KTES** według różnych formatów. Na przykład:

- Kompletna, bieżąca data wg międzynarodowego formatu: &yyy/&o/&d = 2007/01/18



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia

- Kompletna, bieżąca data w formacie amerykańskim: &o/&d/&y = 01/18/07
- Kompletna, bieżąca godzina w formacie 24 godzinnym: &h:&m:&s = 14:50:55
- Kompletna, bieżąca godzina w formacie 12 godzinnym (am/pm): &h:&m:&s&a = 02:50:55pm
- Bieżący dzień w trzyliterowym formacie: &ww = mon
- Bieżący dzień w dziesięcioliterowym formacie: &wwwwwwwww = wednesday
- Bieżący miesiąc w trzyliterowym formacie: &oo = jan
- Bieżący miesiąc w dziewięcioliterowym formacie: &Ooooooooo = January
- Kompletna, bieżąca data w formacie liczbowo/literowym: &ww &oo &d &yyy = thu jan 18 2007

Wyświetlanie	Format
Godzina w formacie 24h	&h
Godzina w formacie 12h	&h&a
Minuty	&m
Sekundy	&s
Dziesięciolecia	&y
Rok	&yyy
Miesiąc	&o
Data	&d
Dzień tygodnia	&ww do &wwwwwwwww
Obecny miesiąc w formacie txt	&oo do &oooooooo



Definiowanie parametrów Opcji (Defining the Options Parameters)

1 – Z okna KTES wybierz zakładkę **Opcje**.

2 – Określ **Ustawienia LCD**:

- **Ukryj numer PIN**: wybierz, aby ukryć numer PIN abonenta. Domyślnie: niewybrane.
- **Opóźnienie podświetlenia**: określa maksymalne opóźnienie, zanim podświetlenie zostanie wyłączone (od 0 sekund do 4 minut 15 sekund). Domyślnie: 20 sekund.
- **Opóźnienie wybierania**: określa maksymalne dopuszczalne opóźnienie pomiędzy wybieraniem kolejnych przycisków przy wprowadzaniu ciągu znaków na klawiaturze (od 0 sekund do 4 minut 15 sekund). Domyślnie: 2 sekundy.
- **Czas na wyszukiwanie abonenta**: wartość ta określa maksymalne opóźnienie dopuszczalne pomiędzy każdym wciśnięciem klawisza, zanim sekwencja zostanie anulowana (od 5 sekund do 4:15 minut). Domyślnie: 15 sekund.
- **Czas na wprowadzenie kodu PIN**: wartość ta określa maksymalne opóźnienie na wprowadzenie pełnego, prawidłowego numeru PIN przed wejściem w tryb programowania systemu (od 5 sekund do 4:15 minuty). Domyślnie: 20 sekund.
- **Czas na wyjście z trybu programowania**: wartość ta określa maksymalne opóźnienie pomiędzy każdym wciśnięciem klawisza, zanim wyjdzie się z trybu programowania i zostanie wyświetlona wiadomość powitalna (od 5 sekund do 9:59 godzin). Domyślnie: 60 sekund.

3 – określ opcje Wymuszenia. Alarm wymuszenia jest wykorzystywany przez abonenta albo pracownika do wezwania pomocy

- Wymuś przy dostępie zezwolonym (**Duress on access granted**): pozwala abonentowi na włączenia alarmu po wprowadzeniu numeru PIN. Domyślnie: niewybrane.
- Wymuś przy dostępie zabronionym (**Duress on access denied**): pozwala abonentowi na włączenia alarmu po wprowadzeniu nieprawidłowego numeru PIN. Domyślnie: niewybrane.
- Przycisk Wymuszenia na klawiaturze (**Keypad duress key**): konfiguruje symbol, który będzie aktywować funkcje wymuszenia. Alarm wymuszenia jest wykorzystywany przez abonenta albo pracownika do wezwania pomocy (wartości od 0 do 9; # oraz *). Domyślnie: 9.

4 – określ opcje Harmonogramu nadzoru:

- **Harmonogram nadzoru zasilania (Power supervision schedule)**: aby zdefiniować harmonogram dla monitorowania zasilania KTES wybierz harmonogram z listy i kliknij OK. Domyślna wartość: brak.
- **Harmonogram nadzoru czujnika antysabotażowego (Tamper switch supervision schedule)**: aby zdefiniować harmonogram dla monitorowania czujnika antysabotażowego KTES wybierz harmonogram z listy i kliknij OK. Domyślna wartość: brak.

5 – kliknij przycisk Zapisz.

Notatka: aby dowiedzieć się więcej, zobacz Definiowanie harmonogramów.



Definiowanie Parametrów przekaźnika stanu (Defining the Status Relay Parameters)

1 – z okna KTES wybierz zakładkę Przekaźnik stanu.

Notatka: aby dowiedzieć się więcej, zobacz Definiowanie przekaźnika.

2 – określ parametry Aktywacji przekaźnika:

- Awaria zasilania (**Power failure**): ten przekaźnik może być aktywowany, kiedy nastąpi awaria zasilania KTES. Domyślnie: brak.

- Awaria baterii (**Battery trouble**): przekaźnik, który zostanie aktywowany, kiedy 12 woltowa bateria zostanie odłączona albo jej napięcie spadnie poniżej 11,5 woltów. Domyślnie: brak.

- Czujnik antysabotażowy w alarmie (**Tamper in alarm**): przekaźnik, który zostanie aktywowany, kiedy powstanie zdarzenie czujnika antysabotażowego KTES. Domyślnie: brak.

- Bufor wypełniony w 70% (**Buffer 70% full**): przekaźnik, który zostanie aktywowany, kiedy bufor zdarzeń oprogramowania EntraPass wypełni się w 70%. Domyślnie: brak.

- **Problem zasilania zamka (Lock power trouble)**: ten parametr definiuj przekaźnik, który zostanie aktywowany, jeśli wystąpi zdarzenie „problem zamka drzwi” albo „zamek rozłączony”. Domyślnie: brak.

- Inne problemy (**Other troubles**): przekaźnik, który zostanie aktywowany, kiedy wystąpią problemy innego rodzaju powiązane z KTES.

- **Grzejnik włączony (Heater kit activated)**: przekaźnik, który zostanie aktywowany, kiedy temperatura spadnie poniżej +5°C. Domyślnie: brak.

- Blokada na wejściu (**Postal lock**): przekaźnik, który zostanie aktywowany wraz ze zgłoszeniem próby wejścia z zamka na drzwiach wejściowych. Domyślnie: brak.

3 – określ Rodzaje powiadomień pagera:

Notatka: aby określić rodzaje powiadomień pagera dla każdego rodzaju zdarzeń, funkcja Raportowanie pagerem musi być włączona.

- dla każdego zdarzenia będziesz mógł skonfigurować rodzaj powiadomień pagera. Możesz wybrać Brak powiadomień (aktywacja przekaźnika dla tego zdarzenia nie zostanie wysłana do pagera), Natychmiastowe powiadomienie (aktywacja przekaźnika dla tego zdarzenia zostanie natychmiast wysłana do pagera), Powiadomienie według harmonogramu (aktywacja przekaźnika dla tego zdarzenia zostanie wysłana do pagera według harmonogramu). Domyślnie: Brak powiadomienia.

Definiowanie opcji pagera (Defining the Pager Options)

1 – z okna KTES wybierz zakładkę Pager.

2 – określ opcje Raportowania pagera:

- Numer pager: numer telefoniczny pagera, na który raportowane będą zdarzenia (max. 24 znaki). Domyślnie: pusty.

- Harmonogram powiadomień pagera: numer harmonogramu, z którego KTES może komunikować zaprogramowane zdarzenia, alarmy oraz problemy do pagera. Wybierz harmonogram z listy i kliknij OK.

Notatka: aby dowiedzieć się więcej, zobacz Definiowanie harmonogramów.

- ID jednostki: identyfikuje KTES, który wysyła kod pagera (0001 do 9999). Domyślnie: 0001.

- Kod przywracania: to kod odpowiadający zdarzeniu, które rozpoczęło stan przywracania dla strefy (000 do 999). Domyślnie: 0.

- Kod alarmu: to kod odpowiadający zdarzeniu, które rozpoczęło stan alarmu dla strefy (000 do 999). Domyślnie: 1.



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia

- Kod czujnika antysabotażowego: to kod odpowiadający zdarzeniu, które rozpoczęło stan czujnika antysabotażowego dla strefy (000 do 999). Domyślnie: 2.
- Kod problemu (trouble): to kod odpowiadający zdarzeniu, które rozpoczęło stan problemu dla strefy (000 do 999). Domyślnie: 3.
- Separator: to znak wykorzystywany do oddzielenia pól (*, # albo ,). Domyślnie: *.
- Znak zakończenia: wskazuje zakończenie połączenia – możesz wprowadzić dowolny znak dla parametru zakończenia (*, # albo ,). Domyślnie: #.

3 – Określ kody pagera dla Zdarzeń:

- Alarm czujnika antysabotażowego: kod oznaczający problem czujnika antysabotażowego (000 do 999). Domyślnie: 100.
- Awaria zasilania (**Power failure**): kod informujący o awarii zasilania KTES (000 do 999). Domyślnie: 101.
- Awaria baterii (**Battery trouble**): kod informujący o problemie z baterią (0 do 999). Domyślnie: 102.
- Bufor zapełniony w 70% (**Buffer 70% full**): kod informujący o fakcie, że bufor zdarzeń oprogramowania EntraPass zapełnił się w 70% (0 do 999). Domyślnie: 103.
- Inne problemy (**Other troubles**): kod informujący o wystąpieniu problemu innego rodzaju powiązanego z KTES (0 do 999). Domyślnie: 104.
- Wymuszone otwarcie drzwi (**Door forced open**): kod informujący o wymuszonym otwarciu drzwi (0 do 999). Domyślnie: 120.
- Drzwi otwarte zbyt długo (**Door open too long**): kod informujący o zbyt długim otwarciu drzwi (0 do 999). Domyślnie: 121.
- Alarm drzwi niezamknięte (**Door alarm on relock**): kod informujący o tym, że drzwi pozostały niezamknięte (0 do 999). Domyślnie: 122.
- Problemy z zamkiem (**Lock trouble**): kod informujący o problemie z nadzorem nad zamkiem (0 do 999). Domyślnie: 123.
- Klawiatura wyłączona (**Keypad disabled**): kod informujący o tym, że klawiatura jest niedostępna (kiedy opcja jest włączona wartości od 0 do 999). Domyślnie: 124.
- Powiadomienie alarmowe (**Duress alarm**): kod informujący o tym, że zostało wysłane powiadomienie alarmowe (powiadomienie alarmowe jest wysyłane przez pracowników albo abonentów z prośbą o pomoc). Wartości: 0 do 999. Domyślnie: 125.
- Przyznano dostęp (**Access granted**): kod informujący o przyznaniu dostępu. Kod ten jest wysłany, kiedy abonent otrzymał dostęp po wprowadzeniu swojego kodu PIN (0 do 999). Domyślnie: 140.
- Nieprawidłowy harmonogram dostępu (**Invalid access schedule**): kod informujący o odmowie dostępu. Kod ten jest wysłany, kiedy abonent nie otrzymał dostępu po wprowadzeniu swojego kodu PIN (0 do 999). Domyślnie: 141.
- Dostęp przyznany przez abonenta (**Access granted by tenant**): kod informujący o przyznaniu dostępu przez abonenta dla gościa (0 do 999). Domyślnie: 142.
- Przekaznik pomocniczy aktywowany przez abonenta (**Auxiliary relay activated by tenant**): kod informujący o przyznaniu dostępu przez abonenta dla gościa do wejścia innego niż główne (0 do 999). Domyślnie: 143.
- Odmowa dostępu przez abonenta (**Access granted by tenant**): kod informujący o odmowie dostępu przez abonenta dla gościa (0 do 999). Domyślnie: 144.
- Abonent śledzony (**Tenant traced**): kod informujący o przyznaniu dostępu dla śledzonego abonenta (0 do 999). Domyślnie: 145.
- Abonent wyłączony (**Disabled tenant**): kod informujący o próbie uzyskania dostępu przez abonenta bez uprawnień (0 do 999). Domyślnie: 146.



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia

- Próba dostępu poza harmonogramem – odmowa (**Other access denied**): kod informujący o próbie uzyskania dostępu przez abonenta poza harmonogramem (0 do 999). Domyślnie: 147

Konfigurowanie parametrów poziomu zarządzania abonenta (Configuring Tenant Administration Level Parameters)

1 – z okna KTES wybierz zakładkę **Poziom zarządzania abonenta (Tenant administration level)**.

2 – określ parametry dostępu: ustaw poziomy zarządzania (Pełen dostęp, Tylko do odczytu, Brak dostępu) dla czterech rodzajów abonentów.

Komentarz (Comment)

Sprawdź: Pole komentarza



Konfiguracja drzwi (Doors Configuration)

To menu służy do definiowania parametrów drzwi, na których czytniki oraz/lub klawiatury są zainstalowane. Drzwi mogą być drzwiami windy, drzwiami wejścia/wyjścia, drzwiami dostępu, etc. Wszystko zależy od tego, jak ustawienia zostaną zaprogramowane. Drzwi mogą być zabezpieczone przez cały czas albo tylko podczas określonego terminarza. Urządzeniami zabezpieczającymi są zazwyczaj elektrozaczepy oraz zwory elektromagnetyczne. Drzwi mogą być wyposażone w jeden albo dwa czytniki; po jednym po każdej stronie. W przypadku, gdy czytniki są po obu stronach ten zewnętrzny trzeba określić, jako czytnik wejścia, a ten wewnętrzny, jako czytnik wyjścia.

Notatka: dla pojedynczej bramki limity są następujące: 2048 połączeń, 10000 drzwi, 100000 kart, 100000 Linii dozorowych (input) i wyjść (output).

Definiowanie ogólnych parametrów drzwi (Defining General Parameters for a Door)

Notatka: jeśli używasz systemu KT-300, pracujesz w systemie h:mm:ss (wartości od 00:00:01 do 9:06:07). Jeśli używasz systemu KT-400, pracujesz w systemie hh:mm:ss (wartości od 00:00:01 do 00:04:15), czyli 255 sekund dla KT-100, KT-200 oraz KT-300; albo 65535 sekund (wartości od 00:00:01 do 18:12:15) dla KT-400.

1 – Na pasku narzędzi **Urządzenia (Devices)**, wybierz przycisk **Drzwi (Door)**.

Notatka: opcje Strefy lokalne (Local area) są dostępne tylko dla kontrolera KT-400 dla multi obiektowej bramki przy włączonej opcji Strefa lokalna kontrolera (Controller local area). Zobacz Definiowanie kontrolera KT-400.

Opcje Różne, Wej./Wyj. oraz Anti-passback nie są dostępne dla drzwi KTES.

2 – Wybierz **Filtr obiektu (Site filter)** z listy.

3 – Wybierz **Bramkę (Gateway)**.

4 – Z listy **Połączenie (Connection)**, wybierz połączenia, na którym znajduje się kontroler.

5 – Z listy Kontroler (Controller) wybierz kontroler, który chcesz zdefiniować. Nazwij go, wypełniając odpowiednie pole.

6 – Z listy Drzwi, wybierz drzwi, które chcesz modyfikować albo definiować. Nowe obiekty są określone czerwonym przyciskiem. Kiedy przycisk zmieni się na zielony, oznacza to, że został zdefiniowany i zapisany.

7 – Określ **Tryb blokowania drzwi (Door Lock Mode)** w zakładce **Ogólne (General)**:

- **Zamek typu NC – bez zasilania zaryglowany (Fail-secure):** zaczep jest zablokowany, w przypadku braku zasilania (zamki drzwi, zaczepy).
- **Zamek typu NO – bez zasilania odryglowany:** wyjście zamka podaje zasilanie w celu zaryglowania drzwi (np. zwora elektromagnetyczna).



8 – W przypadku KTES, przejdź do punktu 13.

9 – Zaznacz opcje Kabina windy, jeżeli drzwi mają być wykorzystane, jako drzwi windy. W przypadku zaznaczenia, wyświetla się zakładka Winda w celu określenia terminarza odblokowania. Domyślnie: niezaznaczona.

10 – **Rejestracja Czasu Pracy** – ustaw funkcje czytnika (Domyślnie Brak)

- **Brak (None):** czytnik jest traktowany tylko, jako czytnik do kontroli dostępu. Odczyt karty generuje tylko zdarzenia „Dostęp zezwolony/Dostęp zabroniony”
- **Wejście RCP (Entry):** drzwi wejściowe są punkt wejścia dla systemu RCP. Aby system odnotował wejście RCP, drzwi muszą zostać otwarte po przyznaniu dostępu (jeżeli został zainstalowany czujnik stanu drzwi). Odczyt karty generuje wtedy drugie zdarzenie „Rejestracja czasu pracy - wejście”
- **Wyjście RCP (Exit):** drzwi wyjściowe punkt wyjścia RCP. Aby system odnotował wyjście, drzwi muszą zostać otwarte po przyznaniu dostępu (jeżeli został zainstalowany czujnik stanu drzwi). Odczyt karty generuje wtedy drugie zdarzenie „Rejestracja czasu pracy - wyjście”

11 – Jeżeli dostępne są Strefy lokalne Kontrolera, przejdź do punktu 11.

12 – Określ **Typ anti-passback dla drzwi (Door Anti-Passback type)** (domyślnie: dostęp):

- **Dostęp (Access):** czytnik jest traktowany, jako czytnik wejścia. Opcje anti-passback nie są wykorzystywane przy drzwiach wejściowych. Generuje tylko zdarzenia „Dostęp zezwolony/Dostęp zabroniony” (“Access granted/Access denied” events).
- **Wejście (Entry):** drzwi wejściowe są punkt wejścia. Aby system odnotował wejście, drzwi muszą zostać otwarte po przyznaniu dostępu.
- **Wyjście (Exit):** drzwi wyjściowe punkt wyjścia. Aby system odnotował wyjście, drzwi muszą zostać otwarte po przyznaniu dostępu.

13 - Przejdź do punktu 13.

Notatka: opcje Brak, „Miękki” anti-passback oraz „Twardy” anti-passback są wykorzystywane tylko z KT-400 oraz Lokalnymi strefami kontrolera.

14 – Określ **Typ anti-passback dla drzwi (Door Anti-Passback type)** (domyślnie: dostęp):

- **Brak (None):** opcja jest wyłączona.
- **„Miękki” anti-passback (Soft anti-passback):** jeżeli strefa znajduje się pod **Dostęp zabroniony, strefa lokalne pełna (Deny Access on Local Area Full)**, natępuje Dostęp zabroniony. Jeżeli użytkownik używa swojej karty do strefy lokalnej, dla przykładu, system przyzna mu dostęp do innej strefy lokalnej, nawet, jeżeli użytkownik nie był w tej strefie wcześniej. System wygeneruje zdarzenie „Dostęp zezwolony – Zła lokalizacja passback” (“Access granted - Passback bad location”)
- **Miękki” anti-passback (Hard anti-passback):**): jeżeli strefa znajduje się pod **Dostęp zabroniony, strefa lokalne pełna (Deny Access on Local Area Full)**, natępuje Dostęp zabroniony. Jeżeli karta została użyta przy czytniku wejścia, nie będzie miała do niego ponownego dostępu, dopóki nie zostanie użyta na odpowiadającym mu czytniku wyjścia. System wygeneruje zdarzenie „Odmowa dostęp – Zła lokalizacja passback” (“Access denied - Passback bad location”)



15 – Określ Strefy lokalne przed (Local area before) oraz Strefy lokalne po (Local area after). Te strefy mogą zostać włączone i określone w Lokalne strefy Kontrolera (**Controller Local Area**).

16 – Określ Opóźnienie dostępu do drzwi (Door access delay):

- **Czas odryglowania (hh:mm:ss) (Unlock time (hh:mm:ss)):** czas, podczas którego drzwi pozostaną odryglowane po prawidłowym odczytaniu karty. Przedział czasu: od 00:00:01 do 00:04:15 (255 sec) dla KT-100, KT-200 oraz KT-300; albo do 18:12:15 (65535 sec.) dla KT-400. Jeżeli są to drzwi windy i przycisk (wejście) jest wykorzystywany do wyboru pięter, jest to czas, podczas którego możliwy jest wybór pięter. Domyślny: 10 sec. Zobacz: **Konfiguracja Linii dozorowej (In Input Configuration)**

- **Czas otwarcia (hh:mm:ss) (Open time (hh:mm:ss)):** czas, podczas którego drzwi mogą pozostać otwarte po prawidłowym odczytaniu karty. Odnosi się tylko do drzwi z określoną linią dozorową czujnika stanu drzwi (door contact input). Przedział czasu: od 00:00:01 do 00:04:15 (255 sec) dla KT-100, KT-200 oraz KT-300; albo do 18:12:15 (65535 sec.) dla KT-400. Po upływie tego czasu system wygeneruje zdarzenie „drzwi otwarte zbyt długo”, a sygnał dźwiękowy ostrzeże użytkownika. Dźwięk będzie trwać przez czas niezbędny do zamknięcia drzwi. Domyślny: 30 sec.

17 – Opcja Przedłużone opóźnienie dostępu do drzwi (hh:mm:ss) (Extended door access delay) gwarantuje dodatkowy czas dostępu do drzwi (czasu, gdy drzwi pozostają niezablokowane i mogą być otwarte). Przydatne dla ułatwienia poruszania się osobom z ograniczoną sprawnością. Określ czas opóźnienie (domyślnie: 00:00:40) oraz czas otwarcia (domyślnie: 00:02:00). Przedział czasu: od 00:00:01 do 00:04:15 (255 sec) dla KT-100, KT-200 oraz KT-300; albo do 18:12:15 (65535 sec.) dla KT-400

18 – Terminarz odryglowania (Unlock Schedule) pozwoli systemowi na odblokowywanie drzwi na określone wcześniej przedziały czasu.



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia

19 – Opcja Pierwsza Osoba (First Person In): podczas terminarza odryglowania drzwi są zamknięte do pierwszego wejścia. Opcja niedostępna dla KT-200; domyślnie: niezaznaczona.

- Dla KT-400 oraz KT-1 można określić **Karencję odryglowania (mm) (Unlock Grace Period (mm))**. Ta opcja umożliwia odryglowanie drzwi podczas terminarza odryglowania, jeżeli pierwszy dostęp został przyznany w określonym przedziale czasu poprzedzającym terminarz odryglowania. Czas może zostać określony od 0 (opcja wyłączona) do 59 minut. Domyślnie: 0. Na przykład: terminarz odryglowania jest zdefiniowany na przedział czasowy: 08:00 do 17:00. **Pierwsza osoba (First Person In)** dostaje 15 minutową **Karencję odryglowania (Unlock Grace Period)**, czyli jej wejście pomiędzy 07:45 a 7:59 pozwoli drzwiom odblokować się automatycznie o 08:00.

20 – wybierz Multi-odczyt karty (Enable Multi-Swipe), aby włączyć/wyłączyć widzialność Zakładki multi-odczytu karty.

21 – Wybierz **Grafika (Graphic)** albo **Podgląd wideo (Video view)**, do którego przypisana jest bramka. Podgląd wideo będzie dostępny tylko wtedy, gdy opcja ta jest udostępniona w EntraPass.

Notatka: EntraPass Corporate oferuje możliwość zaprogramowania wydłużonego czasu dostępu do drzwi dla osób z ograniczeniami ruchowymi. Poza tymi specjalnymi ustawieniami należy również zaprogramować kartę użytkownika pod tą opcję. Dostępne wyłącznie dla KT-100, KT-300 oraz KT-400.



Definiowanie opcji klawiatury drzwi (Defining Door Keypad Options)

Dla kontrolerów KT-100 oraz KT-300 (For KT-100 and KT-300 Controllers)

W opcji definiowania drzwi możemy przypisać przekaźniki, które będą przełączane po wciśnięciu przycisków * albo # na klawiaturze czytnika. Opcja jest dostępna wyłącznie dla KT-100 (firmware 1.04 lub nowszy) oraz KT-300 (firmware 1.16 lub nowszy).

Dla kontrolerów KT-400 (For KT-400 Controllers)

Drzwi mogą zostać zdefiniowane z aktywacją przekaźnika lub grupy przekaźników po wciśnięciu określonego przycisku na klawiaturze.

Notatka: zakładka Klawiatura jest dostępna, jeśli wybrałeś Rodzaj klawiatury podczas definiowania kontrolera przypisanego do drzwi, które były definiowane. Dostępne są 4 przyciski. Pierwsze dwa: # oraz * są odgórnie zdefiniowane i odgrywają taką samą rolę, jak w systemach KT-300. Przyciski 3 oraz 4 można definiować według potrzeb użytkownika.

1 – Wybierz zakładkę Klawiatura z okna Drzwi.

2 – Określ, w jaki sposób dostęp do drzwi jest kontrolowany (domyślnie: Tylko czytnik):

- **Tylko czytnik (Reader only):** zaznacz tę opcję, jeżeli dostęp jest przyznawany przy pomocy czytnika.
- **Czytnik albo klawiatura (Reader or keypad):** zaznacz tę opcję, jeżeli dostęp jest przyznawany przy pomocy czytnika albo klawiatury.

Notatka: opcja może zostać włączona na czytnikach ze zintegrowanymi klawiaturami, jeśli na przykład chcesz użyć wyłącznie klawiatury.

- **Czytnik i klawiatura (Reader and keypad):** zaznacz tę opcję, jeżeli dostęp jest przyznawany przy pomocy czytnika oraz klawiatury. Klawiatura zostanie użyta wyłącznie wtedy, gdy terminarz klawiatury jest aktywny.

3 – Z menu Terminarz Karty i numeru PIN (**Card and PIN schedule**) wybierz terminarz, podczas którego użytkownicy po wczytaniu karty będą musieli wprowadzić numer PIN. Czas pomiędzy wczytaniem karty, a wprowadzeniem numeru PIN jest określany w menu Definiowanie Bramki (opcja **Koniec czasu na klawiaturze (Time-out on keypad)**).

4 – Zaznacz opcję **Włącz wymuszenie (Enable duress)**. Domyślnie: wyłączona.

5 – Wybierz przycisk(i) **Aktywacja przekaźnika klawiatury (Keypad relay activation)**:

- Dla KT-100 oraz KT-300: dla drzwi zdefiniowanych z klawiaturą lub czytnikiem i klawiaturą możesz zaprogramować aktywację przekaźnika przy pomocy przycisków * lub #. W takim wypadku naciśnięcie jednego z nich aktywuje przekaźnik.
- Dla KT-400: dla drzwi zdefiniowanych z klawiaturą lub czytnikiem i klawiaturą możesz zaprogramować aktywację przekaźnika lub grupy przekaźników przy pomocy przycisków * lub #. W takim wypadku naciśnięcie jednego z nich aktywuje przekaźnik lub grupę przekaźników.



Definiowanie opcji czujnika stanu drzwi (Defining Door Contact Options)

W większości aplikacji nisko kosztowy czujnik stanu drzwi jest jedynym elementem nadzorującym, który chroni inwestycję stworzoną w celu ochrony dostępu do drzwi. Zamek drzwi oraz czytnik kart zapewnia bezpieczeństwo oraz zapobiega nieautoryzowanym wejściom tylko wtedy, kiedy drzwi są zamknięte. Prosty czujnik stanu drzwi pozwala monitorować kilka stanów drzwi, m.in. wymuszone otwarcie, drzwi otwarte zbyt długo, etc.

1 – Wybierz zakładkę Czujnik stanu drzwi (Contact) w oknie Drzwi.

2 – Wybierz czujnik z listy.

3 – Wybierz terminarz w Terminarz wyłączenia drzwi (Shunt Door Schedule).

Notatka: czujnik stanu drzwi nie może zostać przypisany do więcej niż dwóch czytników.

Notatka: ta opcja pozwala przypisanie terminarza do czujnika stanu drzwi, aby obejść zdarzenia/alarmy powiązane z nadzorem tego czujnika. Jeśli żaden terminarz nie jest wybrany, system będzie pracował normalnie. W przeciwnym wypadku, system ukryje zdarzenia/alarmy z pulpitu monitorowania zdarzeń:

- Wymuszone otwarcie drzwi (Door Forced open)
- Przywrócone drzwi otwarte przez wymuszenie (Door forced open restored)
- Drzwi otwarte zbyt długo (Door open too long (unless otherwise indicated))
- Drzwi przedalarmem otwarte zbyt długo (Pre-Alarm door open too long)
- Drzwi pozostawione otwarte (Door left open)

4 – Zaznacz Włącz powiadomienie o zbyt długim otwarciu drzwi (Enable door open too long notification), aby nadal kontynuować informacje o zdarzeniach Drzwi otwarte zbyt długo oraz Drzwi przedalarmem otwarte zbyt długo. Przy braku terminarza, opcje nie są dostępne (wyszarzone).

Notatka: dla kontrolerów KT-200, Linia dozorowa 1 (czujnik stanu drzwi) oraz Linia dozorowa 2 (pozwolenie na wyjście) są zarezerwowane dla Drzwi 1 tego kontrolera, podczas gdy Linia dozorowa 9 (czujnik stanu drzwi) oraz Linia dozorowa 10 (pozwolenie na wyjście) są zarezerwowane dla Drzwi 2 tego samego kontrolera. Linia dozorowa wykorzystana do czujnika stanu drzwi albo REX NIE POWINIEN mieć zdefiniowanego terminarza monitorowania w menu Definiowanie Input.

5 – Zaznacz opcje odczytywania:

- Drzwi otwarte: ta opcja pozwala na odczyt kart w trakcie, kiedy drzwi są otwarte. System nie odrygluje drzwi, jeżeli były one wcześniej zaryglowane. Jeśli opcja została wybrana, zdarzenie „Przyznanie dostępu” zostaje utworzone. W przeciwnym razie utworzone jest zdarzenie „Przyznanie dostępu – drzwi otwarte”. Domyślnie: opcja wybrana.
- Drzwi niezablokowane: ta opcja pozwala na odczyt kart w trakcie, kiedy drzwi są odryglowane zdalnie przez operatora albo przez terminarz. Jeśli opcja została wybrana, zdarzenie „Przyznanie dostępu” zostaje utworzone przy przyznaniu dostępu. Aby uniknąć wszystkich zdarzeń przyznania dostępu przy odblokowaniu drzwi, nie zaznaczaj tej opcji. Domyślnie: opcja wybrana.
- Odrygluj przy dostępie (Unlock on access door opened): ta opcja pozwala na odblokowanie dostępu dla drzwi otwartych w dowolnym momencie. Domyślnie: opcja niewybrana.
- Drzwi otwarte zbyt długo – przed alarm (Pre-alarm door opened too long): ta opcja pozwala na wygenerowanie zdarzenia „przed alarm – drzwi otwarte zbyt długo” oraz na uruchomienie sygnału dźwiękowego, kiedy minie połowa opóźnienia określonego w polu Czas otwarcia (Open time). Dźwięk będzie trwał do zamknięcia drzwi. Domyślnie: opcja niewybrana.

Notatka: jeśli drzwi działają pod KT-400, a wprowadzona wartość jest wyższa albo równa niż czas otwarcia, a ta opcja jest wybrana, wyskoczy okienko informujące, że wartość jest nieprawidłowa. Wartość musi się mieścić w przedziale 00:00:01 – 18:12:15 i być niższe czas otwarcia drzwi.



6 – Wybierz odpowiednią opcję **Zamknij ponownie na wejściu (Relock on access)**. Możesz wybrać **Na otwarciu (On door opening)** lub **Na zamknięciu (On door closing)**. Domyślnie: Na otwarciu.

Definiowanie REX (Request To Exit – prośba o wyjście)

Sygnal od REX wskazuje, że ktoś chce wyjść przez kontrolowane drzwi. Urządzenia takie, jak detektory ruchu lub przyciski mogą generować sygnał REX. EntraPass umożliwia użytkownikom konfigurowanie resetowania czasu odryglowania drzwi za każdym razem, gdy główny lub pomocniczy REX jest aktywowany. Ta opcja jest dostępna tylko dla KT-100 (firmware 1.04) oraz KT-300 (firmware 1.16).

1 – Z okna Drzwi, wybierz zakładkę REX. Następnie zaznacz **Zablokuj ponownie po REX (Relock on REX)**:

- **Na otwarciu**, jeśli chcesz zablokować po prawidłowym dostępie.
- **Na zamknięciu**, jeśli chcesz zablokować po zamknięciu.

2 – Dla **Głównego i Pomocniczego REX (Primary and Secondary REX)**, wybierz:

- Przypisz **Czujnik stanu REX (REX contact)**: Wejście linii dozorowej, do którego detektor REX może zostać podłączony. Wejście linii dozorowej musi być lokalne; musi to być Wejście linii dozorowej na drzwiach pod kontrolerem.
- Przypisz **Terminarz REX (Rex schedule)**: kiedy terminarz jest aktywny, kontroler będzie wykrywał sygnały REX. Ta opcja odnosi się tylko do drzwi zdefiniowanych w kontakcie REX.
- Wybierz **Terminarz wiadomości pominięcia REX (Rex Bypass Message schedule)**: kiedy terminarz jest aktywny, zdarzenie nie będzie zapisane w archiwum. Kiedy nie jest aktywny, zdarzenie jest wysyłane do bramki do zarchiwizowania. Przy definiowaniu nowych drzwi, **Terminarz wiadomości pominięcia REX (Rex Bypass Message schedule)**, domyślnie będzie nastawiony na: zawsze aktywny.

Notatka: opcja głównego oraz pomocniczego Terminarza wiadomości pominięcia REX (Rex Bypass Message schedule) będzie dostępna po włączeniu w Parametrach systemu. Zobacz Parametry/Terminarze systemu.

- **Odblokowanie przy REX (Unlock on REX)**: drzwi zostaną odryglowane przez kontrolera, jeżeli prawidłowa prośba o wyjście zostanie przesłana. Ta opcja może być przydatna w przypadku drzwi wyjściowych, takich jak drzwi wewnętrzne, drzwi zaopatrzeniowe lub inne, przez które przechodzą ludzie z towarem. System zezwoli na wyjście i wygeneruje zdarzenie „prośba o wyjścia – uznana” („request to exit granted”), a nie zdarzenie „wymuszone otwarcie drzwi” („door forced open”).
- **Funkcja Resetowanie (REX Resettable REX function)**: czas odryglowania jest resetowany przy prawidłowej prośbie o wyjście. Czas otwarcia oraz odryglowania są definiowane w Definiowanie drzwi (Door definition). Zaznacz tę opcję na przykład przy drzwiach wyjściowych, przez które pracownicy mogą wychodzić pod koniec dnia roboczego (dużo ludzi w krótkich przedziałach czasu), aby nie występowały zdarzenia „drzwi otwarte zbyt długo” (door open too long) oraz „wymuszone otwarcie drzwi” („door forced open”).

Notatka: zaleca się wybranie albo Odblokowanie przy REX (Unlock on REX), albo Funkcja Resetowanie (REX Resettable REX function); nie zaleca się wybierania obu opcji jednocześnie. Jeśli wybierzesz te dwie opcje, drzwi pozostaną odryglowane przez długi okres czasu. Dodatkowo, te opcje nie powinny być używane, jeśli czujnik stanu drzwi nie został zdefiniowany.



Multi-odczyt karty (Card Multi-Swipe)

Ta opcja pozwala na podwójny albo potrójny odczyt karty z nowym firmwarem KT-400 (KT-400: 1.08; KT-400 V1: 1.11).

1 – Wybierz zakładkę Ogólne (General).

2 – Włącz Multi-odczyt karty (Enable Multi-swipe): pojawi się zakładka Multi-odczyt karty (Multi-Swipe). Wyłączenie opcji sprawi, że funkcja przestanie działać, ale zachowa wszystkie wcześniejsze ustawienia.

3 – Wybierz zakładkę Multi-odczyt karty (Multi-swipe).

4 – Terminarz (Schedule): odnosi się zarówno do podwójnego, jak i potrójnego odczytu.

5 – Opóźnienie (Delay): maksymalne opóźnienie pomiędzy odczytami wynosi 3 sekundy. Sygnał dźwiękowy zostanie wygenerowany dwa razy przy podwójnym odczycie, a trzy razy przy potrójnym. Przeciągły sygnał oznacza odmowę dostępu.

6 – Przekaznik (Relay): wybierz przekaznik do aktywowania.

7 – Zamknij po dostępie poprzez Multi-odczyt karty (Relock on access on double/triple swipe): zablokuje drzwi przez użyciem Multi-odczytu karty.

Notatka: domyślnie system ustawia czas odryglowania drzwi na 10 sekund, a czas otwarcia drzwi na 30 sekund. Jeśli drzwi będą otwarte przez ponad 15 sekund po otwarciu, przed-alarm Drzwi otwarte zbyt długo (zobacz Zakładka Czujnik stanu drzwi) zostanie uruchomiony, a czytnik zacznie wydawać sygnał dźwiękowy.

Opóźnienie przed-alarmu Drzwi otwarte zbyt długo obejduje domyślne ustawienie Czasu otwarcia. Na przykład, czas odryglowania 10 sekund, a czas otwarcia 2 minuty. Jeśli opcja przed-alarmu Drzwi otwarte zbyt długo jest wybrana z czasem opóźnienia 00:00:20, na dwadzieścia sekund przed upłynięciem czasu otwarcia system uruchomi przed-alarm.

Ta opcja jest dostępna tylko dla KT-400 z oprogramowaniem 1.08 i wyższym.

Akcje podwójnego/potrójnego odczyt (Double/Triple swipe actions)

- **Włącz przekaznik (Activate relay)**

- **Wyłącz przekaznik (Deactivate relay)**

- **Zarygluj drzwi (Lock door):** opcja **Zamknij po dostępie poprzez podwójny/potrójny odczyt (Relock on access on double/triple swipe)** będzie automatycznie zaznaczona i wyłączona.

- **Prośba o uzbrojenie przyznana – Alarm (Request to arm granted - Alarm interface):** odpowiednik zdalnej operacji uzbrojenia drzwi przy wykorzystaniu funkcjonalności panelu.

- **Czasowo włącz przekaznik (Temporarily activate relay):** wprowadź opóźnienie dla przekaznika albo grupy przekazników (od 00:00:01 do 18:12:15).

- **Czasowo odrygluj drzwi (Temporarily unlock door):** opcja **Zamknij po dostępie poprzez podwójny/potrójny odczyt (Relock on access on double/triple swipe)** będzie automatycznie zaznaczona i wyłączona. Wprowadź opóźnienie (od 00:00:01 do 18:12:15).

- **Przełącz zamek drzwi (Toggle door lock):** opcja **Zamknij po dostępie poprzez podwójny/potrójny odczyt (Relock on access on double/triple swipe)** będzie automatycznie zaznaczona i wyłączona.

- **Przełącz przełącznik (Toggle relay)**

- **Odrygluj drzwi (Unlock door):** opcja **Zamknij po dostępie poprzez podwójny/potrójny odczyt (Relock on access on double/triple swipe)** będzie automatycznie zaznaczona i wyłączona.



Definiowanie funkcji śluzy (Pułapka) (Defining Interlock Options (Mantrap))

Możesz określić opcje Śluzy (Interlock) pomiędzy dwoma drzwiami, aby zsynchronizować czas, w którym te drzwi są zamknięte/otwarte. Opcje Śluzy (Interlock) są określone mianem „pułapki”. Oznacza to, że kiedy użytkownik ma dostęp do pierwszych drzwi, te drzwi najpierw muszą zostać zamknięte i zaryglowane, zanim użytkownik otrzyma dostęp do drugich drzwi. Drzwi pierwsze i drugie muszą być kontrolowane przez ten sam kontroler.

Notatka: opcja Śluzy nie odnosi się do drzwi KTES.

1 – W oknie Drzwi wybierz zakładkę **Różne (Miscellaneous)**.

2 – Z listy wybierz pierwsze drzwi, dla których chcesz ustawić opcje Śluzy (Interlock)

3 – Z listy Czujnik stanu śluzy (Interlock contact), wybierz pierwsze Wejście linii dozorowej dla opcji Śluzy. Wybrane Wejście linii dozorowej musi być Czujnikiem stanu dla drugich drzwi.

4 – Z listy Drzwi wybierz drugie drzwi, dla których chcesz ustawić opcje Śluzy. Wybierz czujnik stanu śluzy dla drugich drzwi. Wybrany Czujnik stanu musi być czujnikiem dla pierwszych drzwi.

5 – Wybierz **Terminarz Śluzy (Interlock schedule)**: drzwi muszą mieć ten sam terminarz. Według tego terminarza sprawdzane są śluzy przed przyznaniem dostępu użytkownikowi.

Notatka: opcja Śluzy (Pułapka) nie odnosi się do drzwi kontrolowanych przez KT-100.

6 – **Opóźnienie raportu wstrzymania przy ponownym zablokowaniu ((Suspend report delay on door relock (hh:mm:ss))** określa czas, w trakcie którego wybrane wejścia nie będą monitorowane przy odblokowaniu drzwi (od 00:00:01 do 18:12:15). Domyślnie: 15 sekund.

7 – w panelu Wyłącz monitorowanie linii dozorowej wybierz wejścia linii dozorowej, które nie będą monitorowane, kiedy drzwi zostaną odryglowane. Pozostaną niemonitorowane przez czas określony w polu Opóźnienie wyłączania (Shunt delay).

Notatka: obiekty Wyłącz wejście linii dozorowej różnią się zależnie od tego, jaki system jest wykorzystany – KT-300 czy KT-400.



Definiowanie drzwi windy (Defining Elevator Doors)

Podczas definiowania drzwi możliwe jest określenie czy drzwi są „normalne” czy są drzwiami do kabiny windy. Jeżeli drzwi zostaną określone, jako drzwi do kabiny windy, w oknie Definiowanie drzwi zostanie wyświetlona zakładka Winda. Ta zakładka jest wykorzystywana do określenia automatycznego terminarza odblokowania dla konkretnych grup pięter.

1 – Z okna Definiowanie drzwi wybierz zakładkę Winda.

2 – Z listy **Terminarz odblokowania #1** wybierz terminarz. Domyślnie, możesz wybrać **Zawsze ważny (Always valid)**. Możesz również stworzyć nowy terminarz.

3 – Z listy **Grupa pięter #1**, wybierz odpowiednią grupę powiązaną z **Terminarz odblokowania #1**. Wyłącznie piętra, które posiadają ważny terminarz w **Definiowanie Grupy Pięter (Floor group definition)**, będą odryglowane i dostępne do wyboru.

4 – Z listy **Terminarz odblokowania #2** wybierz terminarz dla drugiej grupy pięter.

5 – Z listy **Grupa pięter #2**, wybierz odpowiednią grupę powiązaną. Wyłącznie piętra, które posiadają ważny terminarz w **Definiowanie Grupy Pięter (Floor group definition)**, będą odryglowane i dostępne do wyboru.

Notatka: aby dowiedzieć się więcej, jak programować windy przy pomocy przekaźników REB-8, zobacz Konfigurowanie kontrolerów.



Konfigurowanie zdarzeń dla drzwi (Configuring Door Events)

1 – W oknie drzwi wybierz zakładkę Zdarzenia dla drzwi (Door events). W ten sposób określisz przekaźniki albo grupy przekaźników, które mają zostać aktywowane podczas zajścia zdarzenia. Przy użyciu KT-400, można określić tylko przekaźniki.

2 – Wybierz przekaźnik, który będzie aktywowany dla każdego zdarzenia.

3 – Typ powiadomienia pager (Pager call type) (wyłącznie KTES): możesz wybrać **Brak powiadomienia (Do not call)** – informacja o zdarzeniu nie zostanie wysłana; **Powiadom natychmiast (Call immediately)** – informacja zostanie wysłana natychmiast; **Powiadom według terminarza (Call when scheduled)** – informacja zostanie wysłana według terminarza. Domyślnie: Brak powiadomienia.

Notatka: aby określić rodzaje powiadomień pagera dla każdego rodzaju zdarzeń, funkcja Raportowanie pagerem musi być włączona. Zobacz Konfigurowanie KTES.

4 – Po ustawieniu wszystkich opcji zdarzeń dla drzwi, wybierz zakładkę **Zdarzenia dostępu (Access events)**, aby określić przekaźniki (albo grupy przekaźników dla KT-400), które mają być aktywowane przy różnych zdarzeniach.

Notatka: EntraPass oferuje możliwość określenia przekaźnika, który będzie aktywowany, jeśli opcja Wydłużone opóźnienie jest wykorzystana. Użyta karta musi być przypisana do tej funkcji. Tylko KT-100, KT-300, KT-400 oraz KTES mogą być skonfigurowane pod kątem tej opcji.

5 – Wybierz przekaźnik, który będzie aktywowany lokalnie (albo grupy przekaźników dla KT-400) dla każdego zdarzenia.

6 - Typ powiadomienia pager (Pager call type) (wyłącznie KTES): możesz wybrać **Brak powiadomienia (Do not call)** – informacja o zdarzeniu nie zostanie wysłana; **Powiadom natychmiast (Call immediately)** – informacja zostanie wysłana natychmiast; **Powiadom według terminarza (Call when scheduled)** – informacja zostanie wysłana według terminarza. Domyślnie: Brak powiadomienia.

Notatka: aby określić rodzaje powiadomień pagera dla każdego rodzaju zdarzeń, funkcja Raportowanie pagerem musi być włączona. Zobacz Konfigurowanie KTES.



Definiowanie opcji drzwi dla kontrolerów oraz KTES (Defining Door Options for Controllers and the KTES)

Zakładka pojawia się tylko, gdy KT-100, KT-300, KT-400 oraz KTES zostały skonfigurowane w multi-obiektowej bramce.

Wybierz zakładkę **Opcje i system alarmowy (Options and alarm system)**.

- **Nadzorowane urządzenia blokujące drzwi (Supervised door lock device):** ta opcja jest wykorzystywana na przykład w sejfach bankowych, aby kompensować powolny zamek. Dodanie tego opóźnienia sprawia, że nie są generowane fałszywe alarmy „wymuszone otwarcie drzwi”. Domyślnie: niewłączona.
- **Opóźnienie zamka (Motor lock delay)** (nie dla KTES): wprowadź przedział czasu (hh:mm:ss) po jakim drzwi zostaną uznane za zamknięte (od 00:00:00 do 18:12:15).
- Jeżeli wymagane jest odczytanie drugiej karty, wybierz terminarz z listy (nie dla KTES).
- **Przełącznik pracujący synchronicznie z wyjściem zamka (Relay to follow lock output)** (wyłącznie dla KT-400 oraz KTES): przełącznik „podąża” za statusem wyjścia zamka.
- **Włącz funkcję wymuszenia na klawiaturze (Enable duress function on keypad)** (tylko dla KTES): alarm wymuszenia jest wykorzystany przez pracowników albo abonentów do wezwania pomocy. Funkcja ta musi być wcześniej włączona. Zobacz: **Konfigurowanie KTES (KTES Configuration)**.

Notatka: kiedy KT-100, KT-300 oraz KT-400 są zainstalowane na multi obiektowej bramce, system oferuje możliwość wprowadzenia zewnętrznego systemu alarmowego.



Konfigurowanie interfejsów zewnętrznych systemów alarmowych (Configuring External Alarm System Interfaces)

Opcja jest dostępna tylko wtedy, gdy KT-100, KT-300, KT-400 oraz KT-1 zostały skonfigurowane w multi-obiektowej bramce. KT-100, KT-300, KT-400 oraz KT-1 pozwalają na integrację z dowolnym zewnętrznym systemem alarmowym. Po dodaniu tych kontrolerów Kantech do istniejącego systemu alarmowego, użytkownicy kart będą mogli uzbroić/rozbroić istniejące systemy poprzez proste użycie karty przy drzwiach wejścia/wyjścia. Dodanie klawiatury zwiększy bezpieczeństwo systemu, ponieważ użytkownicy będą musieli wprowadzić swój kod PIN (nie odnosi się do drzwi KTES). Istnieją dwa sposoby na uzbrojenie/rozbrojenie albo odroczenie zewnętrznego systemu alarmowego:

- przy prawidłowym wczytaniu karty i uruchomieniu wejścia uzbrajającego.
- przy wprowadzeniu prawidłowego kodu uzbrajającego i uruchomieniu wejścia uzbrajającego.

Może występować dowolna kombinacja tych opcji. Na przykład, system zostanie rozbrojony przy pomocy prawidłowego kodu dostępu, podczas ważnego, zdefiniowanego terminarza i po ważnym, prawidłowym wczytaniu karty.

1 – W oknie Drzwi, wybierz zakładkę **Opcje i systemy alarmowe (Options and Alarm System)**, a następnie kliknij przycisk **Zewnętrzne systemu alarmowe (External alarm system)**. Na ekranie pojawi się okienko **Opcje Systemu alarmowego (Alarm system options)**.

2 – W zakładce **Żądanie uzbrojenia (Arming request)**, wybierz **Linia dozorowa żądania uzbrojenia (Arming request input)**. Będzie to Linia dozorowa, które zostanie aktywowane przy żądaniu uzbrojenia zewnętrznego alarmu.

3 – Kiedy już wybrałeś Wejście linii dozorowej, musisz ustawić **Włącz terminarz żądania uzbrojenia (Enable arming request schedule)**, podczas którego żądanie będzie ważne.

4 – Jeżeli możliwe, wybierz **Poziom dostępu uzbrojenia (Arming access level)**.

- Opcja Grupa pozwala wybrać wszystkie poziomy dostępu.
- Opcja Pojedyncze pozwala wybrać konkretny poziom.



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia

- Jeżeli poziom, którego szukasz nie pojawia się na liście, możesz stworzyć nowy poprzez kliknięcie prawym na pole **Poziom dostępu uzbrojenia (Arming access level)**.

5 – Aby zwiększyć poziom bezpieczeństwa systemu alarmowego:

- **Uzbrojenie po dostępie zezwolonym (Wait for access granted to arm)** wymusi na użytkownika użycia ważnej karty przed wciśnięciem wybranego przycisku.
- **Ponownie zarygluj drzwi po żądaniu uzbrojenia (Relock door on request to arm)**, będzie użyty razem z **Uzbrojenie po dostępie zezwolonym (Wait for access granted to arm)**, aby obejść terminarz.
- **Ponownie zarygluj drzwi przy uzbrojeniu po opóźnieniu wyjścia (Relock door on arming after exit delay)** ponownie zablokuje i uzbroi system po upływie opóźnienia wyjścia.
- **Nie dopuść do uzbrojenia pod wpływem statusu Wejście linii dozorowej (Prevent arming request on input status)** nie dopuści do uzbrojenia systemu, jeżeli Wejście linii dozorowej jest w stanie alarmu.

6 – Określ **Opóźnienia Wyjścia (Exit delay)** oraz **Opóźnienia Wejścia (Entry delay)** (hh:mm:ss). Opóźnienie wejścia to okres, podczas którego, system alarmowy jest omijany po zdarzeniu przyznania dostępu. Opóźnienie wyjścia to przedział czasu, przed którym system alarmowy jest uzbrojony. Maksymalna wartość: 18:12:15 dla obu. Przy użyciu systemu KT-300 maksymalna wartość to 09:06:07. Zazwyczaj opóźnienie wejścia jest krótsze niż opóźnienie wyjścia.

7 – Wybierz Wejście linii dozorowej, które będzie wskazywać **Status panelu zewnętrznego systemu alarmowego (External alarm system panel status)**. Jeżeli status wybranego wejścia jest „normalny”, oznacza to, że panel zewnętrznego alarmu jest uzbrojony.

8 – Wybierz zakładkę Wejście linii dozorowej, aby określić, które urządzenia Wejścia linii dozorowej będą nadzorowane, a które nie, w momencie uzbrojenia systemu alarmowego. Kolumna Opis Wejścia linii dozorowej zawiera wszystkie Wejścia linii dozorowej, które są zdefiniowane w systemie.

- przy użyciu pól, wybierz odpowiednia Wejścia linii dozorowej, które zewnętrzny system alarmowy ma nadzorować. Wybierz również przedmioty, dla których chcesz zawiesić nadzór (przy wejściu, przy wyjściu albo w momencie, gdy system jest rozbrojony).

9 – Wybierz zakładkę **Żądanie rozbrojenia (Disarming request)**, aby wybrać **Wejścia linii dozorowej do wstrzymania uzbrojenia (Input to postpone arming)**.

10 – Wybierz terminarz z listy **Włącz terminarz wstrzymania uzbrojenia (Enable postpone arming schedule)**.

11 – Możesz zaznaczyć pole **Opóźnienie po dostępie zezwolonym (Wait for access granted to postpone)**. Jeżeli ta opcja została wybrana, system alarmowy będzie wstrzymany wyłącznie po wczytaniu ważnej karty i następnie wciśnięciu przez użytkownika wybranego przycisku na Klawiaturze do wstrzymania zewnętrznego systemu alarmowego.

12 – Wybierz **Poziom dostępu do rozbrajania lub opóźnienia rozbrajania (Postpone or disarm access level)** z listy.

13 – Wybierz zakładkę **Przełącznik**, aby określić przełącznik (**Partycja i Przełączniki (Partition and Relays)** dla KT-400, aby określić grupę przełączników) i status Wejścia linii dozorowej dla przełączników zewnętrznego systemu alarmowego.

Notatka: kiedy wybierzesz Przełącznik alarmowy, możesz określić dla niego Rodzaj aktywacji. Może być aktywowany czasowo albo na stałe.

Komentarz (Comment)

Sprawdź: Pole komentarza



Zarządzanie poziomami dostępu do drzwi (Managing Door Access Levels)

Wybierz kartę Poziom dostępu, aby zarządzać harmonogramem poziomu dostępu dla tych drzwi. Ta karta wyświetla wszystkie

poziomy dostępu, do których można przypisać drzwi.

- Aby utworzyć nowy harmonogram, kliknij prawym przyciskiem myszy sekcję Terminarz i wybierz Nowy.
- Aby edytować istniejące harmonogramy, kliknij prawym przyciskiem myszy sekcję Harmonogram i wybierz Edytuj.
- Aby zastosować istniejące harmonogramy do poziomu dostępu, kliknij listę rozwijaną obok harmonogramu.

Aby uzyskać więcej informacji na temat poziomów dostępu, kliknij tutaj.



Konfigurowanie wyjść sterujących (Relay Configuraiton)

Wyjściowe przekaźniki kontrolne (output control relays) znajdujące się na KT-100, KT-200, KT-300, KT-400 oraz KTES mogą być wykorzystywane do aktywowania alarmów albo innych urządzeń, takich jak m.in. klimatyzacja, wentylacja, etc. Te przekaźniki mogą być aktywowane według harmonogramów albo zdarzeń raportowanych przez system. Mogą również zostać aktywowane, aby wskazać stan m.in. systemu alarmowego.

Definiowanie przekaźnika

1 – z zakładki Definiowanie urządzeń wybierz Przekaźnik.

2 – wybierz Filtr obiektów z listy.

3 – wybierz Bramkę.

4 – z listy Połączenie wybierz połączenie, na którym znajduje się kontroler.

5 – z listy Przekaźnik wybierz przekaźnik, który chcesz zdefiniować. Po wybraniu zostanie wyświetlona sekcja języka. Możesz zmienić nazwę wybranego przekaźnika.

6 – w zakładce Ogólne wybierz Tryb działania przekaźnika:

- **Normalny:** przekaźnik jest wyłączony (nieaktywny), aż nie zostanie aktywowany przez operatora, zdarzenia albo harmonogram systemu.

- **Odwrócony:** przekaźnik jest włączony (aktywne albo w stanie uśpienia), aż nie zostanie wyłączony (dezaktywowany) przez operatora, zdarzenia albo harmonogram systemu.

7 – określ Harmonogram automatycznej aktywacji: kiedy ten harmonogram jest ważny, przekaźnik zostanie aktywowany według określonego trybu aktywacji.

8 – określ Akcję wyłączenia przekaźnika: kiedy ten harmonogram jest ważny, przekaźnik zostanie wyłączony (dezaktywowany) według określonego trybu aktywacji.

9 – ustaw Czasowy regulator aktywacji (**Temporary activation timer**), aby określić opóźnienie, na czas którego przekaźnik zostanie czasowo włączony po aktywacji.

Notatka: kiedy licznik jest nastawiony na 0, domyślne opóźnienie aktywacji jest nastawione na 5 sekund. Maksymalny dopuszczalny czas: 9:06:07 (h:mm:ss); dla KT-400, maksymalny dopuszczalny czas to: 18:12:15.

10 – wybierz **Grafikę oraz Podgląd wideo** powiązane z przekaźnikiem.

Komentarz (Comment)

Sprawdź: Pole komentarza



Konfiguracja linii dozorowych (Input Configuration)

Kontrolery drzwi mogą monitorować stan punktów wejść, takich jak: czujnik stanu drzwi, zamki, punkty alarmowe, detektory ruchu, czujniki temperatur, REX, etc. KT-100 monitoruje stan 4 punktów wejść, KT-200 16, KT-300 8, z maksymalnym obciążeniem do 16.

- **Dla KT-200:** wejścia są otwarte lub zamknięte, stykami połączone w serii z jednym rezystorem. Jeżeli styki są połączone w serii z zielonym rezystorem, liczba wejść będzie nieparzysta. Jeżeli styki są połączone w serii z czerwonym rezystorem, liczba wejść będzie parzysta.

- **Wejście linii dozorowej 1** (czujnik stanu drzwi) i **Wejście linii dozorowej 2** (żądanie wyjścia) są zarezerwowane dla Drzwi 1 na kontrolerze, podczas gdy Wejście 9 (czujnik stanu drzwi) i Wejście linii dozorowej 10 (żądanie wyjścia) są zarezerwowane dla Drzwi 2 na tym samym kontrolerze. Wejście linii dozorowej wykorzystane do czujnika stanu drzwi albo czujnika stanu REX NIE POWINNY mieć terminarza „monitorującego” określonego w menu Definiowanie Wejść.

- **Dla KT-100:** Wejście linii dozorowej 1 jest zarezerwowane dla czujnika stanu drzwi, a Wejście linii dozorowej 2 jest zarezerwowane dla żądania wyjścia.

- **Dla KT-300:** Wejście linii dozorowej 1 powinno być zarezerwowane dla czujnika stanu drzwi 1, a Wejście linii dozorowej 2 powinno być użyte dla żądania wyjścia dla drzwi 1 na kontrolerze. Wejście linii dozorowej 3 powinno być zarezerwowane dla czujnika stanu drzwi 2, a Wejście linii dozorowej 4 powinno być użyte dla żądania wyjścia dla drzwi 2 na tym kontrolerze.

- **Dla KT-400:** Wejście linii dozorowej 1 powinno być zarezerwowane dla czujnika stanu drzwi 2, a Wejście linii dozorowej 2 powinno być użyte dla żądania wyjścia dla drzwi 1 (Drzwi REX 1) na kontrolerze. Wejście linii dozorowej 5 powinno być zarezerwowane dla czujnika stanu drzwi 2, a Wejście linii dozorowej 6 powinno być użyte na żądanie wyjścia dla drzwi 2 tego kontrolera. Wejście linii dozorowej 9 powinno być zarezerwowane dla czujnika stanu drzwi 3, a Wejście linii dozorowej 10 powinno być użyte na żądanie wyjścia dla drzwi 3 tego kontrolera. Wejście linii dozorowej 13 powinno być zarezerwowane dla czujnika stanu drzwi 4, a Wejście linii dozorowej 6 powinno być użyte na żądanie wyjścia dla drzwi 4 tego kontrolera.

Notatka: dla pojedynczej bramki limity są następujące: 2048 połączeń, 10000 drzwi, 100000 kart, 100000 Linii dozorowych (input) i wyjść (output).

Definiowanie Wejścia linii dozorowej (Defining Input)

Przy pomocy przycisku **Wejścia linii dozorowej (Input)** na pasku narzędzi Urządzenia możesz definiować Wejścia linii dozorowej. Możesz również definiować Wejścia linii dozorowej przy pomocy programu **Ustawienia ekspresowe (Express Setup)** podczas definiowania kontrolera.

1 – Z paska narzędzi **Urządzenia** wybierz przycisk **Wejścia linii dozorowej**.

2 – Wybierz **Filtr obiektu** z listy.

3 – Wybierz **Bramkę**.

4 – Z listy Połączenie wybierz połączenie, na którym znajduje się kontroler.

5 – Z listy **Wejścia linii dozorowej**, wybierz Wejścia linii dozorowej, które chcesz definiować. Możesz nazwać wybrane Wejścia linii dozorowej.



6 – Z zakładki **Ogólne** przypisz **Terminarz monitorowania** do wybranego wejścia. Według tego terminarza system będzie nadzorować stan wejścia. W trakcie działania terminarza, zmiana w stanie wejścia wygeneruje zdarzenie „**Wejście linii dozorowej w alarmie**” lub „**Przywrócenie wejścia**”.

Wejście linii dozorowej wykorzystane do czujnika stanu drzwi, REX albo Śluzu NIE POWINNO mieć zdefiniowanego terminarza monitorowania.

7 – Określ **Normalne warunki** dla Wejścia linii dozorowej: może być **Otwarte** i **Zamknięte**.

Notatka: przy korzystaniu z pojedynczego lub podwójnego rezystora EOL, ustaw Normalne warunki Wejścia linii dozorowej (Input) na Zamknięte.

8 – Określ **Nienormalne warunki** dla Wejścia linii dozorowej: może być **Alarm** lub **Aktywuj**.

Notatka: przy konfigurowaniu parametrów zdarzenia przy wybranych zdarzeniach Wejście linii dozorowej w alarmie (Input in alarm) albo Wejście linii dozorowej aktywowane (Input activated), tylko Wejścia linii dozorowej (inputs) odpowiadające tym kryteriom są wyświetlone. Zobacz Definiowanie parametrów zdarzeń.

9 – Domyślnie, EntraPass nie wybierze **Wstrzymaj aktualizację statusu (Suspend status update)**, w przypadku braku monitorowania. W razie potrzeby ta opcja może jednak zostać włączona.

10 – Określ **Czas odpowiedzi Wejścia linii dozorowej**. To opóźnienie odpowiada przedziałowi czasu, w którym Wejście linii dozorowej musi pozostać w niezmienionym stanie zanim przejście zostanie rozpoznane. Opóźnienie jest wyznaczone w minutach (mm:ss:cc). Przedział: od 10 sekund do 10:55:35; dla czasu odpowiedzi alarmu oraz przywrócenia po alarmie.

- **Czas odpowiedzi alarmu (Alarm response time (mm:ss:cc)):** opóźnienie zanim system wygeneruje wejście i zdarzenie alarmowe. Domyślnie: 55 cc.

- **Czas przywrócenia po alarmie (Restore response time (mm:ss:cc)):** opóźnienie zanim system wygeneruje zdarzenia przywrócenia wejścia. Domyślnie: 55 cc.

Notatka: określenie czasu odpowiedzi Wejścia linii dozorowej (Input) pozwala na określenie czasu odpowiedzi w przypadku zmiany stanu czujnika stanu drzwi oraz pomaga w wygenerowaniu tylko jednego zdarzenia dla każdego przejścia, jeśli ten czas jest dłuższy niż czas odpowiedzi. Na przykład, opóźnienie 01:00:00 wymaga, aby zdarzenie „trwało” przez przynajmniej 1 minutę, zanim zostanie zareportowane.

11 – Określ opcje Systemu **Wejścia Telefonicznego (Telephone Entry System)** (tylko dla KTES)

Notatka: aby uzyskać dostęp do określenia rodzajów powiadomień pagera, rodzaj połączenia musi być ustawiony na Modem. Zobacz Konfigurowanie połączenia.

- **Typ powiadomienia pager (Pager call type)** (wyłącznie KTES): możesz wybrać **Brak powiadomienia (Do not call)** – informacja o zdarzeniu nie zostanie wysłana; **Powiadom natychmiast (Call immediately)** – informacja zostanie wysłana natychmiast; **Powiadom według terminarza (Call when scheduled)** – informacja zostanie wysłana według terminarza. Domyślnie: Brak powiadomienia.

- Pod typem powiadomienia modemu, przypisz opcję, która najbardziej pasuje do raportowaniu zdarzeń. Domyślnie: Brak powiadomienia.

- **ID pagera Wejścia linii dozorowej (Input pager ID):** wprowadź kod pagera odpowiadający wybranemu wejściu. Możliwe wartości: 201, 202, 203 oraz 204.

Notatka: aby określić rodzaje powiadomień pagera dla każdego rodzaju zdarzeń, funkcja Raportowanie pagerem musi być włączona. Zobacz Konfigurowanie KTES.

12 – Wyłącznie dla KT-400 oraz KTES, zaznacz **Zastąp domyślny EOL (Override default EOL (56K))** i następnie w menu wybierz odpowiedni przedmiot. Domyślnie: niezaznaczone.

13 – Wybierz **Grafika** lub **Podgląd wideo** przypisanych do wejścia.



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia



Definiowanie Przekazników i Wejść linii dozorowej (Defining Relays and Inputs)

1 – Wybierz zakładkę **Przekaznik i Wejście linii dozorowej (Relay and input)**, aby określić przekaznik(i) albo Wejście linii dozorowej (wejścia), które będą aktywowane lub wyłączone, kiedy Wejście linii dozorowej zostanie włączone.

2 – Z listy **Aktywuj przekaznik (Activate relay)**, wybierz przekaznik albo grupę przekazników, które zostaną aktywowane w momencie włączenie wejścia.

3 – **Czasowo włącz przekaznik (Activate relay temporarily)** aktywuje przekaznik według **Parametry czasowej aktywacji (Temporary activation parameters)** zdefiniowane w okienku **Przekaznik**. Domyślnie: niezaznaczone.

4 – W polu **Zegar czasowego wyłączenia (Temporary Shunt Timer (h:mm:ss))** określ przedział czasu, w którym Wejście linii dozorowej nie jest monitorowane. Wartość maksymalna: 18:12:15, kiedy używasz KT-400 albo KTES. Domyślnie: 00:00:00.

Notatka: aby system prawidłowo przeprocesował opóźnienie resetu przy czasowym wyłączeniu, opcja Zegar czasowego wyłączenia (Temporary Shunt Timer) musi być włączona przy definiowaniu Wejścia linii dozorowej (Input), które zresetuje opóźnienie. Na przykład, jeżeli Wejście linii dozorowej 1 czasowo odsunie Wejście linii dozorowej 2, Zegar czasowego wyłączenia (Temporary Shunt Timer) musi zostać określony również przy definiowaniu Wejścia linii dozorowej 2.

5 – Z listy **Wyłącz Wejście linii dozorowej (Shunt input)**, wybierz Wejście linii dozorowej, które nie będzie monitorowane w trakcie, gdy Wejście linii dozorowej będące definiowane jest włączone.

6 – Jeżeli możliwe, zaznacz **Wyłącz Wejście linii dozorowej tymczasowo (Shunt input temporarily)** oraz **Resetuj opóźnienie dla czasowego wyłączenia (Reset delay for shunt temporarily)**. Domyślnie: oba niezaznaczone.

7 – **Opóźnienie przed przywróceniem (Delay before unshunt)**: zakres czasowy od 00:00:01 do 18:12:15.

Notatka: kiedy ustawienia Wejścia linii dozorowej (input) są odtworzone albo przywrócone do normalnych warunków, wyłączone Wejście linii dozorowej również zostanie do nich przywrócone. Odpowiednie zdarzenia zostaną wygenerowane przez system zarówno przy wyłączeniu Wejścia linii dozorowej, jak i przywróceniu.



Definiowanie parametrów linii dozorowej czujnika antysabotażowego oraz stanów alarmowych linii dozorowej (Defining Tamper and Trouble)

- 1** – Wybierz zakładkę **Czujnik antysabotażowy oraz stany alarmowe linii dozorowej (Tamper and trouble)**, aby przypisać przekaźnik albo grupę przekaźników, które mają zostać aktywowane w przypadku sabotażu albo problemu. Ta zakładka dla strefy jest widoczna wyłącznie w DEOL.
- 2** - Z listy **Aktywuj przekaźnik (Activate relay)** (Alarm czujnika antysabotażowego), wybierz przekaźnik albo grupę przekaźników, które zostaną aktywowane, gdy Wejście linii dozorowej jest sabotowane.
- 3** - **Czasowo włącz przekaźnik (Activate relay temporarily)** aktywuje przekaźnik według **Parametry czasowej aktywacji (Temporary activation parameters)** zdefiniowane w okienku **Przekaźnik**. Domyślnie: niezaznaczone.
- 4** - Z listy **Aktywuj przekaźnik (Activate relay)** (Wejście linii dozorowej ma problem), wybierz przekaźnik albo grupę przekaźników, które zostaną aktywowane, gdy Wejście linii dozorowej ma problem.
- 5** - **Czasowo włącz przekaźnik (Activate relay temporarily)** aktywuje przekaźnik według **Parametry czasowej aktywacji (Temporary activation parameters)** zdefiniowane w okienku **Przekaźnik**. Domyślnie: niezaznaczone.

Definiowanie Wejścia linii dozorowej dla drzwi windy (Defining an Input for an Elevator Door)

Kiedy Wejście linii dozorowej, które jest definiowane albo edytowane jest używane, jako kontrola windy, zakładka **Winda** jest wyświetlona w oknie **Definiowanie Wejścia linii dozorowej**. Możesz powiązać wejścia z przyciskiem. Przycisk może zostać wykorzystany przez strażnika albo recepcjonistę, aby czasowo udostępnić piętra zdefiniowane w sekcji **Aktywowanie grupy pięter (Floor group activation)**.

- 1** – W oknie **Definiowanie Wejścia linii dozorowej**, wybierz zakładkę **Winda**.

Notatka: do wyboru będą dostępne wyłączenie piętra oznaczone X w kolumnie Stan w menu Grupa pięter. System udostępni czasowo wybór pięter zgodnie z opóźnieniem zdefiniowanym w menu Drzwi. Aby opcja była aktywowana należy wybrać prawidłowy terminarz (Włącz listę terminarzy). Może istnieć możliwość określenie drzwi, jako kabiny windy, aby uzyskać dostęp do tej zakładki.

- 2** – W sekcji **Wybierz kabinę do aktywacji grupy pięter (Select cab for floor group activation)**, wybierz kabinę powiązaną z wejściem.
- 3** – Wybierz **Grupę pięter** powiązaną z wybraną kabiną, która zostanie włączona, gdy Wejście linii dozorowej zostanie aktywowane.
- 4** – Wybierz terminarz, według którego zdefiniowane Wejście linii dozorowej będzie wykonywać polecenia.



Włączenie zdalnego raportowania zdarzeń (Enabling Remote Event Reporting)

1 – Wybierz zakładkę **Wejście linii dozorowej zdarzeń (Input event)**.

2 – Z listy **Przełącznik lokalnej aktywacji (Local activation relay)**, wybierz przełącznik albo grupę przełączników, które zostaną aktywowane, gdy to Wejście linii dozorowej znajdzie się w alarmie.

Notatka: grupa przełączników jest dostępna wyłącznie przy korzystaniu z KT-400.

3 – Pod **rodzajem powiadomienia modemu** przypisz opcję, która najbardziej pasuje do raportowaniu zdarzeń. Domyślnie: Brak powiadomienia.

Notatka: aby uzyskać dostęp do określenia rodzajów powiadomień modemu, rodzaj połączenia musi być ustawiony na Modem. Zobacz Konfigurowanie połączenia.

Komentarz (Comment)

Sprawdź: Pole komentarza

Konfiguracja wyjść sterujących sygnalizatorami (Output Device Configuration)

Wyjścia (outputs) zazwyczaj kontrolują czynniki LED oraz syreny. Dostępne są 4 wyjścia per KT-200, KT-300 (dwa na drzwi) oraz 16 dla kontrolera KT-400 (4 na drzwi). KT-100 nadzoruje stan dwóch wyjść. Elektryczne wyjścia są konfigurowane, jako otwarty-kolektor. Możesz konfigurować urządzenia wyjścia z menu definiowania kontrolerów albo z okna bramki.

Notatka: dla pojedynczej bramki limity są natępujące: 2048 połączeń, 10000 drzwi, 100000 kart, 100000 wejść (input) i wyjść (output).

Definiowanie opcji dla wyjścia (Defining General Options for an Output)

1 – z okna **Konfigurowanie urządzeń** wybierz **Wyjścia**.

Notatka: sekcja Różne jest ukryta na wypadek korzystania z systemu KT-400, ponieważ elementy są już zdefiniowane w zdarzeniach Bramki/KT-400.

2 – wybierz **Filtr obiektu** z list.

3 – wybierz **Bramkę**.

4 – z listy **Połączenie** wybierz połączenia, gdzie zlokalizowany jest kontroler.

5 – z listy **Wyjście** wybierz wyjście, które chcesz zdefiniować. Po wybraniu, włączona zostanie sekcja języka. Możesz zmienić nazwę wybranego wyjścia.

6 – z zakładki **Ogólne** wybierz **Tryb działania** dla urządzenia (domyślny: **Normalny**):

- **Normalny:** wyjście (output) jest przyłączane do masy w momencie aktywacji.
- **Odwrócony:** w momencie aktywacji wyjście (output) jest obwodem otwartym.

7 – w sekcji **Wybrane drzwi** wybierz drzwi, które będą miały wpływ na konfigurowane wyjście (output):

- **Pierwsze drzwi:** tylko port pierwszych drzwi będzie podążać za stanem zaprogramowanym dla tych zdarzeń.
- **Drugie drzwi:** tylko port drugich drzwi będzie podążać za stanem zaprogramowanym dla tych zdarzeń.

Notatka: ta opcja nie jest dostępna z KT-100 oraz KTES.



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia

8 – ustaw Opóźnienie okresu aktywacji (m:ss) (**Activation period (m:ss) delay**) - określa czas aktywacji, podczas którego wyjście (output) pozostaje aktywne. Zakres od 1 sekundy do 4 minut i 15 sekund. Domyślnie: 5 sekund.

Notatka: ta opcja nie jest dostępna przy korzystaniu z KT-400 oraz KTES.

Notatka: jeśli korzystasz z opcji Integracja wideo, EntraPass umożliwia przypisanie wszystkich komponentów systemu do poglądu wideo w ten sam sposób, w jaki przypisujesz je do interaktywnego planu piętra (grafika). Aby to zrobić wybierz pogląd wideo, w którym chcesz wyświetlić komponenty systemu (stację roboczą, obiekt, bramki, kontroler, etc.).



Powiązanie zdarzeń z zewnętrznymi wyjściami (Associating Events with Auxiliary Outputs)

Zdarzenia systemowe mogą włączyć zewnętrzne wyjścia. Możesz zdefiniować sposób, w jaki zdarzenia będą włączać wyjścia.

1 – wybierz zakładkę Definicja.

2 – w kolumnie Opcje powiąż zdarzenie ze stanem wyjścia. Domyślnie: brak.

- Stały przedział czasowy (**Steady timed**): wyjście nie będzie „migać” oraz pozostanie aktywne przez określony czas aktywacji i następnie powróci do normalnego stanu po upływie tego okresu.
- Migający przedział czasowy (**Flash timed**): wyjście będzie „migać” oraz pozostanie aktywne przez określony czas aktywacji i następnie powróci do normalnego stanu po upływie tego okresu.
- Stały (**Steady**): wyjście z tym ustawieniem nie będzie „migać”, pozostanie aktywne do powrotu do normalnego stanu.
- Migający (**Flash**): wyjście będzie „migać” i pozostanie aktywne do przywrócenia jego normalnych warunków.

Notatka: opóźnienia włączenia-wyłączenia są definiowane podczas definiowania bramki. Zobacz Konfigurowanie bramek EntraPass. Zdarzenia dla włączenia-wyłączenia różnią się zależnie od wybranego rodzaju bramki.

Komentarz (Comment)

Sprawdź: Pole komentarza



Szablony Czytników (Reader Templates)

Użyj szablonu czytnika, aby zdefiniować sposób konfiguracji czytnika. Do szablonów czytnika można używać tylko czytniki kart ioSmart w trybie RS-485. Utworzenie szablonu umożliwia udostępnienie tej samej konfiguracji w wielu czytnikach kart. Aby utworzyć szablon czytnika, wykonaj następujące kroki:

1 - Kliknij kartę **Urządzenia**.

2 - Kliknij **Szablon czytnika** w menu. Gdy pojawi się okno szablon czytnika, kliknij ikonę **Nowy** aby włączyć edycję.

3 - Wybierz **kolor diody** dla stanów, **Buzzer** i **podświetlanie** dla każdego stanu czytnika.

4 - Wybierz opcję **Wyślij UID** dla czytnika. Użyj tej opcji, aby określić, który typ karty jest akceptowany przez czytnik.

- **Nigdy**. Wysyłaj identyfikator karty tylko z kart ioSmart
- **Kiedy inna karta niż ioSmart**. Wyślij identyfikator karty z kart ioSmart i UID z kart innych niż ioSmart.
- **Zawsze (bez szyfrowania)**. Zawsze wysyłaj identyfikator UID z karty.

5 - Wybierz opcję **HID 125 kHz** i **ISO 14438B**, aby zdefiniować technologię karty.

6 - Jeśli kontroler łączy się z czytnikami ioSmart i chcesz włączyć technologię BLE, wybierz Pole wyboru **włącz Bluetooth**. EntraPass domyślnie wybiera pole wyboru **BLE**, ponieważ wszystkie czytniki ioSmart są włączone BLE.

7 - Wybierz intensywność podświetlenia klawiatury w trybie bezczynności.

8 - Ustaw opóźnienia dla czasu błysku LED (ms), czasu trwania sygnału brzęczyka (ms) i podświetlenia klawiatury czas trwania (s).



Konfiguracja zintegrowanych urządzeń (Integrated Panel Configuration)

Minimalne wymagania do Podglądu i Obsługi Zintegrowanych Przycisków (Minimum Requirements to View and Use the Integration Buttons)

- **Integration DLL** musi być wczytane z serwera **EntraPass**. Jeżeli pasek narzędzi nie wyświetla dwóch przycisków, zobacz **Konfiguracja parametrów systemu (System Parameters Configuration)**.

- Zewnętrzne podzespoły muszą być podłączone do portu szeregowego bramki multi-objektowej albo portu seryjnego kontrolera KT-400.

- Zewnętrzne podzespoły muszą być zasilane.

Notatka: zanim zdefiniujesz panel integracji w EntraPass upewnij się, że żadna partycja nie jest uzbrojona. Jeżeli przynajmniej jedna partycja jest uzbrojona programowanie panelu nie będzie możliwe.

1 – Z paska narzędzi **Urządzenia**, kliknij przycisk **Zintegrowany panel (Integrated Panel)**.

2 – Kliknij **Nowy** i przypisz nazwę w dwóch językach.

3 – Wybierz **Panel** z listy.

Zakładka Ogólne (General Tab)

1 – Wybierz **Typ połączenia** z listy.

2 – Wybierz **Model Panelu** z listy.

3 – Jeżeli opcja **Wideo** jest włączona, pojawi się pole **Poglądu Wideo**. W tym przypadku wybierz Pogląd wideo w którym chcesz, aby pojawił się definiowany komponent. Zobacz: Definiowanie poglądu wideo (**Video Views Definition**)

4 – Z listy **Grafika** możesz wybrać grafikę, do której aplikacja jest przypisana. Zobacz: **Definiowanie Grafiki (Graphics Definition)**.

5 – Kliknij przycisk **Konfiguracja**, aby wyświetlić okienko **Panel Konfiguracji (Panel Configuration)**. Wyświetla się inne okienko, zależnie od wybranego typu połączenia:



Podsumowanie parametrów Panelu Konfiguracji

Parametr	NEO połączony z kontrolerem szeregowym lub IP	NEO połączony z bramką szeregową lub IP	PowersSeries połączony z szeregowym kontrolerem	PowersSeries połączony z szeregową bramką	MaxSys połączony z szeregowym kontrolerem	MaxSys połączony z szeregową bramką	Bentel Kyo320 połączony z bramką IP	Honeywell Galaxy Kyo320 połączony z bramką IP	Simplex 4100 połączony z szeregowym kontrolerem	Simplex 4100 połączony z szeregową bramką
Zarządzanie wirtualną strefą. Wybierz: Pojedynczy kontroler albo Wiele kontrolerów	Tak									



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia

Parametr	NEO połączony z kontrolerem szeregowym lub IP	NEO połączony z bramką szeregową lub IP	PowersSeries połączony z szeregowym kontrolerem	PowersSeries połączony z szeregową bramką	MaxSys połączony z szeregowym kontrolerem	MaxSys połączony z szeregową bramką	Bentel Kyo320 połączony z bramką IP	Honeywell Galaxy Kyo320 połączony z bramką IP	Simplex 4100 połączony z szeregowym kontrolerem	Simplex 4100 połączony z szeregową bramką
Model włamań. Wybierz zarządzania dostępem: Przez partycje (uzbrojenie/rozbrojenie systemu przez kod); Przez użytkownika (uzbrojenie/rozbrojenie systemu przez kartę)	Tak		Tak		Tak					
Wybór kontrolera dla przejścia: wybierz kontroler do którego podłączony jest panel, aby ustalić połączenie	Tak		Tak		Tak				Tak	
Numer identyfikacji integracji (wprowadź DSC TL280R)	Tak	Tak								
Kod dostępu integracji (wprowadź DSC TL280R)	Tak	Tak								



EntraPass - Instrukcja instalacji i obsługi programu
Urządzenia

Liczba cyfr (liczba cyfr dla głównego kodu)	Tak	Tak	Tak	Tak	Tak	Tak	Tak			
Główny kod dostępu (wykorzystywany do programowania panelu)	Tak	Tak	Tak	Tak	Tak	Tak				
Domyślny kod dostępu (wybierz z listy)	Tak	Tak	Tak	Tak	Tak	Tak				
Port komunikacji COM (wykorzystywany przy operacjach, gdy system korzysta z trybu „zarządzony przez partycję”)		Tak		Tak		Tak				



EntraPass - Instrukcja instalacji i obsługi programu
Urządzenia

Parametr	NEO połączony z kontrolerem szeregowym lub IP	NEO połączony z bramką szeregową lub IP	PowersSeries połączony z szeregowym kontrolerem	PowersSeries połączony z szeregową bramką	MaxSys połączony z szeregowym kontrolerem	MaxSys połączony z szeregową bramką	Bentel Kyo320 połączony z bramką IP	Honeywell Galaxy Kyo320 połączony z bramką IP	Simplex 4100 połączony z szeregowym kontrolerem	Simplex 4100 połączony z szeregową bramką
Typ komunikacji (wybierz pomiędzy szeregowym RS-232, IP-TCP albo IP-UDP)	Tak	Tak								
Filtr połączenia (do filtrowania kontrolerów na bramce)	Tak	Tak								
Szybkość transmisji (domyślnie: 9600)				Tak		Tak				
Adres IP Ethernet (wprowadź do zapewnienia komunikacji)							Tak	Tak		
Adres nazwy domeny (wprowadź do zapewnienia komunikacji)							Tak	Tak		
Port DSL							Tak			



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia

Parametr	NEO połączony z kontrolerem szeregowym lub IP	NEO połączony z bramką szeregową lub IP	PowersSeries połączony z szeregowym kontrolerem	PowersSeries połączony z szeregową bramką	MaxSys połączony z szeregowym kontrolerem	MaxSys połączony z szeregową bramką	Bentel Kyo320 połączony z bramką IP	Honeywell Galaxy Kyo320 połączony z bramką IP	Simplex 4100 połączony z szeregowym kontrolerem	Simplex 4100 połączony z szeregową bramką
Porty IP (wybierz 3 porty IP do komunikacji z panelem Galaxy)								Tak		
Wartość PIN (wprowadź numer PIN)							Tak			
Zaznacz Zawsze potwierdzają adres MAX przy włączaniu (Always validate MAC address upon startup) , aby sprawdzić czy jest to prawidłowy panel.							Tak			
Importuj punkty IDNet (Import IDNet points) , aby automatycznie zaimportować punkty panelowe zdefiniowane na płycie IDNet.									Tak	Tak



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia

Parametr	NEO połączony z kontrolerem szeregowym lub IP	NEO połączony z bramką szeregową lub IP	PowersSeries połączony z szeregowym kontrolerem	PowersSeries połączony z szeregową bramką	MaxSys połączony z szeregowym kontrolerem	MaxSys połączony z szeregową bramką	Bentel Kyo320 połączony z bramką IP	Honeywell Galaxy Kyo320 połączony z bramką IP	Simplex 4100 połączony z szeregowym kontrolerem	Simplex 4100 połączony z szeregową bramką
Importuj punkty przycisków panelu (Import panel button points), aby wygenerować zdarzenie EntraPass dla przycisków: • Reset systemu • Wyciszenie alarmu • ACK Główny alarm pożarowy • ACK Główny nadzór • ACK Główny Problem • ACK Główny Priorytet									Tak	Tak

Notatka: przy wyborze Dostęp przyznawany przez użytkownika, zakładka Wtargnięcie zostanie włączona (Pasek narzędzi Użytkownika > Karta). Dla KT-400 dostępna jest dodatkowa lista do wyboru kontrolera.

Zakładka Komponentów Panelu (Panel Component Tab (Bentel, DSC Maxsys, NEO, PowerSeries))

Notatka: opcja zależy od rodzaju panelu wtargnięcia. Urządzenie musi najpierw zostać utworzone w EntraPass, aby DLL zostały pobrane do odpowiedniej bramki albo KT-400. Po pobraniu, autodetekcja jest aktywna.



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia

1 – Określ parametry Strefy (Zone), Partycji (Partition), Użytkownika (User) i Wirtualnej strefy (Virtual Zone). Te parametry posiadają następujące wartości maksymalne:

Parametr	PC1616	PC1832	PC1864	HS2016	HS2032	HS2064	HS2128
Strefy	32	32	64	16	32	64	128
Partycje	2	4	8	2	4	8	8
Użytkownicy	48	72	95	48	72	95	95
Wirtualne strefy	-	-	-	16	32	32	32

2 – Wybierz liczbę Stref. Kliknij przycisk po lewej, aby wyświetlić tabelę ze zdefiniowanymi strefami. Kliknij Podgląd albo Edytuj, aby zobaczyć/edytować wybraną strefę w oknie **Zintegrowane komponenty (Integrated Component)**.

3 – Wybierz liczbę Partycji. Kliknij przycisk po lewej, aby wyświetlić tabelę ze zdefiniowanymi partycjami. Kliknij Podgląd albo Edytuj, aby zobaczyć/edytować wybraną partycję w oknie **Zintegrowane komponenty (Integrated Component)**.

4 – Wybierz liczbę Użytkowników. Kliknij przycisk po lewej, aby wyświetlić tabelę ze zdefiniowanymi użytkownikami. Kliknij Podgląd albo Edytuj, aby zobaczyć/edytować wybranego użytkownika w oknie **Zintegrowane komponenty (Integrated Component)**.

5 – Wybierz liczbę Wirtualnych stref (wyłącznie panele Neo podłączone do KT-1/KT-400). Odpowiednia liczba wirtualnych wejść zostanie dodana do **Zintegrowanego Komponentu (Integrated Component)**. Pamiętaj, że konfigurowanie wirtualnych stref w **Panelu Zintegrowanym (Integrated Panel)** umożliwia podgląd wszystkich stref na jednej stronie, w przeciwieństwie do **Zintegrowanego Komponentu (Integrated Component)**, który wyświetli tylko jedną strefę naraz.

Notatka: domyślna liczba Wirtualnych stref jest maksymalną wartością opisaną w powyższej tabelce. Celem tej opcji jest stworzenie „wirtualnych” stref w panelu alarmów, aby otrzymywać polecenia grup wybranego Wejścia linii dozorowej (input), drzwi albo zdarzeń bramki. Te polecenia są transmitowane z panelu do stacji centralnej. Panel zintegrowany Neo 1.1 wspiera 16 albo 32 wirtualnych stref: 16 dla HS2016, 32 dla HS2032, HS2064 oraz HS2128.

Notatka: opcja dostępna wyłącznie dla KT-400 oraz KT-1. Wymagany jest nowy firmware (1.16.xx dla KT-400, 1.22.xx dla KT-401, 1.02.xx dla KT-1)

6 – Kliknij przycisk Lista Wirtualnych Stref (Virtual Zone List). Tabela pozwala przypisać komponenty Kantech do wirtualnych stref DSC.

Notatka: kolumna Strefa fizyczna wyświetla się tylko przy prawidłowej komunikacji panelu DSC.

- Dla każdego Drzwi, Wejścia linii dozorowej lub Zdarzenia wybierz numer strefy oraz rodzaj zdarzenia (Alarm, Problem, Czujnik antysabotażowy), które mają zostać wysłane do centrali. Pozostałe dostępne strefy znajdują się po prawej.



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia

Komponent	Zdarzenie EntraPass	Raport Alarm	Raport Problemu	Raport Czujnika antysabotażowego
Wejście linii dozorowej	Wejście linii dozorowej w alarmie / Wejście linii dozorowej przywrócone albo w normalnym stanie	X		
	Wejście linii dozorowej w Problemie / Wejście linii dozorowej przywrócone		X	
	Wejście linii dozorowej Czujnika antysabotażowego w alarmie / Wejście linii dozorowej przywrócone			X
Drzwi	Wymuszone otwarcie / drzwi przywrócone	X		
	Drzwi otwarte za długo / drzwi przywrócone		X	
	Awaria zamka drzwi / drzwi przywrócone		X	
Wymuszenie	Opcje wymuszenia	X		
Kontrolery	Awaria zasilania AC / przywrócone		X	
	Przełącznik Czujnika antysabotażowego w alarmie / przywrócone			X
	Awaria dodatkowego zasilania / przywrócone		X	
	Awaria zasilania czytnika / przywrócone		X	
	Awaria baterii / przywrócone		X	
	Awaria komunikacji modułu / przywrócone		X	
	Awaria zasilania DC / przywrócone		X	
	Awaria zasilania zamka / przywrócone		X	
	Problemy z zasilaniem kontrolera (KT-1)		X	
Dostęp zabroniony	Dostęp zabroniony – Zły status karty		X	
	Dostęp zabroniony – Karta zgubiona lub skradziona			X
	Dostęp zabroniony – Karta wygasła	X		

- Kliknij przycisk **Dodaj**, aby dodać nowe zdarzenie do listy, albo przycisk **Usuń**, żeby usunąć zaznaczone zdarzenie.
- Kliknij **Zapisz** albo **Anuluj**, aby wrócić do okna **Zintegrowany Panel (Integrated Panel)**.
- **Drukowanie:** użyj przycisku **Drukuj** z sekcji **Wirtualna Strefa Podsumowanie (Virtual Zone Summary)**, aby wysłać parametry konfiguracyjne wirtualnej strefy do centrali.



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia

Wirtualna strefa NEO	Strefa NEO	Typ komponentu	Komponent	Zgłoś Alarm	Zgłoś Problem	Zgłoś Sabotaż
1	110	Drzwi	Drzwi #1	Tak		Tak
2	111	Drzwi	Drzwi #5	Tak	Tak	
3	112	Wejście linii dozorowej	Wejście linii dozorowej #1	Tak	Tak	Tak
4	114	Kontroler	Kontroler #4	Tak		

Zakładka RS-232 (RS-232 Tab)

1 – Wybierz **Port komunikacyjny COM (Communication port COM)** oraz **Szybkość transferu (Baud rate)** z listy.

2 – Kliknij **Zapisz**.

Konfiguracja zintegrowanych modeli (Integrated Component Configuration)

Zintegrowane komponenty (Integrated Component) mogą obsługiwać dowolny typ panelowych komponentów (partycje, strefy, etc.) pod dowolnym typem panelów (kontrola temperatury, kontrola naporu, etc.)

1 – Z paska narzędzi **Urządzenia**, wybierz **Zintegrowane panele**.

2 – Wybierz **Komponent** z listy.

Notatka: możesz korzystać z listy na pasku narzędzi, aby sortować wyświetlane komponenty po rodzaju.

3 – Wybierz **Typ komponentu**.

4 – Kliknij przycisk **Konfiguracja (Configuration Form)**, aby wyświetlić okienko **Zasilanie DSC (DSC Power Series)**.

5 – Dla typu **Użytkownika**, wprowadź **Kod dostępu użytkownika (User access code)**. Ten kod to **numer PIN**, wykorzystany do uzbrojenia i rozbrojenia partycji.

6 – Dla panelu **Simplex**, wybierz odpowiednie wartości, aby określić punkt docelowy urządzenia panelu ogniowego. Po tym, jak urządzeniu zostanie przyznany adres (zdalnie lub automatycznie zaimportowany z IDNet), użytkownik nie będzie miał możliwości zmiany – chyba, że punkt zostanie usunięty i nowy zostanie utworzony.

7 – Dla **Wirtualnej strefy**: Celem tej opcji jest stworzenie „wirtualnej” strefy w panelu alarmu, która będzie otrzymywać polecenia z grupy wybranych przekaźników, drzwi lub innych zdarzeń z bramki. Te polecenia są następnie transmitowane z panelu do stacji centralnej.

Notatka: Panel zintegrowany Neo 1.1 wspiera 16 albo 32 wirtualnych stref: 16 dla HS2016, 32 dla HS2032, HS2064 oraz HS2128.

Notatka: opcja dostępna wyłącznie dla KT-400 oraz KT-1. Wymagany jest nowy firmware (1.16.xx dla KT-400, 1.22.xx dla KT-401, 1.02.xx dla KT-1)

- Wybierz **Typ połączenia** z listy (Drzwi, Wejścia linii dozorowej lub Zdarzenia).
- Wybierz zdarzenie (sprawdź tabelę z listą zdarzeń opartych na wybranych typach komponentów).



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia

Komponent	Zdarzenie EntraPass	Raport Alarm	Raport Problemu	Raport czujnika antysabotażowego
Wejście linii dozorowej	Wejście linii dozorowej w alarmie / Wejście linii dozorowej przywrócone albo w normalnym stanie	X		
	Wejście linii dozorowej w Problemie / Wejście linii dozorowej przywrócone		X	
	Wejście linii dozorowej czujnika antysabotażowego w alarmie / Wejście linii dozorowej przywrócone			X
Drzwi	Wymuszone otwarcie / drzwi przywrócone	X		
	Drzwi otwarte za długo / drzwi przywrócone		X	
	Awaria zamka drzwi / drzwi przywrócone		X	
Wymuszenie	Opcje wymuszenia	X		
Kontrolery	Awaria zasilania AC / przywrócone		X	
	Przełącznik czujnika antysabotażowego w alarmie / przywrócone			X
	Awaria dodatkowego zasilania / przywrócone		X	
	Awaria zasilania czytnika / przywrócone		X	
	Awaria baterii / przywrócone		X	
	Awaria komunikacji modułu / przywrócone		X	
	Awaria zasilania DC / przywrócone		X	
	Awaria zasilania zamka / przywrócone		X	
	Problemy z zasilaniem kontrolera (KT-1)		X	

Urządzenia

Konfiguracja zintegrowanych paneli

Komponent	Zdarzenie EntraPass	Raport Alarm	Raport Problemu	Raport czujnika antysabotażowego
Dostęp zabroniony	Dostęp zabroniony – Zły status karty		X	
	Dostęp zabroniony – Karta zgubiona lub skradziona			X
	Dostęp zabroniony – Karta wygasła	X		

- Dla typu komponentu Drzwi lub Wejścia linii dozorowej, wskaż źródło komponentu (kontroler).
- Wybierz odpowiednią **Akcję komponentu (Component action)**, która będzie raportowana dla wirtualnej strefy i kliknij **OK**.

8 – Jeżeli opcja **Wideo** jest włączona, pojawi się pole **Poglądu Wideo** (tylko dla stref i partycji). W tym przypadku wybierz **Pogląd wideo**, w którym chcesz, aby pojawił się definiowany komponent. Zobacz: Definiowanie poglądu wideo (**Video Views Definition**)



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia

9 – Z listy **Grafika** możesz wybrać grafikę, do której aplikacja jest przypisana. Zobacz: **Definiowanie Grafiki (Graphics Definition)**.

Notatka: przycisk **Szczegóły** jest dostępny wyłącznie komponentów Użytkownik oraz Wirtualna strefa.

10 – Kliknij **Zapisz**.



Zakładka Wyzwalacz i Alarm (Trigger and Alarm tab)

Karta alarmu i wyzwalacza jest dostępna dla następujących elementów menu:

- Urządzenia ... Bramka GSI
- Urządzenia ... Magistrale
- Urządzenia ... Kontrolery KT
- Urządzenia ... Drzwi
- Urządzenia ... Przekaznik
- Urządzenia ... Linie Dozorowe
- Urządzenia ... KTES
- Definicja ... System alarmowy
- Definicja ... Obszar
- Definicja ... Guard Tour

Ta karta wyświetla podsumowanie wszystkich Wyzwalaczy i alarmów powiązanych z wybranym urządzeniem. Na karcie wyświetlane są następujące informacje:

Nagłówek	Opis
Zdarzenie	Na przykład „Drzwi zablokowane przez operatora”. Uwaga: ten nagłówek jest dostępny tylko wtedy, gdy tryb zdarzeń przypisanych do operatora został włączony.
Opis wyzwalacza	Nazwa wyzwalacza. Jest to podane, gdy stworzony jest wyzwalacz
Źródło	Wskazuje, czy wyzwalacz jest pojedynczym wyzwalaczem lub częścią grupy wyzwalającej
Wyzwalacz zdarzenia	Wskazuje, że dla tego zdarzenia został utworzony wyzwalacz zdarzenia
Alarm	Wskazuje, czy alarm jest powiązany z wyzwalaczem
Wyłączone	Wskazuje, czy wyzwalacz jest wyłączony
Grupa wyzwalaczy	Jeśli wyzwalacz jest częścią grupy, zostanie tutaj wyświetlony

Aby wyświetlić, dodać, edytować i usunąć wyzwalacz, wybierz wyzwalacz z listy i kliknij prawym przyciskiem myszy, aby otworzyć menu. Usunięcie wyzwalacza usunie tylko wyzwalacz, nie usunie aplikacji ani wybranego makropolecenia.

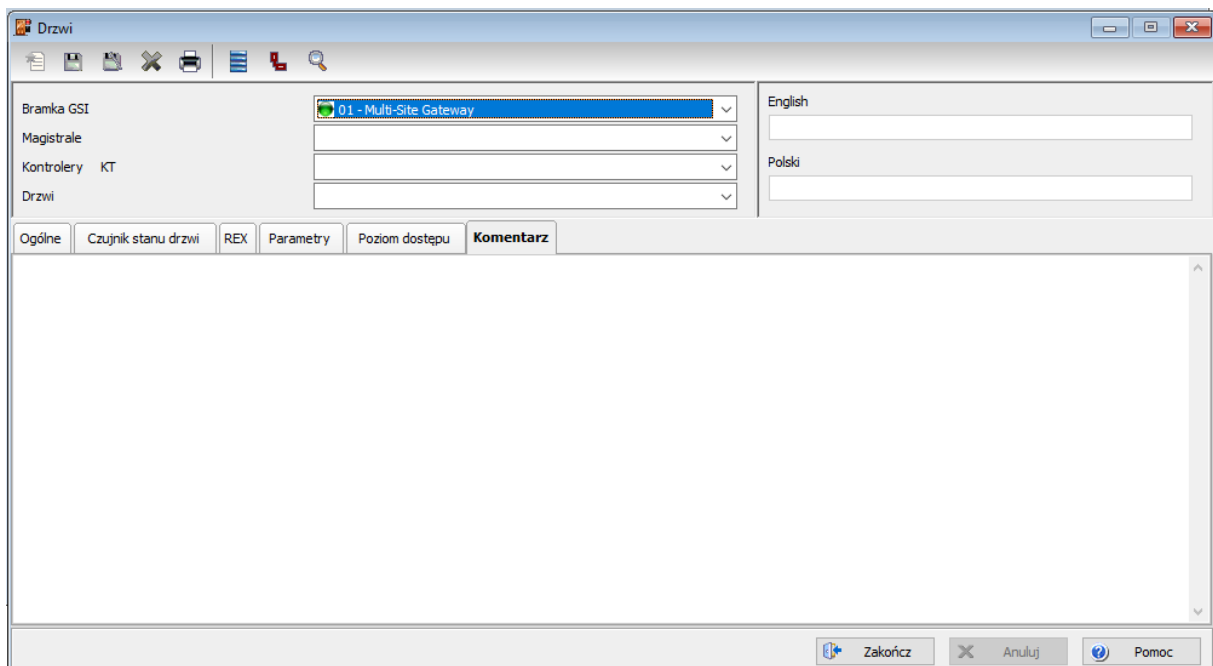


Pole komentarzy (Comment Field)

Pole komentarza jest dostępne dla następujących komponentów:

- Aplikacja EntraPass
- Aktywny katalog
- Bramka
- Obiekt
- Połączenie
- Kontroler
- Drzwi
- Przekaznik
- Wejścia linii dozorowej
- Wyjścia

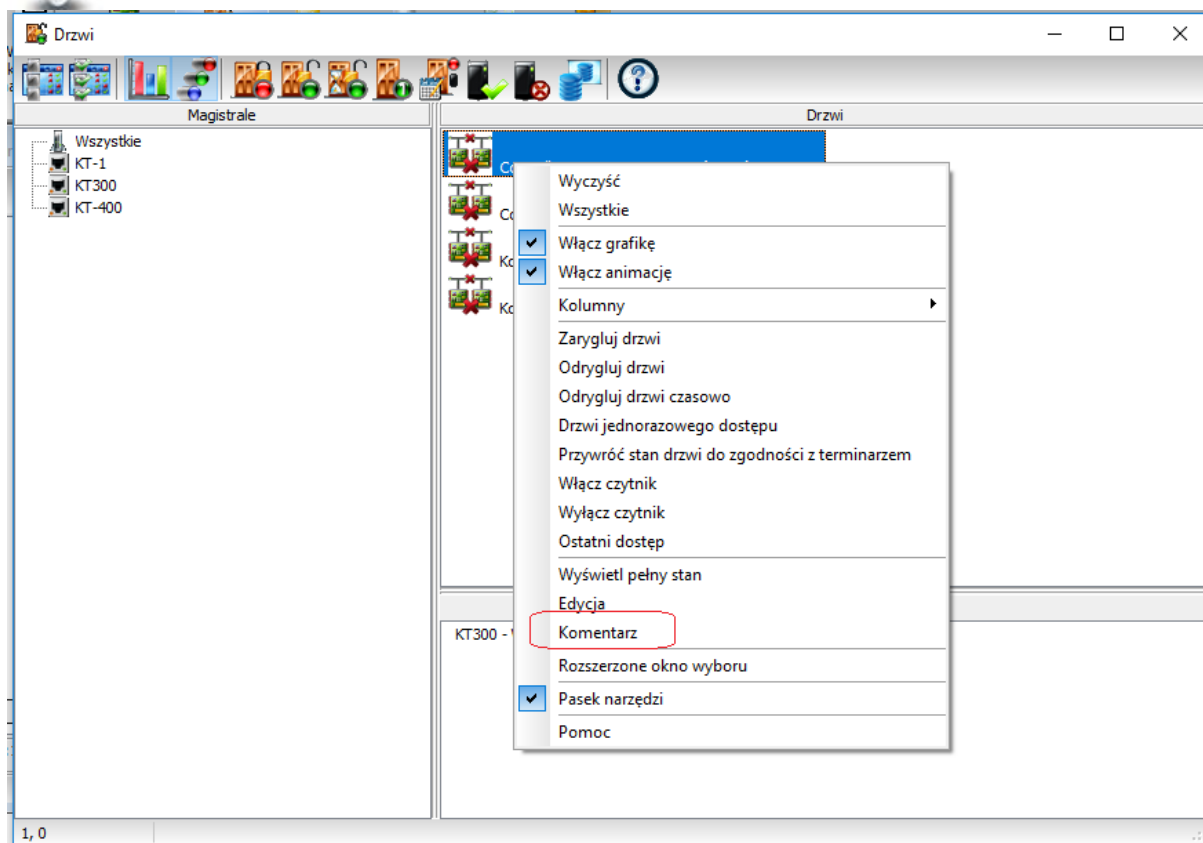
Pole komentarza może być zmodyfikowane albo usunięte w dowolnym momencie. Jego długość jest nieograniczona. Poniżej przykład z menu Urządzenia/Drzwi:



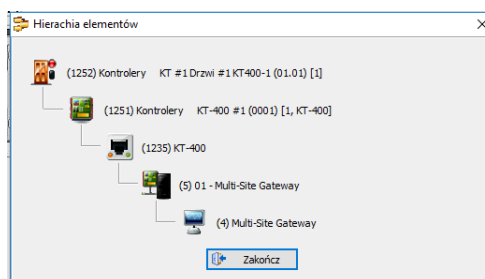
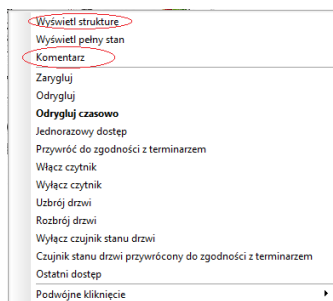
- Kliknij dwukrotnie w pole, aby wejść w tryb edycji.
- Komentarze mogą być również wyświetlane z okna Operacje (Operation), po kliknięciu prawym przyciskiem myszy na komponencie:



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia



- Komentarze mogą być również wyświetlane z Okna zdarzeń albo z grafiki (po kliknięciu prawym przyciskiem myszy na komponencie wybierz **Pokaż opiekuna/kontroler (View parent/controller)**). Pojawi się następujące okno:



- Przekieruj kursor nad kontroler, aby wyświetlić powiązane z nią komentarze.



EntraPass - Instrukcja instalacji i obsługi programu Urządzenia



Wideo

Definiowanie kamery

Definiowanie kamer (Camera Definition)

EntraPass oferuje możliwość nazw do kamer, presetów oraz wzorów w celu ułatwienie identyfikacji na pulpicie Wideo oraz wśród wszystkich zdarzeń wideo systemu.

Definiowanie kamery oznacza określenie:

- Typu
- Presetów (dla kopułkowych)
- Wzorów (dla kopułkowych)

Nazwa kamery jest wyświetlona podczas podglądu na żywo albo podglądu nagranych zdarzeń wideo (tylko Intellex). Domyślne nazwy: Kamera1, Kamera2, KameraN, gdzie N to numer ostatniej kamery.

Definiowanie kamery (Defining a Camera)

1 – Z paska narzędzi okna **Wideo**, kliknij **Kamera**. Pojawi się nowe okno.

2 – Wybierz kamerę, którą chcesz zdefiniować, następnie przypisz jej nazwę. Jeżeli system działa w dwóch językach zaleca się przypisanie nazwy w dwóch polach.

3 – Wybierz typ kamery z listy:

- **Stała kamera (Fixed camera)**: brak presetów/wzorów; użytkownicy nie mogą kontrolować stałych kamer.
- **Kopułkowa (Dome)**: presetów oraz wzory (tylko Intellex) dostępne; wybór tej opcji pozwala użytkownikowi kontrolować kamerę. Jeżeli wybrałeś tę opcję, przypisz nazwy do presetów.

4 – Zaznacz opcję **Pokaż kamerę (Show camera)**, aby kamera była dostępna do wyboru i wyświetlenia na pulpicie **Podgląd wideo (Video view)**. Ważne jest, aby zaznaczyć tę opcję, jeżeli kamera ma być dostępna w EntraPass. Tylko użytkownicy o specjalnych przywilejach będą mogli sprawdzić kamerę bez zaznaczonej opcji **Pokaż kamerę**. Aby przypisać pozwolenie dla użytkownika przejdź: System > Definiowanie użytkownika > Przywileje.



Notatka: jeśli nie zaznaczysz pola Pokaż kamerę, kamera nie zostanie wyświetlona w oknie Poglądu wideo (Podgląd wideo > Modyfikuj komponenty podglądu wideo) i tym samym nie zostanie przypisana do podglądu w Pulpicie wideo. Ta opcja umożliwia ukrycie kamery z wszelkiego podglądu. Użytkownicy bez odpowiednich uprawnień nie będą mogli wyszukiwać, eksportować, podglądać ani przeprowadzić jakiejkolwiek operacji na kamerze, do której nie mają pozwolenia dostępu. Pomimo to, wszystkie połączenia oraz odniesienia do tej kamery zostaną zachowane. Ta opcja różni się od usunięcia kamery właśnie tym, że przy usunięciu połączenia także są usuwane.

5 – Zaznacz opcję Wybierz konkretne zdarzenia (Select specific events), jeżeli chcesz, aby kamera nagrywała konkretne zdarzenia. Domyślnie, wszystkie zdarzenia kamery są wyświetlone na liście Zdarzenia wideo. Możesz jednak dzięki tej opcji zdecydować, które zdarzenia będą nagrywane przez konkretne kamery. Kiedy to zrobisz, pojawi się zakładka Zdarzenie. Możesz ją wybrać i konkretne zdarzenia będą nagrywane przez określone kamery.

6 – Przy pomocy kontroler góra/dół, ustaw liczbę presetów i wzorów dla wybranej kamery, jeżeli wybrana kamera jest kamerą kopułkową. Kiedy to zrobisz, w oknie **Kamera** pojawi się zakładka **Preset** albo **Wzór (Preset or Pattern)**.

7 – Wybierz typ podglądu, który chcesz, aby się wyświetlał przy alarmie.

- Podgląd wideo (Video View): wybrany podgląd będzie wyświetlony przy alarmie na wybranej kamerze.
- Podgląd grafiki (Graphic View): wybrany podgląd grafiki będzie wyświetlony przy alarmie na wybranej kamerze.

Powiązanie kamery z ikoną (Associating a Camera with an Icon)

EntraPass oferuje możliwość przypisania konkretnych przycisków do kamery dla łatwej identyfikacji m.in. na pulpicie Wideo.

1 – Z okna Kamera, wybierz kamerę, którą chcesz przypisać do przycisku, następnie kliknij na wybrany przycisk. Pojawi się okno **Wybierz przycisk (Select button)**.

2 – Wybierz odpowiedni przycisk do przypisania do odpowiedniej kamery. Kliknij na niego podwójnie, aby zamknąć okno. Kiedy to zrobisz, kamera zostanie powiązana z przyciskiem.

- Przycisk **Kamera** na pasku narzędzi w oknie **Kamera** pozwala na dodawanie przycisków do listy dostępnych przycisków.



Definiowanie Presetów i wzorów (Defining Presets and Patterns)

1 – Z okna Serwer wideo wybierz zakładkę Preset (albo Wzór), aby przypisać nazwy do presetów.

2 – Wybierz komórkę tabeli i nadpisz domyślną nazwę. Jeżeli korzystasz z systemu w dwóch językach, wprowadź nazwę w obu, a następnie kliknij Zamknij, aby zamknąć okno.

Notatka: jeśli wybierzesz preset albo wzór, a następnie klikniesz na przycisk Domyślny, to przypisana nazwa zostanie zastąpiona nazwą domyślną.

Definiowanie zdarzeń nagranych przez kamerę (Defining Events Recorded by a Camera)

Jeżeli w zakładce **Ogólne** wybrana jest opcja **Wybierz konkretne zdarzenia**, musisz:

- Wybrać zdarzenia, które będą nagrywane przez definiowaną kamerę i które będą wysyłane do serwera EntraPass. Ta opcja jest wyłączona, jeżeli kamera jest podłączona do Intellex LT DVR.
- Wybierz albo zdefiniuj terminarz, który będzie wykorzystany przez serwer wideo do raportowania wybranych zdarzeń do serwera EntraPass. Ten terminarz może zostać wykorzystany, jako filtr, do ograniczenia przepływu wiadomości z serwera wideo, do serwera EntraPass. Określenie przedziału czasowego pozwoli na przesyłanie zdarzeń, które miały miejsce podczas określonego przedziału czasu.

Wybieranie zdarzeń i terminarzy kamery (To Select Camera Events and Schedules)

1 - Z okna Kamera, wybierz zakładkę Zdarzenie. Zwyczajne zdarzenia kamery są wyświetlone w oknie. Są to specyficzne zdarzenia dla wybranego rejestratora.

2 – Wybierz terminarz dla raportowania zdarzeń kamery. Tylko zdarzenie, które będą miały miejsce podczas określonego przedziału czasu będą wysyłane do serwera EntraPass. Kliknięcie prawym na pole **Terminarz raportu zdarzeń (Event report schedule)**, pozwoli użytkownikowi na stworzenie nowego albo na wybranie istniejącego terminarza. Aby zdefiniować terminarz, upewnij się, że wybierasz odpowiednią kategorię dla tego terminarza. Na przykład, jeżeli przypisujesz albo definiujesz terminarz systemu (dla stacji roboczej, użytkownika, parametrów zdarzenia, przełączników wideo), ten terminarz będzie dostępny do wyboru komponentów tej kategorii. Jeżeli wybierasz terminarz dla fizycznych komponentów, takich jak: kontrolery, drzwi, Wejścia linii dozorowej; ich terminarze będą pogrupowane. Jeżeli zdefiniowałeś dwa obiekty w swoim systemie, będą istniały dwie osobne grupy terminarzy dla każdego połączenia. Możesz zdefiniować do 99 terminarzy dla każdego połączenia.

3 – Wybierz zdarzenia kamery, które chcesz wysłać do serwera EntraPass. Wybór zdarzeń do wysłania jest sposobem na kontrolowanie przepływu danych wideo, a tym samym na ograniczenie zużycia przepustowości. Lista zdarzeń jest zależna od serwera wideo:

- **Zawansowany alarm detekcji ruchu (Camera advanced motion alarm) (tylko Intellex):** kamera wyśle każde zdarzenie związane z alarmem detekcji ruchu.
- **Alarm kamery (Camera alarm) (tylko Intellex):** kamera wyśle każde zdarzenie związane ze zmianą, jak zaszła w określonym obszarze.
- **Alarm świetlny (Camera light alarm) (tylko Intellex):**
- **Alarm detekcji ruchu (Camera motion alarm):** kamera wyśle do serwera EntraPass wszystkie zdarzenia, związane z dowolnym ruchem, które zaszły w określonym obszarze.
- **Obejście kamery (Camera override) (tylko Intellex):**



EntraPass - Instrukcja instalacji i obsługi programu Wideo

- **Obszar kamery (tylko Intellex):** kamera będzie wysyłać wszystkie segmenty wideo powiązane z elementem, który wszedł do/wyszedł z monitorowanego obszaru, do serwera EntraPass.

- **Tekst alarmowy kamery (Camera text alarm) (tylko Intellex):**

4 – Wybierz zakładkę Komentarz Video Vault, jeżeli chcesz dodać informacje odnośnie definiowanej kamery. Pliki KVI oraz KVA z tej kamery, które będą zapisywane w EntraPass Video Vault, będą wyświetlane z komentarzem wprowadzonym w tym oknie.

5 – Wprowadź komentarz, który chcesz powiązać z definiowaną kamerą, po czym zapisz i zamknij okno.

Komentarz (Comment)

Sprawdź: Pole komentarza.



Bieżące nagrania (Current Recording)

Opcja Bieżące nagrania pozwala użytkownikom na przeglądanie listy wszystkich bieżących nagrań. Informacje wyświetlane zależą od źródła wywołania nagrywania:

- Rozpoczęte przez przełącznik
- Rozpoczęte przez użytkownika
- Rozpoczęte przez alarm na serwerze wideo

Przeglądanie bieżących nagrań (Viewing the Current Recordings)

1 – Z paska narzędzi Wideo, wybierz Bieżące nagrania. Wyświetli się okno pokazujące wszystkie bieżące nagrania.

Poniższa tabela przedstawia informacje wyświetlone w oknie Bieżące nagrania, w zależności od źródła nagrań.

Zainicjowane przez	Informacja
Alarm serwera wideo	Zainicjowana przez Nazwa zdarzenia Data rozpoczęcia oraz czas

Zainicjowane przez	Informacja
Przełącznik wideo	Zainicjowana przez Przełącznik wideo Parametry nagrywania Zdarzenie Data rozpoczęcia oraz czas Pozostały czas dla nagrania
Użytkownik	Zainicjowana przez Stacja robocza Nazwa użytkownika Data rozpoczęcia oraz czas Pozostały czas dla nagrania



EntraPass Video Vault (EntraPass Video Vault Browsing)

EntraPass Video Vault oferuje prosty sposób zachowywania ważnych danych wideo do późniejszego wykorzystania. Nagrania wideo mają „krótki czas życia”, zależny od ustawień serwera wideo oraz możliwości. Ponadto, ponieważ nagrania zabierają ogromne przestrzenie powierzchni dyskowej, wykorzystania narzędzia takiego jak EntraPass Video Vault umożliwia lepsze zarządzanie i łatwiejsze odzyskiwanie nagrań wideo. Interfejs EntraPass Video Vault umożliwia monitorowanie aktywności archiwizowania. Interfejs umożliwia nawigację zbliżoną do nawigacji w systemie Windows i daje możliwość użytkownikom (z odpowiednimi przywilejami) na odtwarzanie segmentów wideo zachowanych w EntraPass Video Vault.

Przeglądanie zarchiwizowanych segmentów wideo z EntraPass Video Vault (Viewing Video Segments Archived in the EntraPass Video Vault)

1 – Z głównego okna Wideo, wybierz **Przeglądaj Video Vault**.

2 – Aby obejrzeć wybrany segment, wybierz segment wideo, a następnie kliknij przycisk **Odtwórz z Video Vault (Play from Video Vault)**.

Przeglądanie eksportowanych plików wideo (Exported Video Viewing)

EntraPass pozwala na podgląd wszystkich wyeksportowanych plików wideo. Ta opcja pozwala na przeglądanie listy wszystkich wyeksportowanych plików wideo oraz na podgląd głównych kadrów eksportowanych sekwencji wideo dla formatów KVI oraz KVA. Co więcej, użytkownicy mogą eksportować segmenty wideo przed ich wyświetleniem.

1 – Z paska narzędzi Wideo, wybierz przycisk Podgląd eksportowanego pliku wideo (View exported vide). Folder wideo z listą wszystkich wyeksportowanych sekwencji wideo otworzy się automatycznie.

2 – Wybierz sekwencje wideo. Miniatura wideo pojawi się lewej-dolnej części okna. Katalog zawiera informacje o Dacie oraz czasie, kiedy wideo zostało nagrane, formacie pliku oraz nazwie pliku. Możesz kliknąć przycisk Podgląd, aby wyświetlić szczegóły o eksportowanym wideo.



Eksport plików wideo (Exporting Video Files)

EntraPass eksportuje segmenty wideo w czterech formatach: KVI oraz KVA.

- Format KVI (Kantech Video Intellex). Dane są przechowywane w formacie Intellex (.img). Przy pomocy VideoPlayerIntellex.exe można obejrzeć plik.
- Format KVA (Kantech Video AVI). Dane są przechowywane w formacie AVI (.avi). Przy pomocy VideoPlayerIntellex.exe można obejrzeć plik.
- Format AVI
- Format IMG
- Format PS

Użytkownicy EntraPass mają dwie opcje eksportowania nagrań wideo:

- Z listy Zdarzenia wideo (bez podglądu wideo)
- Z okna odtwarzania wideo: w tym wypadku, wideo jest odtworzone przed wysłaniem.

1 – Z listy Zdarzenia wideo, wybierz zdarzenie, które chcesz eksportować.

2 – Kliknij przycisk Eksportuj. Pojawi się okno **Wprowadź nazwę pliku wideo (Enter a video filename)**.

3 – Wprowadź nazwę pliku. Domyślnie, plik jest w formacie KVI. Plik zostanie zapisany w EntraPass program files:\Kantech\Server CE\Video.

Notatka: pliki wideo mogą być podglądane w oknie Eksportowane wideo (zakładka Wideo > Eksportowane wideo). Plik jest wyświetlony ze swoją nazwą, datą oraz czasem. Kluczowe klatki (jeśli jakieś są przypisane) również mogą zostać wyświetlone w tym oknie.

4 – Kliknij Zapisz, aby zamknąć okno Wprowadź nazwę pliku wideo. Pojawi się okno **Opis i hasło (Description and password)**.



Wyszukiwanie zdarzeń wideo (Finding Video Events)

Przejdź do **Wideo > Lista zdarzeń wideo** i kliknij przycisk **Szukaj (Search)**, aby znaleźć i sprawdzić segment wideo. Jeżeli przycisk Szukaj nie znajduje się na ekranie, kliknij przycisk **Menu**, aby go wyświetlić.

- Zakładka Serwer wideo pozwala na wyszukanie segmentów wideo na konkretnym serwerze wideo.
- Zakładka Zdarzenia pozwala filtrować zdarzenia.
- Zakładka Opcje pozwala na określenie rozmiaru wideo, którego szukasz. Użytkownik musi posiadać odpowiednia prawa dostępu, aby wykonać to zadanie.
- Zakładka **Status archiwum (Archive state)** pozwala filtrować zarchiwizowane zdarzenia według ich statusów.

1 – Z listy Zdarzenia wideo, kliknij przycisk Szukaj.

Notatka: jeśli przyciski Menu oraz Legenda nie są aktywowane, okno nie wyświetli w swojej dolnej części ani legendy, ani przycisków.

2 – Z okna **Znajdź zdarzenia wideo (Find video events)**, wybierz datę początkową i czas, oraz datę zakończenia i czas; dla segmentów wideo, których szukasz.

Notatka: przycisk Legenda pozwala wyświetlić legendę powiązaną ze zdarzenia wideo. Przycisk Odtwórz oraz Kopiuj z Video Vault są włączone, jeśli wybrane zdarzenia wideo zostały już zarchiwizowane w EntraPass Video Vault.

3 – Wybierz serwer wideo, który chcesz włączyć do wyszukiwania. Możesz wybrać **Wszystkie serwery wideo**, jeżeli chcesz sprawdzić wszystkie serwery wideo zdefiniowane w systemie.

Notatka: jeśli zdarzenie zostało zarejestrowane przez więcej niż jeden serwer wideo, przynajmniej jeden z nich musi zostać wybrany, aby zdarzenie zostało włączone do listy.

4 – Wybierz zakładkę Zdarzenia, aby filtrować zdarzenie, które mają być włączone do raportu. Jeżeli wybierzesz **Wszystkie zdarzenia (All events)**, wszystkie konkretne zdarzenia zostaną zaznaczone.

5 – Wybierz zakładkę Opcje, aby filtrować segmenty wideo według ich długości.

6 – Zaznacz opcję **Limit długości segmentu wideo (Video segment duration limit)**, następnie wprowadź długość **Większa niż (mm:ss) (Greater than)** oraz **Mniejsza niż (mm:ss) (Smaller than)**. Wartości są wprowadzone w minutach i sekundach. Opcja pozwala ograniczyć zakres poszukiwań według wyznaczonych kryteriów.

7 – Wybierz zakładkę **Status archiwum (Archive state)**, aby filtrować zdarzenia według ich statusów.

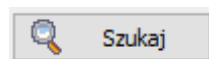


8 – Zaznacz opcję **Status archiwum (Archive state)**, aby określić, które zdarzenia mają być uwzględnione w filtrze. Jeżeli chcesz, aby wszystkie zdarzenia były uwzględnione, nie zaznaczaj tej opcji.

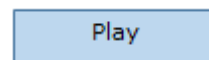
9 – Kliknij przycisk OK, aby wrócić do okna **Listy zdarzeń wideo**.

Przycisk Odtwórz oraz Kopiuj z Video Vault są włączone, jeśli wybrane zdarzenia wideo zostały już zarchiwizowane w EntraPass Video Vault. Zarchiwizowane zdarzenia są oznaczone (oflagowane) na zielono.

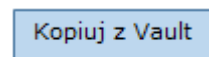
10 – Do wykonania tych czynności służą przyciski opisane poniżej:



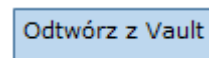
Przycisk Szukaj: można wyszukać zdarzenia powiązane z segmentami wideo.



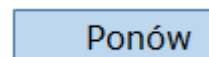
Przycisk Odtwórz (Play): włącza podgląd zdarzenia wideo. Po jego kliknięciu pulpit wideo wyświetla zdarzenie wideo. Jeżeli tylko jedna kamera była wykorzystana – jak to ma miejsce najczęściej – system wyświetli czas zdarzenia wideo. Jeżeli zdarzenie było nagrane przez więcej niż jedną kamerę (na jednym serwerze), serwer wideo wybierze najbardziej optymalny układ wyświetlania. Jeżeli zdarzenie wideo było zarejestrowane przez więcej, niż jeden serwer, możliwe jest wybranie konkretnego serwera wideo. Na przykład, 2x2 dla maksimum 4 kamer, 3x3 dla 9 oraz 4x4 na 16. Dla zdarzeń o różnych długościach, zdarzenia będą wyświetlane w kolejności zstępującej. Warto odnotować, że ta opcja ma pewne ograniczenia przy wykorzystaniu w systemach nieskonfigurowanych na ciągłe nagrywanie, ponieważ nie wyświetli kamer działających poza określonym przedziałem czasu.



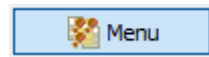
Przycisk **Kopiuj z Vault (Copy from Vault)**: pozwala użytkownikowi pobrać segmenty wideo, które zostały zarchiwizowane w EntraPass Video Vault.



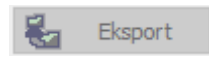
Przycisk **Odtwórz z Vault (Play from Vault)**: pozwala użytkownikowi na podgląd segmentów wideo, które zostały zarchiwizowane w EntraPass Video Vault.



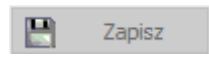
Przycisk **Ponów anulowane (Retry aborted)**: pozwala wznowić dowolny proces archiwizowania, który wcześniej został zatrzymany.



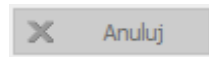
Przycisk **Menu**: wyświetla przyciski w dolnej części ekranu; przycisk Legenda: wyświetla informacje na temat statusów wyświetlanych zdarzeń nagrań wideo.



Formaty KVI (Kantech Video Intellex), KVA (Kantech Video AVI), IMG, AVI oraz PS są dostępne do eksportowania. Pozwalają przechowywać powiązane z nimi dane, powiązane ze zdarzeniami wideo.



Przycisk **Zapisz**: jest dostępny po wprowadzeniu danych w pole Komentarz. Pozwala zachować komentarze powiązane ze zdarzeniami wideo.



Przycisk **Anuluj**: jest dostępny, gdy pole Komentarz jest modyfikowane. Pozwala odrzucić komentarz i wrócić do poprzedniej wartości pola.



Parametry nagrywania (Recording Parameters)

Menu Parametry nagrywania pozwala na określenie parametrów, które kontrolują nagrywanie wideo na powiązanie tych parametrów (np. źródło wideo, kamery, etc.) z przełącznikami wideo. Dla każdego zdarzenia nagrywania trzeba określić konkretne parametry (np. źródło serwera wideo, kamera, etc.).

Nagranie może zostać przerwane przez licznik czasu (maksymalny czas nagrania) albo przez przełącznik, kiedy **Przełącznik przerwania nagrywania** jest włączony. Komponent źródłowy musi być określony dla każdego rodzaju zdarzenia. Na przykład, komponent „drzwi” musi być określony dla zdarzenia „Wymuszenie otwarcia”. Akcja (czy to rozpoczęcia nagrania, czy przerwania) również musi zostać określona.

EntraPass daje możliwość powiązania wielu parametrów nagrywania z jednym przełącznikiem. W takim przypadku, wszystkie nagrania będą powiązane z jednym zdarzeniem i możliwe będzie zapisanie wszystkich segmentów nagrania, jako pojedyncze nagranie zdarzenia.

Ustawianie parametrów nagrywania (Setting Up Recording Parameters)

Okna Nagranie wideo, pozwala skonfigurować sposób, w jaki EntraPass Video nagrywa wideo. Musisz posiadać odpowiednia uprawnienia, aby korzystać z tej opcji. Nie ma ograniczeń, co do ilości określanych parametrów nagrywania. Następujące informacje mogą być określone:

- Nazwa: w dwóch językach.
- Źródło nagrania wideo (serwer oraz kamera).
- Presety oraz wzory.
- Przełącznik początku nagrywania.
- Czas przed-alarmem
- Maksymalny łączny czas nagrania

1 – Z paska narzędzi **Wideo**, kliknij przycisk **Parametry nagrywania**. Pojawi się okno **Parametry nagrywania** z aktywną zakładką **Ogólne**.

2 – Kliknij przycisk **Nowy**, aby stworzyć nowe **Parametry nagrywania** (albo wybierz z listy już istniejące), a następnie przypisz im nazwę.

3 – Z okna Serwer wideo, wybierz serwer wideo, który będzie wykorzystany dla Parametrów nagrywania.

4 – Z listy Kamera, wybierz kamerę dla tych Parametrów nagrywania.



Wideo

EntraPass - Instrukcja instalacji i obsługi programu Wideo

Pulpit wideo

Notatka: jeśli wybrana kamera to kamera kopułkowa, możesz określić nazwę oraz numer Presetu albo Trasy. Określanie tych opcji pozwoli nakierować kamerę na konkretną pozycję. Należy przy tym pamiętać, że opcja pre-alarmu może nie działać dobrze z opcjami presetu/trasy. Pre-alarm może zostać aktywowany w momencie, kiedy kamera jest skierowana na obszar inny niż ten, na którym zaistniało zdarzenie.

5 – Z okna Przełącznik początku nagrywania (Start recording trigger), wybierz Przełącznik wideo, który chcesz powiązać z Parametrami nagrywania, które są definiowane. W oknie są wyświetlone wszystkie przełączniki wideo zdefiniowane w systemie.

6 – W sekcji Czas (Timings), określ:

- **Czas przed-alarmem (Pre-alarm time) (m:ss):** ta opcja umożliwia pobranie z serwera segmentu wideo, który został nagrany przed nagrywaniem. Na przykład, jeżeli nagrywanie zostało włączone o 2:00, a czas przed-alarmem jest nastawiony na 1min, segment nagrania rozpocznie się o 1:59.
- **Maksymalny łączny czas nagrania (m:ss):** ta opcja pozwala określić czas nagrania. Uwzględnia **czas przed-alarmem**, ale nie **Opóźnienie nagrywania po-alarmie (Post-alarm recording delay)**. Maksimum: 5 minut.

Ustawianie parametrów przełącznika przerywania nagrywania (Setting Up Stop Recording Trigger Parameters)

Jeżeli chcesz powiązać określone parametry nagrywania z przełącznikiem przerywania nagrywania, wybierz opcję **Przełącznik przerywania nagrywania (Stop recording trigger)**. W oknie **Parametry nagrywania** pojawi się zakładka **Przełącznik przerywania nagrywania (Stop recording trigger)**.

1 – W oknie Parametry nagrywania, wybierz **Przełącznik przerywania nagrywania (Stop recording trigger)**.

- **Opóźnienie nagrywania po-alarmie (m:ss) (Post-alarm recording delay (m:ss)):** to opóźnienie umożliwia systemowi przerywanie nagrywania, gdy warunek „opóźnienie zakończenia nagrywania” został spełniony. Najeżdżanie kursorem na pole powoduje wyświetlenie zakresu dopuszczalnych wartości.
- **Przełącznik (Trigger):** wybierz jeden (albo więcej) przełącznik, który przerwie nagrywanie.

Notatka: możesz utworzyć nowe przełączniki „przerwij nagrywanie” klikając prawym na polu wyświetlania przełączników.



Pulpit wideo (Video Desktop)

Pulpit wideo pozwala wyświetlić i monitorować, w czasie rzeczywistym, skonfigurowane kamery, które są podłączone do sieci.

Wyświetlanie Podglądu wideo (Displaying a Video View)

1 – Z głównego okna EntraPass, wybierz zakładkę Pulpity; następnie wybierz pulpit dedykowany do Wideo. Zostanie wyświetlone okno **Podgląd wideo**.

Notatka: Pulpit wideo będzie pusty przy pierwszym otwarciu. Będzie również wyświetlona wiadomość „Brak wybranych podglądów wideo”.

2 – Z listy wybierz podgląd wideo. Możesz edytować podgląd (Podgląd wideo > wybierz konkretny podgląd > Modyfikuj przyciski komponentów podglądu wideo).

3 – Przyciski pozwalają na wykonanie następujących zadań:



Przy pomocy tych przycisków możesz wybrać rozmiar wyświetlanego wideo.



Te przyciski są konfigurowane w Poziomie bezpieczeństwa użytkownika. Umożliwiają wykonywanie zaprogramowanych zadań, takich jak, wyświetlanie nagrań wideo ze stałym albo zmiennym opóźnieniem; lub generowanie zdarzeń wideo ze stałym bądź zmiennymi parametrami. Zobacz: **Definiowanie poziomu bezpieczeństwa (Security Level Definition)**.



Przy pomocy tych przycisków możesz **Stworzyć** albo **Edytować** podgląd wideo.



Przy pomocy tego przycisku możesz wyświetlić mozaikowo wszystkie kamery, albo jedną z kamer, zdefiniowane w systemie.



Pomoc i Zamknij. Standardowe przyciski EntraPass.

4 – Kliknij przycisk **Wyświetl selektor widoku (Show view selector)**, aby wyświetlić okno **Selektor widoku (View selector)**. To okno pozwala na wybór konkretnego widoku albo na monitorowanie konkretnego wzoru kamery. Na przykład, jeżeli wybierzesz komórkę w **Selektorze widoku**, sekwencja zostaje przerwana w celu wyświetlenia wybranej komórki.

Notatka: jeśli otworzysz selektor widoku wideo w czasie, kiedy kamera nagrywa, przycisk kamery zacznie migać do czasu zakończenia nagrania.

5 – W wyświetlanym widoku możesz kliknąć na przycisk kamery kopułkowej, aby wyświetlić przyciski kontrolne dla tej kamery (ruch, zoom, etc.). Dostępne opcje są zależne od **systemu zarządzania wideo (Digital Video Management)** podłączonego do twojego systemu. Aby uzyskać dodatkowe informacje sprawdź dokumentację DVMS.

Notatka: jeśli twoja kamera kopułkowa posiada ustawione zaprogramowane wcześniej trasy, możesz zdefiniować widok wyświetlający jedną lub kilka z tych tras. Zobacz Definiowanie widoków wideo.



Lista zdarzeń wideo (Video Event List)

Okna **Listy zdarzeń wideo** wyświetla wszystkie segmenty wideo zarejestrowane w systemie i przechowywane w bazie danych serwera wideo, jak i w EntraPass Video Vault. Te segmenty mogą pochodzić z trzech źródeł:

- **Przełączników wideo (Video triggers)**
- Żądanie użytkowników
- Automatyczne nagrania z serwera wideo

Notatka: użytkownicy muszą mieć prawa dostępu do serwera wideo, aby przeprowadzić działania na zdarzeniach wyświetlonych na liście Zdarzeń wideo. Na przykład, jeśli użytkownik nie ma przypisanych pozwoleń na wykorzystanie konkretnego serwera wideo, użytkownik nie będzie mógł sprawdzić zdarzeń pochodzących z tego serwera. Pozwolenia są przypisywane podczas definiowania poziomu bezpieczeństwa: System > Poziom bezpieczeństwa.

Korzystanie z Listy zdarzeń wideo (Using the Video Event List)

Okno Listy zdarzeń wideo wyświetla wszystkie zdarzenia wideo oraz ich opisy. Użytkownicy EntraPass mogą:

- Wyszukać konkretne zdarzenie w oparciu o datę i czas wykonania nagrania.
- Odtworzyć segment wideo.
- Eksportować segment do późniejszego wykorzystania
- Wyświetlić albo skopiować segment z EntraPass Video Vault
- Ponowić wszystkie przerwane transfery: chodzi o transfery segmentów, które zostały oznaczone do archiwizowania, ale których transfer do EntraPass Video Vault nie został przeprowadzony.

Odnajdywania zdarzeń wideo (Finding Video Events)

Przejdź do **Wideo > Lista zdarzeń wideo** i kliknij przycisk **Szukaj (Search)**, aby znaleźć i sprawdzić segment wideo. Jeżeli przycisk Szukaj nie znajduje się na ekranie, kliknij przycisk **Menu**, aby go wyświetlić.

- Zakładka Serwer wideo pozwala na wyszukanie segmentów wideo na konkretnym serwerze wideo.
- Zakładka Zdarzenia pozwala filtrować zdarzenia.
- Zakładka Opcje pozwala na określenie rozmiaru wideo, którego szukasz. Użytkownik musi posiadać odpowiednia prawa dostępu, aby wykonać to zadanie.
- Zakładka **Status archiwum (Archive state)** pozwala filtrować zarchiwowane zdarzenia według ich statusów.

1 – Z listy Zdarzenia wideo, kliknij przycisk Szukaj.



Notatka: jeśli przyciski Menu oraz Legenda nie są aktywowane, okno nie wyświetli w swojej dolnej części ani legendy, ani przycisków.

2 – Z okna Znajdź zdarzenia wideo (Find video events), wybierz datę początkową i czas, oraz datę zakończenia i czas; dla segmentów wideo, których szukasz.

Notatka: przycisk Legenda pozwala wyświetlić legendę powiązaną ze zdarzenia wideo. Przycisk Odtwórz oraz Kopiuj z Video Vault są włączone, jeśli wybrane zdarzenia wideo zostały już zarchiwizowane w EntraPass Video Vault.

3 – Wybierz serwer wideo, który chcesz włączyć do wyszukiwania. Możesz wybrać **Wszystkie serwery wideo**, jeżeli chcesz sprawdzić wszystkie serwery wideo zdefiniowane w systemie.

Notatka: jeśli zdarzenie zostało zarejestrowane przez więcej niż jeden serwer wideo, przynajmniej jeden z nich musi zostać wybrany, aby zdarzenie zostało włączone do listy.

4 – Wybierz zakładkę Zdarzenia, aby filtrować zdarzenie, które mają być włączone do raportu. Jeżeli wybierzesz **Wszystkie zdarzenia (All events)**, wszystkie konkretne zdarzenia zostaną zaznaczone.

5 – Wybierz zakładkę Opcje, aby filtrować segmenty wideo według ich długości.

6 – Zaznacz opcję Limit długości segmentu wideo (Video segment duration limit), następnie wprowadź długość **Większa niż (mm:ss) (Greater than)** oraz **Mniejsza niż (mm:ss) (Smaller than)**. Wartości są wprowadzone w minutach i sekundach. Opcja pozwala ograniczyć zakres poszukiwań według wyznaczonych kryteriów.

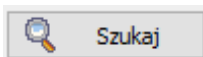
7 – Wybierz zakładkę Status archiwum (Archive state), aby filtrować zdarzenia według ich statusów.

8 – Zaznacz opcję Status archiwum (Archive state), aby określić, które zdarzenia mają być uwzględnione w filtrze. Jeżeli chcesz, aby wszystkie zdarzenia były uwzględnione, nie zaznaczaj tej opcji.

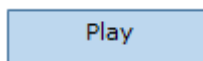
9 – Kliknij przycisk OK, aby wrócić do okna Listy zdarzeń wideo.

Przycisk Odtwórz oraz Kopiuj z Video Vault są włączone, jeśli wybrane zdarzenia wideo zostały już zarchiwizowane w EntraPass Video Vault. Zarchiwizowane zdarzenia są oznaczone (oflagowane) na zielono.

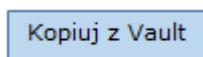
10 – Do wykonania tych czynności służą przyciski opisane poniżej:



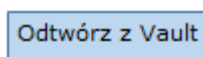
Przycisk Szukaj: można wyszukać zdarzenia powiązane z segmentami wideo.



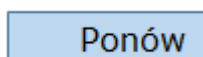
Przycisk Odtwórz (Play): włącza podgląd zdarzenia wideo. Po jego kliknięciu pulpit wideo wyświetla zdarzenie wideo. Jeżeli tylko jedna kamera była wykorzystana – jak to ma miejsce najczęściej – system wyświetli czas zdarzenia wideo. Jeżeli zdarzenie było nagrane przez więcej niż jedną kamerę (na jednym serwerze), serwer wideo wybierze najbardziej optymalny układ wyświetlania. Jeżeli zdarzenie wideo było zarejestrowane przez więcej, niż jeden serwer, możliwe jest wybranie konkretnego serwera wideo. Na przykład, 2x2 dla maksimum 4 kamer, 3x3 dla 9 oraz 4x4 na 16. Dla zdarzeń o różnych długościach, zdarzenia będą wyświetlane w kolejności zstępującej. Warto odnotować, że ta opcja ma pewne ograniczenia przy wykorzystaniu w systemach nieskonfigurowanych na ciągłe nagrywanie, ponieważ nie wyświetli kamer działających poza określonym przedziałem czasu.



Przycisk **Kopiuń z Vault (Copy from Vault)**: pozwala użytkownikowi pobrać segmenty wideo, które zostały zarchiwizowane w EntraPass Video Vault.



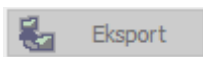
Przycisk **Odtwórz z Vault (Play from Vault)**: pozwala użytkownikowi na podgląd segmentów wideo, które zostały zarchiwizowane w EntraPass Video Vault.



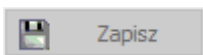
Przycisk **Ponów anulowane (Retry aborted)**: pozwala wznowić dowolny proces archiwizowania, który wcześniej został zatrzymany.



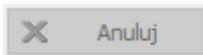
Przycisk **Menu**: wyświetla przyciski w dolnej części ekranu; przycisk Legenda: wyświetla informacje na temat statusów wyświetlanych zdarzeń nagrań wideo.



Formaty KVI (Kantech Video Intellex), KVA (Kantech Video AVI), IMG, AVI oraz PS są dostępne do eksportowania. Pozwalają przechowywać powiązane z nimi dane, powiązane ze zdarzeniami wideo.



Przycisk **Zapisz**: jest dostępny po wprowadzeniu danych w pole Komentarz. Pozwala zachować komentarze powiązane ze zdarzeniami wideo.



Przycisk **Anuluj**: jest dostępny, gdy pole Komentarz jest modyfikowane. Pozwala odrzucić komentarz i wrócić do poprzedniej wartości pola.

Odtwarzanie segmentów wideo (Playing Video Segments)

Okno **Lista zdarzeń wideo** jest podzielone na panele: **lewy** wyświetla wszystkie zdarzenia wideo otrzymane według ustalonych kryteriów wyszukiwania; **dolny** wyświetla legendę, opisującą status każdego zdarzenia. Zawiera także przyciski, które umożliwiają użytkownikom wykonywanie operacji na nagraniach; **prawy** zawiera trzy zakładki:

- **Szczegóły (Details)**: wyświetla opis zdarzenia wideo uwzględniający: serwer wideo, który nagrał zdarzenie, informacje o użytkowniku, który był zalogowany, etc.
- **Kamery**: pokazuje kamery, które są powiązane z wybranym zdarzeniem.
- **Obraz**: zawiera główny kadr sekwencji wideo. Z tego panelu możesz przypisać główny kadr nagrania i powiązać go z segmentem wideo.

Notatka: nagrania wideo mogą być streamingowane z lewego panelu (przycisk Włącz) albo z zakładki Kamera. Możesz również sprawdzić nagrania kamery z pulpitu Wiadomości. Aby to zrobić wybierz zdarzenie nagrania wideo, kliknij na nim prawym przyciskiem i wybierz Nagrania wideo > Włącz z menu skrótów



EntraPass - Instrukcja instalacji i obsługi programu Wideo



1 – Z listy **Zdarzenie wideo**, wybierz zdarzenie i kliknij przycisk **Odtwórz**. Wybrany fragment pojawi się w oknie **Odtwarzanie wideo (Video Playback)**.

2 – Możesz wybrać zakładkę Kamery, aby sprawdzić informacje o kamerze, która zarejestrowała wybrane zdarzenie:

- Datę oraz czas rozpoczęcia/zakończenia zajścia zdarzenia.
- Czas nagrania (mm:ss): długość segmentu wideo. Długość jest określana w momencie definiowania parametrów nagrywania (menu Wideo > Parametry nagrywania).
- Przełącznik wideo: przełącznik jest definiowany w menu **Przełącznik wideo (Video trigger)**, a następnie wybierany podczas definiowania **Parametrów nagrywania**.

Notatka: wskaźnik statusu obok nazwy serwera wideo wskazuje obecny status połączenia serwera.

3 – Możesz:

- Kliknąć przycisk **Odtwórz**, aby wyświetlić ten segment wideo z wybranej kamery (całe nagranie). Obraz wideo pojawia się także na **pulpicie Wideo**.
- Kliknąć przycisk Eksport, aby wyeksportować segment wideo do późniejszego wykorzystania. Zobacz: **Eksportowanie plików wideo (Exporting Video Files)**.



Łączenie fragmentów wideo z głównymi kadrami (Linking Video Clips with Key Frames)

Użytkownicy EntraPass mają możliwość zapisywania stałych obrazów, które najlepiej reprezentują sekwencję wideo, przypisując ten obraz do całego nagrania wideo. Może to być przydatne w momencie, jeżeli jedno zdarzenie zostało zarejestrowane przy więcej niż jedną kamerę i chcesz powiązać nagranie z bardziej sprecyzowanym obrazem. Odtworzenie zdarzenia wideo pozwoli użytkownikom na wybór najlepszego kadru/obrazu dla tego zdarzenia wideo, wykonania zrzutu obrazu (snap), wklejenie go i zapisania. Możliwe jest także pobranie zapisanego wcześniej obrazu i przypisania go do segmentu wideo, albo wklejenie zrzutu obrazu wykonanego wcześniej.

1 – Z listy **Zdarzenia wideo**, wybierz zdarzenie, po czym kliknij zakładkę **Obraz** (prawy panel).

2 – W oknie **Obraz**, masz do wyboru:

- Importuj obraz (Import image): kliknij przycisk Importuj, aby pobrać wcześniej zapisany albo wyeksportowany obraz.
- Wklej obraz (Paste image): kliknij ten przycisk, aby wkleić wykonany wcześniej zrzut obrazu. Przycisk jest dostępny wyłącznie wtedy, jeżeli zrzut obrazu został wykonany. Możesz najpierw odtworzyć nagranie, wykonać zrzut obrazu i następnie go wkleić.
- Wyczyść (Clear): kliknij przycisk Wyczyść, aby usunąć wyświetlany obraz.



Eksportowanie plików wideo (Exporting Video Files)

EntraPass eksportuje segmenty wideo w czterech formatach: KVI oraz KVA.

- Format KVI (Kantech Video Intellex). Dane są przechowywane w formacie Intellex (.img). Przy pomocy VideoPlayerIntellex.exe można obejrzeć plik.
- Format KVA (Kantech Video AVI). Dane są przechowywane w formacie AVI (.avi). Przy pomocy VideoPlayerIntellex.exe można obejrzeć plik.
- Format AVI
- Format IMG
- Format PS

Użytkownicy EntraPass mają dwie opcje eksportowania nagrań wideo:

- Z listy Zdarzenia wideo (bez podglądu wideo)
- Z okna odtwarzania wideo: w tym wypadku, wideo jest odtworzone przed wysłaniem.

1 – Z listy Zdarzenia wideo, wybierz zdarzenie, które chcesz eksportować.

2 – Kliknij przycisk Eksportuj. Pojawi się okno **Wprowadź nazwę pliku wideo (Enter a video filename)**.

3 – Wprowadź nazwę pliku. Domyślnie, plik jest w formacie KVI. Plik zostanie zapisany w EntraPass program files:\Kantech\Server CE\Video.

Notatka: pliki wideo mogą być podglądane w oknie Eksportowane wideo (zakładka Wideo > Eksportowane wideo). Plik jest wyświetlony ze swoją nazwą, datą oraz czasem. Kluczowe klatki (jeśli jakieś są przypisane) również mogą zostać wyświetlone w tym oknie.

4 – Kliknij Zapisz, aby zamknąć okno Wprowadź nazwę pliku wideo. Pojawi się okno **Opis i hasło (Description and password)**.

Ochrona nagrania wideo przy pomocy hasła (Protecting a Video with a Password)

Możesz chronić eksportowane nagrania wideo przy pomocy hasła. Użytkownik musi wprowadzić hasło, aby wyświetlić eksportowane pliki.

Notatka: zabezpieczenie hasłem występuje tylko dla formatów KVI oraz KVA.

1 – Wybierz wideo, które chcesz eksportować i kliknij przycisk **Eksportuj**.

2 – W oknie **Wprowadź nazwę pliku wideo (Enter Video file name)** wprowadź opis dla tego segmentu wideo i kliknij **Zapisz**. Pojawi się okno **Opis i hasło (Description and password)**.

3 – Zaznacz pole Użyj hasła (Use password), jeżeli chcesz zwiększyć zabezpieczenie segmentu wideo. Użytkownicy będą musieli wprowadzić hasło, aby wyświetlić zapisany segment wideo.

4 – Wprowadź hasło oraz potwierdzenie hasła w wyświetlanym polu.

5 – Kliknij OK, aby zamknąć okno Opis i hasło. Kliknij OK, aby zamknąć wiadomość systemową, która potwierdza eksport.



Odtwarzanie nagrań wideo (Video Playback)

Opcja odtwarzania nagrań wideo oferuje możliwość odtwarzania nagrań wideo z 16 kamer jednocześnie. Musisz określić przedział czasu nagrania. Maksymalny czas: 1 godzina:

- Wybierz kamery z lewego panelu.
- Złap i przeciągnij kamery do obszaru **Odtwarzania wideo**.

Wyświetlanie Odtwarzania wideo (Viewing a Video Playback)

1 – Z okna Odtwarzanie wideo, określ Datę początkową i czas oraz datę końcową i czas, dla nagrania wideo, które chcesz wyświetlić. Maksymalny czas: 1 godzina.

2 – Z lewego panelu wybierz kamerę i przeciągnij ją do prawego panelu. Będzie wyświetlana przez czas określony, jako czas początkowy i końcowy. Przy pomocy przycisków w dolnej części Okna odtwarzania możesz: odtworzyć, przyspieszyć, przewinąć albo zastopować wyświetlanie.

Notatka: jeśli wybrane nagrania jest niedostępne, odpowiednia wiadomość zostanie wyświetlona w dolnej części okna; przyciski Snap oraz Eksportuj pozostaną wyłączone. Jeśli nagranie jest dostępne, wiadomość odnośnie wyświetlenia nagrania zostanie wyświetlona.

- Snap: wykonuje zrzut wyświetlanego obrazu i zachowuje go w folderze \tmp\image. Zapisany obraz jest następnie wykorzystany, jako obraz reprezentujący daną sekwencję wideo. Później, wykonany zrzut obrazu będzie automatycznie wyświetlony na liście **Wyświetl wyeksportowane nagrania (View exported video)** podczas przeglądania wyeksportowanych nagrań wideo. Zaleca się dodanie komentarza do wykonanego zrzutu; komentarz pojawi się przy obrazie.

- **Eksport (Export)**: eksportuje fragment wideo do późniejszego wykorzystania.

- Zaznacz do archiwizowania: zaznacz sekwencję wideo do zarchiwizowania.



Notatka: korzystając z paska na dole prawego panelu możesz zwiększyć/zmniejszyć prędkość odtwarzania nagrania, które aktualnie oglądasz.

3 – Aby zapisać konkretny obraz z nagrania, kliknij przycisk **Snap**.

4 – Zaakceptuj nazwę domyślną albo wprowadź nową nazwę dla nagrania wideo. Nagranie zostanie zapisane w: Program files\Kantech\Server_CE\Tmp\Image. Obraz wideo może być wyświetlony przy pomocy Windows Paint.

Notatka: dla TVR II sekwencja wideo może być odtworzona tylko do przodu. Slider może zostać przesunięty tylko w prawą stronę. Dodatkowo dodano nowy przycisk, dzięki któremu można skoczyć 30 sekund wstecz w stosunku do aktualnej sekwencji.

Konfiguracja serwera wideo (Video Server Configuration)

Serwer wideo jest podłączony do EntraPass przez konkretny adres IP. Serwer wideo zachowuje, przechowuje oraz rozprowadza dane wideo na pulpity EntraPass w celach monitorowania oraz nadzoru. Dostęp do danych wideo jest możliwy poprzez stacje robocze EntraPass (z odpowiednimi upoważnieniami; przez sieć). Aby mieć dostęp do opcji wideo w EntraPass, serwer wideo musi być zidentyfikowany w EntraPass. Aby tego dokonać, trzeba:

- Zdefiniować ustawienia komunikacji serwera wideo
- Określić parametry wideo, w tym liczbą kamer podłączonych do serwera
- Ustawić opóźnienia komunikacyjne
- Określić parametry dla EntraPass Video Vault, etc.

Notatka: integracja wideo Panasonic oraz American Dynamics nie są kompatybilne z systemami Windows Server 2003 oraz 2008.



Definiowanie ustawień komunikacji serwera wideo (Defining the Video Server Communication Settings)

- 1 – Z głównego okna EntraPass, kliknij zakładkę **Wideo**, a następnie na pasku narzędzi kliknij przycisk **Serwer wideo**. Okno **Serwera wideo** z zakładką **Ogólne** zostanie wyświetlone.
- 2 – Z listy **Serwer wideo**, wybierz serwer, który chcesz konfigurować. Przypisz mu nazwę.
- 3 – Z listy **Typ serwera wideo**, wybierz typ rejestratora dla serwera wideo, który konfigurujesz.



Notatka: aktualna wersja oprogramowania integruje się z American Dynamics Intellex oraz HDVR. EntraPass wspiera HDVR-2U, HDVR-4U, wszystkie wersje Intellex: DVMS8000 (do 8 kamer) oraz DVMS16000 (do 16 kamer), Intellex IP (do 16 strumieni), Intellex Ultra (16 kanałów) oraz Intellex LT. Ta wersja ogranicza liczbę kamer do 4, 8 lub 16 zależnie od wybranego Intellex LT (LT-4, LT-8 lub LT-16). EntraPass wspiera również poniższe modele:

- **AD-TVR-04:** 4 kanałowy AD TVR 04 (modele: ADTVR04050, ADTVR04100).
- **AD-TVR-08:** 8 kanałowy AD TVR 08 (modele: ADTVR08100, ADTVR08200).
- **AD-TVR-16:** 16 kanałowy AD TVR 16 (modele: ADTVR16050, ADTVR16100, ADTVR16200, ADTVR16400).
- **AD-TVR-VS:** 4 wejścia wideo AD TVR-VS.
- **AD-NVR:** umożliwia użytkownikom przeglądanie, zarządzanie oraz kontrolowanie wideo, nagrywanego na AD-NVR poprzez oprogramowanie EntraPass:
 - o Obsługuje do 128 kamer IP
 - o Strumieniowanie obrazu: do 400 Mb/sec
 - o Podstawowe modele posiadają ograniczoną analitykę wideo, która może zostać zaktualizowana do pełnej analityki.
 - o Jeden zdefiniowany przycisk odtwarzania wideo.
 - o Podłączenie do EntraPass poprzez połączenie IP. Nie potrzeba dodatkowych interfejsów.



EntraPass - Instrukcja instalacji i obsługi programu Wideo

o Wideo na żywo oraz odtworzenie nagrań na tym samym ekranie:



4 – Zaznacz opcję online, aby poinformować EntraPass, że serwer jest online.

Notatka: opcja online musi być odznaczona, kiedy serwer jest offline przez dłuższy okres czasu (np. naprawa). W innym przypadku EntraPass będzie sprawdzał serwer wideo, co może powodować zawieszenie się systemu.

5 – W polu adres IP, określ statyczny adres IP serwera wideo. Upewnij się, że serwer wideo jest ustawiony na statyczny adres IP. Aby dowiedzieć się więcej o adresie IP serwera wideo, skontaktuj się z administratorem sieci.



EntraPass - Instrukcja instalacji i obsługi programu Wideo

6 – Nazwa domeny (Domain name): adres domeny serwera wideo.

7 – Określ informacje o porcie dla wideo (tylko dla Intellex), komunikacji (Intellex, HDVR oraz TVR II) oraz zdarzeń (tylko dla Intellex). Upewnij się, że są to te same porty, z których korzysta rejestrator.

Notatka: port TCP jest wykorzystywany przez aplikację wideo do komunikacji z EntraPass. Opcje wyświetlane w sekcji portu TCP różnią się, zależnie od konfigurowanego urządzenia. Aby dowiedzieć się więcej o portach i ich ustawieniach skontaktuj się ze swoim administratorem sieci albo sprawdź dokumentację DVR.

8 – Zaznacz opcję **Pomiń PING przy identyfikacji (Bypass Ping for identification)** (tylko dla Intellex), jeżeli chcesz ograniczyć wykorzystanie pasma. Jeżeli ta opcja nie zostanie zaznaczona, stacja robocza będzie bez przerwy wysyłała zapytanie o identyfikację serwera.

9 – Zaznacz opcję **Określ login serwera wideo (Specify video server login)** (tylko dla Intellex), jeżeli chcesz, aby użytkownicy wprowadzili swoje dane logowania przed uzyskaniem dostępu do serwera wideo. Jeżeli ta opcja zostanie wybrana, zakładka **Login** pojawi się w oknie **Serwer wideo**.

10 – Zaznacz opcję **Pomiń wiadomości rejestratora (Bypass DVR Messages)**, jeżeli chcesz odrzucić/anulować wszystkie wiadomości pochodzące od Intellex.

11 – W sekcji parametry serwera wideo:

- Wprowadź liczbę kamer. Aby uzyskać informacje na temat kamery z serwera kliknij przycisk **Importuj dane kamery (Import camera details)**. Ten przycisk oferuje szybki sposób na zdefiniowanie kamery podłączonej do serwera wideo. Jeżeli klikniesz ten przycisk, EntraPass połączy się z serwerem wideo i pobierze liczbę oraz domyślne nazwy wszystkich kamer podłączonych do rejestratora.

- **Określ częstotliwość odpytywania (Specify the Polling frequency)** (mm:ss): częstotliwość ta odnosi się do opóźnień pomiędzy dwoma zapytaniami pochodzącymi z serwera Kantech do Serwera wideo. Ta operacja jest procesowana przez interfejs Serwera wideo Kantech.

- **Określ Odpytywanie przed utratą komunikacji (Polls before Communication failure)**: liczba nieudanych zapytań, zanim serwer EntraPass uzna serwer wideo za niepodłączony (offline). Na przykład, jeżeli wprowadzisz w tym polu wartość 4, EntraPass podejmie cztery próby połączenia się z serwerem wideo zanim uzna serwer za niepodłączony (offline).

- **Określ Dostosowanie strefy czasowej (Indicate the Time zone adjustment)**: przy pomocy strzałek góra/dół możesz określić dostosowanie strefy czasowej, jeżeli serwer EntraPass i serwer rejestratora nie są w tej samej strefie czasowej. Dostosowanie odnosi się do różnicy czasowej pomiędzy strefami. Dostosowanie pozwala stacjom roboczym na otrzymywanie zdarzeń wygenerowanych przez serwer rejestratora, według czasu serwera EntraPass.

- Zaznacz pole **Synchronizacja zegara (Time for clock synchronization)** (tylko dla Intellex): określa moment dnia, w którym serwer wideo zsynchronizuje się serwerem Kantech w celu pobrania daty i czasu. Ta operacja jest procesowana przez interfejs Serwera wideo Kantech.

Notatka: serwer EntraPass służy, jako odnośnik, co do określenia czasu. Serwer wideo będzie procesował czas według czasu serwera EntraPass. Na przykład, jeżeli czas serwera EntraPass to 3:00, a czas serwera wideo to 2:00, to dopasowanie Strefy czasowej będzie miało wartość -1, dzięki czemu serwer wideo będzie mógł wyświetlić prawidłową informację na temat zdarzenia, które miało miejsce w określonym czasie.



Poprawianie bezpieczeństwa serwerów wideo (Enhancing the Security of Video Servers)

1 – Jeżeli twój serwer wideo Intellex jest zabezpieczony przez Policy Manager, użytkownik musi użyć nazwy domeny, konkretnego loginu oraz hasła, aby uzyskać dostęp do serwera wideo. Musisz zaznaczyć **Określ login dla serwera wideo (Specify Video server login)** w zakładce Ogólne.

Notatka: dla serwera HDVR albo TVR II wymagany jest login oraz hasło.

Notatka: aby poznać szczegóły dotyczące parametrów bezpieczeństwa serwera wideo skontaktuj się z administratorem sieci.

2 – Jeżeli opcja **Określ login dla serwera wideo (Specify Video server login)** jest zaznaczona, wyświetli się zakładka **Login**.

3 – Wprowadź dane logowania do odpowiednich pól:

- Nazwa domeny: wprowadź nazwę domeny Serwera wideo Intellex (nie wykorzystywaną przez HDVR oraz TVR II).
- Login: wprowadź login wykorzystywany do zalogowania się do serwera wideo.
- Hasło: wprowadź hasło.
- Potwierdź hasło: potwierdzenie musi być identyczne, jak wprowadzone wcześniej hasło. Jeżeli pojawi się wiadomość o błędzie, upewnij się, że Caps Lock nie jest włączony. W przypadku HDVR albo TVR II hasło odpowiada temu, które jest przypisane do serwera rejestratora.



Zdalne połączenie wideo (Remote Video Connection)

Funkcja ta umożliwia kontrolowanie wideo serwera z aplikacji RemoteVideoProcess.exe, zainstalowanej na serwerze lub dowolnym komputerze podłączonym do tej samej sieci.

Po zarejestrowaniu opcji Zdalnego połączenia wideo, nowe parametry mogą zostać skonfigurowane w oknie Serwera wideo.

- Adres IP
- Nazwa domeny (domeny, z której RemoteVideoProcess.exe zostanie uruchomiony)
- Port do komunikacji (port otwarty przez aplikację RemoteVideoProcess.exe do monitorowania nadchodzących zapytań z serwera EntraPass).

Notatka: RemoteVideoProcess.exe nie jest dostępny z serwera redundantnego.

Notatka: opcja Video viewer – dostępna podczas procesu instalowania EntraPass – musi zostać użyta, aby funkcja RemoteVideoProcess mogła zadziałać.

Notatka: zainstalowanie Zdalnego połączenia wideo (Remote Video Connection) doda 128 nowych wideo serwerów.

Definiowanie EntraPass Video Vault (Defining the EntraPass Video Vault)

Zakładka Parametry EntraPass Video Vault pozwala na określenie ustawień terminarza archiwizowania oraz częstotliwości transferu (o ile aplikacja została wcześniej aktywowana w EntraPass i następnie skonfigurowana).

- Aby zobaczyć szczegóły na temat instalowania EntraPass Video Vault, zobacz **Dodawanie komponentów systemu (Adding System Components)**.
- Aby zobaczyć szczegóły na temat konfigurowania aplikacji EntraPass Video Vault, zobacz **Konfigurowanie aplikacji EntraPass Video Vault (Configuring the EntraPass Video Vault Application)**.



- Aby dowiedzieć się więcej o korzystaniu z **EntraPass Video Vault**, zobacz dział poświęcony **EntraPass Video Vault**.

1 – Z okna Serwer wideo (Video server), wybierz zakładkę Parametry Video Vault (Video Vault parameters).

2 – Wprowadź informacje dla aplikacji EntraPass Video Vault:

- Aplikacja Video Vault: nazwa aplikacji EntraPass Video Vault połączonej z wybranym serwerem wideo.
- **Terminarz archiwizacji (Archive schedule):** wybrany terminarz określa przedział czasu, w trakcie którego segmenty wideo będą zapisywane. Gdy terminarz jest ważny, wszystkie segmenty wideo pochodzące z przełączników zdefiniowanych przez użytkownika, przełączników serwera wideo albo manualnych przełączników, będą zapisywane w celach archiwizacji.

3 – Określ Parametry transferu segmentów wideo (Video segment transfer parameters):

- **Interwał transferu (Transfer interval) (hh:mm):** interwał określony w tym polu wskazuje przedział, podczas którego segmenty wideo są pobierane z serwera wideo. Ta opcja ogranicza pobieranie danych oraz dostęp do serwera wideo do określonego przedziału czasu.

Notatka: serwer pozwala na jedno wyszukiwanie na raz. Na przykład, jeśli zadany okres to 02:00 → 04:00, segmenty wideo będą wyszukiwane przez dwie godziny dziennie. Okres 18:00 → 06:00 oznacza wyszukiwanie dwunastogodzinne, od 18:00 do 06:00.

- **Powiadom w przypadku niepowodzenia transferu (Notify on transfer failure) (dni):** ta liczba określa ilość dni przeznaczonych na pobranie wideo. Jeżeli segment wideo nie został pobrany po upływie czasu (ilość dni) określonego w tym polu, segment jest uważany za nie do odzyskania w celach archiwizacji, a EntraPass Video Vault nie poinformuje użytkownika o niepowodzeniu.

- **Język pliku (File language):** ta opcja może być wykorzystana wyłącznie przy formatach KVI oraz KVA. Użytkownicy mogą wybrać pomiędzy językiem angielskim i francuskim w celu określenia języka, który zostanie wykorzystany do opisu zarchiwizowanych danych.

- **Format pliku wideo (Video file format):** wybierz format pliku wideo, który będzie pobierany:

o **Domyślny Video Vault:** jest to format określony dla wybranego EntraPass Video Vault (Urządzenia > aplikacja EntraPass > (wybrana aplikacja Video Vault) > zakładka Proces Video Vault)

o **KVI (Kantech Video Intellex).** KVI zawiera miniaturę, kontekstową informację wideo oraz umieszcza cyfrowy znak wodny na obrazie. Musi być odtwarzany przy pomocy Intellex Video Player, który korzysta z American Dynamics API. Musisz być pewny, że API zostało zainstalowane na klienckim komputerze.

o **KVA (Kantech Video AVI).** KVA zawiera miniaturę, kontekstową informację wideo oraz nie umieszcza cyfrowego znaku wodnego na obrazie. Pliki wideo mogą być odtworzone przy pomocy Windows Media Player albo innego odtwarzacza plików AVI.



EntraPass - Instrukcja instalacji i obsługi programu Wideo

- o **AVI (Audio Video Interlaced)**. Pliki AVI mogą być odtworzone przy pomocy Windows Media Player.
- o **IMG**, format Intellex. Pliki są przechowywane w formacie .img i mogą być odtworzone przy pomocy Intellex Video Player.
- o **PS**: skompresowany format wideo HDVR.

4 – Dla zwiększenia bezpieczeństwa wybierz opcję **Użyj hasła dla plików w formacie KVI oraz KVA (Use a password for KVI and KVA file formats)**, jeżeli chcesz chronić zarchiwizowane segmenty wideo tego typu plików hasłem. Upewnij się, że informacje wprowadzone w pola **Hasło** i **Potwierdź hasło** są takie same. Przed wyświetleniem segmentów wideo zarchiwizowanych w EntraPass Video Vault, użytkownik będzie musiał wprowadzić hasło. Zarchiwizowane pliki wideo mogą być przeglądane w oknie **Przeglądaj Video Vault (Browse Video Vault window)**.

Komentarz (Comment)

Sprawdź: Pole komentarza



Przełączniki wideo (Video Triggers)

Przełączniki wideo to zdarzenia systemowe, które rozpoczynają albo przerywają nagrywanie. Dowolne zdarzenie powiązane z wybranym typem kontrolera może aktywować nagrywanie, w tym zdarzenia specjalne pochodzące z serwera wideo. Komponent źródłowy musi być określony dla każdego typu zdarzenia aktywującego. Na przykład, komponent „drzwi” musi być określony dla wiadomości „wymuszone otwarcie”. Nie ma limitu ograniczającego ilość zdefiniowanych przełączników wideo.

Definiowanie przełączników wideo (Defining Video Triggers)

Następujące informacje mogą zostać określone:

- Nazwa (w dwóch językach)
- Typ komponentu: typ komponentu, który zostanie zaprogramowany dla przełącznika. Zdarzenia są powiązane z komponentami systemu: bramką, połączeniem, kontrolerem, etc.

W oparciu o zdarzenie, które zaszło na wybranym komponencie systemu, przełącznik rozpocznie albo przerwie nagrywanie.

Notatka: lista parametrów zależy od rodzaju serwera wideo podłączonego do EntraPass. Może się różnić zależnie od dostępnych opcji oraz decyzji odnośnie implementacji.



1 – Z paska narzędzi **Wideo**, wybierz przycisk **Przełącznik wideo (Video trigger)**. Pojawi się nowe okno.

2 – Kliknij przycisk **Nowy** (albo wybierz istniejący przełącznik, jeżeli chcesz go zmodyfikować). Przypisz mu nazwę.

Notatka: wiadomość alarmowa jest wyświetlona, kiedy próbujesz zapisać, zanim wybierzesz rodzaj komponentu oraz zanim zdefiniujesz komponent, który ma służyć, jako przełącznik (trigger).

3 – Z listy **Komponent**, wybierz komponent, który uruchomi zdarzenie nagrywania (np. kontroler drzwi).

4 – Jako źródło przełącznika możesz wybrać: **Pojedynczy**, **Grupa** albo **Wszystkie komponenty**.

5 – Użyj przycisku trzech kropek, aby wybrać komponent.

6 – Z listy Terminarz przełącznika (Trigger schedule) wybierz terminarz dla przełącznika. W razie potrzeby możesz określić konkretny terminarz dla tego przełącznika (Definiowanie > Terminarz). Jeżeli do przełącznika nie zostanie przypisany terminarz, przełącznik zostanie wyłączony.

7 – Z listy **Kategoria zdarzenia**, wybierz pomiędzy grupami zdarzeń: **EntraPass** albo **Wtargnięcia**.

Notatka: to pole jest dostępne wyłącznie wtedy, kiedy Panel wtargnięcia został skonfigurowany.

8 – Kliknij zakładkę **Zdarzenia** i wybierz zdarzenia z listy.

Tworzenie i modyfikacje okien wideo (Video Views Creation and Modification)

Presety oraz wzory wideo pozwalają na przeprowadzenie wielu akcji (w przypadku koputek). Są one konfigurowane na pulpicie dedykowanym do Podglądu wideo. Umożliwiają optymalizację czasu przeznaczonego na podgląd wideo przy wyświetlaniu nagrań przy pomocy zaprogramowanych podglądów.

EntraPass umożliwia użytkownikowi zdefiniowanie szerokiego zakresu wyświetlania, zależnie od jego potrzeb:

- Pojedyncza kamera
- Wiele kamer
- Wiele grafik oraz kamer
- Widok serwera: tworzony poprzez przeciągnięcie serwera w pole wyświetlania.
- Wiele serwerów wideo: zależnie od potrzeb, można tworzyć podglądy z wielu serwerów wideo.



Modyfikowanie poglądu wideo (Modifying a Video View)

1 – W oknie **Podgląd wideo**, kliknij **Modyfikuj komponenty podglądu wideo (Modify Video view components)**, aby edytować albo stworzyć nową zawartość **Pulpitu podglądu wideo**.

2 – Z lewego panelu wybierz kamerę, preset albo wzór, po czym przeciągnij go do komórki w prawym panelu. Kamera jest identyfikowana po nazwie. Preset jest identyfikowany po nazwie kamery i własnej nazwie.

Notatka: konkretna kamera może zostać wyświetlona w więcej niż jednej komórce; w tym przypadku opcja **Włącz sekwencje wideo** musi być dostępna. Grafika może zostać wyświetlona tylko w jednej komórce.

Notatka: Podgląd wideo może wyłącznie wyświetlać kamery z tego samego rodzaju DVR (HDVR, Intellex, TVR)

Notatka: maksymalna liczba dostępnych TVR to 40.

3 – Wybierz układ kamery klikając na przycisk w górnej części prawego panelu, aby określić ilość obrazów, jaką chcesz wyświetlić:

- Kliknij 1 X 1, aby wyświetlić 1 obraz
- Kliknij 2 X 2, aby wyświetlić 4 obrazy
- Kliknij 3 X 3, aby wyświetlić 9 obrazów
- Kliknij 4 X 4, aby wyświetlić 16 obrazów

Notatka: możesz stworzyć podgląd przeciągając serwer wideo w odpowiednie pole. Ten podgląd będzie zawierać wszystkie kamery z tego konkretnego serwera.

Notatka: liczba wyświetlanych obrazów wpływa na przepustowość sieci. Na przykład, jeśli wyświetlasz 4x4, przepustowość będzie mniejsza niż przy wyświetlaniu 1x1.

4 – Kliknij przycisk **Test**, aby wyświetlić wyniki. Wyświetlany Podgląd wideo pojawia się na Pulpicie wideo w celu monitorowania oraz nadzoru (Pulpity > Pulpity dedykowane do monitoringu wideo).



EntraPass - Instrukcja instalacji i obsługi programu Wideo



Notatka: aby usunąć kamerę z komórki kliknij na nią prawym, a następnie wybierz Usuń z menu skrótów.

5 – Kliknij przycisk **Zamknij**, aby zamknąć okno **Testuj wideo**.

Definiowanie okien wideo (Video Views Definition)

Po zdefiniowaniu serwera wideo oraz zidentyfikowaniu kamer, użytkownicy mogą zdefiniować podglądy wideo, które będą wyświetlane na pulpicie Wideo. Użytkownicy EntraPass będą mogli wykorzystać skonfigurowane wcześniej presety i wzory.

Urządzenia EntraPass (stacje robocze, bramki, obiekty, kontrolery, etc.) mogą zostać powiązane z podglądami wideo. Podgląd wideo może zostać wybrany w trakcie definiowanie komponentu, aby wyświetlić ten komponent w podglądzie wideo.

Definiowanie parametrów ogólnych dla podglądu wideo (Defining General Parameters for a Video View)

1 – Wybierz Podgląd wideo z paska narzędzi Wideo. Okno Podglądu wideo – z zakładką Ogólne – zostanie wyświetlone.

2 – Z listy Podgląd wideo wybierz podgląd (albo kliknij Nowy, aby utworzyć nowy), po czym przypisz mu nazwę. Jeżeli system działa w dwóch językach, przypisz dwie.



Definiowanie podglądu wideo

3 – Z listy Serwer wideo, wybierz typ serwera (Intellex, HDVR albo TVR).

4 – Z listy **Domyślny rozmiar wideo (Default size on video)**, wybierz odpowiedni rozmiar wyświetlania obrazu: możesz wybrać mniejszy rozmiar, jeżeli musisz wyświetlić okno **Wideo** razem z innym oknem.

- Duży: 1024x768
- Średni: 800x600
- Mały: 640x480
- Bardzo mały: 400x300
- **Ostatnio użyty (Last used)**: wyświetla rozmiar ostatnio użyty na **Pulpicie wideo**.

5 – Z listy **Domyślny rozmiar grafiki (Default size on graphic)**, wybierz rozmiar obrazu, wybierz odpowiedni rozmiar wyświetlania obrazu (Duży, Średni, Mały, Bardzo mały, Ostatnio użyty).

6 – Określ Procentową częstotliwość odświeżania przy pomocy strzałek góra/dół.

Notatka: Procentowa częstotliwość odświeżania jest powiązana z kompresją/jakością obrazu. Jakość obrazu wpływa na wydajność systemu: im wyższa jakość, tym mniejsza kompresja i mniejsza wydajność systemu. Jeśli nastawisz wysoką wartość częstotliwości odświeżania (> 80), kompresja będzie niska. W efekcie aplikacja będzie używać dużą część przepustowości sieci. Poniższa tabela zestawia rekomendowane opcje:

Jakość	Opis	Wynik
80 i więcej	Wysoka jakość	Obrazy są zapisywane w najwyższej jakości, przy wykorzystaniu najniższego poziomu kompresji. To ustawienie wymaga najwyższego nakładu przestrzeni do zapisu oraz przepustowości sieci.
50	Normalna, domyślna	Obrazy są zapisywane w normalnej jakości. To ustawienie zapewnia równowagę pomiędzy kompresją, a wymaganą przestrzenią do zapisu. Mniej znaczące różnice między obrazami są ignorowane.
40	Niska jakość	Obrazy są zapisywane w niskiej jakości, przy wykorzystaniu najwyższego poziomu kompresji. To ustawienie wymaga najmniejszego nakładu przestrzeni do zapisu oraz przepustowości sieci.

7 – Zaznacz opcję **Ponowne załadowanie opóźnienia podglądu wideo (Re-initialize video view delay)** (mm:ss), jeżeli chcesz, aby system odświeżył wyświetlany obraz. Jeżeli zaznaczysz tą opcję, wyświetlany obraz zostanie automatycznie zaktualizowany po upływie określonego opóźnienia. Ta opcja jest bardzo przydatna, jeżeli określony obraz kamery zawiera wzory albo presety.

8 – W sekcji Kontrola wideo, wybierz:



Definiowanie podglądu wideo

- **Pokaż tylko nakładkę Intellex oraz HDVR (Show overlay Intellex and HDVR only):** zaznacz tą opcję, jeżeli chcesz, aby identyfikacja kamery (nazwa kamery i serwera) została wyświetlona na **Pulpicie wideo**.
- **Pokaż kontrolki kamery (Show camera control):** zaznacz tą opcję przy kamerach kopułkowych. Umożliwia ona użytkownikowi kontrolowanie kamery kopułkowej. Opcja nie jest dostępna dla kamer stałych.
- **Pokaż metryki (Show metrics)** (tylko dla Intellex): ta opcja umożliwia wyświetlenie liczby klatek na sekundę (fps) oraz liczby bitów na sekundę (Bps) dla wybranej kamery. Informacja jest wyświetlona w górnej części okna **Wideo** (oraz na **Pulpicie wideo**).
- **Auto-ukrywanie tekstu (Auto-hide text)** (tylko dla Intellex): jeżeli ta opcja jest wybrana, system nie będzie wyświetlać informacji powiązanych z kamerą.
- **Włącz zoom obrazu (Enable image zoom)** (tylko dla Intellex): zaznacz tą opcję, jeżeli chcesz wyświetlać wartość przybliżenia dla wybranej kamery.

9 – Zaznacz Włącz wzór wideo (Enable video pattern), aby zmieniać obrazy w oknie Wideo. Jeżeli określiłeś układ, jako 2x2, wtedy wzór będzie się składać z czterech, zmieniających się obrazów według opóźnienia określonego w polu **Opóźnienie wyświetlania kamery (Camera display delay)**. Jeżeli nie zaznaczysz tej opcji, podgląd wideo będzie wyświetlać wszystkie kamery jednocześnie.

Notatka: sekcja Włącz wzór wideo jest dostępna, kiedy komponenty zostały przypisane do podglądu wideo.

10 – Zaznacz Opóźnienie przed uruchomieniem sekwencji (Delay before launching sequences) (m:ss), aby określić opóźnienie przejścia, zanim obrazy zaczną wyświetlać się w oknie **Wideo**.

11 – Określ opóźnienie wyświetlania dla: kamer, presetów, wzorów i grafik.

Notatka: to opóźnienie określa okres czasu, podczas którego wideo albo grafika będą wyświetlane w Podglądzie wideo, zanim zostaną zastąpione przez następne wideo/grafikę. Maksymalne opóźnienie 9:59 sekundy. Poniższa tabela przedstawia minimalne/domyślne opóźnienia.

Opóźnienie	Minimum (sek)
Opóźnienie, przed uruchomieniem sekwencji	2 sekundy
Opóźnienie wyświetlania kamery	3 sekundy
Opóźnienie wyświetlania presetu	5 sekund
Opóźnienie wyświetlania wzoru	10 sekund
Opóźnienie wyświetlania grafiki	5 sekund

12 – Wybierz zakładkę Szczegóły (Details), aby wyświetlić dane odnośnie wybranego podglądu: serwerów wideo, kamer oraz – gdy to możliwe – presetów i wzorów.



EntraPass - Instrukcja instalacji i obsługi programu Wideo



System

Active Directory

Opcja Active directory (AD) pozwala EntraPass na import oraz synchronizację Użytkowników z AD z Operatorami i użytkownikami EntraPass. Do przesyłania informacji pomiędzy serwerem EntraPass, a klientami AD, EntraPass wykorzystuje protokół LDAP. Opcja synchronizacji eliminuje zdalne tworzenie oraz nadzorowanie użytkowników AD w EntraPass, podczas gdy integracja AD pozwala na autoryzację SSO. Oznacza to, że Użytkownicy są weryfikowani przez uwierzytelnienia Windows i są automatycznie logowani na stację roboczą EntraPass przy pomocy jednego kliknięcia. Zarządzanie użytkownikami może również być przeprowadzane przez połączenie AD, co znacznie ułatwia samo zarządzanie. Może istnieć do 10 połączeń AD w tym samym czasie.

Notatka: aby uruchomić usługę EntraPass LDAP musisz zainstalować Microsoft's .NET Framework. Zainstaluj .NET 4.6.1 na tym samym urządzeniu, na którym zainstalowany jest SmartLink.

Musisz wprowadzić ustawienia sieci oraz AD dla serwera, do którego chcesz się podłączyć.

1 – wybierz przycisk **Active directory** w zakładce **System**. Zostanie wyświetlone okno **Active directory** z zakładką **Ogólne**.

2 – kliknij przycisk Nowy, aby stworzyć nowy **Active directory**, po czym wprowadź wszystkie niezbędne informacje.

Notatka: pole Włącz usługę Active directory jest automatycznie wybrane.

3 – wprowadź adres IP albo nazwę domeny dla serwera, na którym zapisany jest **Active directory**. Aplikacja LDAP wykorzystuje Port 389 dla TCP oraz UDP.

4 – pole Interwał synchronizacji (hh:mm:ss) określa czas interwału pomiędzy ostatnią, a kolejną Synchronizacją.

Notatka: po pierwszym zainstalowaniu LDAP, EntraPass przeprowadza pełną Synchronizację. Przy restarcie EntraPass przeprowadza częściową Synchronizację, podczas gdy SmartLink tylko aktualizuje nowe albo modyfikowane wpisy.

5 – musisz przypisać **SmartLink** do Active directory, ponieważ aplikacja LDAP łączy się z usługą SmartLink Web.



Active Directory

Notatka: kilka połączeń SmartLink jest możliwe na tym samym SmartLink. Maksymalna liczba Active directories zdefiniowana w EntraPass to 10.

6 – w **Ustawieniach Active directory** wypełnij następujące pola:

- **LDAP Base DN (Operator):** nazwa wykorzystywana, jako punkt startowy do wyszukiwania serwera dla Operatorów EntraPass, na przykład: EntraPass.
- **LDAP Base DN (Użytkownik):** nazwa wykorzystywana, jako punkt startowy do wyszukiwania serwera dla Użytkowników EntraPass, na przykład: UżytkownikEntraPass.
- **LDAP Binding DN:** nazwa użytkownika konta AD, które chcesz połączyć z Active directory.
- **Hasło LDAP:** hasło AD dla Użytkownika konta AD.
- **Potwierdź hasło LDAP:** potwierdź hasło.

Notatka: jeśli połączenie jest prawidłowe nastąpi synchronizacja. Status usługi LDAP będzie wyświetlany w kilku lokacjach, np.: System / Active directory, Status / Aplikacja / SmartLink, pasek systemu Windows / Kontrola usługi LDAP, oraz w oknie aplikacji SmartLink.

7 – kliknij Importuj AD/LDAP. Jeśli połączenie jest zakończone sukcesem, w obszarze **Zaimportowane pola** wyświetlona zostaje liczba pól dostępnych z serwera AD.

Notatka: przycisk Importuj AD/LDAP będzie zaszarzony, jeśli LDAP Base DN (Użytkownik) jest pusty, albo serwer AD lub Nazwa domenu są puste.

8 – dla użytkownika karta Mapowanie użytkownika definiuje, które atrybuty usługi Active Directory są mapowane do jakie pola bazy danych EntraPass. Tutaj można dostosować pola używane w synchronizacji użytkowników. Poniższa tabela 1 opisuje, które pola bazy danych EntraPass można zmapować.

9 – przy pomocy przycisku **Synchronizuj teraz** możesz zdalnie rozpocząć synchronizację z wybranym serwerem AD.

Notatka: przycisk jest nieaktywny (wyszarzony), jeśli Active directory jest niepołączony.

10 – w zakładce Mapowanie znajdziesz trzynaście pól, z którymi może zsynchronizować się EntraPass. Pierwsze 9 jest obowiązkowych i tylko do odczytu, ale pozostałe 4 są opcjonalne i są oddane do twojej dyspozycji. Większość pól tylko do odczytu odnosi się do hasła Active directory oraz elementów/warunków z nim powiązanych. Powodem ku temu jest to, że EntraPass nie przechowuje haseł w bazie danych. AD w pełni kontroluje hasła.



EntraPass - Instrukcja instalacji i obsługi programu System

Jeśli wybierzesz Skorzystaj z daty końcowej (Use expiry date) oraz Data końcowe operatora (Operator expiry date), AD będzie kontrolować, kiedy konto traci wartość. Jeśli odznaczysz te pola, ustawienia EntraPass pozostaną aktywne. Wybierz pole Obraz, jeżeli chcesz przechowywać obrazy operatora. EntraPass może importować obrazy jpeg oraz miniatury. Jeśli wybierzesz pole E-mail możliwe jest zaimportowanie oraz przechowanie jednego lub wielu adresów operatora.

11 - Więcej informacji na temat zakładki *Komentarz znajdziesz na str. 212*

Tabela 1. Pola bazy danych EntraPass – mapowanie. Pola TBD mogą być personalizowane.

Table 1 : EntraPass database fields for user mapping. The TBD field can be customized by you.

EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card User Name	Display Name (DisplayName)	(mandatory)
Card Type (integer)	TBD	AD fields drop list returns attributes of types: - integer - numerical string - enumeration
Start Date (date)	TBD	AD fields drop list returns attributes of types: - Generalized Time - UTC Coded Time
User End Date (shortint)	TBD	AD fields drop list returns attributes of types: - integer - enumeration - boolean
End Date (date)	TBD	AD fields drop list returns attributes of types: - Generalized Time - UTC Coded Time
Card # 1 - Card Number (char)	TBD	AD fields drop list returns attributes of types: - print case string - replica link (type received from AD as octet string) - case insensitive string - case sensitive string - unicode string - numerical string - octet string - SID (type received from AD as octet string)
Card # 1 - Display Card Number (shortint)	TBD	AD fields drop list returns attributes of types: - integer - enumeration - boolean



EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card # 1 - User expiration date (shortint)	TBD	AD fields drop list returns attributes of types: - integer - enumeration - boolean
Card # 1 - Expiration Date (date)	TBD	AD fields drop list returns attributes of types: - Generalized Time - UTC Coded Time
Card # 1 - Expiration Hour (date)	TBD	AD fields drop list returns attributes of types: - Generalized Time - UTC Coded Time
Card # 1 - Trace (shortint)	TBD	AD fields drop list returns attributes of types: - integer - enumeration - boolean
Card # 1 - Stolen/lost (shortint)	TBD	AD fields drop list returns attributes of types: - integer - enumeration - boolean
Card # 2 - Card Number (char)	TBD	AD fields drop list returns attributes of types: - print case string - replica link (type received from AD as octet string) - case insensitive string - case sensitive string - unicode string - numerical string - octet string - SID (type received from AD as octet string)
Card # 2 - Display Card Number (shortint)	TBD	AD fields drop list returns attributes of types: - integer - enumeration - boolean
Card # 2 - User expiration date (shortint)	TBD	AD fields drop list returns attributes of types: - integer - enumeration - boolean



EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card # 2 - Expiration Date (date)	TBD	AD fields drop list returns attributes of types: • Generalized Time • UTC Coded Time
Card # 2 - Expiration Hour (date)	TBD	AD fields drop list returns attributes of types: • Generalized Time • UTC Coded Time
Card # 2 - Trace (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Card # 2 - Stolen/lost (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Card # 3 - Card Number (char)	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card # 3 - Display Card Number (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Card # 3- User expiration date (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Card # 3 - Expiration Date (date)	TBD	AD fields drop list returns attributes of types: • Generalized Time • UTC Coded Time



EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card # 3 - Expiration Hour (date)	TBD	AD fields drop list returns attributes of types: • Generalized Time • UTC Coded Time
Card # 3 - Trace (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Card # 3 - Stolen/lost (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Card # 4 - Card Number (char)	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card # 4 - Display Card Number (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Card # 4 - User expiration date (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Card # 4 - Expiration Date (date)	TBD	AD fields drop list returns attributes of types: • Generalized Time • UTC Coded Time
Card # 4 - Expiration Hour (date)	TBD	AD fields drop list returns attributes of types: • Generalized Time • UTC Coded Time



EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card # 4 - Trace (shortint)	TBD	AD fields drop list returns attributes of types: - integer - enumeration - boolean
Card # 4 - Stolen/lost (shortint)	TBD	AD fields drop list returns attributes of types: - integer - enumeration - boolean
Card # 5 - Card Number (char)	TBD	AD fields drop list returns attributes of types: - print case string - replica link (type received from AD as octet string) - case insensitive string - case sensitive string - unicode string - numerical string - octet string - SID (type received from AD as octet string)
Card # 5 - Display Card Number (shortint)	TBD	AD fields drop list returns attributes of types: - integer - enumeration - boolean
Card # 5 - User expiration date (shortint)	TBD	AD fields drop list returns attributes of types: - integer - enumeration - boolean
Card # 5 - Expiration Date (date)	TBD	AD fields drop list returns attributes of types: - Generalized Time - UTC Coded Time
Card # 5 - Expiration Hour (date)	TBD	AD fields drop list returns attributes of types: - Generalized Time - UTC Coded Time
Card # 5 - Trace (shortint)	TBD	AD fields drop list returns attributes of types: - integer - enumeration - boolean



EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card # 5 - Stolen/lost (shortint)	TBD	AD fields drop list returns attributes of types: - integer - enumeration - boolean
Card Information 1 (up to 10 with EP Corporate)	TBD	AD fields drop list returns attributes of types: - print case string - replica link (type received from AD as octet string) - case insensitive string - case sensitive string - unicode string - numerical string - octet string - SID (type received from AD as octet string)
Card Information 2	TBD	AD fields drop list returns attributes of types: - print case string - replica link (type received from AD as octet string) - case insensitive string - case sensitive string - unicode string - numerical string - octet string - SID (type received from AD as octet string)
Card Information 3	TBD	AD fields drop list returns attributes of types: - print case string - replica link (type received from AD as octet string) - case insensitive string - case sensitive string - unicode string - numerical string - octet string - SID (type received from AD as octet string)
Card Information 4	TBD	AD fields drop list returns attributes of types: - print case string - replica link (type received from AD as octet string) - case insensitive string - case sensitive string - unicode string - numerical string - octet string - SID (type received from AD as octet string)



EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 5	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 6	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 7	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 8	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)



EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 9	TBD	AD fields drop list returns attributes of types: - • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 10	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 11 (up to 40 with EP Global)	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 12	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)



EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 13	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 14	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 15	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 16	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)



EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 17	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 18	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 19	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string - unicode string - numerical string - octet string - SID (type received from AD as octet string)
Card Information 20	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 21	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)



EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 22	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 23	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 24	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 25	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)



EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 26	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 27	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 28	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 29	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)



EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 30	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 31	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 32	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 33	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)



EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 34	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 35	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 36	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 37	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)



EntraPass fields	Active Directory fields	Possible AD fields Syntax
Card Information 38	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string SID (type received from AD as octet string)
Card Information 39	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Information 40	TBD	AD fields drop list returns attributes of types: • print case string • replica link (type received from AD as octet string) • case insensitive string • case sensitive string • unicode string • numerical string • octet string • SID (type received from AD as octet string)
Card Filter (Hatrix only) (integer)	TBD	AD fields drop list returns attributes of types: • integer • numerical string • enumeration
Privileged Operation (Global Gateway only) (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean
Supervisor level (Global/Hatrix only) (shortint)	TBD	AD fields drop list returns attributes of types: • integer • enumeration • boolean



EntraPass fields	Active Directory fields	Possible AD fields Syntax
Delete when expired (shortint)	TBD	AD fields drop list returns attributes of types: - integer - enumeration - boolean
Wait for Keypad (shortint)	TBD	AD fields drop list returns attributes of types: - integer - enumeration - boolean
PIN (char)	TBD	AD fields drop list returns attributes of types: - print case string - replica link (type received from AD as octet string) - case insensitive string - case sensitive string - unicode string - numerical string - octet string - SID (type received from AD as octet string)
Card State (shortint)	TBD	AD fields drop list returns attributes of types: - integer - enumeration - boolean
Disable Passback (shortint)	TBD	AD fields drop list returns attributes of types: - integer - enumeration
Extended Door Access	TBD	AD fields drop list returns attributes of types: - integer - enumeration
Allow Multi-Swipe (shortint)	TBD	AD fields drop list returns attributes of types: - integer - enumeration
Picture (binary)	TBD	AD fields drop list returns attributes of types: - replica link (type received from AD as octet string) - octet string - SID (type received from AD as octet string)



EntraPass fields	Active Directory fields	Possible AD fields Syntax
Badge Layout (integer)	TBD	AD fields drop list returns attributes of types: - integer - numerical string - enumeration
Bar Code (shortint)	TBD	AD fields drop list returns attributes of types: - integer - enumeration
Value (char)	TBD	AD fields drop list returns attributes of types: - print case string - replica link (type received from AD as octet string) - case insensitive string - case sensitive string - unicode string - numerical string - octet string - SID (type received from AD as octet string)
Enable usage restriction (shortint)	TBD	AD fields drop list returns attributes of types: - integer - enumeration
Maximum card usage (integer)	TBD	AD fields drop list returns attributes of types: - integer - numerical string - enumeration
Manual Operation only (shortint)	TBD	AD fields drop list returns attributes of types: - integer - enumeration
Card access group (shortint)	TBD	AD fields drop list returns attributes of types: - integer - enumeration
Comment (char)	TBD	AD fields drop list returns attributes of types: - print case string - replica link (type received from AD as octet string) - case insensitive string - case sensitive string - unicode string - numerical string - octet string - SID (type received from AD as octet string)



EntraPass - Instrukcja instalacji i obsługi programu System



EntraPass - Instrukcja instalacji i obsługi programu System



EntraPass - Instrukcja instalacji i obsługi programu System



EntraPass - Instrukcja instalacji i obsługi programu System



EntraPass - Instrukcja instalacji i obsługi programu System



EntraPass - Instrukcja instalacji i obsługi programu System



Powiązania (Associations)

Powiązania to mechanizm logicznego grupowania urządzeń. Gdy jedno z urządzeń w asocjacji zmieni stan, w jakim udostępniane są inne urządzenia w stowarzyszeniu. Na przykład powiązanie może obejmować drzwi i dwie kamery w tym samym obszarze. Po otwarciu drzwi następuje bezpośrednie połączenie z dwoma kamerami w tym stowarzyszeniu. Ta funkcja jest wymagana dla aplikacji EntraPass Go Install.

UWAGA: W każdym powiązaniu obsługiwanych jest maksymalnie 8 urządzeń.

Aby utworzyć nowe powiązanie, wykonaj następujące kroki.

- 1 - Wybierz przycisk Powiązania na karcie Urządzenia.
- 2 - Kliknij przycisk Nowy, aby utworzyć nowe powiązanie.
- 3 - Dodaj opisową nazwę do powiązania. Na przykład „Wejście główne”.
- 4 - Każda karta zawiera listę obsługiwanych urządzeń w tej kategorii. Na przykład w zakładce Drzwi wszystkie wyświetlane są obsługiwane drzwi. Zaznacz pola wyboru urządzeń, które chcesz dodać do powiązania.
- UWAGA: Drzwi, wejścia, przekaźniki, kamery (tylko Exacq), partycje (tylko DSC) i strefy (tylko DSC) są wspierane w stowarzyszeniach.
- 5 - Kliknij przycisk Zapisz, aby zapisać skojarzenie.
- 6 - Aby usunąć powiązanie, wybierz powiązanie z listy rozwijanej i wybierz przycisk Usuń.
- 7 - Aby zmodyfikować powiązanie, wybierz powiązanie z listy rozwijanej, wprowadź zmiany i kliknij Zapisz.

UWAGA: Jeśli kamera i drzwiczki zostaną dodane do powiązania, ta kamera zostanie również automatycznie dodana

definicji tego drzwi. Jeśli kamera została wcześniej dodana do innych drzwi, pojawi się widok wideo automatycznie dodawane do definicji drzwi. Jeśli do drzwi zostanie dodana więcej niż jedna kamera, pierwsza

kamera zostanie dodana do definicji drzwi.



Raport z uruchomienia (Commissioning)

Uruchomienie to narzędzie, które wykonuje serię testów w celu sprawdzenia, czy każde urządzenie zostało poprawnie zainstalowane. Proces uruchamiania utrzymuje status uruchomienia każdego obsługiwanego urządzenia, które można wykorzystać wygenerować raport uruchomienia. Ta funkcja jest wymagana dla aplikacji EntraPass Go Install.

Uruchomienie jest dostępne dla następujących elementów:

- Drzwi.
- Wejścia.
- Przekazniki.
- Strefy (tylko DCS).
- Kamery (tylko Exacq).
- Partycje (tylko DSC).

Aby wyświetlić stan uruchomienia urządzenia, wybierz urządzenie z karty **Urządzenia**.

Jeśli uruchomienie jest obsługiwane przez urządzenie, dostępna będzie karta Uruchomienie. Ta karta zawiera następujące elementy:

- Wyniki testów - w tym dane historyczne.
- Data i godzina uruchomienia.
- Komentarze.
- Zdjęcia.

Status każdego urządzenia może być Nie wykonano, Żądany, Przekazany lub Niepowodzenie. Operator może zmienić status urządzenia na żądanie, aby zmusić urządzenie do przeprowadzenia testu uruchomienia.

UWAGA: Raport uruchomienia jest dostępny w zakładce Raport.



Tworzenie/modyfikowanie poziomu dostępu dla operatora (Creating/Modifying an Operator Security Level)

Przypisanie poziomu dostępu ma kluczowe znaczenie dla systemu. Jeżeli do poziomu dostępu przypisze się pełen dostęp do menu systemu, operatora z tym poziomem bezpieczeństwa może mógł zmieniać/modyfikować parametry systemu. Upewnij się, że każdy operator otrzyma poziom bezpieczeństwa odpowiedni do jego zadań.

Obiekty w oknie Poziom bezpieczeństwa są przedstawione w drzewku, ze wszystkimi komponentami dostępnymi do wyboru. Ta struktura umożliwia łatwe wybranie komponentu przy przyznawaniu poziomu bezpieczeństwa dla operacji zdalnych. Każdy poziom bezpieczeństwa jest identyfikowany odpowiednim kolorem: pełen dostęp (zielony), tylko do odczytu (żółty), brak dostępu (czerwony). Osoba zarządzająca bezpieczeństwem albo operator z odpowiednimi uprawnieniami może w łatwy sposób zmienić albo przypisać komponent do niższego poziomu bezpieczeństwa (zmiana koloru poprzez podwójne kliknięcie).

Notatka: operatorzy nie będą widzieć obiektów, do których nie mają uprawnień.

1 – W zakładce System, wybierz przycisk Poziom bezpieczeństwa. Pojawi się nowe okno z aktywną zakładką Menu.

2 – Z listy wybierz Poziom bezpieczeństwa, który chcesz modyfikować.

- Aby stworzyć nowy poziom bezpieczeństwa, kliknij Nowy.

3 – W zakładce Menu, kliknij podwójnie na obiekt, aż przypiszesz mu odpowiedni status: pełen dostęp (zielony), tylko do odczytu (żółty), brak dostępu (czerwony). Aby być bardziej konkretnym odnośnie przyznanych uprawnień, możesz zaznaczyć odpowiednie obiekty znajdujące się po lewej stronie.

Notatka: operator posiadający uprawnienia „Tylko do odczytu” nie będzie mógł wydrukować komponentów w EntraPass.



Tworzenie / modyfikacja operatorów (Creating or Editing an Operator)

1 – Z zakładki System, wybierz przycisk Operator (Operator).

Notatka: w prawym górnym rogu można znaleźć informację na temat Stacji roboczej EntraPass, na której zalogował się operator oraz datę ostatniego logowania.

2 – W nowym oknie wprowadź Nazwę operatora. Składa się ona z maksymalnie 40 znaków alfanumerycznych (wliczając spacje). Ta nazwa będzie wyświetlana na liście wiadomości pulpitu oraz w raportach.

3 – Opcjonalnie, wprowadź adres **email** operatora.

4 – Wprowadź Nazwę Login (Login name) dla operatora. Nazwa może zawierać od 6 do 20 znaków alfanumerycznych (wliczając spacje).

Notatka: przy logowaniu należy wprowadzić login oraz hasło, aby system mógł zweryfikować prawa dostępu. Login jest wyświetlany w szczegółowych informacjach na temat zdarzenia, kiedy zdarzenia operatora są generowane (np. zdalne działania, logowania, etc.).

5 – W polu Hasło, które będzie wykorzystywane przy logowaniu dla określonej Nazwy Login. Hasło jest alfanumeryczne i składa się maksymalnie 20 znaków (minimum siedem). Hasło nie jest wyświetlone, ani drukowane. System wyświetla hasło w postaci gwiazdek.

Notatka: zwróć uwagę na wielkie/małe litery przy wprowadzaniu hasła.

6 – W polu Potwierdź hasło, wprowadź ponownie hasło, aby je potwierdzić. Jeżeli hasło nie będzie się zgadzać z ustalonym wcześniej hasłem, pojawi się wiadomość o błędzie.

7 – W sekcji **Język**, zaznacz odpowiednią opcję wyświetlania języka dla operatora. Jeżeli zmienisz opcje język wyświetlania, zmiany zostaną wprowadzone po przelogowaniu się operatora. Jeżeli operator wyloguje się z aplikacji, następny operator, który zaloguje się do aplikacji zobaczy okno startowe w języku używanym przez ostatniego operatora.



8 – W sekcji **Przywileje (Privileges)**:

- Wybierz opcję **Auto-potwierdzenie (Auto acknowledge)**. Po jej wybraniu, przycisk **Manualnie (Manual)** zostanie dodany do pulpitu Alarmów. Operator może wybrać, czy zdarzenia będą potwierdzane automatycznie czy manualnie.
 - Wybierz opcję **Zastąp obszar roboczy stacji roboczej (Override workstation workspace message)**. Ta opcja sprawia, że podstawowe ustawienia obszaru roboczego stacji roboczej zostaną zignorowane i operator otrzyma zdarzenia ze wszystkich stacji roboczych i bramek.
 - Zaznacz opcję **Przywileje**, jeżeli chcesz, aby operator miał dostęp do poglądu kamer wideo. Wideo > Kamera > Pokaż opcje kamery.
 - **Automatyczne wyświetlanie wideo (Automatic video display)**: ta opcja informuje system, że dla operatora zalogowanego ma automatycznie wyświetlić nagranie wideo w przypadku zdarzenia alarmowego. Jeżeli **Pulpit alarmów** jest skonfigurowany i otwarty, wideo jest wyświetlane automatycznie. Jeżeli nie jest otwarty, system sprawdza ustawienia wyświetlania wideo dla tej stacji roboczej (Urządzenia > Wiadomości 2 z 2 > Wyłącz auto-wyświetlanie wideo; jeżeli ta opcja nie jest zaznaczona, system sprawdza ustawienia dla tego operatora: operator > Automatyczne wyświetlanie wideo).
- Notatka: opcja Pomiń przestrzeń stacji roboczej to przywilej przyznany operatorom. Pozwala im otrzymywać zdarzenia niezależnie od tego, na jakiej stacji roboczej są aktualnie zalogowani. Jeśli ta opcja jest wybrana razem z: Wprowadź parametry operatora dla wiadomości oraz Wprowadź parametry operatora dla alarmów; to podstawowa konfiguracja zostanie pominięta, a zdarzenia będą filtrowane według poziomu bezpieczeństwa użytkownika, który jest aktualnie zalogowany do stacji roboczej.
- Jeżeli jest to wymagane, zaznacz **Pozwól na logowanie do EntraPass Web (Allow login to EntraPass Web)** dla operatora. Komponent EntraPass Web musi zostać zarejestrowany wraz z Serwerem EntraPass, aby ta opcja była dostępna.
 - Zaznacz **Filtruj raporty przy użyciu obszaru roboczego (Filter reports using workspace)**, dla wszystkich **raportów na żądanie i raportów wej./wyj.**, które mają zostać przygotowane według uprawnień operatora zdefiniowanych w jego obszarze roboczym.

Notatka: aby wybrany komponent pracował prawidłowo, musi mieć również wybrany „nadrzędny” komponent. W innym przypadku nie zostanie wyświetlony w raporcie, nawet, jeżeli opcja Filtruj raporty przy wykorzystaniu przestrzeni roboczej (Filter reports using workspace) jest wybrana.

9 – Kliknij zakładkę **Zabezpieczenie (Security)**, aby ustawić parametry dostępu dla operatora.



EntraPass - Instrukcja instalacji i obsługi programu System

10 – Z menu Terminarz logowania (Login Schedule), wybierz terminarz, podczas którego operator może zalogować się do systemu. Możesz chcieć przygotować, a następnie przypisać, specjalny terminarz dla operatora (Definiowanie > Terminarz),

Notatka: aby umożliwić operatorowi logowanie się do różnych aplikacji EntraPass albo do serwerów EntraPass, wybierz pole Pozwól na logowanie do aplikacji oraz/albo Pozwól na logowanie do serwera (System > Poziom bezpieczeństwa > zakładka Różne).

11 – Z menu Poziom bezpieczeństwa, wybierz poziom bezpieczeństwa, który określi, do jakich komponentów dany operator ma dostęp. Poziom bezpieczeństwa składa się z wielu menu, przez które operator może modyfikować bazę danych, tworzyć komponenty, przeglądać komponenty systemu i zdarzeń, etc.

Notatka: można zdefiniować do 250 poziomów bezpieczeństwa; EntraPass oferuje 3 zdefiniowane poziomy bezpieczeństwa (Instalator, Administrator, Strażnik) przy konfigurowaniu. Domyślne ustawienia dla Instalatora dają dostęp do wszystkich komponentów systemu. Instalator musi zaprogramować pozostałe poziomy bezpieczeństwa, aby ograniczyć ich dostęp do menu poleceń oraz/albo opcji.

12 – Z menu Obszar roboczy, wybierz obszar roboczy, który określi do jakich fizycznych komponentów operator będzie dostęp.

Notatka: kiedy instalujesz EntraPass po raz pierwszy, EntraPass oferuje jedną wbudowaną Przestrzeń roboczą instalatora.

13 – W sekcji Zabezpieczenie (Security) możesz edytować opcje zabezpieczeń aktualnie wyświetlonego profilu operatora:

- Wyłącz operatora: czasowo zawiesza albo ogranicza dostęp operatora do systemu, bez wykorzystania daty końcowej dla operatora. Po wybraniu tej opcji i operatora, dany operator nie będzie mógł uruchomić aplikacji.
- Zmień hasło przy następnym logowaniu: operator będzie musiał zmienić hasło przy następnym logowaniu.
- Wyłącz operatora po wprowadzeniu złego hasła: ogranicza ilość powtórzeń hasła przy nieprawidłowym wprowadzeniu hasła. Na przykład, ustawienie tej wartości na 3, pozwala operatorowi trzykrotnie popełnić błąd przy wprowadzaniu hasła.
- Dni przed resetem hasła: po upływie czasu określonego, operator będzie musiał zmienić hasło.



EntraPass - Instrukcja instalacji i obsługi programu System

- Użyj daty końcowej: musisz wybrać datę końcową dla operatora.
- Data końcowa dla operatora: działa z opcją **Użyj daty końcowej (Use expiry date)**, pozwala wyłączyć dostęp dla operatora w konkretnym dniu.
- **Równoległe logowanie (Concurrent Logins):**
 - **Zaznacz Zezwól (Enabled)**, aby zezwolić na równoległe logowania do aplikacji EntraPass.
 - Aby pozwolić na równoległe logowania do aplikacji EntraPass **PRZEZ** EntraPass Webstations, zaznacz **Zezwól na równoległe logowania do Webstations (Enabled with concurrent logins from WebStations)**

Notatka: aby ta opcja była wyświetlona komponent EntraPass Web powinien zostać zarejestrowany w serwerze EntraPass.



Równoległe logowanie (Concurrent Logins)

Aplikacja EntraPass umożliwia równoczesne albo równoległe logowanie EntraPass Web do tej samej aplikacji EntraPass. Trzeba to zaplanować z wyprzedzeniem, tak, aby w momencie instalowania albo aktualizowania aplikacji, posiadać wszystkie wymagane certyfiakty. Szczegóły poniżej:

Numer elementu	Opis	Maksymalna ilość równoległych loginów (połączeń)
EntraPass Corporate Edition		
E-COR-WEB-1	1 połączenie Web	50
E-COR-WEB-3	3 połączenia Web	
EntraPass Global Edition		
E-GLO-WEB-1	1 połączenie Web	200
E-GLO-WEB-3	3 połączenia Web	

Notatka: zmiany wprowadzane do aktualnie wyświetlanego profilu zostaną wprowadzone przy następnym logowaniu.

- 1 – Kliknij zakładkę **Domyślne wartości (Default value)**, aby wybrać obowiązkowe typy kart (opcjonalnie).
- 2 – Zaznacz opcję **Obowiązkowe pole (Mandatory field)**, aby ją włączyć.
- 3 – Kliknij w trzy kropki, aby wybrać typ karty.

Filtrowanie zdarzeń pulpit (Filtering Desktop Events),

UWAGA: Opcja filtrowania zdarzeń pulpitu jest dostępna tylko wtedy, gdy tryb [Zdarzeń przypisanych do operatora](#) został włączony.

Możesz wybrać typ zdarzenia wyświetlany na wykazie zdarzeń dla każdego operatora. Wydarzenia są pogrupowane 4 różne grupy wyboru. Dla każdej grupy wyboru możesz edytować nazwę (kliknij dwukrotnie kartę nazwa) i edytuj wydarzenia w grupie. Aby odfiltrować zdarzenia dla operatora, wykonaj następujące czynności:

- 1 - Kliknij kartę Wybór zdarzenia na pulpicie.
- 2 - Wybierz grupę zdarzeń. Każda grupa może mieć przypisany obszar roboczy.
 - Domyślne.
 - Invalid.
 - Watchable.
 - Wszystko.
- 3 - Wybierz lub usuń zaznaczenie zdarzeń z grupy zdarzeń. Kliknij prawym przyciskiem myszy okno, aby otworzyć Rozszerzone okno wyboru.
- 4 - Kliknij ikonę zapisu. Na karcie Wartość domyślna w sekcji Bieżący wybór można wybrać grupę zdarzeń

przypisany do którego pulpitu.

UWAGA: Operatorzy zalogowani na stacjach roboczych z włączonym dedykowanym pulpitem zdarzeń będą domyślnie ustawieni na konfiguracja filtra zdarzeń stacji roboczych.



Struktura bazy danych (Database Structure Definition)

Użyj menu Struktura bazy danych, aby przeglądać bazę danych systemu. Menu wyświetli całą strukturę bazy danych, wliczając:

- Fizyczne komponenty (aplikacje EntraPass, bramki, obiekty, kontrolery, drzwi, przekaźniki, etc.)
- Logiczne komponenty (karty, terminarze, raporty, instrukcje, grupy, etc.).

Użytkownik może edytować albo sortować komponenty systemu z okna **Struktura bazy danych**.

Podgląd komponentów bazy danych (Viewing the Database Components)

1 – Z paska narzędzi System, kliknij na przycisk Struktura bazy danych.

Notatka: jeśli opcja Wideo jest dostępna w EntraPass, jej komponenty zostaną wyświetlone w wyszukiwarce Bazy danych.

2 – Aby wyświetlić wyłącznie Komponenty fizyczne, wybierz przycisk komponenty fizyczne. Tylko komponenty fizyczne bazy danych zostaną wyświetlone.

Notatka: domyślnie, fizyczne komponenty są zawsze wyświetlone.

3 – Aby wyświetlić wyłącznie Komponenty logiczne, wybierz przycisk komponenty logiczne. Komponenty logiczne bazy danych zostaną wyświetlone razem z komponentami fizycznymi.

4 – Możesz użyć przycisku Odśwież, aby otrzymać najbardziej aktualne informacje zapisane w bazie danych serwera.

5 – Możesz wybrać **Rozwiń wszystko (Full expand)**, aby w pełni rozwinąć strukturę drzewa i sprawdzić wszystkie pod-komponenty wybranego komponentu. Na przykład, jeżeli użyjesz tego przycisku na kontrolerze, system wyświetli komponenty kontrolera (drzwi, Wejścia linii dozorowej, przekaźniki) w prawej części okna.



6 – Możesz wybrać Zwiń wszystko (Full collapse), aby w pełni zwinąć strukturę drzewa i tym samym ukryć wszystkie pod-komponenty wybranego komponentu.

7 – Aby edytować komponent, kliknij na nim prawym przyciskiem i z menu wybierz **Edytuj**. System wyświetli odpowiednie okno, abyś mógł zmodyfikować jego parametry.

8 – Aby posortować komponent, kliknij na nim prawym przyciskiem i z menu wybierz Sortuj po (Sorted by). Sortowanie komponentów w prawym panelu okna ułatwia wyszukiwanie. Możesz sortować po komponencie albo po nazwie.

Notatka: możesz określić, w jaki sposób fizyczny adres komponentu będzie wyświetlony. Będzie to również miało wpływ na sposób sortowania komponentów. Zobacz Definiowanie poziomu bezpieczeństwa.

Definiowanie parametrów zdarzeń (Event Parameters Definition)

UWAGA: Funkcja parametrów zdarzenia została zastąpiona przez Zdarzenia przypisane do operatora. Aby uzyskać więcej informacji, kliknij [tutaj](#).

Definiowanie parametrów zdarzeń jest jedną z najważniejszych funkcji systemu. Możesz określić sposób, w jaki system będzie procesować każde zdarzenie. Możesz, na przykład:

- Przekierowywać zdarzenia do urządzeń zewnętrznych.
- Wysyłać instrukcje do aplikacji SmartLink.
- Określać terminarze, które pozwolą – na przykład – wysyłać alarmy do aplikacji EntraPass wyłącznie nocą.
- Wysyłać konkretne zdarzenie do konkretnej aplikacji EntraPass, etc.

Istnieje ponad 400 zdarzeń systemowych. Najczęściej występujące to:

- Przyznanie dostępu
- Wejście linii dozorowej w alarmie
- Karta zmodyfikowana przez użytkownika, etc.

Zdarzenia są powiązane z komponentami systemu, takimi jak: drzwi, kontrolery, bramki, etc. Każda wiadomość o zdarzeniu jest powiązana z komponentem systemu oraz urządzeniem wyjściowym albo grupą urządzeń. Na przykład, zdarzenie Przyznania dostępu może zostać zdefiniowane dla każdego indywidualnych drzwi albo domyślnie może być zdefiniowane dla wszystkich drzwi. Ta elastyczność umożliwia określenie różnych działań i reakcji.



Definiowanie parametrów zdarzeń (Defining Events Parameters)

Okienko **Parametry zdarzeń** pozwala użytkownikowi na dostosowanie zdarzeń systemowych. Możesz określić zdarzenia, które będą drukowane automatycznie albo, które będą potwierdzone podczas konkretnego terminarza. Możesz również wysłać instrukcje, aby poinformować użytkownika przy pomocy innych metod (np. email, pager, etc.) o wygenerowaniu alarmu. Domyślnie, wszystkie zdarzenia są zdefiniowane tak, aby były wyświetlane na wszystkich **Pulpitach wiadomości (Message desktops)**, ze wszystkich **aplikacji EntraPass** zdefiniowanych w systemie. Możesz dostosować swoje zdarzenia systemowe poprzez ręczne przypisanie zdarzeń i komponentów. Istnieją dwa sposoby przypisania: ręczne oraz domyślne.

- Domyślne przypisania: są ustawione (preset) w systemie. Domyślnie, wszystkie wiadomości o zdarzeniach występują na wszystkich komponentach powiązanych z nimi i są wyświetlane na **Pulpitach wiadomości (Messages desktops)**. Możesz zachować ustawienia domyślne.

Domyślne przypisania		Komentarze
Komponent	Stacja robocza	
Domyślny	Domyślna	Wszystkie zdarzenia, ze wszystkich komponentów są wysłane do wszystkich stacji roboczych
Domyślny	Stacja robocza 2	Wszystkie zdarzenia, ze wszystkich komponentów są wysłane tylko do stacji roboczej 2
Drzwi 1	Domyślna	Tylko zdarzenia pochodzące z Drzwi 1 są wysłane do wszystkich stacji roboczych

- Ręczne przypisania: są ustawiane przez administratora i pozwalają na wysłanie wiadomości do Pulpitów wiadomości dla konkretnych zdarzeń. Poniższa tabela pokazuje trzy rodzaje ręcznych powiązań:

Domyślne przypisania		Komentarze
Komponent	Stacja robocza	
Konkretny	Konkretna	Zdarzenia generowane przez Drzwi 1 są wysłane tylko do stacji roboczej 1
Konkretny	Nieokreślona lub domyślna	Zdarzenia generowane przez Drzwi 1 są wysłane do wszystkich stacji roboczych (domyślne)
Nieokreślony lub domyślny	Konkretna	Tylko zdarzenia pochodzące z dowolnych drzwi (Domyślnie) są wysłane tylko do stacji roboczej 1

Notatka: zdalne powiązania są priorytetowe względem domyślnych powiązań. Jeśli zdalnie ustawisz powiązanie pomiędzy wiadomościom na temat zdarzenia oraz komponentem, domyślne powiązanie jest ignorowane. Może zostać przywrócone po usunięciu zdalnego powiązania. Zdalne powiązania powinny być używane ostrożnie.

1 – W zakładce System, kliknij Parametry zdarzenia.

2 – Z listy **Kategoria zdarzenia (Event category)** wybierz kategorię, wybierając pomiędzy **Zdarzenia kontroli dostępu (Access control events)** i Zdarzenia dotyczące wtargnięcia (**Intrusion events**).



EntraPass - Instrukcja instalacji i obsługi programu System

3 – Z listy Zdarzeń, wybierz zdarzenie, dla którego chcesz określić ustawienia.

Notatka: domyślnie, wszystkie zdarzenia mają zostać wysłane na Pulpit wiadomości wszystkich stacji roboczych EntraPass posiadających zawsze ważny terminarz, określony w systemie. Zaleca się zachowanie wszystkich ustawień domyślnych, zwłaszcza wtedy, kiedy te ustawienia dotyczą wszystkich komponentów/zdarzeń. Możesz jednak stworzyć zdalne połączenie, jeśli chcesz, aby konkretne zdarzenie generowało konkretny alarm albo wiadomość. Wybrane zdarzenie pojawi się na wszystkich drzwiach oraz zostanie wyświetlone na wszystkich stacjach roboczych EntraPass.

4 – Sekcja Ustawienia wyświetlania, określa opcje wyświetlania: domyślnie, wszystkie zdarzenia są zaprogramowane tak, aby wyświetlały się w oknie Pulpitu wiadomości na wszystkich stacjach roboczych EntraPass w systemie. Mają przypisany terminarz: Zawsze ważne.

Notatka: jeśli korzystasz z aplikacji SmartLink, ten terminarz musi pozostać „Zawsze ważny”. W przeciwnym razie wiadomości/polecenia nie będą przesyłane do aplikacji.

5 – Z menu Drukuj, wybierz terminarz, aby określić, kiedy zdarzenia będą drukowane. Kiedy ten terminarz jest ważny, wybrane zdarzenie zostanie wydrukowane na drukarce określonej na stacji roboczej, do której zostało wysłane.

6 – Z listy kolorów, wybierz kolor, który zostanie wykorzystany do wyświetlenia zdarzenia na Pulpicie wiadomości. Domyślnie kolory są ustawione następująco:

- **Czerwony** – zdarzenia alarmowe.
- **Zielony** – elementy wracają do normalnego stanu.
- **Żółty** – ostrzeżenia i błędy.
- **Niebieski** – inne zdarzenia.

7 – W sekcji Ustawienia alarmu, określ:

- Alarm (terminarz): kiedy terminarz jest ważny, zdarzenie zostanie wysłane do Pulpitu alarmów wybranej stacji roboczej i będzie wymagało potwierdzenia od użytkownika.
- Instrukcje: wybierz instrukcję, która zostanie wysłana na Pulpit instrukcji razem ze zdarzeniem do potwierdzenia. Instrukcje mogą być wysłane wyłącznie wtedy, kiedy terminarz alarmu jest ważny.

Notatka: w przypadku aplikacji SmartLink instrukcja nie wymaga tego, aby terminarz alarmu był prawidłowy. Pole Terminarz alarmu możesz pozostawić puste, a instrukcja i tak zostanie wysłana.

8 – Przypisz Poziom priorytetu (Priority level) do zdarzenia. Określisz w ten sposób sekwencję, w jakiej wiadomości alarmowe będą wyświetlane użytkownikowi. Priorytety są określone według podstawowych wartości: 0 = wyższe, 9 = niższe).

9 – W sekcji **SmartLink**, kliknij trzy kropki, aby wybrać Terminarz zadań (**Task schedule**).

10 – Kliknij trzy kropki, aby wybrać Terminarz zadań (**Task schedule**).



EntraPass - Instrukcja instalacji i obsługi programu System



Tworzenie powiązań (Creating Associations)

1 – W oknie **Parametry zdarzenia (Event parameters)**, z listy wybierz **Kategorię zdarzenia (Event category)** oraz **Zdarzenie**. Z panelu komponentów (po lewej) wybierz komponent, a następnie wybierz aplikację EntraPass, do której wiadomość o zdarzeniu zostanie wysłana.

2 – Kliknij przycisk **Zapisz**, aby stworzyć nowe powiązanie. Na przykład, zdarzenia Pełen dostęp – drzwi otwarte, które zostaną wygenerowane na konkretnych drzwiach, zostaną wysłane na przypisaną wcześniej stację roboczą (wybraną z prawego panelu).

Notatka: przycisk **Zapisz** jest dostępny tylko wtedy, kiedy wybrane zdarzenie/komponent staje się częścią powiązania.

Domyślne parametry podglądu (Viewing Default Parameters)

1 – Z panelu komponentów (po lewej) wybierz komponent, a następnie wybierz aplikację EntraPass, do której wiadomość o zdarzeniu zostanie wysłana.

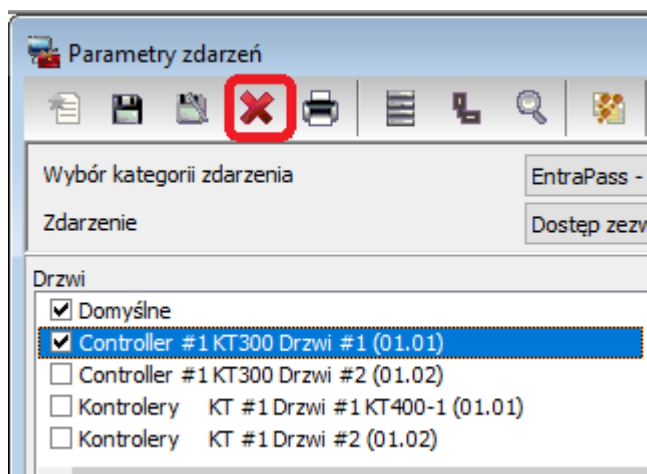
2 – Kliknij przycisk **Sprawdź ustawienia domyślne (View default parameters)** na pasku narzędzi, aby sprawdzić ustawienia domyślne. W wyświetlonym polu będzie można sprawdzić, czy parametry były ustawione ręcznie czy były ustawione, jako domyślne.

3 – Kliknij ponownie na **Sprawdź ustawienia domyślne (View default parameters)**, aby zamknąć pole wiadomości.

Usuwanie oraz przywracanie powiązań (Deleting and Restoring Associations)

Przykład: możesz zdecydować, że zdarzenie z konkretnego komponentu nie powinno być więcej wysyłane na Pulpit wiadomości wszystkich stacji roboczych, ani na konkretny pulpit. Aby to osiągnąć musisz usunąć istniejące powiązanie. Zaleca się ostrożność przy korzystaniu z tej opcji.

1 – W oknie **Parametry zdarzenia**, wybierz kategorię, a następnie z listy **Zdarzenie**, wybierz zdarzenie, które chcesz modyfikować.



2 – Na pasku narzędzi kliknij przycisk **Usuń**.

3 – W oknie **Usuń parametry zdarzenia (Delete event parameters)** wybierz:

- Przywróć domyślne: ta opcja przywróci ustawienia domyślne dla alarmów i wyświetlania.
- Wstrzymaj wiadomości: pola ustawień alarmów i wyświetlania pozostaną puste, gotowe na wprowadzenie nowych informacji. Po usunięciu ustawień będziesz musiał zdefiniować je na nowo.
- Anuluj: kliknij, jeżeli chcesz anulować operację usuwania.

Drukowanie parametrów zdarzeń (Printing Event Parameters)

EntraPass pozwala na drukowanie parametrów zdarzenia (ustawień alarmu i wyświetlania) dla wybranego zdarzenia.

1 – Z okna Parametry zdarzenia, wybierz przycisk Drukarka.

2 – W panelu **Wybierz zdarzenia**, wybierz zdarzenia, które mają być uwzględnione w wydruku; albo przy pomocy przycisku **Wybierz wszystkie**, wybierz wszystkie zdarzenia z wyświetlonej listy.

3 – W panelu **Wybierz stacje robocze**, wybierz stacje robocze (albo stację roboczą) EntraPass, które mają być uwzględnione w wydruku; albo przy pomocy przycisku **Wybierz wszystkie**, wybierz wszystkie stacje robocze EntraPass z wyświetlonej listy.

- **Drukuj puste pola (Print empty fields):** system wydrukuje pola, które nie zawierają żadnych informacji. Tylko tytuł pola zostanie wydrukowany.
- **Drukuj z wartościami domyślnymi (Print with default values):** system wydrukuje domyślne powiązania jak i ręcznie zmieniona powiązania.

Notatka: jeśli nie wybierzesz tego pola w raporcie zostaną wyświetlone tylko zdalne powiązania. Jeśli nie masz zdalnych powiązań (komponent x ze stacją roboczą y) raport będzie pusty.



- **Drukuj opisy komponentów (Print components reference):** system wydrukuje fizyczny adres komponentu obok identyfikacji komponentu.
- Przy pomocy przycisku Czcionka (Font) możesz zmienić rozmiar oraz typ czcionki dla raportu.
- Wydruk można sprawdzić przed drukowaniem przy pomocy przycisku **Podgląd**.

Definiowanie instrukcji (Instructions Definition)

To menu jest wykorzystywane do określania instrukcji, które muszą być przypisane do zdarzeń. W momencie, kiedy wygenerowany jest alarm, instrukcja zostanie wyświetlona w oknie Instrukcji do potwierdzenia. Zazwyczaj, każda linia będzie zawierała pojedynczą wytyczną; instrukcja odpowiedzi będą się składać z kilku wytycznych (linii). Pozwala to na większą elastyczność, gdy wymagane są modyfikacje.

Definiowanie instrukcji (Defining an Instruction)

- 1 – Z głównego okna **Systemu**, wybierz przycisk **Instrukcja**.
- 2 – Aby stworzyć nową, kliknij Nowa. Aby modyfikować instrukcję, wybierz jedną z listy.
- 3 – Wprowadź nazwę/identyfikację instrukcji.
- 4 - Jeżeli do alarmu jest przypisana opcja **Obowiązkowego komentarza do alarmów (Mandatory Alarm Comment)**, użytkownik będzie musiał wprowadzić komentarz, aby oznaczyć alarm, jako potwierdzony.
- 5 – Wybierz odpowiednią zakładkę z językiem, aby wprowadzić instrukcję. Instrukcje są wprowadzane w jednym wybranym języku.

Notatka: możesz wprowadzić do 511 znaków (ze spacjami) per instrukcja.

- 6 – Aby przypisać instrukcję do zdarzeń, zobacz **Definiowanie parametrów zdarzenia (Event Parameters Definition)**.

Definiowanie filtrów zdarzeń (Message Filters Definition)

Opcja Filtr wiadomości (Message filter) pozwala na określenie filtrów. Filtry są wykorzystywane do podglądu konkretnego wyboru zdarzeń. Istnieje wiele rodzajów filtrów: zdarzenia dostępu, zdarzenia kontrolera, etc. Dostęp do filtrów mają wszyscy użytkownicy. Możesz wybierać oraz tworzyć filtry bezpośrednio z **pulpitu „Filtrowanych wiadomości”** albo z menu **Filtry wiadomości**.

Notatka: zobacz Pulpit „Filtrowanych wiadomości”, aby dowiedzieć się więcej.

Definiowanie zdarzenia dla filtra wiadomości (Defining Event for a Message Filter)



EntraPass - Instrukcja instalacji i obsługi programu System

- 1 – W głównym oknie Systemu, kliknij przycisk **Filtr wiadomości (Message Filter)**. Pojawie się nowe okno.
 - 2 – Z listy **Filtr wiadomości**, wybierz typ wiadomości o zdarzeniu (zdarzenia drzwi, zdarzenia przełączników, etc.), dla którego chcesz określić filtr. Możesz również kliknąć przycisk **Nowy**, aby stworzyć nowy filtr.
 - 3 – Z listy **Zdarzenie**, wybierz zdarzenia, które mają się pojawić w wybranych filtrach. Możesz wybrać opcję **Wybierz wszystkie zdarzenia (Select all events)**, jeżeli nie chcesz wybierać konkretnych zdarzeń. Na przykład, dla filtra **Zdarzenia drzwi**, możesz wybrać wszystkie zdarzenia albo zdarzenia odmowy dostępu.
 - 4 – Wybierz zakładkę **Filtry drzwi (Door filters)**, aby wyfiltrować drzwi, które będą wysyłać wiadomość na pulpit. Dodatkowo, jeżeli wyfiltrowane są „zdarzenia dostępu”, obrazy posiadacza karty może zostać wyświetlony razem ze zdarzeniem (o ile obrazy są przypisane posiadaczy kart). Możesz wybrać, które drzwi wyświetlą obraz posiadacza karty, kiedy wygenerowane jest zdarzenie dla tych drzwi.
 - 5 – Wybierz opcję **Wszystkie drzwi** albo wybierz konkretny drzwi, dla których obrazy posiadaczy kart będą wyświetlane przy **Zdarzeniu drzwi**.
 - 6 – Wybierz filtr, który będzie wykorzystany do filtrowania **Zdarzeń drzwi**:
 - **Filtr dla drzwi**: tylko zdarzenia powiązane z wybranymi drzwiami będą wysyłane do pulpitu „**Filtrowanych wiadomości**” (**Filtered Message desktop**).
 - **Filtr dla obrazu**: obrazy posiadaczy kart powiązane z kartami użytymi na wybranych drzwiach będą wysyłane do pulpitu „**Filtrowanych wiadomości**” (**Filtered Message desktop**).
 - **Filtry dla drzwi i obrazów**: zdarzenia drzwi powiązane z wybranymi drzwiami oraz obrazy posiadaczy kart, które wywołały zdarzenie drzwi dla wybranych drzwi, będą wysyłane do pulpitu „**Filtrowanych wiadomości**” (**Filtered Message desktop**).
 - 7 – Wybierz aplikację **EntraPass**, aby filtrować aplikację, które będą wysyłać wiadomości do pulpitu „**Filtrowanych wiadomości**” (**Filtered Message desktop**).
 - 8 – Zaznacz opcję **Wszystkie aplikacje EntraPass**, aby otrzymywać wszystkie zdarzenia pochodzące ze wszystkich aplikacji **EntraPass** zdefiniowanych w systemie. Można również wybrać wyświetlanie zdarzeń z konkretnej aplikacji. Aby to osiągnąć, wybierz aplikację **EntraPass**, z której chcesz otrzymywać zdarzenia.
 - 9 – Wybierz zakładkę **Bramka i połączenie (Gateway and connection)**, aby filtrować zdarzenia z bramek i obiektów wysyłane do pulpitu „**Filtrowanych wiadomości**” (**Filtered Message desktop**).
 - 10 – Zaznacz opcję **Wszystkie zdarzenia**, aby otrzymywać zdarzenia pochodzące z komponentów bramek albo obiektów. Możesz wybrać bramkę albo połączenie, które wyśła zdarzenie do wyświetlenia.
- Notatka: jeśli korzystasz z filtrów, system pobiera zdarzenia, które są już wyświetlane na twoim Pulpicie wiadomości i sortuje te zdarzenia według ustawień wybranych filtrów. Jeśli zdarzenia pochodzące z konkretnej bramki są wyświetlane na twoim Pulpicie wiadomości, a ta bramka nie jest wybrana przy definiowaniu filtrów, zdarzenia te nie zostaną wyświetlone.
- 11 – Wybierz zakładkę **Specjalny filtr (Special filter)**, aby filtrować zdarzenia według ich typu.



EntraPass - Instrukcja instalacji i obsługi programu System

- **Obraz:** wszystkie zdarzenia powiązane z obrazem posiadacza karty będą wyświetlane na pulpicie „**Filtrowanych wiadomości**” (**Filtered Message desktop**).
- **Fail-soft:** wszystkie zdarzenia wygenerowane przez kontroler działający w trybie autonomicznym z awarią komunikacji będą wysyłane do pulpitu „**Filtrowanych wiadomości**” (**Filtered Message desktop**). Wiadomości fail-soft są identyfikowane przez znak +.
- **Wideo:** wszystkie zdarzenia nagrania wideo będą wysyłane do pulpitu „**Filtrowanych wiadomości**” (**Filtered Message desktop**).

Notatka: jeśli korzystasz z filtrów, system pobiera zdarzenia, które są już wyświetlane na twoim Pulpicie wiadomości i sortuje te zdarzenia według ustawień wybranych filtrów. Jeśli zdarzenia pochodzące z konkretnej bramki są wyświetlane na twoim Pulpicie wiadomości, a ta bramka nie jest wybrana przy definiowaniu filtrów, zdarzenia te nie zostaną wyświetlone.

Definiowanie operatorów (Operators Definition)

Przy pomocy menu Operator (Operator) można definiować operatorów systemu oraz określać ich poziom bezpieczeństwa i przywileje. Operator jest odpowiedzialny za wypisywanie kart, prowadzenia operacji na komponentach systemu, zgłaszanie raportów, uzbrajanie systemu, etc. Ze względów bezpieczeństwa, każdy operator z dostępem do bazy danych systemu, powinien mieć określony profil, aby wszystkie akcje wykonane w systemie mogły zostać sprawdzone. Należy stworzyć przynajmniej jedno konto operatora albo zmodyfikować istniejące, aby operator mógł korzystać z EntraPass oraz otrzymywać wiadomości o zdarzeniach. W systemie skonfigurowanych jest trzech operatorów. Są powiązani z trzema poziomami dostępu:

- **Installer** (login i hasło: kantech): pełen dostęp do podglądu, modyfikowania, usuwania, drukowania komponentów.
- **Administrator** (login: kantech1; hasło: kantech): średni dostęp z ograniczonymi uprawnieniami do menu systemu.
- **Guard** (login: kantech2; hasło: kantech): ograniczony dostęp do menu systemu.

Notatka: możesz zdefiniować operatora korzystając z domyślnych operatorów albo możesz stworzyć nowego operatora. Zobacz Definiowanie poziomu bezpieczeństwa, aby dowiedzieć się więcej.

Notatka: kiedy aplikacja Active directory jest włączona, nowy domyślny operator LDAP Interface jest stworzony i jest dostępny na liście Operatorzy.



Tworzenie oraz edytowanie Operatora (Creating or Editing an Operator)

1 – Z zakładki System, wybierz przycisk **Operator** (Operator).

Notatka: w prawym górnym rogu można znaleźć informację na temat Stacji roboczej EntraPass, na której zalogował się Operator oraz datę ostatniego logowania.

2 – W nowym oknie wprowadź Nazwę Operatora. Składa się ona z maksymalnie 40 znaków alfanumerycznych (wliczając spacje). Ta nazwa będzie wyświetlana na liście wiadomości pulpitu oraz w raportach.

3 – Opcjonalnie, wprowadź adres **email** Operatora.

4 – Wprowadź Nazwę Login (Login name) dla użytkownika. Nazwa może zawierać od 6 do 20 znaków alfanumerycznych (wliczając spacje).

Notatka: przy logowaniu należy wprowadzić login oraz hasło, aby system mógł zweryfikować prawa dostępu. Login jest wyświetlany w szczegółowych informacjach na temat zdarzenia, kiedy zdarzenia Operatora są generowane (np. zdalne działania, logowania, etc.).

5 – W polu Hasło, które będzie wykorzystywane przy logowaniu dla określonej Nazwy Login. Hasło jest alfanumeryczne i składa się maksymalnie 20 znaków (minimum siedem). Hasło nie jest wyświetlone, ani drukowane. System wyświetla hasło w postaci gwiazdek.

Notatka: zwróć uwagę na wielkie/małe litery przy wprowadzaniu hasła.

6 – W polu Potwierdź hasło, wprowadź ponownie hasło, aby je potwierdzić. Jeżeli hasło nie będzie się zgadzało z ustalonym wcześniej hasłem, pojawi się wiadomość o błędzie.

7 – W sekcji **Język**, zaznacz odpowiednią opcję wyświetlania języka dla Operatora. Jeżeli zmienisz opcję język wyświetlania, zmiany zostaną wprowadzone po przelogowaniu się Operatora. Jeżeli Operator wyloguje się z aplikacji, następny Operator, który zaloguje się do aplikacji zobaczy okno startowe w języku używanym przez ostatniego Operatora.

8 – W sekcji **Przywileje (Privileges)**:

- Wybierz opcję **Auto-potwierdzenie (Auto acknowledge)**. Po jej wybraniu, przycisk **Manualnie (Manual)** zostanie dodany do pulpitu Alarmów. Operator może wybrać czy zdarzenia będą potwierdzane automatycznie czy manualnie.
- Wybierz opcję **Zastąp obszar roboczy stacji roboczej (Override workstation workspace message)**. Ta opcja sprawia, że podstawowe ustawienia obszaru roboczego stacji roboczej zostaną zignorowane i użytkownik otrzyma zdarzenia ze wszystkich stacji roboczych i bramek.
- Zaznacz opcję **Przywileje**, jeżeli chcesz, aby Operator miał dostęp do poglądu kamer wideo. Wideo > Kamera > Pokaż opcje kamery.



EntraPass - Instrukcja instalacji i obsługi programu System

- **Automatyczne wyświetlanie wideo (Automatic video display):** ta opcja informuje system, że dla Operatora zalogowanego ma automatycznie wyświetlić nagranie wideo w przypadku zdarzenia alarmowego. Jeżeli **Pulpit alarmów** jest skonfigurowany i otwarty, wideo jest wyświetlane automatycznie. Jeżeli nie jest otwarty, system sprawdza ustawienia wyświetlania wideo dla tej stacji roboczej (Urządzenia > Wiadomości 2 z 2 > Wyłącz auto-wyświetlanie wideo; jeżeli ta opcja nie jest zaznaczona, system sprawdza ustawienia dla tego Operatora: Użytkownik > Automatyczne wyświetlanie wideo).

Notatka: opcja Pomiń przestrzeń stacji roboczej to przywilej przyznany Operatorom. Pozwala im otrzymywać zdarzenia niezależnie od tego, na jakiej stacji roboczej są aktualnie zalogowani. Jeśli ta opcja jest wybrana razem z: Wprowadź parametry Operatora dla wiadomości oraz Wprowadź parametry Operatora dla alarmów; to podstawowa konfiguracja zostanie pominięta, a zdarzenia będą filtrowane według poziomu bezpieczeństwa Operatora, który jest aktualnie zalogowany do stacji roboczej.

- Jeżeli jest to wymagane, zaznacz **Pozwól na logowanie do EntraPass Web (Allow login to EntraPass Web)** dla użytkownika. Komponent EntraPass Web musi zostać zarejestrowany wraz z Serwerem EntraPass, aby ta opcja była dostępna.

- Zaznacz **Filtruj raporty przy użyciu obszaru roboczego (Filter reports using workspace)**, dla wszystkich **raportów na żądanie i raportów wej./wyj.**, które mają zostać przygotowane według uprawnień Operatora zdefiniowanych w jego obszarze roboczym.

Notatka: aby wybrany komponent pracował prawidłowo, musi mieć również wybrany „nadrzędny” komponent. W innym przypadku nie zostanie wyświetlony w raporcie, nawet, jeżeli opcja Filtruj raporty przy wykorzystaniu przestrzeni roboczej (Filter reports using workspace) jest wybrana.

9 – Kliknij zakładkę **Zabezpieczenie (Security)**, aby ustawić parametry dostępu dla Operatora.

10 – Z menu Terminarz logowania (Login Schedule), wybierz terminarz, podczas którego Operator może zalogować się do systemu. Możesz chcieć przygotować, a następnie przypisać, specjalny terminarz dla Operatora (Definiowanie > Terminarz),

Notatka: aby umożliwić Operatorowi logowanie się do różnych aplikacji EntraPass albo do serwerów EntraPass, wybierz pole Pozwól na logowanie do aplikacji oraz/albo Pozwól na logowanie do serwera (System > Poziom bezpieczeństwa > zakładka Różne).

11 – Z menu Poziom bezpieczeństwa, wybierz poziom bezpieczeństwa, który określi, do jakich komponentów dany Operator ma dostęp. Poziom bezpieczeństwa składa się z wielu menu, przez które użytkownik może modyfikować bazę danych, tworzyć komponenty, przeglądać komponenty systemu i zdarzeń, etc.

Notatka: można zdefiniować do 250 poziomów bezpieczeństwa; EntraPass oferuje 3 zdefiniowane poziomy bezpieczeństwa (Instalator, Administrator, Strażnik) przy konfigurowaniu. Domyślne ustawienia dla Instalatora dają dostęp do wszystkich komponentów systemu. Instalator musi zaprogramować pozostałe poziomy bezpieczeństwa, aby ograniczyć ich dostęp do menu poleceń oraz/albo opcji.

12 – Z menu Obszar roboczy, wybierz obszar roboczy, który określi do jakich fizycznych komponentów Operator będzie dostęp.



Notatka: kiedy instalujesz EntraPass po raz pierwszy, EntraPass oferuje jedną wbudowaną Przestrzeń roboczą instalatora.

13 – Etykieta **Active directory** jest widoczne w dolnej, lewej części ekranu wyłącznie przy aktywacji aplikacji **Active directory**. Kiedy wprowadzisz **Profil** dla Operatora, ten profil będzie wykorzystany, jako szablon dla Operatora tej kategorii. Po synchronizacji z Active directory, **Nazwa domeny (Domain name)** oraz serwer **Active directory**, są wyświetlane w polach tylko do odczytu.

Notatka: przed synchronizacją musisz zdalnie zdefiniować profil Operatora. Profil musi istnieć w EntraPass i pasować dokładnie do podgrupy (pod nazwą pasującą do bazy LDAP) w Active directory. Ikona Szukaj na pasku narzędzi pozwala Operatorowi na wyszukiwanie przez nazwy profilowe (należy zwrócić uwagę na wielkie/male litery).

14 – Jeżeli zaznaczysz pole **Wyłącz synchronizację (Disable synchronization)**, **Active directory** przestaje aktualizować jakiekolwiek dane. Operator nadal istnieje w EntraPass, ale nie będzie aktualizowany przez synchronizację.

15 – W sekcji Zabezpieczenie (Security) możesz edytować opcje zabezpieczeń aktualnie wyświetlonego profilu Operatora:

- Wyłącz Operatora: czasowo zawiesza albo ogranicza dostęp Operatora do systemu, bez wykorzystania daty końcowej dla Operatora. Po wybraniu tej opcji i Operatora, dany Operator nie będzie mógł uruchomić aplikacji.
- Zmień hasło przy następnym logowaniu: Operator będzie musiał zmienić hasło przy następnym logowaniu.
- Wyłącz Operatora po wprowadzeniu złego hasła: ogranicza ilość powtórzeń hasła przy nieprawidłowym wprowadzeniu hasła. Na przykład, ustawienie tej wartości na 3, pozwala Operatorowi trzykrotnie popełnić błąd przy wprowadzaniu hasła.
- Dni przed resetem hasła: po upływie czasu określonego, Operator będzie musiał zmienić hasło.
- Użyj daty końcowej: musisz wybrać datę końcową dla Operatora.
- Data końcowa dla Operatora: działa z opcją **Użyj daty końcowej (Use expiry date)**, pozwala wyłączyć dostęp dla Operatora w konkretnym dniu.
- **Równoległe logowanie (Concurrent Logins):**
 - **Zaznacz Zezwól (Enabled)**, aby zezwolić na równoległe logowania do aplikacji EntraPass.
 - Aby pozwolić na równoległe logowania do aplikacji EntraPass **PRZEZ** EntraPass Webstations, zaznacz **Zezwól na równoległe logowania do Webstations (Enabled with concurrent logins from WebStations)**

Notatka: aby ta opcja była wyświetlona komponent EntraPass Web powinien zostać zarejestrowany w serwerze EntraPass.



EntraPass - Instrukcja instalacji i obsługi programu System



Równoległe logowanie (Concurrent Logins)

Aplikacja EntraPass umożliwia równoczesne albo równoległe logowanie EntraPass Web do tej samej aplikacji EntraPass. Trzeba to zaplanować z wyprzedzeniem, tak, aby w momencie instalowania albo aktualizowania aplikacji, posiadać wszystkie wymagane certyfiakty. Szczegóły poniżej:

Numer elementu	Opis	Maksymalna ilość równoległych loginów (połączeń)
EntraPass Corporate Edition		
E-COR-WEB-1	1 połączenie Web	50
E-COR-WEB-3	3 połączenia Web	
EntraPass Global Edition		
E-GLO-WEB-1	1 połączenie Web	200
E-GLO-WEB-3	3 połączenia Web	

Notatka: zmiany wprowadzane do aktualnie wyświetlanego profilu zostaną wprowadzone przy następnym logowaniu.

1 – Kliknij zakładkę **Domyślne wartości (Default value)**, aby wybrać obowiązkowe typy kart (opcjonalnie).

2 – Zaznacz opcję **Obowiązkowe pole (Mandatory field)**, aby ją włączyć.

3 – Kliknij w trzy kropki, aby wybrać typ karty.

Definiowanie wiadomości przy logowaniu dla pojedynczego operatora (Defining a Login Message for a Single Operator)

1 – Z menu **System**, wybierz **Operator (Operator)**.

2 – Z listy wybierz Operatora.

3 – Kliknij zakładkę **Wiadomość przy logowaniu**.

4 - Określ powtarzalność:

- **Brak (None)**.
- **Zawsze (Always)**: ta wiadomość pojawi się zawsze po logowaniu.
- **Tylko raz (Only once)**: ta wiadomość pojawi się tylko raz na Operatora.
- **Aż do (Until)**: ta wiadomość będzie się pojawiać, aż do określonej daty.
- **Tylko raz, aż do (Only once until)**: ta wiadomość będzie się pojawiać, aż do określonej daty albo do otrzymania wiadomości przez Operatora.

5 – Wybierz **Wyłącz wszystkie wiadomości przy logowaniu**, aby wyłączyć otrzymywanie tego rodzaju wiadomości dla wybranego Operatora.

6 – Wprowadź tekst wiadomości w pola po prawej (główny i drugi język).

7 – Kliknij **Zapisz**.



EntraPass - Instrukcja instalacji i obsługi programu System



Definiowanie poziomów dostępu dla operatorów (Security Level Definition)

Poziom bezpieczeństwa odnosi się do zgody udzielanej operatorowi na dostęp do komponentów logicznych EntraPass oraz do przeprowadzania działań na tych komponentach.

Notatka: musisz zaprogramować odpowiednie poziomy bezpieczeństwa, jeśli chcesz ograniczyć dostęp operatora do poleceń oraz/albo opcji w menu systemu.

Możliwe jest dopasowanie poziomu bezpieczeństwa operatora; system pozwala na stworzenie do 250 poziomów bezpieczeństwa. Każdy operator posiada oddzielny login, hasło oraz odpowiedni poziom bezpieczeństwa. W EntraPass skonfigurowanych jest trzech operatorów i trzy poziomy bezpieczeństwa: Instalator, Administrator oraz Strażnik.

- Instalator:

- o Login i hasło: kantech

- o Poziom bezpieczeństwa: domyślnie, użytkownik określony, jako Instalator ma pełny dostęp do menu systemu. Może odczytać i edytować komponenty systemu oraz posiada nieograniczony dostęp do systemu,

- Administrator:

- o Login: kantech1; hasło: kantech

- o Poziom bezpieczeństwa: Administrator. Domyślnie, użytkownika określony, jako Administrator posiada ograniczony dostęp do menu systemu.

- Operator:

- o Login: kantech2; hasło: kantech

- o Poziom bezpieczeństwa: Operator. Domyślnie, użytkownika określony, jako Strażnik posiada ograniczony dostęp do menu systemu.



Tworzenie/modyfikowanie poziomu bezpieczeństwa dla operatora (Creating/Modifying an Operator Security Level)

Przypisanie poziomu bezpieczeństwa ma kluczowe znaczenie dla systemu. Jeżeli do poziomu bezpieczeństwa przypisze się pełen dostęp do menu systemu, operator z tym poziomem bezpieczeństwa może mógł zmieniać/modyfikować parametry systemu. Upewnij się, że każdy operator otrzyma poziom bezpieczeństwa odpowiedni do jego zadań.

Obiekty w oknie Poziom bezpieczeństwa są przedstawione w drzewku, ze wszystkimi komponentami dostępnymi do wyboru. Ta struktura umożliwia łatwe wybranie komponentu przy przyznawaniu poziomu bezpieczeństwa dla operacji zdalnych. Każdy poziom bezpieczeństwa jest identyfikowany odpowiednim kolorem: pełen dostęp (zielony), tylko do odczytu (żółty), brak dostępu (czerwony). Osoba zarządzająca bezpieczeństwem albo operator z odpowiednimi uprawnieniami może w łatwy sposób zmienić albo przypisać komponent do niższego poziomu bezpieczeństwa (zmiana koloru poprzez podwójne kliknięcie).

Notatka: operatorzy nie będą mogli zobaczyć obiektów, do których nie dostali uprawnień.

1 – W zakładce System, wybierz przycisk Poziom bezpieczeństwa. Pojawi się nowe okno z aktywną zakładką Menu.

2 – Z listy wybierz Poziom bezpieczeństwa, który chcesz modyfikować.

- Aby stworzyć nowy poziom bezpieczeństwa, kliknij Nowy.

3 – Wybierz zakładkę systemu (**stacja robocza, EntraPass Web, EntraPass Go** albo **Smartlink API**).

4 – Kliknij podwójnie na obiekt, aż przypiszesz mu odpowiedni status: pełen dostęp (zielony), tylko do odczytu (żółty), brak dostępu (czerwony). Aby być bardziej konkretnym odnośnie przyznanych uprawnień, możesz zaznaczyć odpowiednie obiekty znajdujące się po lewej stronie.

Notatka: użytkownik posiadający uprawnienia „Tylko do odczytu” nie będzie mógł wydrukować komponentów w EntraPass.



Definiowanie opcji logowania dla operatora (Defining Login Options for an Operator)

Zakładka Różne (**Miscellaneous**), pozwala określić login operator oraz opcje wyświetlania systemu:

- Opcje logowania operator: można udostępnić albo ograniczyć możliwość logowania się do stacji roboczej albo serwera EntraPass.
- Wyświetlanie aktywnych okien na pulpicie: EntraPass pozwala trzymać pięć aktywnych okien na pulpicie.
- Opcje wyświetlania komponentów: komponenty mogą być wyświetlane z, albo bez ich fizycznych adresów. Adres fizyczny może być wyświetlany po lewej albo po prawej stronie nazwy komponentu.

1 – Wybierz zakładkę **Różne**, aby określić parametry dla poziomu bezpieczeństwa, który jest aktualnie definiowany.

2 – W sekcji **Ograniczenia logowania (Login restrictions)**, wybierz odpowiednią opcję logowania:

- Wybierz **Logowanie na serwerze (Allow login on server)**, aby pozwolić na logowanie na serwer EntraPass (główny albo redundantny).
- Wybierz **Logowanie na stacji roboczej (Allow login on workstation)**, aby pozwolić na logowanie do dowolnej aplikacji w systemie.

3 – Sekcja **Zachowaj pulpit aplikacji (Keep on application desktop)** pozwala operatorowi zwiększyć liczbę aktywnych okien na pulpicie. Operator może mieć otwarte pięć okien: jedno okno konfiguracji i cztery okna innych kategorii. Okna EntraPass są klasyfikowane według pięciu kategorii:

- Ekran konfiguracji: ta grupa zawiera wszystkie menu, które pozwalają na programowanie systemu: menu operatora (karty, identyfikatory, poziomy dostępu, etc.); menu Definiowania; menu Grup, menu Urządzeń; menu Systemu; menu Wideo; etc.
- Ekran operacji: ta grupa zawiera wszystkie elementy menu **Operacje** oraz opcje **Odtwarzania wideo**.
- Ekran statusów: ta grupa zawiera okna m.in. menu Statusów, menu Bieżącego nagrywania.
- Ekran bazy danych: następujące menu zaliczają się do tego kategorii: menu Opcje (format karty, hasło, wybór języka, opcje drukarki, etc.); menu Elementów i Użytkowników (przepustki, etc.); Podgląd raportu; Operacje wej./wyj.; etc.
- Ekran raportów: Szybki raport, Raport na żądanie, Raport wej./wyj., etc.

Notatka: ta opcja umożliwia operatorowi na posiadanie więcej niż jednego aktywnego okna na pulpicie. Poprzez wciśnięcie ALT-F6 użytkownik może przenosić okna zarówno na tył, jak i na przód zależnie od tego, które okno chce wyświetlić.

4 – W sekcji Adres komponentów, określ, jak adres będzie wyświetlany. Będzie to miał wpływ na to, jak komponenty będą sortowane.

- Wyświetl po lewej – komponenty będą sortowane po adresie (np. 01.01.01 Kontroler xyz).
- Wyświetl po prawej – komponenty będą sortowane po nazwie (np. Kontroler xyz 01.01.01).
- Brak wyświetlania – adres nie będzie wyświetlany (np. Kontroler xyz), a komponenty będą sortowane po nazwie.

5 – Sekcja Różne (opcje do wybrania):

- Ukryj zawartość pin posiadacza karty.
- Ukryj kamerę z podglądu wideo.

Notatka: zaznaczenie opcji Ukryj kamerę z podglądu wideo informuje system o potrzebie zweryfikowania pozwoleń dostępu do kamer przed wczytaniem podglądu wideo. Na przykład, jeśli poziom bezpieczeństwa wybranego operatora daje mu dostęp do serwera wideo, ale nie do wszystkich kamer zdefiniowanych w tym



serwerze, system ukryje te kamery, które nie zostały zaznaczone przy przypisywaniu dostępu do serwera wideo. Zobacz Konfigurowanie serwera wideo.

Ukrywanie informacji o karcie (Hiding Card Information)

EntraPass oferuje możliwość ukrycia pól informacji o karcie. Na przykład, możesz zdecydować, że dany poziom bezpieczeństwa (np. Strażnik), będzie mógł sprawdzić albo modyfikować pola informacji o karcie. Aby to zrobić, wybierz poziom bezpieczeństwa, następnie – w zakładce **Pola bazy danych karty (Card database fields)** – zaznacz pola, które chcesz ukryć.

1 – Wybierz zakładkę **Pola bazy danych karty (Card database fields)**, aby ograniczyć ilość pól karty, które są widoczne dla operatora z przypisanym poziomem bezpieczeństwa.

2 – Wybierz pola, które będą ukryte dla wybranego poziomu bezpieczeństwa. Kliknij na polu kilkukrotnie, aby uzyskać dostęp do kolejnych statusów (Normalny, Ukryty, Tylko do odczytu).



Przypisywanie przycisku niestandardowego wideo (Assigning Video Custom Buttons)

EntraPass oferuje możliwość dopasowania pięciu przycisków do wykorzystania w interfejsie wideo. Instalatorzy systemu oraz administratorzy mogą dopasować przyciski do użytku przez operatora. Na przykład, przycisk ustawiony na **Odtwarzanie ze stałym opóźnieniem** z określonym przed-nagraniowym i nagraniowym opóźnieniem oraz konkretnym poziomem bezpieczeństwa pozwoli operatorowi

na aktywowanie działań powiązanych z konkretnym przyciskiem. Jeżeli przypiszesz niestandardowy przycisk do konkretnego działania (odtwarzania albo generowanie zdarzeń wideo), dodatkowe przyciski zostaną dodane do Pulpitu wideo (Pulpity > Pulpit dedykowany do podglądu wideo).

1 – Z listy Poziom bezpieczeństwa wybierz poziom, który chcesz zdefiniować/edytować.

2 – Wybierz zakładkę Przycisk niestandardowego wideo (Video custom button), aby przypisać upoważnienia do tego operatora. Następujące upoważnienia mogą zostać przyznane:

- Odtwarzanie ze stałym opóźnieniem
- Odtwarzanie z niestandardowym opóźnieniem
- Generowanie zdarzenia nagrywania ze stałymi parametrami
- Generowanie zdarzenia nagrywania z niestandardowymi parametrami

3 – Wybierz opcje, które chcesz przypisać do modyfikowanego operatora.

Notatka: wciśnięcie przycisku powiązanego z Odtwarzaniem ze stałym opóźnieniem rozpocznie odtwarzanie z określonym czasem, uwzględniające czas nagrywania przed-alarmem oraz maksymalny czas nagrywania.



Definiowanie poziomu dostępu do programu dla operatorów (Workspace Definition)

Obszar roboczy pozwala administratorowi systemu na przyznawanie albo odebranie operatorom dostępu do komponentów systemu, takich jak: bramki, obiekty, przekaźniki, etc. Obszary robocze są definiowane według typu zadań, które operatorzy będą mogli przeprowadzać w EntraPass: tworzenie oraz edytowanie elementów, przegląd komponentów, drukowanie list albo raportów, etc. Operatorzy przypisani do danego obszaru roboczego nie będą mogli zobaczyć, ani modyfikować komponentów EntraPass, które nie są zdefiniowane dla danego obszaru roboczego. Obszary robocze mogą również być wykorzystane przez operatorów do rozróżniania informacji, które chcą wyświetlić na ekranie. Na przykład, Administrator Systemu, który ma dostęp do wszystkich komponentów systemu EntraPass może chcieć sprawdzić tylko wybrane komponenty. W takim wypadku, Administrator może zdefiniować obszar roboczy dla tego środowiska i pracować według tych parametrów.

Notatka: kiedy instalujesz EntraPass po raz pierwszy, EntraPass oferuje jedną wbudowaną Przestrzeń roboczą instalatora.

Filtrowanie obszarów roboczych (Workspace Filtering)

- Filtrowanie hierarchiczne: pozycje na liście będą wyświetlone zależnie od pozycji wybranej poziom wyżej. Na przykład, przy wybraniu konkretnego obiektu (opiekun), system automatycznie przestawi się na wyświetlanie wyłącznie odpowiednich kontrolerów. Jeżeli wybierzesz konkretny kontroler (opiekun), system wyświetli tylko odpowiednie drzwi, i tak dalej.

Notatka: jeśli zakładka jest pusta, sprawdź czy wybrałeś komponenty z ich „opiekuna”.

- Po wybraniu trybu filtrowania hierarchicznego, pozostanie on aktywny we wszystkich zakładkach.

Wybieranie aplikacji EntraPass (Selecting EntraPass Applications)

Ta opcja pozwala wybrać aplikacje, które będą dostępne dla operatora przypisanego do danego obszaru roboczego. Na przykład, obszar roboczy (Admin) nie będzie mógł sprawdzić wiadomości wysłanych przez aplikację EntraPass SmartLink, ponieważ nie jest ona przypisana do tego obszaru roboczego.

1 – Z zakładki Obszar roboczy, wybierz obszar roboczy, który chcesz zdefiniować albo edytować.

Notatka: kiedy operator jest dopuszczony do korzystania z Pulpitu wiadomości alarmów sieciowych (menu Pulpity), tylko alarmy zdarzeń pochodzących z aplikacji EntraPass oraz komponentów aplikacji, które są wybrane w tym oknie, będą wyświetlane. Ustawienia przestrzeni roboczej działają, jako filtr dla Pulpitu wiadomości alarmów sieciowych.

- Wybierz **Wszystkie aplikacje EntraPass**, jeżeli chcesz, aby wszystkie wyświetlone aplikacje były dostępne dla operatora przypisanego do obszaru roboczego.

- Możesz wybrać pojedynczą aplikację z wyświetlonej listy.

2 – Zapisz swoje zmiany.



Definiowanie Bramek i obiektów (Defining Gateways and Sites)

1 – Przejdź do zakładki **Bramka i obiekt**, aby wybrać listę bramek i obiektów, które będą dostępne dla operatora przypisanego do obszaru roboczego.

- Wybierz **Wszystkie bramki i obiekty**, jeżeli chcesz, aby wszystkie wyświetlone bramki i obiekty były dostępne dla operatora przypisanego do obszaru roboczego.

- Możesz wybrać pojedyncze bramki i obiekty z wyświetlonej listy.

2 – Zapisz swoje zmiany.

Definiowanie terminarzy (Defining Schedules)

1 – Przejdź do zakładki **Terminarz**, aby wybrać listę terminarzy, które będą dostępne dla operatora przypisanego do obszaru roboczego.

- Wybierz **Wszystkie terminarze**, jeżeli chcesz, aby wszystkie wyświetlone terminarze były dostępne dla operatora przypisanego do obszaru roboczego.

- Możesz wybrać pojedyncze terminarze z wyświetlonej listy.

2 – Zapisz swoje zmiany.

Definiowanie kontrolerów (Defining Controllers)

1 – Przejdź do zakładki **Kontroler**, aby wybrać listę kontrolerów, które będą dostępne dla operatora przypisanego do obszaru roboczego.

- Wybierz **Wszystkie kontrolery**, jeżeli chcesz, aby wszystkie wyświetlone kontrolery były dostępne dla operatora przypisanego do obszaru roboczego.

- Możesz wybrać pojedyncze kontrolery z wyświetlonej listy.

2 – Zapisz swoje zmiany.

Notatka: kiedy wybierasz kontroler, wybierasz również wszystkie komponenty zdefiniowane „pod” albo powiązane z wybranym kontrolerem (np. drzwi, przekaźniki, etc.). Upewnij się, że wybrałeś również bramkę (zakładka Bramka albo zakładka Obiekt), dla której wybrany kontroler jest zdefiniowany. Jeśli bramka nie zostanie wybrana, kontroler nie będzie dostępny nawet, jeśli zostanie wybrany z listy.



Definiowanie drzwi (Defining Doors)

1 – Przejdź do zakładki **Drzwi**, aby wybrać listę drzwi, które będą dostępne dla operatora przypisanego do obszaru roboczego.

- Wybierz **Wszystkie drzwi**, jeżeli chcesz, aby wszystkie wyświetlone drzwi były dostępne dla operatora przypisanego do obszaru roboczego.
- Możesz wybrać pojedyncze drzwi z wyświetlonej listy.

2 – Zapisz swoje zmiany.

Definiowanie przekaźników (Defining Relays)

1 – Przejdź do zakładki **Przekaźnik**, aby wybrać listę przekaźników, które będą dostępne dla operatora przypisanego do obszaru roboczego.

- Wybierz **Wszystkie przekaźniki**, jeżeli chcesz, aby wszystkie wyświetlone przekaźniki były dostępne dla operatora przypisanego do obszaru roboczego.
- Możesz wybrać pojedyncze przekaźniki z wyświetlonej listy.

2 – Zapisz swoje zmiany.

Definiowanie wejść (Defining Inputs)

1 – Przejdź do zakładki **Wejście linii dozorowej**, aby wybrać listę wyjść, które będą dostępne dla operatora przypisanego do obszaru roboczego.

- Wybierz **Wszystkie wejścia**, jeżeli chcesz, aby wszystkie wyświetlone wejścia były dostępne dla operatora przypisanego do obszaru roboczego.
- Możesz wybrać pojedyncze wejścia z wyświetlonej listy.

2 – Zapisz swoje zmiany.



Definiowanie poziomów dostępu (Defining Access Levels)

Przypisywanie poziomów dostępu do obszaru roboczego pozwala kontrolować poziomy dostępu, które operator może definiować i modyfikować.

1 – Przejdź do zakładki **Poziom dostępu**, aby wybrać listę poziomów dostępu, które będą dostępne dla operatora przypisanego do obszaru roboczego.

- Wybierz **Wszystkie poziomy dostępu**, jeżeli chcesz, aby wszystkie wyświetlone poziomy dostępu były dostępne dla operatora przypisanego do obszaru roboczego.
- Możesz wybrać pojedyncze poziomy dostępu z wyświetlonej listy.

2 – Zapisz swoje zmiany.

Notatka: upewnij się, że wybrałeś również bramkę, dla której wybrany poziom dostępu jest zdefiniowany. Jeśli bramka nie zostanie wybrana, poziom dostępu nie będzie dostępny nawet, jeśli zostanie wybrany z listy.

Definiowanie typów kart (Defining Card Types)

Ta opcja ogranicza działania operatora. Typy kart, które nie zostaną wybrane w tym menu, nie będą dostępne dla operatora w przypadku tworzenia albo edytowania przez niego kart.

1 – Przejdź do zakładki **Typ karty**, aby wybrać typy kart, które będą dostępne dla operatora przypisanego do obszaru roboczego.

- Wybierz **Wszystkie typy kart**, jeżeli chcesz, aby wszystkie wyświetlone typy kart były dostępne dla operatora przypisanego do obszaru roboczego.
- Możesz wybrać pojedyncze typy kart z wyświetlonej listy.

2 – Zapisz swoje zmiany.



Definiowanie grupy dostępu dla kart (Defining Card Access Group)

Ta opcja przyznaje dostęp operatorom do konkretnych grup dostępu kart dla operacji wsadowych według ich obszaru roboczego.

1 – Przejdź do zakładki **Grupa dostępu dla karty**, aby wybrać listę grup dostępu dla kart, które będą dostępne dla operatora przypisanego do obszaru roboczego.

- Wybierz **Wszystkie grupy dostępu dla karty**, jeżeli chcesz, aby wszystkie wyświetlone grupy dostępu dla karty były dostępne dla operatora przypisanego do obszaru roboczego.
- Możesz wybrać pojedyncze grupy dostępu dla kart z wyświetlonej listy.

2 – Zapisz swoje zmiany.

Definiowanie raportów (Defining Reports)

Ta opcja przyznaje operatorom dostęp do konkretnych raportów według ich obszaru roboczego. Na przykład, administrator systemu może mieć dostęp do wszystkich raportów, które mogą być wygenerowane, podczas gdy Kierownik Strażników może mieć dostęp wyłącznie do raportów tras strażników. Raporty będą generowane z listy zarchiwizowanych wiadomości na pulpicie stacji roboczej. Kiedy raport zostanie przypisany do obszaru roboczego, operatorzy będą mieli dostęp wyłącznie do raportów korespondujących z ich obszarem roboczym.

1 – Przejdź do zakładki **Raport**, aby wybrać listę raportów, które będą dostępne dla operatora przypisanego do obszaru roboczego.

- Wybierz **Wszystkie raporty**, jeżeli chcesz, aby wszystkie wyświetlone raporty były dostępne dla operatora przypisanego do obszaru roboczego.
- Możesz wybrać pojedyncze raporty z wyświetlonej listy.

2 – Zapisz swoje zmiany.

Definiowanie grafik (Defining Graphics)

1 – Przejdź do zakładki **Grafika**, aby wybrać listę grafik, które będą dostępne dla operatora przypisanego do obszaru roboczego.

- Wybierz **Wszystkie grafiki**, jeżeli chcesz, aby wszystkie wyświetlone grafiki były dostępne dla operatora przypisanego do obszaru roboczego.
- Możesz wybrać pojedyncze grafiki z wyświetlonej listy.

2 – Zapisz swoje zmiany.



Definiowanie operatorów (Defining Operators)

Ze względów bezpieczeństwa, operator może sprawdzić oraz zmienić prawa innego operatora. Użyj zakładki operator w celu ograniczenia możliwości sprawdzenia, edytowania albo usunięcia jednego operatora przez drugiego.

1 – Przejdź do zakładki operator, aby wybrać listę **operatorów**, którzy będą dostępni dla operatora przypisanego do obszaru roboczego.

- Wybierz **Wszyscy operatorzy** albo **Indywidualny operator** z listy.

2 – Zapisz swoje zmiany.

Definiowanie szablonu identyfikatorów (Defining Badge Layouts)

1 – Użyj zakładki **Układ identyfikatorów**, aby określić, który układ identyfikatorów będzie dostępny dla operatora przypisanego do obszaru roboczego.

2 – Przejdź do zakładki **Układ identyfikatorów**.

- Wybierz **Wszystkie układy identyfikatorów** albo **Indywidualny układ identyfikatorów** z listy.

3 – Zapisz swoje zmiany.

Definiowanie obszarów roboczych (Defining Workspaces)

Ta opcja daje operatorowi dostęp do informacji odnoszących się do konkretnych obszarów roboczych według innych obszarów roboczych. Na przykład, Strażnicy w systemie mogą mieć przypisany do siebie obszar roboczy według stref, które patrolują oraz rodzajom informacji, które mogą sprawdzić i edytować w EntraPass. Natomiast Kierownik strażników, musi mieć dostęp do informacji dostępnych dla wszystkich strażników pracujących w jego dziale. W tym przypadku, obszary robocze Kierownika będą zawierać wszystkie obszary robocze Strażników zdefiniowane w systemie.

1 – Przejdź do zakładki **Obszar roboczy**, aby wybrać listę obszarów roboczych, które będą dostępne dla operatora przypisanego do obszaru roboczego.

- Wybierz **Wszystkie obszary robocze**, jeżeli chcesz, aby wszystkie wyświetlone obszary robocze były dostępne dla operatora przypisanego do obszaru roboczego.
- Możesz wybrać pojedyncze obszary robocze z wyświetlonej listy.

2 – Zapisz swoje zmiany.



Określanie poziomu bezpieczeństwa (Specifying Security Level)

Zakładka Poziom bezpieczeństwa w obszarze roboczym ogranicza operatorów do wybrania, który poziom bezpieczeństwa mogą przydzielić przy tworzeniu/modyfikowaniu operatorów.

1 – Przejdź do zakładki **Poziom bezpieczeństwa**, aby wybrać poziom(y) bezpieczeństwa, które chcesz przyznać dla tego obszaru roboczego.

- Wybierz **Wszystkie poziomy bezpieczeństwa**, jeżeli chcesz przypisać wszystkie poziomy bezpieczeństwa do obszaru roboczego.
- Możesz wybrać pojedyncze poziomy bezpieczeństwa z wyświetlonej listy.

2 – Zapisz swoje zmiany.

Definiowanie serwerów wideo (Defining Video Servers)

Lista serwerów wideo pozwala na przypisanie albo na ograniczenie dostępu operatora do konkretnych serwerów wideo oraz kamer. Na przykład, nawet, jeżeli poziom dostępu obszaru roboczego pozwala na dostęp do serwera wideo, nadal posiadasz możliwość zablokowania dostępu do określonej kamery. Ta opcja ułatwia definiowanie oraz modyfikowanie dostępu do serwera wideo, podglądu oraz innych elementów menu.

1 – Przejdź do zakładki **Serwery wideo**, aby wybrać listę serwerów wideo, które będą dostępne dla operatora przypisanego do obszaru roboczego.

- Wybierz **Wszystkie serwery wideo**, jeżeli chcesz, aby wszystkie wyświetlone serwery wideo były dostępne dla użytkownika przypisanego do obszaru roboczego.
- Możesz wybrać pojedyncze serwery wideo z wyświetlonej listy.

2 – Zapisz swoje zmiany.

Notatka: aby filtrować podglądy wideo dostępne dla użytkownika, przestrzeń robocza użytkownika musi mieć prawa dostępu do serwera wideo powiązanego z konkretnym podglądem wideo. Na przykład, jeśli użytkownicy posiadają dostęp do podglądu wideo, ale ich przestrzeń robocza nie daje im dostępu do serwera wideo, gdzie określony jest ten podgląd, nie będzie on dostępny dla użytkowników działających w tej przestrzeni.



Definiowanie kamer (Defining Cameras)

1 – Przejdź do zakładki **Kamera**, aby wybrać listę kamer, które będą dostępne dla użytkownika przypisanego do obszaru roboczego.

- Wybierz **Wszystkie kamery**, jeżeli chcesz, aby wszystkie wyświetlone kamery były dostępne dla użytkownika przypisanego do obszaru roboczego.
- Możesz wybrać pojedyncze kamery z wyświetlonej listy.

2 – Zapisz swoje zmiany.

Definiowanie podglądów wideo (Defining Video Views)

1 – Przejdź do zakładki **Podglądy wideo**, aby wybrać listę podglądów wideo, które będą dostępne dla użytkownika przypisanego do obszaru roboczego.

- Wybierz **Wszystkie podglądy wideo**, jeżeli chcesz, aby wszystkie wyświetlone podglądy wideo były dostępne dla użytkownika przypisanego do obszaru roboczego.
- Możesz wybrać pojedyncze podglądy wideo z wyświetlonej listy.

2 – Zapisz swoje zmiany.

Definiowanie zadań (Defining Tasks)

Przypisywanie zadań do obszaru roboczego pozwala kontrolować zadanie, które użytkownik może definiować i modyfikować.

1 – Przejdź do zakładki **Makro-polecenia**, aby wybrać listę zadań, które będą dostępne dla użytkownika przypisanego do obszaru roboczego.

- Wybierz **Wszystkie zadania**, jeżeli chcesz, aby wszystkie wyświetlone zadania były dostępne dla użytkownika przypisanego do obszaru roboczego.
- Możesz wybrać pojedyncze zadania z wyświetlonej listy.

2 – Zapisz swoje zmiany.



Definiowanie paneli (Defining Panels)

Przypisywanie paneli do obszaru roboczego pozwala kontrolować panele, które użytkownik może definiować i modyfikować.

1 – Przejdź do zakładki **Panel**, aby wybrać listę paneli, które będą dostępne dla użytkownika przypisanego do obszaru roboczego.

- Wybierz **Wszystkie panele**, jeżeli chcesz, aby wszystkie wyświetlone panele były dostępne dla użytkownika przypisanego do obszaru roboczego.
- Możesz wybrać pojedyncze panele z wyświetlonej listy.

2 – Zapisz swoje zmiany.

Definiowanie komponentów paneli (Defining Panel Components)

Przypisywanie komponentów paneli do obszaru roboczego pozwala kontrolować komponenty paneli, które użytkownik może definiować i modyfikować.

1 – Przejdź do zakładki **Komponenty paneli**, aby wybrać listę komponentów paneli, które będą dostępne dla użytkownika przypisanego do obszaru roboczego.

- Wybierz **Wszystkie komponenty paneli**, jeżeli chcesz, aby wszystkie wyświetlone komponenty paneli były dostępne dla użytkownika przypisanego do obszaru roboczego.
- Możesz wybrać pojedyncze komponenty paneli z wyświetlonej listy.

2 – Zapisz swoje zmiany.



Definiowanie zdarzeń (Defining Events)

Ta opcja jest wykorzystywana do definiowania wiadomości o zdarzeniu, które są wyświetlane użytkownikowi przypisanemu do obszaru roboczego.

1 – Przejdź do zakładki **Zdarzenia**, aby wybrać listę zdarzeń, które zostaną wyświetlone na obszarze roboczym użytkownika.

- Wybierz **zdarzenia**, które chcesz, aby były dostępne dla użytkownika przypisanego do obszaru roboczego.

2 – Zapisz swoje zmiany.

Definiowanie dostępu do programu dla operatora (Operators in Workspace)

1 – Ze względów bezpieczeństwa, użytkownik może sprawdzić oraz zmienić prawa innego użytkownika. Dodatkowa tabela została zintegrowana w obszarze roboczym w celu ograniczenia możliwości sprawdzenia, edytowania albo usunięcia jednego użytkownika przez drugiego.

2 – Z menu **System**, wybierz **Obszar roboczy**.

3 – Z listy wybierz użytkownika.

4 – Wybierz zakładkę **Użytkownik**. Zostanie wyświetlona lista użytkowników, którzy są widoczni dla wybranego użytkownika na liście **obszaru roboczego**.

Historia Zmian (Audit)

Użyj ikony Audytu, aby zobaczyć, który operator wprowadził zmiany lub usunąć komponent.

1 - Aby otworzyć okno Historii zmian, kliknij zakładkę System i kliknij Historia zmian.

2 - Aby wybrać operatora, wybierz z listy Operator.

3 - Aby wybrać komponent, wybierz jedną z następujących filtrów na liście Akcja.

- Wszystko
- Stwórz
- Zmiana
- Usuń

4 - W polu Data i godzina rozpoczęcia wybierz datę i godzinę rozpoczęcia wyszukiwania.

5 - W polu Data i godzina zakończenia wybierz datę i godzinę zakończenia wyszukiwania. Kliknij Wyszukaj.

Wyniki wyszukiwania wypełniają dwie tabele, pierwsza tabela zawiera następujące informacje o komponentach:

- Kolumna oznaczona kolorem: wskazuje, czy komponent został utworzony, zmodyfikowany lub usunięty.
 - o Zielony: Utwórz
 - o Niebieski: Modyfikuj
 - o Czerwony: Usuń
- Data i godzina: data i godzina utworzenia, modyfikacji lub usunięcia karty.
- Typ: menu, które zostało zmienione.



EntraPass - Instrukcja instalacji i obsługi programu System

- Typ komponentu: komponent, który został zmieniony.
- Count: liczba zmienionych pól.

Druga tabela zawiera następujące informacje o komponentach:

- Referencje: pozycja odniesienia do zmiany.
- Nazwa pola: nazwa pola GUI.
- Stara wartość: wartość przed wystąpieniem zmiany.
- Nowa wartość: wartość, gdy system zapisał zmianę.
- Opis pola: opis nazwy pola.

Aby uzyskać dostęp do następujących opcji kolumn, kliknij ikonę w lewym górnym rogu tabeli.

- Typ danych: typ danych bazy danych:
 - TimeStamp
 - Integer
 - Obiekt
 - Komponenty
- Nazwa tabeli: nazwa tabeli bazy danych.

UWAGA: Zdefiniuj wyniki na podstawie ilości rekordów lub daty. Aby uzyskać więcej informacji, zobacz zakładkę Historia zmian i w parametrach Systemu.

Aby uzyskać dostęp do menu kontekstowego, wybierz wpis tabeli i kliknij prawym przyciskiem myszy. Dostępne są następujące opcje:

- Wybrano eksport CSV: wyeksportuj wybrany wpis ścieżki audytu karty do pliku w formacie CSV.
- Eksportuj wszystkie pliki CSV: wyeksportuj całą zawartość ścieżki audytu karty do pliku w formacie CSV.
- Wyświetl starą wartość: wyświetl okno z wartością przed zmianą.
- Wyświetl starą wartość nadrzędną: wyświetl okno nadrzędnego wybranego komponentu z wcześniejszą wartością zmiany.
- Wyświetl link starej wartości: wyświetl okno reprezentujące łącze do komponentu z wartością przed zmianą.
- Wyświetl nową wartość: wyświetl okno z wartością po zmianie.
- Wyświetl nową wartość nadrzędną: wyświetl okno nadrzędnego wybranego komponentu z wartością po zmianie.
- Wyświetl link nowej wartości: wyświetl okno przedstawiające łącze do komponentu z wartością po zmianie.



EntraPass - Instrukcja instalacji i obsługi programu System



Raporty

Archiwum raportów zdarzeń

Archiwum raportów zdarzeń (Archive Viewing)

Opcja Archiwum umożliwia użytkownikom przeglądanie raportów, które zostały zdefiniowane i zachowane w systemie. Użytkownicy mogą korzystać z niej do przeglądania raportów w dowolnym formacie, albo do zmian w raporcie przed wydrukiem.

Notatka: kiedy utworzysz raport (csv, db albo dbf) system automatycznie stworzy plik rdf. Ten plik jest wylistowany w oknie Archiwum. Po kliknięciu Podgląd system automatycznie uruchamia odpowiedni program, aby wyświetlić raport.

Wyświetlanie raportu (Displaying a Report)

1 – Na pasku narzędzi Raport, kliknij przycisk Archiwum. System wyświetli domyślny punkt docelowy. Jeżeli raport był zapisany w innej lokalizacji, przeszukaj dysk w celu znalezienia pliku.

2 – Wybierz raport, który chcesz sprawdzić. Jeżeli podłączona jest drukarka, przycisk Podgląd jest dostępny. Służy do sprawdzenia raportu przed wydrukiem.

Notatka: aby zrobić podgląd albo wydrukować raport musisz mieć zainstalowaną drukarkę na swoim komputerze. Aby ustawić drukarkę, kliknij na Start > Ustawienia > Drukarki > Dodaj drukarkę. Aby uzyskać dodatkowe informacje skontaktuj się z administratorem systemu.

3 – Kliknij przycisk **Szczegóły (Details)**, aby wyświetlić informacje o raporcie. Pojawi się okno **Szczegóły raportu (Report details)**, zawierające informacje powiązane z wybranym raportem, takie jak: nazwa pliku, tytuł, typ, data, etc. Pole **Stacja robocza, jako filtr raportu (Workspace as report filter)** wskazuje, czy raport był filtrowany według wymagań stacji roboczej użytkownika.

4 – Kliknij przycisk **Szczegóły** ponownie, aby zamknąć okno Szczegóły raportu.

5 – Kliknij przycisk **Podgląd**, aby wyświetlić raport w oknie Podgląd raportu.

Przeglądanie raportów (Previewing Reports)

1 – W oknie **Archiwum (Archive)**, z prawego panelu wybierz raport, który chcesz obejrzeć. Jeżeli wybrałeś raport wygenerowany w Sybase, okno Opcje Raportu pozwoli ci dostosować raport przed wydrukiem.

Notatka: jeśli wybierzesz CSV, jako typ raportu, zostanie on wygenerowany w oknie WordPad w formacie tekstowym.

2 – Określ opcje filtrów. Wprowadź tekst w polu Wyszukaj opis (Search description). Raporty zostaną posortowane w taki sposób, że pozostawione zostaną tylko te, które zawierają wprowadzony tekst. Możesz dodatkowo sprecyzować filtr:



EntraPass - Instrukcja instalacji i obsługi programu Raporty

- **Zawiera (Contains):** wszystkie zdarzenia, które zawierają określony tekst zostaną uwzględnione w raporcie.
- **Zaczyna się od (Starts with):** wszystkie zdarzenia, które zaczynają się od określonego tekstu zostaną uwzględnione w raporcie.
- **Kończy się na (Ends with):** wszystkie zdarzenia, które kończą się na określony tekst zostaną uwzględnione w raporcie.
- **Zawiera dokładnie (Exact words):** wszystkie zdarzenia, które zawierają dokładnie określony tekst zostaną uwzględnione w raporcie.

3 – Kliknij przycisk **Podgląd**, wybierz **drukarkę** z listy i kliknij **OK**. System wyświetli wyniki raportu. Z nowego okna możesz:

- Wyszukać tekst w raporcie.
- Wydrukować raport
- Zachować raport (PDF, RTF, HTML oraz TXT)
- Wczytać raport (.QRP)

4 – Kliknij Właściwości (Properties), aby uzyskać dostęp do okna Szczegóły raportu (Reports details), gdzie wyświetlone są informacje:

- **Nazwa pliku raportu (Report file name):** wyświetla adres zapisania pliku oraz jego nazwę.
- **Tytuł raportu (Report title):** wyświetla tytuł raportu.
- **Data rozpoczęcia (Start date):** raporty są tworzone dla określonego przedziału czasu. Ta opcja określa datę początkową tego przedziału.
- **Data zakończenia (End date):** raporty są tworzone dla określonego przedziału czasu. Ta opcja określa datę zakończenia tego przedziału.
- **Zamówiony (Requested):** wyświetla datę i czas zamówienia raportu.
- **Dostarczony (Delivered):** wyświetla datę i czas, kiedy raport był wyprodukowany i wydrukowany.
- **Zamówiony przez (Requested by):** wyświetla nazwę użytkownika, który zamówił raport.
- **Zliczanie (Count):** wyświetla liczbę transakcji w raporcie.
- **Procesowanie wyjścia (Output process):** wyświetla liczbę możliwych/dostępnych szablonów w raporcie.



EntraPass - Instrukcja instalacji i obsługi programu Raporty

Przeglądanie raportów czasu pracy (Previewing In/Out Reports)

1 – W oknie Archiwum (Archive), wybierz raport, który chcesz obejrzeć. Jeżeli raport został określony jako „Wyświetl raport czasu pracy” (“Display In/Out Report”) oraz format wyjścia został zdefiniowany, jako „Baza danych Sybase” („Sybase Database”), pojawi się następujące okno.

2 – Wybierz opcje wyświetlania:

- **Grupuj przez (Group by):** wybierz tę opcję w celu ułatwienia zarządzania. Dane mogą grupowane przez nazwy posiadaczy karty albo przez numery kart.
- **Sortuj przez (Sort by):** możesz wybrać porządek sortowania: przez nazwy użytkowników albo przez numery kart.
- **Typ raportu (Report type):** wybierz tę opcję w celu ułatwienia zarządzania.

3 – Kliknij **Podgląd**, aby wyświetlić raport. Z nowego okna możesz albo zapisać raport (format .QRP), albo go wydrukować.



Raport użycia kart (Card Use Report)

Opcja Raport wykorzystania karty jest wykorzystywana to stworzenia raportów, które wylistują posiadaczy kart, którzy wygenerowali (albo nie) zdarzenia przez określoną liczbę dni (albo w konkretnym dniu). Na przykład, użytkownik może zamówić raport uwzględniający zdarzenia „przyznanie dostępu”, które zostały wygenerowane od konkretnego momentu/daty. System wyświetla pięć typów zdarzeń:

- Dostęp zabroniony (zła lokalizacja, zły poziom dostępu, etc.)
- Przyznanie dostępu.
- Baza danych (zdarzenia, które miały wpływ na bazę danych, np. zmiana definicji karty)
- Zdarzenia wej./wyj (wejścia, wyjścia)
- Inne zdarzenia

1 – W oknie **Raport wykorzystania Karty (Card Use Report)** wybierz raport z listy. Jeżeli tworzysz nowy raport kliknij przycisk Nowy na pasku narzędzi. Następnie wprowadź niezbędne informacje w sekcji **Język**.

2 – Możesz również zaznaczyć opcję **Procesuj oddzielnie (Process separately)**, jeżeli chcesz, aby zdarzenia były procesowane osobno dla każdej karty. Na przykład, jeżeli chcesz raport dla „**Zdarzenia odmowy dostępu**” oraz „**Zdarzenia przyznania dostępu**”, i nie zaznaczysz opcji **Procesuj oddzielnie**, otrzymasz raport zawierający oba typy zdarzeń. Jeżeli zaznaczysz opcję **Procesuj oddzielnie**, raport wyświetli oba zdarzenia osobno.

3 – Zaznacz opcję **Nadpisz istniejący plik wyjściowy (Overwrite existing output file)**, jeżeli chcesz, aby system zastąpił plik wyjściowy za każdym razem, gdy raport jest automatycznie wygenerowany według ustawień określonych w zakładce Terminarz automatycznych raportów (**Automatic report schedule**).

4 – Zaznacz **Włącz żądania EntraPass Web (Allow EntraPass Web Requests)**, dla żądań z EntraPass Web.

Notatka: aby ta opcja była wyświetlona komponent EntraPass Web powinien zostać zarejestrowany w serwerze EntraPass.

5 – Określ opcje wykorzystania karty (Nieużywana od; oraz Używana od) oraz określ przedział czasu.

6 – Aby określić potrzebny przedział czasu, kliknij przycisk Od (From) i wybierz datę. Możesz skorzystać z kalendarza, albo wprowadzić potrzebną ilość dni.

7 – Po zakończeniu definiowania raportu, zapisz go. Możesz go zamówić przy pomocy przycisku **Żądanie raportu (Report request)** na pasku narzędzi **Raport**.

Terminarz automatyczne raportu (Automatic Report Schedule)

Wybierz zakładkę Terminarz automatycznych raportów, aby określić automatyczne ustawienia dla twoich raportów w taki sposób, aby mogły być automatycznie generowane w razie potrzeby.



Definiowanie szablonów raportów (Custom Reports Definition)

Opcja **Definiowanie szablonów raportów (Custom Reports Definition)** pozwala użytkownikom na zdefiniowanie raportów na żądanie wraz z ich parametrami automatycznego wykonania. Raporty, które są zdefiniowane przy pomocy automatycznych ustawień, są automatycznie generowane w określonym czasie. Mogą również w razie potrzeby zostać przygotowane zdalnie.

Korzystanie z domyślnego raportu „wszystkich zdarzeń” (Using the Default “All Events” Report)

Możesz wygenerować domyślny raport zawierający wszystkie zdarzenia. Domyślny raport to **Raport Historyczny (typ) (Historical report)**. EntraPass umożliwia wysłanie automatycznego raportu w emailu.

1 – Na pasku narzędzi Raport, kliknij przycisk Raport na żądanie. Pojawie się nowe okno.

2 – Dla raportów **Wszystkie zdarzenia (All events)** tylko sekcja języków może być modyfikowana.

Definiowanie szablonów raportów (Defining a Custom Report)

Parametry ogólne

1 – Na pasku narzędzi **Raport**, kliknij **Raport na żądanie**. Pojawie się nowe okno.

2 – Jeżeli chcesz stworzyć nowy raport kliknij przycisk **Nowy** i wprowadź wszystkie niezbędne informacje. Aby zmodyfikować istniejący raport, wybierz go z listy **Raport**.

3 – Do wykorzystania możesz zaznaczyć opcję **Wszystkie zdarzenia (All events)** albo wybrać konkretny typ zdarzeń z listy.

4 – Wybierz **Filtr Zdarzeń (Events filter)**:

- **Normalny i nieprawidłowy (Normal & abnormal)**: zaznacz, aby w raporcie uwzględniać zarówno zdarzenia normalne, jak i nieprawidłowe.
- **Normalny (Normal)**: **Szybki raport** może tworzyć raporty w oparciu o normalne zdarzenia. W raportach dostępu, normalne zdarzenia to np. przyznanie dostępu.



- **Nieprawidłowy (Abnormal):** takie zdarzenia, jak np. Dostęp zabroniony (zły poziom dostępu), nieprawidłowe odłączenia serwera, błąd komunikacji bramki, wszystkie zdarzenia powiązane z niezakończeniem procesu; są traktowane, jako nieprawidłowe.

- **Zdarzenia do podglądu (Watchable events):** są to wybrane zdarzenia, które mogą zostać wyświetlone w EntraPass Web Watchlist.

5 - Zaznacz opcję Nadpisz istniejący plik wyjściowy (Overwrite existing output file), jeżeli chcesz, aby system zastąpił plik wyjściowy za każdym razem, gdy raport jest automatycznie wygenerowany według ustawień określonych w zakładce Terminarz automatycznych raportów (**Automatic report schedule**).

6 – Zaznacz Pomiń stację roboczą operatora (Bypass operator workspace), aby zgłosić raport bez uwzględnienia uprawnień stacji roboczej operatora.

7 - Zaznacz pole Włącz żądania EntraPass Web (Allow EntraPass Web Requests), dla żądań z EntraPass Web. Komponent EntraPass Web musi zostać zarejestrowany z serwerem EntraPass, aby to pole zostało wyświetlone.

8 – Filtr „Źródło” (Origin Filter): ten filtr jest wykorzystany do określenia raportu zdarzeń pochodzących z jednego źródła (lub kilku źródeł). Jeżeli w filtrze zaznaczone jest jedno, albo wiele źródeł (połączenie, bramka, obiekt albo aplikacja), zakładka Źródło (Origin) zostanie dodana. Zakładka umożliwia użytkownikowi wybranie jednego (lub więcej) komponentu powiązanego z wybranym źródłem.

9 – Filtr Komponent (Component filter): wybierz **Tryb filtra (Filter mode),** aby komponenty były uwzględniane. Zaznacz pole wyboru, aby wyświetlić usunięte komponenty.

10 – Konkretny przedział czasu (Specific time frame): tylko zdarzenie, które miały miejsce w określonym przedziale czasu, zostaną uwzględnione w raporcie.

Wybierania zdarzeń (Events Selection)

1 – Z listy wybierz kategorię zdarzeń.

2 – Wybierz Wszystkie zdarzenia (All events), albo osobno wybierz wszystkie zdarzenia, które chcesz uwzględnić w raporcie.

3 – Jeżeli wybrałeś Zaznacz wszystkie zdarzenia (Select all events), możesz również wybrać, który status komponentu wyświetlić (Nowy, Modyfikuj albo Usuń). W raporcie, zdarzenia będą przetwarzane przy pomocy następujących znaków: + (Nowy); = (Modyfikuj); - (Usuń).

Notatka: pola pod Konkretnym zdarzeniem bazy danych są wyświetlone tylko wtedy, kiedy zdarzenie bazy danych jest wybrane.

Notatka: zakładka Wybór zdarzeń zawiera listę zdarzeń, zależną od wybranych filtrów.

Komponenty (Components)

Jeżeli wybrałeś **Tryb filtrowania,** zakładka **Komponenty** zostanie wyświetlona wyłącznie wtedy, gdy odpowiednie zdarzenia są wybrane. Musisz określić komponenty, które mogą mieć wpływ na raport.

1 – Przejdź do zakładki Komponent.

2 – Wybierz typ komponentu, aby wyświetlić jego elementy w panelu po prawej. Jeżeli wybrałeś Typ karty, prawy panel wyświetli wszystkie typy kart zdefiniowane w systemie.



Karty (Cards)

1 – W oknie Raportów na żądanie, przejdź do zakładki Karty. Wyświetla się tylko wtedy, gdy zdarzenia dostępu są wybrane. Przy jej pomocy możesz dodać dodatkowe filtry do swojego raportu.

2 – Wybierz opcję **Wszystkie karty**, aby uwzględnić wszystkie karty. Jeżeli to zrobisz, pozostałe pola zostaną wyłączone. Jeżeli wybierzesz opcję **Użyj typ karty, jako filtr (Use card type as filter)**, będziesz mógł dodać filtry do swojego raportu. Możesz przejrzeć pola, które są uwzględnione/nieuwzględnione, jako filtry i określić dolne/górne przedziały dla każdego wyboru.

3 – Z listy **Tryb filtra (Filter mode)** określ, czy system ma wykluczyć lub włączyć zakres wartości, który określasz w polach górny/dolny przedział. Kiedy wybrany jest tryb filtra, pola „przedział” („boundary”) są dostępne.

4 – Wprowadź zakres wartości w polach **dolny/górny przedział** zgodnie z wyborem w polu **Tryb filtra**. Mogą to być, na przykład, litery alfabetu (indeks filtra po nazwach; albo cyfry, jeżeli indeks jest po numerach kart). Możesz użyć nazwy posiadacza karty i określić górny/dolny przedział w zakresie liter od A do F. Tym samym system uwzględni wszystkie zdarzenia, w których pojawiają się wybrane drzwi oraz zdarzenia, w których pojawiają się określone numery kart ale wyłącznie dla posiadaczy kart, których nazwy zaczynają się na litery od A do F.

Notatka: użytkownicy mogą wybrać więcej niż jeden filtr dla danego raportu korzystając z indeksu filtrów. Zdarzenia są filtrowane zależnie od tego, ile filtrów zostało określonych dla danego raportu.

Terminarz automatycznych raportów (Automatic Report Schedules)

Wybierz zakładkę Terminarz automatycznych raportów, aby określić ustawienia dla twoich raportów w taki sposób, aby mogły być automatycznie generowane w razie potrzeby. Ustawienia określają:

- Częstotliwość: jak często raport powinien być generowany (brak, tygodniowo, miesięcznie, jednorazowo)
- Przedział czasu raportu
- Proces wyjścia (wyświetlenie, druk)
- Typ wyjścia (dBase, Sybase, CSV, PDF)
- Miejsce docelowe (stacja robocza)
- Język i nazwa pliku

1 – W oknie **Raporty na żądanie (Custom report)**, przejdź do zakładki Terminarz automatycznych raportów.

2 – Z listy wybierz Tryb terminarza wybierz częstotliwość generowania raportów:

- **Brak (None)**: raport jest generowany zdalnie na żądanie.
- **Tygodniowo (Weekly)**: zaznacz dzień, w którym raport ma być generowany automatycznie.
- **Miesięcznie (Monthly)**: określ dzień (np. drugi piątek każdego miesiąca albo 15 dzień każdego miesiąca), w którym raport ma być generowany automatycznie.
- **Jednorazowo (Once)**: raport zostanie wygenerowany automatycznie w wybranym dniu.



EntraPass - Instrukcja instalacji i obsługi programu Raporty

3 – Kliknij przycisk **Więcej (More)**, aby określić dodatkowe opcje.

4 – Zdefiniuj poziom priorytetu – od 1 do 99, gdzie 1 jest procesowany przed 99.

5 – W polu **Rozpocznij (Start report)**, wprowadź czas rozpoczęcia generowania raportu przez system.

6 – Określ **Parametry terminarza (Scheduling parameters)**.

Notatka: te ustawienia są ignorowane, jeśli raport jest zamówiony zdalnie przez użytkownika.

- **Rozpocznij na określony czas (Start this many days back)**: raport zacznie zbierać zdarzenia przez liczbę dni określoną w polu rozpoczynając od bieżącej daty.
- **Rozpocznij o (Start at this time)**: po określenie ilości dni, określ czas rozpoczęcia (np. 07:00).
- **Zakończ po tylu dniach (Stop this many days back)**: raport uwzględni liczbę dni wpisaną w to pole, w oparciu o aktualną datę.
- **Zakończ o (Stop at this time)**: po określenie ilości dni, określ czas zakończenia (np. 17:00), czyli tym samym dzień i czas, kiedy system przestanie zbierać dane.

Notatka: czas rozpoczęcia oraz zakończenia są określane tylko dla pierwszego i ostatniego dnia. Na przykład, jeśli zaczynasz zbierać zdarzenia w poniedziałek o 8:00, a kończysz w piątek o 17:00, wszystkie zdarzenia pomiędzy poniedziałkiem 8:00, a piątkiem 17:00 zostaną włączone.

Określanie dodatkowych opcji dla automatycznych raportów (Specifying Additional Options for an Automatic Report)

1 – Kliknij przycisk  **More**, aby dodać więcej ustawień do raportu automatycznego terminarza. Po kliknięciu tego przycisku pojawi się nowe okno.

2 – Z listy **Typ wyjścia bazy danych (Database output type)** wybierz format pliku wyjściowego (Sybase, DBase IV, CSV, PDF, Excel, RTF albo Text).

3 – Z listy Proces wyjścia bazy danych (**Database output proces**), wybierz szablon, który zostanie wykorzystany przy tworzeniu raportu.

Notatka: z listy Proces wyjścia bazy danych możesz wybrać Raport email, jeśli chcesz, aby ten raport był automatycznie wysyłany do określonego odbiorcy. Jeśli wybierzesz tą opcję, opcje email zostaną wyświetlone na tej samej stronie. EntraPass pozwala zabezpieczyć raport hasłem przed wysłaniem. Po wybraniu opcji email, pojawia się opcja użycia dowolnego dostępnego SmartLink. Pozwoli ona na wykorzystanie dowolnego dostępnego SmartLink do wysłania email.



EntraPass - Instrukcja instalacji i obsługi programu Raporty

Tabela pokazuje różnice pomiędzy formatami bazy danych, a ich wyjściowymi formatami plików:

Baza danych	Opis
SyBase	Baza danych EntraPass.
Dbase IV	Popularny format systemu zarządzania bazą danych, który jest wspierany przez większość systemów zarządzania bazami danych. Nawet systemy, które nie korzystają z formatu DBase są w stanie importować/eksportować dane w tym formacie. Wyjściowy format plików: .db oraz .rdf.
CSV	Zachowa raport w formacie CSV (Comma separated values). Format danych, w którym każdy fragment danych oddzielony jest przecinkiem. Ten format jest popularny w przypadkach przenoszenia danych z jednej aplikacji do drugiej, ponieważ większość systemów baz danych jest w stanie importować/eksportować dane w tym formacie.
Excel	Pliki Microsoft Excel
PDF	Portable Document Format (PDF) to otwarty standard wymiany dokumentów. Może być otwarty przy pomocy darmowej aplikacji Adobe Reader.
RTF	Format służący do między-platformowej wymiany informacji między procesorami tekstów. Większość procesorów tekstu jest w stanie odczytać i zapisać w jakiejś formie format RTF.
Tekst	Plik tekstowy, którego struktura składa się z sekwencji wierszy. Może być otwarty przy pomocy większości narzędzi do obróbki tekstu.

4 – Możesz wybrać opcję **Automatycznego nazewnictwa pliku (...)** (**Automatic file name (...)**). Domyślnie: `YYY_MM_DD-HH_MM_SS.X`, czyli rok_miesiąc_dzień-godzina_minuta_sekunda.roszerzenie.

5 – Wybierz język raportu oraz przeznaczenie.



Definiowanie formatu wyjściowego raportu (Defining a Report Output Format)

Raporty historyczne oraz raporty wykorzystania karty (Historical and Card use reports)

1 – Jeżeli wybierzesz **Tylko baza danych (Database only)** (CSV, Sybase oraz Dbase): raport uwzględni następujące informacje: sekwencja zdarzeń, data i czas, wiadomość zdarzenia, typy opisów, nazwy opisów oraz numer karty.

Notatka: raport Tylko baza danych jest zapisany w folderze raportów w określonym formacie. Nie będzie on ani wydrukowany, ani wyświetlony.

2 – Jeżeli wybierzesz **Wyświetl raport na żądanie (Display custom report) – Wyświetl raport ostatniej transakcji karty (Display card last transaction report) (tylko Sybase)**: raport zostanie automatycznie wyświetlony na pulpicie po zakończeniu. Możesz go dostosować przed wydrukiem. Raport będzie zawierać następujące informacje: sekwencja zdarzeń, data i czas, wiadomość o zdarzeniu, numer karty oraz opisy (od 1 do 4), które zawierają szczegóły zdarzenia

3 – Raport drukowany po sekwencji (tylko Sybase) (Report printed by sequence (Sybase Only)): ten raport jest sortowany według numeru sekwencji (kolejność generowania) oraz drukowany automatycznie na drukarce stacji roboczej będącej miejscem docelowym.

4 – Raport drukowany po dacie i czasie (tylko Sybase) (Report printed by date and time): ten raport jest sortowany według daty i czasu oraz drukowany automatycznie na drukarce stacji roboczej będącej miejscem docelowym.

Notatka: drukowane raporty (opcja trzy i cztery) będą zapisywane w folderze raportów w określonym formacie. Będą one drukowane, ale nie będą wyświetlane.

5 – Raport drukowany po zdarzeniach (tylko Sybase) (Report printed by event): ten raport jest sortowany według wiadomości o zdarzeniu (alfabetycznie) oraz drukowany automatycznie na drukarce stacji roboczej będącej miejscem docelowym. Raport zostanie zapisany w folderze raportów, ale nie zostanie wyświetlony.



Raporty czasu pracy (In/Out Reports)

Raporty czasu pracy zostaną zapisane w folderze raportów, nie są ani drukowane, ani wyświetlane. Użytkownik musi zdalnie znaleźć raport, aby go wyświetlić. Może również skorzystać z menu Archiwum.

1 - Pojedynczy plik ze wszystkimi danymi (tylko CSV): raport zostanie wygenerowany w jednym pliku zawierającym wszystkie dane i opisy (data i czas, ID transakcji, nazwa użytkownika karty oraz opis drzwi)

2 – Baza danych z transakcjami (CSV oraz DBaseIV) (Database with transactions (CSV & DBase IV)): raport jest generowany ze wszystkimi danymi i transakcjami w jednym pliku. Zawiera datę i czas, ID transakcji, numer karty oraz nazwę posiadacza karty.

3 – Wyświetl raport czasu pracy (tylko Sybase) (Display In/Out report (Sybase only)): po ukończeniu raport zostanie automatycznie wyświetlony na pulpicie. Możesz go dostosować przed wydrukiem. Zawiera: numer karty, nazwę posiadacza karty, czas wejścia, czas wyjścia, zawartość pól z informacjami karty, sumę godzin na posiadacza karty.

4 – Dwie bazy danych ze wszystkimi danymi (Sybase oraz DbaseIV) (Two (2) databases with all data (Sybase & DbaseIV)): raport zostanie wygenerowany w dwóch osobnych plikach:

- jeden zawierający: datę, czas, wiadomość zdarzeń (typ transakcji), **pk_karty**, **pk_drzwi**, **pk_grupa_drzwi** (**pkcard**, **pkdoor**, **pkdoorgroup**).
- drugi zawierający: opis pk (wyjaśniający **pk_karty**, **pk_drzwi**, **pk_grupy_drzwi** (**pkcard**, **pkdoor**, **pkdoorgroup**)), numer karty, obiekt i zawartość pól z informacjami karty.

Notatka: PK odnosi się do unikatowego numeru komponentu w systemie.

5 – Pojedyncza baza danych ze wszystkimi danymi (Sybase & DbaseIV): raport zostanie wygenerowany w jednym pliku zawierającym wszystkie dane i opisy (data i czas, ID transakcji, numer karty, etc.)

6 – Kompilacja CSV raportu nt. czasu pracy (tylko CSV) (CSV compilation In/Out (CSV Only)): raport zostanie wygenerowany w dwóch plikach. Jeden będzie zawierać sumę, dla przykładu, godzin po oddziale, a drugi plik będzie zawierać szczegółowe informacje. Zależnie od tego ile dni zawartych jest w raporcie, kolumna „dzień” będzie dodana dla każdego z nich.

- **Automatyczna nazwa pliku (Automatic file name):** wybierz tę opcję, jeżeli chcesz, aby system automatycznie używał daty i czasu, jako nazwy pliku. Nie możesz wykorzystać opcji **Nadpisz istniejący plik wyjściowy (Overwrite existing output file)**, jeżeli korzystasz z opcji **Automatyczna nazwa pliku (Automatic file name)**.
- **Nazwa pliku (File name):** jeżeli chcesz nadpisywać ten sam raport (na przykład – co tydzień), możesz wprowadzić nazwę pliku. Dzięki temu w momencie, kiedy raport zostanie włączony według specyfikacji, nowy raport zastąpi stary.
- **Miejsce docelowe (Destination):** jest to miejsce, do którego raport ma zostać automatycznie wysłany/wydrukowany.
- **Język (Report language):** to pole jest wykorzystywane do wprowadzenia dodatkowych informacji do twojego raportu. Wybierz z listy.



Definiowanie terminarza automatycznego generowania raportu (Defining Automatic Report Schedules)

Wybierz zakładkę Terminarz automatycznych raportów, aby określić ustawienia dla twoich raportów w taki sposób, aby mogły być automatycznie generowane w razie potrzeby. Ustawienia określają:

- Częstotliwość: jak często raport powinien być generowany (brak, tygodniowo, miesięcznie, jednorazowo)
- Przedział czasu raportu
- Proces wyjścia (wyświetlenie, druk)
- Typ wyjścia (dBase, Sybase, CSV, PDF)
- Miejsce docelowe (stacja robocza)
- Język i nazwa pliku

1 – Z listy wybierz Tryb terminarza wybierz częstotliwość generowania raportów:

- Brak (None): raport jest generowany zdalnie na żądanie.
- Tygodniowo (**Weekly**): zaznacz dzień, w którym raport ma być generowany automatycznie.
- Miesięcznie (**Monthly**): określ dzień (np. drugi piątek każdego miesiąca albo 15 dzień każdego miesiąca), w którym raport ma być generowany automatycznie.
- Jednorazowo (**Once**): raport zostanie wygenerowany automatycznie w wybranym dniu.

2 – Zdefiniuj poziom priorytetu – od 1 do 99, gdzie 1 jest procesowany przed 99.

3 – W polu **Rozpocznij (Start report)**, wprowadź czas rozpoczęcia generowania raportu przez system.

4 – Określ **Parametry terminarza (Scheduling parameters)**.

Notatka: te ustawienia są ignorowane, jeśli raport jest zamówiony zdalnie przez użytkownika.

- **Rozpocznij na określony czas (Start this many days back):** raport zacznie zbierać zdarzenia przez liczbę dni określoną w polu rozpoczynając od bieżącej daty.
- **Rozpocznij o (Start at this time):** po określeniu ilości dni, określ czas rozpoczęcia (np. 07:00).
- **Zakończ po tylu dniach (Stop this many days back):** raport uwzględni liczbę dni wpisaną w to pole, w oparciu o aktualną datę.



EntraPass - Instrukcja instalacji i obsługi programu Raporty

- **Zakończ o (Stop at this time):** po określenie ilości dni, określ czas zakończenia (np. 17:00), czyli tym samym dzień i czas, kiedy system przestanie zbierać dane.

Notatka: czas rozpoczęcia oraz zakończenia są określane tylko dla pierwszego i ostatniego dnia. Na przykład, jeśli zaczynasz zbierać zdarzenia w poniedziałek o 8:00, a kończysz w piątek o 17:00, wszystkie zdarzenia pomiędzy poniedziałkiem 8:00, a piątkiem 17:00 zostaną włączone.

Określanie dodatkowych opcji dla automatycznych raportów (Specifying Additional Options for an Automatic Report)

1 – Kliknij przycisk , aby dodać więcej ustawień do raportu automatycznego terminarza. Po kliknięciu tego przycisku pojawi się nowe okno.

2 – Z listy **Typ wyjścia bazy danych (Database output type)** wybierz format pliku wyjściowego (Sybase, DBase IV, CSV, PDF, Excel, RTF albo Text).

3 – Z listy Proces wyjścia bazy danych (**Database output proces**), wybierz szablon, który zostanie wykorzystany przy tworzeniu raportu.

Notatka: sprawdź poniższą tabelę, aby uzyskać szczegółowe informacje na temat rodzaju wyjścia (output) oraz procesów wyjścia (output). Pokazuje ona porównanie różnych formatów raportów.

Baza danych	Opis
SyBase	Baza danych EntraPass.
Dbase IV	Popularny format systemu zarządzania bazą danych, który jest wspierany przez większość systemów zarządzania bazami danych. Nawet systemy, które nie korzystają z formatu DBase są w stanie importować/eksportować dane w tym formacie. Wyjściowy format plików: .db oraz .rdf.
CSV	Zachowa raport w formacie CSV (Comma separated values). Format danych, w którym każdy fragment danych oddzielony jest przecinkiem. Ten format jest popularny w przypadkach przenoszenia danych z jednej aplikacji do drugiej, ponieważ większość systemów baz danych jest w stanie importować/eksportować dane w tym formacie.
Excel	Pliki Microsoft Excel
PDF	Portable Document Format (PDF) to otwarty standard wymiany dokumentów. Może być otwarty przy pomocy darmowej aplikacji Adobe Reader.
RTF	Format służący do między-platformowej wymiany informacji między procesorami tekstów. Większość procesorów tekstu jest w stanie odczytać i zapisać w jakiejś formie format RTF.
Tekst	Plik tekstowy, którego struktura składa się z sekwencji wierszy. Może być otwarty przy pomocy większości narzędzi do obróbki tekstu.

4 – Możesz wybrać opcję **Automatycznego nazewnictwa pliku (...)** (**Automatic file name (...)**). Domyślnie: YYYY_MM_DD-HH_MM_SS.X, czyli rok_miesiąc_dzień-godzina_minuta_sekunda.roszerzenie.

5 – Wybierz język raportu oraz miejsce docelowe.

6 – Wybierz miejsce docelowe.



Definiowanie szablonów raportów RCP (In/Out Reports Definition)

Ta opcja umożliwia definiowanie raportów czasu pracy na żądanie, z automatycznymi parametrami wykonania.

Notatka: raporty mogą być definiowane z automatycznymi ustawieniami, aby mogły być generowane w miarę potrzeb; albo mogą być zamawiane w sposób zdalny przez użytkownika przy pomocy odpowiedniego przycisku. Przy zamówieniu zdalnym, automatyczne ustawienia są ignorowane

Definiowanie szablonów raportów RCP (Defining In/Out Reports)

1 – Na pasku narzędzi Raport, kliknij przycisk Raport Wej./wyj.

2 – Jeżeli wybrałeś opcję **Drzwi**, wyłącznie drzwi określone, jako **Drzwi wej./wyj.** (menu **Definiowanie drzwi**) są wyświetlone. Zaznacz **Zobacz usunięte drzwi (View deleted doors)**, aby dodać do listy drzwi wcześniej usunięte. Jeżeli wybrałeś opcję **Grupa drzwi (Door group)**, opcja **Zobacz usunięte drzwi (View deleted doors)** nie jest dostępna. System wyświetli grupy drzwi w twoim systemie.

3 – Zaznacz opcję **Nadpisz istniejący plik wyjściowy (Overwrite existing output file)**. Jeżeli tego nie zrobisz system utworzy nowy plik wyjściowy.

4 – Zaznacz **Wyświetl godziny i minuty (Display Hours and Minutes)**, aby dodać je do raportu.

5 – Wybierz zakładkę Karta, aby dodać inne filtry do raportu.

Ogólne | Events selection | Elementy | **Karty** | Terminarz

☐ Wszystkie karty
☐ Użyj typu karty jako filtru

Numer karty: Wkluczenie

Indeks filtru	Typ filtru
Nazwisko użytkownika	Brak
Nazwisko użytkownika	Brak
Card Information 2	Brak
Card Information 3	Brak

Notatka: zakładka Rodzaj karty pojawia się, kiedy pole Wybierz typ karty jest zaznaczone.

6 – Wybierz **indeks filtra**, po czym wybierz jego **tryb** (Brak, Zawiera, Wyklucza). Następnie wprowadź zakres wartości w odpowiednich polach. Aby uwzględnić wszystkie pola, nastaw typ filtra na: Brak. Na przykład, jeżeli wybrałeś indeks filtra „Numer karty”, nastaw tryb filtra na: Brak; dzięki temu wszystkie zdarzenia wywołane przez karty zostaną uwzględnione w raporcie.

7 – Aby dodać informacje do kryteriów sortowania, wybierz odpowiednią pozycję z listy **Dodatkowe informacje (Additional information)**.

Notatka: powtórz te kroki dla wszystkich pól informacyjnych karty, które są wylistowane w polu indeks filtrów. Możesz wykorzystać nazwę użytkownika karty i określić górną/dolną wartość graniczną od A do F, aby system uwzględnił tylko te zdarzenia, w których pojawił się określony numer karty, ale tylko dla użytkowników, których nazwa zaczyna się określonej wartości.

8 – Wybierz zakładkę Karta, jeżeli jest dostępna. Następnie określ typy kart, które będą uwzględnione w raporcie. Ta zakładka pojawia się, jeżeli zaznaczyłeś opcję **Użyj filtra typu wiadomości (Use card type filter)**.



9 – Wybierz zakładkę **Terminarz automatycznych raportów (Automatic report schedule)**, aby określić informacje dla automatycznych raportów. Zobacz: **Definiowanie terminarzy automatycznych raportów (Defining Automatic Report Schedules)**.

10 – Wybierz zakładkę **Zasady (Rules)**, aby określić zasady Wej./wyj. w **raportach czasu pracy (employee time reports)**. Zasady mogą zostać stworzone, aby określić przedziały czasu, jako konkretne wartości. Na przykład, wszystkie wejścia pracowników pomiędzy 07.50, a 08.15, mogą zostać zaraportowane, jako wejścia o 08.00.

- Zaznacz opcje **Zachowaj tylko pierwsze Wejście linii dozorowej (Pierwsze Wej.) oraz ostatnie wyjście (Ostatnie Wyj.) (Keep only the first entry (first IN) and the last exit (last OUT))**, aby otrzymać zakres czasu pomiędzy pierwszym odczytaniem karty na czytniku wejścia, i ostatnim odczytaniem tej karty na czytniku wyjścia.



Generowanie raportów RCP (In/Out Reports Request)

Opcja **Generowanie raportów RCP (Request In/Out reports)** jest wykorzystane, aby otrzymać zdefiniowany wcześniej raport Wej./wyj., który został stworzony przy wykorzystaniu menu **Definiowanie szablonów raportów RCP (In/Out Report Definition)**. Ta opcja jest przydatne, kiedy chcesz obejść ustawienia automatyczne.

Notatka: jeśli raport zawiera automatyczne ustawienia, zostaną one zignorowane.

Zdalne żądanie raportu czasu pracy (Requesting a In/Out Report Manually)

- 1 – Na pasku narzędzi Raport, kliknij przycisk Raporty czasu pracy. Pojawi się nowe okno.
- 2 – Z panelu Lista raportów (Report list), wybierz raport, który chcesz uruchomić.
- 3 – Określ Datę i czas, oraz parametry wyjścia.
- 4 - Zdefiniuj poziom priorytetu – od 1 do 99, gdzie 1 jest procesowany przed 99.
- 5 – Kliknij Wykonaj (Execute).

Notatka: dla Wyjścia (outout) Sybase system wyświetla okno podglądu raportu. Aby otrzymać raport w innym formacie będziesz go musiał wydobyć zdalnie, ponieważ nie jest ani drukowany, ani wyświetlany. Aby zobaczyć wszystkie raporty, które zostały wygenerowane użyj przycisku Archiwum na pasku narzędzi Raportów. Zobacz Definiowanie formatu raportów (Defining a Report Output Format), aby dowiedzieć się więcej.



Korekty raportów RCP (Operations on In/Out)

Użyj opcji **Korekty raportów RCP (Operation on In/Out)**, aby zdalnie wprowadzić, dodać lub usunąć transakcje wej./wyj. do bazy danych. Ta opcja może być przydatna dla organizacji, które wykorzystują opcje wej./wyj. przy systemie wynagrodzeń.

Dodawanie transakcji do bazy danych wej./wyj. (Adding a Transaction in the In/Out Database)

1 – Na pasku narzędzi Raport, kliknij przycisk **Dostosowanie Wej./wyj. (In/Out Adjustment)**.

2 – Wprowadź numer Karty, dla której chcesz zmodyfikować transakcje wej./wyj., następnie kliknij przycisk **Wczytaj (Load)**. Jeżeli nie znasz numeru, możesz użyć przycisku **Znajdź**.

Notatka: pole numer karty jest wymagane do rozpoczęcia wczytywania.

3 – Wybierz opcję **Podgląd usuniętych transakcji (View deleted transactions)**, jeżeli chcesz sprawdzić transakcje, które zostały niedawno usunięte. Usunięte transakcje są oznaczone X w kolumnie **Usunięte**.

4 – Wybierz opcję **Znajdź usunięte karty (Find deleted cards)**, jeżeli chcesz odnaleźć usuniętą kartę. Nie odnosi się do wpisów, które zostały wprowadzone ręcznie.

5 – Określ datę początkową, czyli dzień, w którym system zacznie zbierać informacje o zdarzeniach, poprzez kliknięcie na przycisk Kalendarz oraz wybranie odpowiedniej daty. Tylko zdarzenia, które miały miejsce w dniu określonym przez datę początkową, oraz później, będą wyświetlone.

Notatka: pole Data rozpoczęcia jest wymagane do rozpoczęcia wczytywania.

6 – Określ datę końcową, czyli dzień, w którym system przestanie zbierać informacje o zdarzeniach. Tylko zdarzenia, które miały miejsce w dniu określonym przez datę końcową, oraz wcześniej, będą wyświetlone. Jeżeli nie określisz daty końcowej, system uwzględni wszystkie dane aż do obecnej daty.

7 – Z listy Połączenie, wybierz odpowiednie połączenie, żeby wyświetlić drzwi wej./wyj.

Notatka: bramka jest wymagana do rozpoczęcia wczytywania.

8 – Możesz zaznaczyć opcję Wszystkie drzwi (All Doors). Zostaną zaznaczone wszystkie drzwi znajdujące się pod polem. Możesz również wybrać konkretne drzwi. Wszystkie zdarzenie wej./wyj., które zostały wygenerowane dla wybranych drzwi zostaną wyświetlone.

9 – Zaznacz opcję **Zobacz usunięte drzwi (View deleted doors)**, dzięki czemu drzwi, które nie są już określone, jako **Drzwi wej./wyj.** (ale były, jako takie określone w przeszłości) zostaną wyświetlone.

Notatka: drzwi są wymagane do rozpoczęcia wczytywania.

10 – Wprowadź niezbędne informacje w tabeli transakcji. Tabela transakcji pokazuje transakcje wybranego posiadacza karty:



EntraPass - Instrukcja instalacji i obsługi programu Raporty

- Kolumna usunięte pokazuje transakcje, które zostały usunięte. Są zidentyfikowane przez X.
- Kolumna data wskazuje datę, kiedy transakcja miała miejsce.
- Kolumna Czas wskazuje czas, kiedy posiadacz karty wszedł/opuścił strefę.
- Kolumna Transakcja wskazuje typ transakcji. Dla każdej transakcji wejścia, powinna być transakcja wyjścia.
 - o Wejście – wskazuje, że jest to transakcja wejścia wygenerowana w momencie, kiedy posiadacz karty użył karty przy drzwiach zdefiniowanych, jako wejściowe.
 - o Wyjście – wskazuje, że jest to transakcja wyjścia wygenerowana w momencie, kiedy posiadacz karty użył karty przy drzwiach zdefiniowanych, jako wyjściowe.
 - o Zdalne wejście – wskazuje, że jest to transakcja wejścia, która została zdalnie wprowadzona lub dodana w systemie. Kiedy zdalnie wprowadzisz transakcję, musisz określić czy jest to transakcja wejścia, czy wyjścia. Dla każdej transakcji wejścia, musi być transakcja wyjścia.
 - o Zdalne wyjście – wskazuje, że jest to transakcja wyjścia, która została zdalnie wprowadzona lub dodana w systemie. Kiedy zdalnie wprowadzisz transakcję, musisz określić czy jest to transakcja wejścia, czy wyjścia. Dla każdej transakcji wejścia, musi być transakcja wyjścia.
- Kolumna drzwi wskazuje, które drzwi zostały użyte przez użytkownika. Kiedy zdalnie wprowadzisz transakcję, musisz określić drzwi według typu transakcji: wejścia, czy wyjścia.

Notatka: jeśli wprowadzasz operacje wejścia wyłącznie drzwi określone, jako „drzwi wejściowe” zostaną wyświetlone na liście. Analogicznie, jeśli wprowadzasz operacje wyjścia wyłącznie drzwi określone, jako „drzwi wyjściowe” zostaną wyświetlone na liście.

11 – Kliknij przycisk **Wczytaj (Load)**, aby wczytać transakcje z serwera dla wybranego posiadacza karty. Musisz wprowadzić numer karty, wybrać bramkę/połączenie oraz drzwi, a następnie kliknąć przycisk **Wczytaj (Load)**. Przycisk zostaje wyłączony po wczytaniu transakcji.

12 – Kliknij przycisk **Dodaj**, aby dodać transakcje do istniejącej listy transakcji. Nowa transakcja zostanie dodana na końcu listy.

13 – Użyj przycisku **Wstaw**, aby wstawić transakcję pomiędzy istniejące transakcje, albo powyżej dowolnej transakcji.

14 – Kliknij przycisk **Anuluj**, aby anulować dowolne wstawienie albo modyfikacje PRZED zapisaniem.

Notatka: jeśli usuwasz operację, która została wprowadzona zdalnie, zostaje ona permanentnie usunięta z listy w przeciwieństwie do operacji wygenerowanych przez kontroler. Te po usunięciu są oznaczone X w kolumnie Usunięte.



Podgląd raportów RCP (Previewing In/Out Reports)

1 – W oknie Archiwum (Archive), wybierz raport, który chcesz obejrzeć. Jeżeli raport został określony jako „Wyświetl raport czasu pracy” (“Display In/Out Report”) oraz format wyjścia został zdefiniowany, jako „Baza danych Sybase” („Sybase Database”), pojawi się następujące okno.

2 – Wybierz opcje wyświetlania:

- **Grupuj przez (Group by):** wybierz tę opcję w celu ułatwienia zarządzania. Dane mogą grupowane przez nazwy posiadaczy karty albo przez numery kart.
- **Sortuj przez (Sort by):** możesz wybrać porządek sortowania: przez nazwy użytkowników albo przez numery kart.
- **Typ raportu (Report type):** wybierz tę opcję w celu ułatwienia zarządzania.

3 – Kliknij **Podgląd**, aby wyświetlić raport. Z nowego okna możesz albo zapisać raport (format .QRP), albo go wydrukować.



Podgląd raportów (Previewing Reports)

1 – W oknie **Archiwum (Archive)**, z prawego panelu wybierz raport, który chcesz obejrzeć. Jeżeli wybrałeś raport wygenerowany w Sybase, okno Opcje Raportu pozwala ci dostosować raport przed wydrukiem.

Notatka: jeśli wybierzesz CSV, jako typ raportu, zostanie on wygenerowany w oknie WordPad w formacie tekstowym.

2 – Określ opcje filtrów. Wprowadź tekst w polu Wyszukaj opis (Search description). Raporty zostaną posortowane w taki sposób, że pozostawione zostaną tylko te, które zawierają wprowadzony tekst. Możesz dodatkowo sprecyzować filtr:

- **Zawiera (Contains):** wszystkie zdarzenia, które zawierają określony tekst zostaną uwzględnione w raporcie.
- **Zaczyna się od (Starts with):** wszystkie zdarzenia, które zaczynają się od określonego tekstu zostaną uwzględnione w raporcie.
- **Kończy się na (Ends with):** wszystkie zdarzenia, które kończą się na określony tekst zostaną uwzględnione w raporcie.
- **Zawiera dokładnie (Exact words):** wszystkie zdarzenia, które zawierają dokładnie określony tekst zostaną uwzględnione w raporcie.

3 – Kliknij przycisk **Podgląd**, wybierz **drukarke** z listy i kliknij **OK**. System wyświetli wyniki raportu. Z nowego okna możesz:

- Wyszukać tekst w raporcie.
- Wydrukować raport
- Zachować raport (PDF, RTF, HTML oraz TXT)
- Wczytać raport (.QRP)

4 – Kliknij Właściwości (Properties), aby uzyskać dostęp do okna Szczegóły raportu (Reports details), gdzie wyświetlone są informacje:

- **Nazwa pliku raportu (Report file name):** wyświetla adres zapisania pliku oraz jego nazwę.
- **Tytuł raportu (Report title):** wyświetla tytuł raportu.
- **Data rozpoczęcia (Start date):** raporty są tworzone dla określonego przedziału czasu. Ta opcja określa datę początkową tego przedziału.
- **Data zakończenia (End date):** raporty są tworzone dla określonego przedziału czasu. Ta opcja określa datę zakończenia tego przedziału.
- **Zamówiony (Requested):** wyświetla datę i czas zamówienia raportu.
- **Dostarczony (Delivered):** wyświetla datę i czas, kiedy raport był wyprodukowany i wydrukowany.
- **Zamówiony przez (Requested by):** wyświetla nazwę użytkownika, który zamówił raport.
- **Zliczanie (Count):** wyświetla liczbę transakcji w raporcie.
- **Procesowanie wyjścia (Output process):** wyświetla liczbę możliwych/dostępnych szablonów w raporcie.



Szybki raport (Quick Report Definition)

Opcja **Szybki raport (Quick report)** oferuje szybką metodę tworzenia raportów dla określonych typów zdarzeń. Na przykład, możliwe jest stworzenie raportu dotyczącego wszystkich normalnych albo nieprawidłowych zdarzeń dostępu w kilka sekund. Plik **Szybkich raportów** mogą być przeglądane dzięki **EntraPass Quick Viewer**, narzędziu które pozwala użytkownikom na wyświetlanie plików Szybkich raportów oraz wszystkich plików .QRP. Quick Viewer jest uruchamiany z menu Start Windows.

Definiowanie Szybkich raportów (Defining a Quick Report)

1 – Na pasku narzędzi **Raport**, kliknij **Zgłoszenie szybkiego raportu (Quick report request)**.

2 – Z listy **Zdarzenie**, wybierz typ zdarzenia dla raportu (dostęp, kontroler, drzwi, przekaźnik, etc.). Jeżeli wybrałeś „zdarzenia dostępu”, zakładka Karta zostanie wyświetlona w oknie.

3 – Spośród opcji Typ zdarzenia, wybierz typ zdarzenia, który należy uwzględnić w raporcie.

- **Normalny (Normal): Szybki raport** może tworzyć raporty w oparciu o normalne zdarzenia. W raportach dostępu, normalne zdarzenia to np. przyznanie dostępu.
- **Nieprawidłowy (Abnormal):** takie zdarzenia, jak np. Dostęp zabroniony (zły poziom dostępu), nieprawidłowe odłączenia serwera, błąd komunikacji bramki, wszystkie zdarzenia powiązane z niezakończeniem procesu; są traktowane, jako nieprawidłowe.
- **Normalny i nieprawidłowy (Normal & abnormal):** zaznacz, aby w raporcie uwzględniać zarówno zdarzenia normalne, jak i nieprawidłowe.
- **Niestandardowe zdarzenie (Custom events):** zaznacz, aby uwzględniać własne zdarzenia. Zakładka **Niestandardowe (Custom)** pojawia się, gdy **Niestandardowe zdarzenia (Custom events)** są wybrane. Ta opcja pozwala użytkownikowi na wybranie tych komponentów, które wygenerowały wybrane zdarzenia według ustawień w polu „zdarzenia”.

Notatka: kiedy korzystasz z pola Zdarzenie musisz określić, które komponenty będą/nie będą wykorzystane. Po wybraniu zdarzenia, system wyświetli wszystkie drzwi bramki. Jeśli wybierzesz kontroler, system wyświetli wszystkie kontrolery dla bramki. Po wybraniu zdarzenia wybierz kontrolery, które będą włączone do raportu.

4 - Wybierz zakładkę Karta, aby określić szczegóły filtru raportu. Zakładka Karta pojawia się tylko wtedy, gdy zdarzenie powiązane z kartą jest wybrane.

5 – Z listy Indeks karty (Card index), określ informacje, które będą wykorzystane, jako filtr. Na przykład, jeżeli wybrałeś „numer karty”, tylko zdarzenia dostępu, w których pojawia się zdefiniowany numer karty, zostaną wybrane.

6 – W zakładce **Nazwa raportu (Report name)**, wprowadź nazwę raportu (ta nazwa zostanie wyświetlona na raporcie).

Notatka: jeśli wybierzesz Numer karty, pola Wartości graniczne wyświetlają domyślne wartości, które można zastąpić numerem karty. Są one w tym momencie edytowalne i możesz wprowadzić do nich tekst. Na przykład, możesz określić dolną wartość, jako A oraz górną, jako F. System uwzględni te zdarzenia, w których określone są wybrane drzwi oraz wykorzystane są karty, których nazwa zawiera się w przedziale A-F. Jeśli zaznaczysz Wszystkie, edytowalne pola są wyłączone.

7 – W zakładce **Data rozpoczęcia/zakończenia**, wprowadź datę i czas, po których system zacznie zbierać zdarzenia. Na przykład, jeżeli wprowadzisz 7:00, a zdarzenie będzie miało miejsce o 6:00, nie zostanie ono uwzględnione. Aby wybrać zdarzenia, które zaszyły w określonym przedziale czasu, użyj zakładki **Przedział czasu (Time period)**.



EntraPass - Instrukcja instalacji i obsługi programu Raporty

8 – W zakładce **Przedział czasu (Time period)**, zaznacz opcję **Konkretny przedział czasu (Specific time frame)**, aby uwzględnić zdarzenia pasujące do określonego przedziału czasu. Wprowadź określony czas do raportu.

9 – Jeżeli chcesz nadpisać ostatni plik, wybierz zakładkę **Różne (Miscellaneous)** i zaznacz **Nadpisz istniejący plik wyjściowy (Overwrite existing output file)**. Jeżeli to zrobisz, obecnie domyślny plik wyjściowy zostanie zastąpiony przez nowy.

10 - Zdefiniuj poziom priorytetu – od 1 do 99, gdzie 1 jest procesowany przed 99.

11 – Określ parametry wyjścia:

- **Typ wyjścia bazy danych (Database output type)** wybierz format pliku wyjściowego (Sybase, DBase IV, CSV, PDF, Excel, RTF albo Text).

- **Katalog:** pokazuje lokalizację, w której raport został zapisany i jest przechowywany. Domyślnie: C:\ProgramFiles\Kantech\Sever_CE\Report\your file.xx.

- **Nazwa pliku wyjściowego (Output file name):** wskazuje nazwę pliku wyjściowego. Domyślnie, raporty są zapisywane w C:\ProgramFiles\Kantech\Sever__CE\Report\your file.xx. Nazwa pliku raportu składa się z daty i czasu, w którym raport został utworzony. Możesz dowolnie zmieniać nazwę pliku, ale nie zmieniaj rozszerzenia.

- **Proces wyjścia bazy danych (Database output process):** wybierz odpowiedni proces wyjścia. Szablon raportu jest powiązany z każdym wyjściem.

- o Tylko w bazie danych: raport zostanie zapisany w bazie danych systemu.

- o Wyświetl raport: raport zostanie wyświetlony na ekranie.

- o Wydrukuj raport według (sekwencji, daty i czasu, zdarzenie: raport zostanie wydrukowany według określonej kolejności.

- o Wyślij raport emailem: raport zostanie wysłany emailem do określonej grupy odbiorców/adresów email.

- **Wyślij do stacji roboczej:** wybierz stację roboczą, do której szybko raport. Lista uwzględnia wszystkie stacje robocze, na których została zainstalowana aplikacja SmartLink. Jeżeli SmartLink jest zainstalowany na, na przykład, dwóch stacjach roboczych podłączonych do sieci, możesz wygenerować raport na jednej stacji roboczej i wysłać wyniki do drugiej, wybierając SmartLink, który koresponduje ze stacją roboczą, na której chcesz wyświetlić raport.

12 – Kliknij **Wykonaj**, aby uruchomić raport.

13 – Kliknij **Podgląd**, aby sprawdzić raport.



Historia generowania raportów (Report Log)

Okno **Historii generowania raportów (Report Log)** pozwala na podgląd szczegółowej listy całej historii raportów przeprosesowanych przez system.

1 – Aby zobaczyć wszystkie Logi raportów, wybierz przycisk **Historia generowania raportów (Report log)** z menu **Raport (Report)**.

2 – Kliknij na **Filtr tekstu (Text filter)**, aby wyświetlić okno Filtra tekstu. Wprowadź ciąg tekstu (np. Kantech), a system wyświetli tylko logi zawierające określony tekst.

3 – Kliknij przycisk **Odśwież**, aby zaktualizować wyświetlane dane.

4 - Kolumny:

- **Data zgłoszenia:** ustawione sekwencyjnie, wprowadzenie innej metody przerywa sekwencyjność.
- **Zgłoszone przez:** po wybraniu, kolumny będą sortowane według kolumny **Zgłoszone przez (Requested by)** w porządku alfabetycznym.
- **Nazwa raportu:** po wybraniu, kolumny będą sortowane według kolumny **Nazwa raportu (Report name)** w porządku alfabetycznym.
- **Data od:** po wybraniu, kolumny będą sortowane według kolumny **Data od (Date from)** w porządku alfabetycznym.
- **Data do:** po wybraniu, kolumny będą sortowane według kolumny **Data do (To Date)** w porządku alfabetycznym.

5 – Aby usunąć wszystko z okna, wybierz **Usuń wszystko (Delete all)** (menu pojawi się po kliknięciu prawym w oknie)

6 - Pola:

- **Typ raportu (Report Type):** pokazuje typ raportu.
- **Procesowane przez (Process By):** pokazuje, która aplikacja wykonała raport.
- **Stacja robocza dodana (Workspace applied):** pokazuje, czy stacja robocza została dodana.
- **Przeznaczenie (Destination):** pokazuje, gdzie raport został dostarczony.
- **Wykorzystany szablon (Used Template):** pokazuje wszystkie dll wykorzystane przy raporcie.
- **Tematy w raporcie (Items in report):** ilość tematów w raporcie.
- **Data zgłoszenia (Requested date):** data i czas zgłoszenia potrzeby raportu.
- **Data kolejki (Queued date):** pokazuje, kiedy raport został dodany do kolejki generowania raportów (data, czas i czas oczekiwania).
- **Data procesowania (Process date):** pokazuje, kiedy proces został rozpoczęty.
- **Data dostarczenia (Delivery date):** pokazuje, kiedy raport został dostarczony.
- **Data zakończenia (Completion date):** pokazuje datę końcową i czas wykonania raportu.
- **Stan zakończenia (Completion State):** pokazuje, czy raport został ukończony z sukcesem, czy nie.



Stan generowania raportu (Report State)

Użyj opcji Stan raportu, aby wyświetlić listę oraz statusy wszystkich raportów, które nadal są „oczekujące”. Z paska narzędzi **Raport**, kliknij **Stan generowania raportu**.

Pola stanu raportu (Report state fields):

- **Priorytet (Priority)**: priorytet obsługi wiadomości (1 do 99). Priorytet 1 będzie przeprocesowany przed priorytetem 99.
- **CPU**: użycie CPU na raport (Niskie, Normalne, Wysokie).
- **Raport (Report)**: nazwa raportu.
- **Przeznaczenie (Destination)**: wyświetla nazwę stacji roboczej albo SmartLink, do których raport zostanie wysłany.
- **Postęp (Progress)**: kiedy raport jest procesowany, wyświetla datę od początku do końca.
- **Zliczenie (Count)**: wskazuje liczbę wpisów w raporcie.

Wybierz raport, po czym kliknij na niego prawym przyciskiem, aby wyświetlić menu:

- **Następny do procesowania (Next to be processed)**: wskazuje, że ten raport ma zostać przeprocesowany, jako następny.
- **Promuj (Promote)**: zwiększa priorytet raportu.
- **CPU**: pozwala zmienić użycie CPU na raport.
- **Pomoc (Help)**: kliknij, aby zobaczyć pokrewne tematy.

Menu kontekstowe dla procesowanych raportów (Contextual menu for in process reports):

Wybierz raport, po czym kliknij na niego prawym przyciskiem, aby wyświetlić menu:

- **Przerwij z danymi (Abort with data)**: ta funkcja przerywa proces, a zebrane informacje są wysłane do odbiorcy.
- **Przerwij bez danych (Abort without data)**: ta funkcja przerywa proces, a zebrane informacje są usunięte.
- **Priorytet (Priority)**: pozwala zmienić użycie CPU na raport.
- **Pomoc (Help)**: kliknij, aby zobaczyć pokrewne tematy.

Notatka: czerwona kropka oznacza oczekujący raport czasu pracy. Zielona, że raport jest przygotowywany.



Podgląd raportów zdarzeń (Requesting Reports)

Przy pomocy tej opcji użytkownicy mogą zażądać zdefiniowanego wcześniej Raportu historycznego (Historical report) albo Raportów wykorzystania karty (Card use reports), które zostały utworzone przy pomocy menu Raport na żądanie (Custom report). Użytkownicy mogą przesłać emailen ten raport to jednego, lub wielu odbiorców.

Notatka: jeśli twój raport zawiera automatyczne ustawienia, zostaną one zignorowane. Musisz wprowadzić nowe ustawienia.

1 – Na pasku narzędzi Raportu, kliknij przycisk Żądanie raportu (Report Request). Zostanie wyświetlone okno Żądania raportu.

2 – Z jednej z list wybierz raport, który chcesz uruchomić.

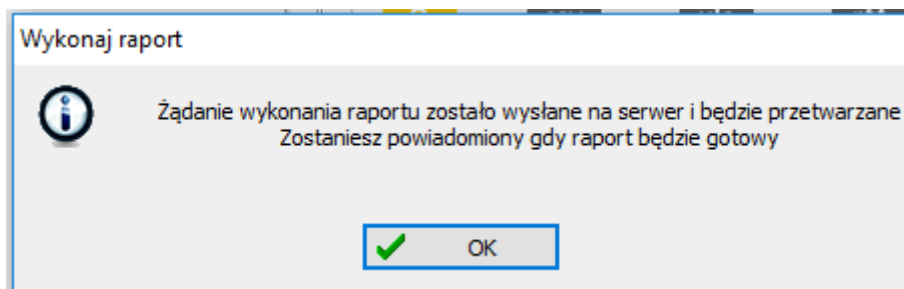
3 – Zdefiniuj poziom priorytetu – od 1 do 99, gdzie 1 jest procesowany przed 99.

4 – Możesz zdefiniować parametry, włączając formaty pliku wyjściowego (Sybase, DBase IV, CSV, PDF, Excel, RTF albo Text), folder docelowy, nazwę pliku, etc.

Notatka: z listy możesz wybrać Wyślij raport – umożliwia to wysłanie raportu emailen automatycznie do określonego odbiorcy. EntraPass umożliwia zabezpieczenie raportu hasłem przed wysłaniem.

Notatka: jeśli wybrany jest Raport wykorzystania karty, sekcja Data i czas jest wyłączona.

5 – Kliknij Wykonaj (Execute). Wiadomość systemowa poinformuje o tym, że raport jest procesowany.



6 – Wybierz Pogląd (Preview), aby zdefiniować raport i opcje filtrowania. Ułatwi to odczytywanie raportu, poprzez dodanie kolorystyki, obramowania zdarzeń, etc.; albo poprzez sortowanie zdarzeń w raporcie (po numerze ID, alfabetycznie, etc.).

7 – Wprowadź opis. Raport jest aktualizowany w czasie rzeczywistym, gdy wprowadzisz opcję filtra.

8 – Przy pomocy przycisku **Podgląd** możesz sprawdzić raport, a przy pomocy przycisku **Właściwości** – szczegóły raportu.



EntraPass - Instrukcja instalacji i obsługi programu Raporty



Raport śledzący (Roll Call Reports)

Raport śledzący jest wykorzystywany do zrobienia zdjęcia osób, które wykorzystały kartę na określonym czytniku lub grupie czytników w określonym przedziale czasu – resetu. Przy pomocy śledzenia (Roll call), jedno albo wiele drzwi w EntraPass może zostać skonfigurowane, jako punkty wejścia. W oparciu o dane o ostatniej lokacji, przez którą przeszedł posiadacz karty, użytkownik otrzyma raport podsumowujący, kto wszedł na obiekt.

Raport śledzący jest obsługiwany przez serwer EntraPass. Aby działał prawidłowo, serwer i bramka muszą być uruchomione.

Funkcje:

- Do 8 raportów ewakuacyjnych może zostać skonfigurowane przez EntraPass.
- Drzwi muszą być przypisane do numeru raportu (1-8), aby być brane pod uwagę pod kątem raportów śledzących (Zobacz: **Konfiguracja drzwi (Doors Configuration)**).
- Raport śledzący wylistuje wszystkich posiadaczy kart, którzy wykorzystali kartę przy zdefiniowanym czytniku. W raporcie uwzględnieni będą tylko ci użytkownicy, którzy weszli na obiekt po ostatnim resetie obiektu.
- Aby stworzyć funkcjonalność „wejście-wyjście” („in-out”), użytkownik musi upewnić się, że drzwi oznaczone jako wyjściowe (dla budynku lub połączenia) mają różne numery apelu.

Generowanie raportu śledzącego (Roll Call Report generation)

1 – Na pasku narzędzi Raport, kliknij przycisk Raport śledzący.

2 – Wybierz sektor.

3 – Określ miejsca docelowe raportu:

- **Miejsce docelowe raportu:** przy pomocy przycisku trzech kropek wybierz miejsce docelowe.
- **Drukarka:** wybierz drukarkę z listy.
- **Adresat email:** wprowadź nazwę odbiorcy raportu.

Przykład raportu śledzącego (Example of a Roll Call Report)

TRACKING AND MUSTER VIEW REPORT				
<u>Area Name</u>	<u>Card ID</u>	<u>Status</u>	<u>Card Holder</u>	<u>Reader</u>
<u>Time & Date</u>				
On Site	29	Valid Card, door used	Bloggs Fred	Front Door - IN
15:22:07 16/03/2005				
	26	Valid Card, door used	Davies David	Front Door - IN
15:22:05 16/03/2005				
	27	Valid Card, door used	Johnson Sam	Front Door - IN
15:22:03 16/03/2005				
	30	Valid Card, door used	Smith John	Front Door - IN
15:22:09 16/03/2005				
	28	Valid Card, door used	Wilson Jane	Front Door - IN
15:21:59 16/03/2005				



Specyfikacja specjalnych opcji dla automatycznego generowania raportów (Specifying Additional Options for an Automatic Report)

1 – Kliknij przycisk , aby dodać więcej ustawień do raportu automatycznego terminarza. Po kliknięciu tego przycisku pojawi się nowe okno.

2 – Z listy **Typ wyjścia bazy danych (Database output type)** wybierz format pliku wyjściowego (Sybase, DBase IV, CSV, PDF, Excel, RTF albo Text).

3 – Z listy Proces wyjścia bazy danych (**Database output proces**), wybierz szablon, który zostanie wykorzystany przy tworzeniu raportu.

Notatka: z listy możesz wybrać Wyślij raport – umożliwia to wysłanie raportu emailiem automatycznie do określonego odbiorcy. EntraPass umożliwia zabezpieczenie raportu hasłem przed wysłaniem.

Tabela pokazuje różnice pomiędzy formatami bazy danych, a ich wyjściowymi formatami plików:

Baza danych	Opis
SyBase	Baza danych EntraPass.
Dbase IV	Popularny format systemu zarządzania bazą danych, który jest wspierany przez większość systemów zarządzania bazami danych. Nawet systemy, które nie korzystają z formatu DBase są w stanie importować/eksportować dane w tym formacie. Wyjściowy format plików: .db oraz .rdf.
CSV	Zachowa raport w formacie CSV (Comma separated values). Format danych, w którym każdy fragment danych oddzielony jest przecinkiem. Ten format jest popularny w przypadkach przenoszenia danych z jednej aplikacji do drugiej, ponieważ większość systemów baz danych jest w stanie importować/eksportować dane w tym formacie.
Excel	Pliki Microsoft Excel
PDF	Portable Document Format (PDF) to otwarty standard wymiany dokumentów. Może być otwarty przy pomocy darmowej aplikacji Adobe Reader.
RTF	Format służący do między-platformowej wymiany informacji między procesorami tekstów. Większość procesorów tekstu jest w stanie odczytać i zapisać w jakiejś formie format RTF.
Tekst	Plik tekstowy, którego struktura składa się z sekwencji wierszy. Może być otwarty przy pomocy większości narzędzi do obróbki tekstu.

4 – Możesz wybrać opcję **Automatycznego nazewnictwa pliku (...)** (**Automatic file name (...)**). Domyślnie: YYYY_MM_DD-HH_MM_SS.X, czyli rok_miesiąc_dzień-godzina_minuta_sekunda.roszerzenie.

5 – Wybierz język raportu oraz przeznaczenie.



EntraPass - Instrukcja instalacji i obsługi programu Raporty



Opcje

Terminarz kopii systemu (Backup Scheduler)

Kopia zapasowa to kopia bazy danych systemu, która służy, jako zastępstwo albo alternatywa w przypadku awarii komputera. W przypadku awarii twojego komputera systemowego, możesz przywrócić kopię zapasową na inny komputer (na którym zainstalowana jest aplikacja EntraPass).

- Twórz kopię zapasową swoich plików regularnie, przynajmniej raz w tygodniu.
- Rekomendujemy utworzenie dwóch kopii zapasowych twoich plików bazy danych. Zapisz je w osobnych lokalizacjach.
- Aby utworzyć kopię zapasową, możesz wykorzystać:
 - o menu zakładki Serwer/Kopia zapasowa,
 - o **Terminarz kopii zapasowej (Backup Scheduler)**,
 - o Aplikację **Dublowania bazy danych (Mirror Databas)**,
 - o inne oprogramowanie lub podzespoły zewnętrzne (nie zalecamy oprogramowania zewnętrznego).

Notatka: domyślnie, kiedy zachowujesz albo odtwarzasz plik, Bazy danych serwera będą czasowo wyłączone (nie będą dostępne). Stacje robocze nie będą w stanie modyfikować baz danych.

Program **Terminarz kopii zapasowej (Backup Scheduler)** jest wykorzystany do automatycznego tworzenia kopii zapasowych twoich danych, archiwów, bazy danych wej./wyj. Określ ustawienia domyślne, a system sam zrobi resztę.

Konfigurowanie kopii zapasowej, kiedy serwer EntraPass działa jako usługa (Configuring the Backup when the EntraPass Server is Running as a Service)

Poniższe kroki są wymagane, kiedy serwer EntraPass działa, jako usługa i musisz utworzyć kopię zapasową do innego komputera **wewnątrz tej samej grupy roboczej albo domeny**.

Notatka: aby wykonać następujące czynności musisz posiadać pełne przywileje administratora. Jeżeli takowych nie posiadasz albo nie znasz Windows Administrative Tools, skontaktuj się ze swoim administratorem sieci.

- 1 – Z serwera EntraPass, idź to Opcje > Parametry systemu > Serwer > Informacje logowania usługi.
- 2 – Wypełnij wszystkie wymagane pola: nazwa domeny, login, hasło, potwierdzenie hasła.



EntraPass - Instrukcja instalacji i obsługi programu Opcje

Notatka: Nazwa domeny albo Grupa robocza musi być taka sama zarówno dla serwera EntraPass, jak i komputera zapasowego.

3 – Kliknij OK.

Ustawienie terminarza Automatycznego tworzenia kopii zapasowych systemowej bazy danych (Scheduling Automatic Backups of the System Database).

1 – Z paska narzędzi Opcje, wybierz **Terminarz kopii zapasowej (Backup Scheduler)**.

2 – Wybierz zakładkę korespondującą do informacji, które chcesz zabezpieczyć: Dane, Archiwum, Wej/Wyj albo Zdarzenia Wideo.

Notatka: domyślnie, każdej niedzieli o 4:00, system automatycznie wykona kopię zapasową wszystkich plików dla wszystkich nowych instalacji. Ustawienie godziny na 4:00 wiąże się z tym, że inne zadania nie będą miały wpływu na wykonanie zapisu.

3 – Wybierz opcję **Automatyczne tworzenie kopii zapasowej (Automatic backup option)**.

4 – Wybierz **folder Kopii zapasowej**:

- Domyślny folder: nazwa folderu jest generowana automatycznie według następującej zasady: X_YYYY_MM_DD_HH_MM_SS, gdzie X = dane albo archiwa albo wej/wyj (D, A, T), Y = rok, M = miesiąc, D = dzień, H = godzina, MM = minuty, S = sekundy.

Notatka: domyślnie, system zapisuje wszystkie informacje pochodzące z: C:\Program files\Kantech\Server\Data albo Archive albo Time on video albo V . Informacje są wysyłane do: C:\Program files\Kantech\Server\Backup\X_YYYY_MM_DD_HH_MM_SS .

- Konkretny folder: zachowa pliki w folderze według domyślnego nazewnictwa w folderze XXX.

5 – Wybierz typ kopii zapasowej: opcje zależą od rodzaju danych, które chcesz zapisać.

• Dane (Data):

- Osobne pliki: wykonana kopię zapasową bazy danych plik po pliku.
- Samorozpakowujący się skompresowany plik: utworzy plik wykonywalny (*.exe), który skompresuje informacje¹, aby zredukować ilość miejsca na dysku zajmowaną przez kopię zapasową.

• Archiwalne, Czasu pracy oraz Zdarzenia Wideo (Archive, In/Out and Video Event):



EntraPass - Instrukcja instalacji i obsługi programu Opcje

- o Osobne pliki (pełna kopia zapasowa): wykona kopię zapasową całej bazy danych.
- o Samorozpakowujący się skompresowany plik (pełna kopia zapasowa): utworzy plik wykonywalny (*.exe), który skompresuje informacje¹, aby zredukować ilość miejsca na dysku zajmowaną przez kopię zapasową.
- o Osobne pliki (przyrostowa kopia zapasowa): wykona kopię zapasową całej bazy danych. Tylko informacje zmodyfikowane od ostatniej kopii zapasowej zostaną zachowane.
- o Samorozpakowujący się skompresowany plik (przyrostowa kopia zapasowa): utworzy plik wykonywalny (*.exe), który skompresuje informacje¹, aby zredukować ilość miejsca na dysku zajmowaną przez kopię zapasową. Tylko informacje zmodyfikowane od ostatniej kopii zapasowej zostaną zachowane.

Notatka: przywracanie Samorozpakowującej się kopii zapasowej po aktualizacji EntraPass może być wykonane tylko z serwera, na którym została utworzona Samorozpakowująca się kopia zapasowa.

Notatka: jeśli wybierzesz Pełna kopia zapasowa, za każdym razem, kiedy kopia zapasowa zostanie utworzona, powstanie również nowy podfolder z danymi albo samorozpakowującym się plikiem. Jeśli korzystasz z przyrostowych kopii zapasowych zapisane zostaną tylko informacje, które zostały zmodyfikowane od ostatniego zapisu. Jeśli będziesz chciał przywrócić informacje, będziesz musiał przywracać wszystkie podfoldery, jeden po drugim.

6 – Wybierz częstotliwość tworzenia kopii zapasowej:

- Cotygodniowa: kopia zapasowa zostanie utworzona raz w tygodniu, co tydzień; określ dzień na wykonanie kopii zapasowej (np. każdy czwartek).
- Comiesięczna: kopia zapasowa zostanie utworzona raz w miesiącu, co miesiąc; określ dzień na wykonanie kopii zapasowej (np. każdy pierwszy dzień miesiąca)
- Codzienna: kopia zapasowa zostanie utworzona raz w miesiącu.

7 – Określ czas, o której zostanie wykonana kopia zapasowa (format 24 godzinny).

8 – Wybierz **Teraz (Now)**, jeżeli chcesz wykonać kopię zapasową natychmiast po zachowaniu parametrów.

Notatka: dla Mirror Database oraz Serwera Redundantnego opcja Konfiguruj automatyczne tworzenie kopii zapasowej jest niedostępna.

9 – Powtórz kroki od 1 do 8 dla wszystkich zakładek.

10 – Kliknij OK, aby zapisać.



Modyfikacja hasła do rejestracji aplikacji (Connection Password Modification)

Hasło połączenia jest wykorzystywane do autentyfikacji stacji roboczej EntraPass przy serwerze EntraPass. Okno hasła połączenia wyświetla się automatycznie, gdzie system nie został jeszcze zarejestrowany.



CAUTION:

Keep in mind that there is no way to reset the connection password if forgotten after its modification.

Notatka: jeśli w celach autentyfikacji nie korzystasz z hasła, użytkownik będzie musiał skorzystać z głównego, domyślnego hasła w celu autentyfikacji stacji roboczej. Domyślne hasło połączenia to kantech (zwróć uwagę na wielką/małą literę).

Zmianie hasła połączenia (Changing the Connection Password)

- 1 – Z głównego okna Opcji, wybierz przycisk **Hasło połączenia (Connection password)**.
- 2 – Wprowadź obecne hasło (wielkość liter ma znaczenie), w polu **Stare hasło (Old authentication password)**. Domyślne: kantech.
- 3 – Wprowadź nowe hasło autentyfikacji w polu **Nowe hasło (New authentication password)**.
- 4 – Potwierdź nowe hasło w polu **Potwierdź hasło (Verify authentication password)**.
- 5 – Kliknij OK. Jeżeli pojawi się wiadomość o błędzie, upewnij się, że dane, które wpisałeś w pola **Nowe hasło** i **Potwierdź hasło** zostały wprowadzone prawidłowo.

Notatka: hasło połączenia jest inne niż hasło użytkownika. Hasło połączenia jest wykorzystywane do autentyfikacji stacji roboczej, podczas, gdy hasło użytkownika jest wykorzystywane do otwarcia sesji.



Parametry definiowania kart (Credentials Parameters)

Karta (Card)

Dzięki zakładce Karta, Administrator Systemu będzie miał możliwość przeniesienia swojego systemu EntraPass do zaawansowanego zarządzania użytkownikami, gdzie użytkownicy są zarządzani poprzez swoje nazwy oraz numery kart. Każdy użytkownik karty będzie zarządzany poprzez nazwę użytkownika i przez 5 różnych numerów. Umożliwi to tworzenie kart, bez przypisywania nowym kartom numerów. Zobacz: **Wprowadzanie nowej karty w Zaawansowanym zarządzaniu (Issuing a New Card in Enhanced User Management Environment)**.

Notatka: ta opcja będzie wykorzystana razem z EntraPass Web w celach zarządzania kartami.

Notatka: umożliwienie przejścia do zaawansowanego zarządzania jest nieodwracalne przy wykorzystaniu oprogramowania. Jednakże, kiedy system przenosi dane, kopia zapasowa jest utworzona w EntraPass, aby mógł być przywrócony do poprzedniego działania.

- **Przenieś do zaawansowanego zarządzania (Migrate to enhanced user management):** domyślnie – zaznaczona. Zobacz: **Wprowadzanie nowej karty w Zaawansowanym zarządzaniu (Issuing a New Card in Enhanced User Management Environment)**.

Po zaznaczeniu i kliknięciu OK, ekran ostrzeżenia zostanie wyświetlony z informacją, że akcja jest nieodwracalna przed utworzeniem kopii zapasowej danych przez EntraPass.

Po zakończeniu procesu, zauważysz, że opcja została wyłączona w zakładce Karta.

Włącz wyjątki w poziomach dostępu (Enable access level exceptions): Kiedy zaznaczone, wyjątki mogą zostać dopuszczone do każdych drzwi. Przy aktywacji, użytkownik dostanie wiadomość z ostrzeżeniem, że proces przeładowywania kontrolera może zwolnić. Aby przypisać konkretny terminarz do drzwi, zobacz: **Wyjątki dostępu (Access Exception)**.



Zdarzenia definiowane przez klienta (Custom Messages)

Ta opcja pozwala użytkownikowi z odpowiednim poziomem dostępu na definiowanie **Zdarzenia definiowanych przez klienta**, które mogą wygenerować zdarzenie w oparciu o terminarz. Do 10 niestandardowych komunikatów może zostać zaprogramowanych do uruchomienia zdarzenia w określonym czasie. A każdy komunikat może zostać uruchomiony, kiedy terminarz stanie się ważny, nieważny, etc. Inaczej: możesz uruchomić do 20 zdarzeń, jeżeli weźmiesz pod uwagę początek/koniec przedziału terminarza. Każde zdarzenie będzie wyświetlone na **Liście wiadomości** na **Pulpicie**.

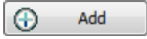
Ustawianie Zdarzeń definiowanych przez klienta (Setting up Custom Messages)

- 1 – Z paska narzędzi **Opcji**, kliknij **Zdarzenia definiowane przez klienta**.
- 2 – W pierwszej zakładce wprowadź pierwszą wiadomość, którą chcesz wyświetlić na Liście wiadomości. Dwa pola są dostępne dla głównego języka i drugiego.
- 3 – Wybierz zdefiniowany wcześniej terminarz, który określi, kiedy zdarzenie będzie uruchomione.
- 4 – Zaznacz czy chcesz, aby zdarzenie było uruchomione przy zmianie statusu terminarza.
- 5 – Przejdź do drugiej zakładki i wprowadź drugą wiadomość; kontynuuj według tego schematu.

Informacje dotyczące dystrybutora (Dealer Information)

Szczegóły pola Informacje (About Box Details)

Aby dodać informacje dotyczące dystrybutora w oknie **Informacje (About)**, wybierz **Wyświetl szczegóły w polu Informacji (Display details in About box)**

- 1 – Wypełnij informacje dotyczące dystrybutora i dodaj logo przy pomocy przycisku .
- 2 – Wypełnij dane Informacje o obiekcie (**Site information**)
- 3 – Kliknij OK, aby zakończyć.

Przypomnienie KAP (Kap Reminder)

Wiadomość z przypomnieniem pojawi się, aby poinformować użytkownika, że okres KAP dobiega końca. Przypomnienie może zostać przesłane jako: wiadomość pop-up (wyskakująca), albo email.

Wyskakujące wiadomości (Pop-up Message)

Wiadomość wyskakująca jest automatycznie generowana przez EntraPass, aby przypomnieć użytkownikowi o tym, że okres KAP dobiega końca:

- 60 dni przed końcem.
- 30 dni przed końcem.
- W dniu upływu terminu ważności.
- 30 dni po terminie ważności.

Wiadomość z przypomnieniem musi zostać potwierdzona przez użytkownika. Zostanie odnotowana w bazie danych zdarzeń oraz zostanie umieszczona w raportach.



EntraPass - Instrukcja instalacji i obsługi programu Opcje

Email

Okno Informacji dotyczących dystrybutora (Dealer Information) zostało zmodyfikowane, aby umożliwić konfigurację przypomnienia email. Do 4 adresatów może zostać dodanych. Kliknięcie **Wyślij przypomnienie teraz (Send reminder now)** zapisze informacje i wyśle przypomnienie natychmiast.

Nowe zdarzenie zostanie zapisane na liście zdarzeń.

Każda stacja robocza otrzyma 60 sekundową wiadomość wyskakującą (pop-up).

Notatka: opcja Przypomnienie KAP (Kap Reminder) może zostać również wywołana z okna Pomoc (About).



Format wyświetlania numeru karty (Defining a Card Display Format)

System EntraPass może obsługiwać wiele rodzajów czytników. Zależnie od rodzaju czytnika, format wyświetlania karty może się różnić. Okienko **Format wyświetlania (Display format)** pozwoli ci określić format, który będzie automatycznie ustawiany w momencie tworzenia nowej karty.

1 – Na pasku narzędzi Opcje, kliknij przycisk **Format wyświetlania (Display format)**.

Notatka: sekcje Karta #1-5 nie zostaną wyświetlone, o ile opcja Zaawansowanego zarządzania nie jest włączona.

2 – Wybierz format dla **Karta #1**.

- **Dziesiętny (Decimal)**
- **Ósemkowy (Octal)**: każda cyfra ósemkowa odpowiada dokładnie trzem cyfrom binarnym. Format ósemkowy do zapisu używa ośmiu cyfr, od 0 do 7. Programy często wyświetlają dane w tym formacie, ponieważ jest stosunkowo czytelny dla użytkowników i łatwo tłumaczy się na format binarny.
- **Szesnastkowy (Hexadecimal)**: każda cyfra odpowiada czterem cyfrom binarnym. Format szesnastkowy do zapisu używa 16 znaków: cyfr, od 0 do 9; oraz liter od A do F. Na przykład liczba 15 (format dziesiętny) jest wyrażona jako F w szesnastkowym. Programy często wyświetlają dane w tym formacie, ponieważ jest łatwiejszy w odczycie dla użytkownika niż system binarny.
- **FIPS (Federal Information Processing Standard)**, czyli publicznie ogłaszany standard federalnego rządu Stanów Zjednoczonych. Ten format może korzystać z danych > 32 bity.

3 – Zaznacz pole **Użyj formatu wielu kart (Use multiple card format)**, jeżeli twoje środowisko działania zawiera wiele typów czytników i chcesz mieć możliwość wyboru typu czytnika (innego niż domyślny), przy tworzeniu nowej karty.

4 – Wybierz jeden z procesów **Powiel numer PIN (Duplicate PIN)**.

- **Brak powielenia (No duplication)**: błąd wyświetla się na stacji roboczej; pole PIN zostanie zresetowane do wartości domyślnej (00000) oraz zostanie podświetlone. Wprowadź nowy, ważny numer PIN. Tylko PIN 00000 zostanie powielony, niezależnie od ustawień.
- **Powiadom o powieleniu (Notify when duplication)**: serwer sprawdza, czy numer PIN istnieje. Jeżeli istnieje, pojawia się pole z wiadomością, informującą o tym. Przycisk **Szczegóły** pozwoli wyświetlić listę użytkowników karty, którym został przypisany ten PIN.
- **Powielenie (Duplication)**: nie zostanie przeprowadzone żadne sprawdzenie, PIN zostanie zaakceptowany nawet, jeżeli jest powielony.

5 – **Długość numeru PIN (tylko KT-400) (Number of PIN digits)**: możesz wybrać długość: 4, 5 lub 6 znaków (Zobacz: **Definiowanie Opcji Karty (Card Options Definition)**).

Notatka: numer PIN musi zostać ustawiony oraz zachowany, aby uniemożliwić duplikację w przypadku utraty danych lub uzupełnienia przez system.

6 – Gdy wybrano opcję **Zaawansowanego zarządzania (Enhanced User Management)**, wybierz alternatywny format wyświetlania dla **Karty #2**. Powtórz Krok 6 dla **Karty #3**, **Karty #4** oraz **Karty #5**.

7 – Aby określić ogólny format wyświetlania dla KT-100, KT-300 oraz KT-400, wybierz odpowiednią opcję:

- **24-bit Wiegand, 5-cyforwy PIN (domyślnie KT-200)**: do 24-bitów dla KT-100, KT-200, KT-300 oraz KT-400.
- **32-bit, 5-cyforwy PIN**: do 32 bitów dla KT-100, KT-300 oraz KT-400.
- **24-bit Wiegand, 6-cyforwy PIN**: do 24-bitów dla KT-100, KT-300 oraz KT-400.
- **Do 16 znaków ABA, 6-cyforwy PIN**: do 16 dla KT-100, KT-300 oraz KT-400.



Notatka: kontrolery KT-100, KT-300 oraz KT-400 wykonają twardy reset przy zmianie formatu karty. Unikaj zmiany formatu karty, ponieważ może się to wiązać z utratą informacji.

Changing from a 24 bit to 32 bit Global Card Format

Zmiana z 24-bitowego na 32-bitowy format globalnej karty rozszerza ilość kart, które można skonfigurować EntraPass.

26-bitowy czytnik Wiegand ioProx nie obsługuje zmiany formatu karty globalnej 24-bitowej na 32-bitową. Jeśli masz połączenie 26-bitowych czytników Wiegand ioProx XSF i ioProx, nie zmieniaj ręcznie formatu lub włącz funkcję automatycznej konwersji. Najpierw musisz zastąpić 26-bitowe czytniki Wiegand

Czytniki XSF.

Aby ręcznie zmienić format 24-bitowej na 32-bitową kartę globalną, wykonaj następujące kroki:

- 1 - Kliknij kartę Opcje i wybierz z menu Format wyświetlania.
- 2 - W obszarze Format karty globalnej wybierz kartę 32-bitową, 5-cyfrową opcję PIN.
- 3 - Kliknij OK. Jeśli dokonałeś zmiany z 24-bitowej karty Wiegand, pięć lub sześć cyfr, na kartę 32-bitową, pięć cyfr PIN, monit wyświetlający pytanie, czy karty muszą zostać przekonwertowane na 32-bitowy z rozszerzeniem o Facility Code.

- Jeśli klikniesz **Tak**, wprowadź wartość rozszerzonego FC(2 znaki HEX).
- Po kliknięciu przycisku **Nie** zostanie wyświetlony monit o włączenie funkcji **automatycznej konwersji**.

UWAGA: Możliwość zmiany formatu karty globalnej z 24-bitowej na 32-bitową nie jest dostępna, gdy uruchomiony z serwera zapasowego.

EntraPass nie tworzy kopii zapasowych danych automatycznie po przełączeniu z formatu 24-bitowego na 32-bitowy.

W stacji roboczej EntraPass tworzy kopię zapasową systemu przed konwersją.

Po zmianie formatów KT-100, KT-200 i KT-300 automatycznie wykonują twardy reset. Dla KT-1 i KT-400 zmiana jest płynna.

Konwersja automatyczna (Auto Conversion)

Po zaznaczeniu pola wyboru Użyj automatycznej konwersji dla kart 24-bitowych legacy w wyświetlania okno, EntraPass automatycznie konwertuje wszystkie karty do formatu karty 32-bitowej. Wartość domyślna zostanie wyczyszczona.

Aby włączyć to pole wyboru, musisz ustawić format karty globalnej na 32-bitową kartę, 5-cyfrową opcję PIN.

Po wybraniu funkcji automatycznej konwersji i braku konwersji kart na format 32-bitowy, system automatycznie modyfikuje numer karty i wyzwala modyfikację definicji karty. Wydarzenia muszą być łagodnymi zdarzeniami bez awarii. Ta funkcja jest dostępna w bramie GSI, bramce globalnej i bramce KT-NCC.

UWAGA: Funkcja automatycznej konwersji jest dostępna z serwera zapasowego/



Kolor i priorytet zdarzenia (Event Color and Priority)

Możesz zmienić kolor i priorytet każdego wydarzenia.

- 1 - Na pasku narzędzi Opcje kliknij przycisk Kolor i priorytet zdarzenia.
- 2 - Użyj filtru Tekstowego, aby wyszukać zdarzenia.
- 3 - Wybierz niestandardowy kolor i poziom priorytetu zdarzenia. 0 jest najwyższym priorytetem, a 9 najniższym.
- 4 - Wybierz Nieprawidłowy, aby wydarzenie stało się nietypowym zdarzeniem. Zdarzenia, takie jak odmowa dostępu (zły poziom dostępu, wymagany poziom nadzorcy), nieprawidłowe połączenie serwera stacji roboczej, awaria komunikacji z bramą, lub wszystkie zdarzenia związane z procesem, który nie jest zakończony (na przykład niepowodzenie przeładowania sterownika) uważany za nienormalny. Jest to później wykorzystywane do generowania raportów.
- 5 - Wybierz Watchable, aby wydarzenie było możliwe do oglądania. Są to wstępnie wybrane zdarzenia, które mogą być wyświetlane EntraPass Web Watchlist. Można go użyć do wydania raportu zdarzeń związanych z EntraPass Web.



Integracja (Integration)

Zakładka **Integracja** pozwala użytkownikowi na wybranie podzespołów, które zostały zintegrowane z EntraPass przez Kantech.

Rejestracja DLL (DLL registration): Dostępne DLL w tym menu zostaną wykorzystane do określenia, jaki typ podzespołów klient podłączy do EntraPass.

- Kliknij **Dodaj**, aby zintegrować następne DLL. Zobacz: **Konfiguracja integrowanych paneli (Integrated Panel Configuration)**.

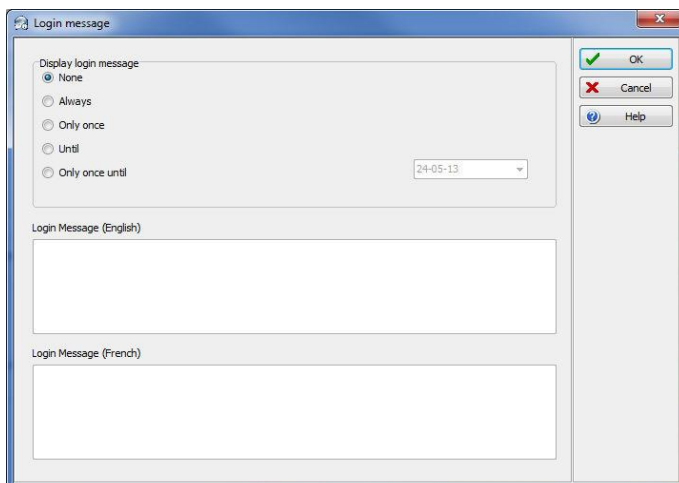
Notatka: integracja DLL musi zostać wykonana na serwerze EntraPass, aby skomunikować się z multi obiektową bramką, gdzie fizycznie są podłączone oraz zasilane elementy zewnętrzne.

Wirtualna klawiatura (Virtual keypad): ta zakładka pozwala użytkownikowi dostosować wyświetlanie ekranu wirtualnej klawiatury. Trzy tryby wyświetlania mogą zostać wybrane: **Niezakotwiczony**, **Modalny** albo **Zawsze na wierzchu (Floating, Modal or Stay on top)**

Info podczas logowania operatora (Login Messages)

Ta opcja pozwala wprowadzić tekst, który będzie wyświetlany innym operatorom, gdy zalogują się na stacjach roboczych.

1 – Z menu **Opcje, wybierz **Info podczas logowania operatora**.**



2 – Określ powtarzalność:

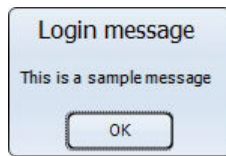
- **Brak (None).**
- **Zawsze (Always):** ta wiadomość pojawi się zawsze po logowaniu.
- **Tylko raz (Only once):** ta wiadomość pojawi się tylko raz na użytkownika.
- **Aż do (Until):** ta wiadomość będzie się pojawiać, aż do określonej daty.
- **Tylko raz, aż do (Only once until):** ta wiadomość będzie się pojawiać, aż do określonej daty albo do otrzymania wiadomości przez użytkownika.

3 – Wprowadź wiadomość w polu prawej.

4 – Kliknij OK.



Przykład wyświetlania wiadomości (Message display example):





Konfigurowanie urządzeń multimedialnych (Multimedia Devices Configuration)

Opcja Urządzenia multimedialne pozwala na ustawienie:

- Alarmów dźwiękowych
- Urządzeń do nagrywania wideo
- Urządzeń do zapisywania podpisów
- Urządzeń wideo

Wybierania dźwięku alarmu (Selecting an Alarm Sound)

1 – Z głównego okna **Opcji**, wybierz **Urządzenia multimedialne**.

2 – Zaznacz **Przypisz dźwięk alarmu (Assign alarm sound)**, jeżeli chcesz otrzymywać powiadomienie dźwiękowe o alarmie.

3 – Wybierz dźwięk z listy.

4 – Wybierz **Priorytet (Priority level)** dla wybranego dźwięku.

Notatka: Priorytet odnosi się do kolejności, według której wiadomości alarmowe są wyświetlane w Pulpicie alarmów. W EntraPass poziom 0 przypisany jest najwyższemu priorytetowi, a poziom 9 najniższemu. Zobacz Definiowanie parametrów zdarzenia, aby dowiedzieć się więcej.

5 – Kliknij przycisk **Odtwórz (Play)**, aby odtworzyć wybrany dźwięk.

6 – Kliknij przycisk **Dodaj (Add)**, aby dodać nowy dźwięk z osobistych plików.

Notatka: sekcja Bieżący wybór wyświetla dźwięk obecnie wybrany (wykorzystywany). Możesz określić opóźnienie dźwięku alarmu w polu Opóźnienie.



Definiowanie opcji wideo (Defining Video Options)

- 1 – Z okna Urządzenia multimedialne, wybierz zakładkę Nagrywanie wideo (Video capture).
- 2 – Zaznacz **Włącz nagrywanie wideo (Enable video capture)**, aby włączyć opcje nagrywania.
 - Urządzenie MCI: standardowe sterowniki Windows.
 - Urządzenia TWAIN: sterowniki TWAIN. (Zalecane).
 - Użyj nakładki: opcja dla urządzeń zapisywania obrazów.
 - Włącz menu kontroli: włącza opcje (zoom, nachylenie) dla urządzeń zapisywania obrazów.
 - Numer urządzenia MCI: wybierz numer identyfikacyjny dla urządzenia MCI.
 - Portret: ustawienia portretowe dla zachowanych obrazów.
 - Horyzontalne: ustawienia horyzontalne dla zachowanych obrazów. (Domyślne).
- 3 – Kliknij przycisk Test, aby zweryfikować funkcje kamery.

Ustawienie Skanera do wzoru podpisu (Setting Up the Signature Capture Device)

- 1 – Z okna Urządzenia multimedialne, wybierz zakładkę Podpis (Signature).
- 2 – Zaznacz **Włącz pad podpisów (Enable Signature pad)**.
- 3 – Z listy obsługiwanych urządzeń, wybierz sterowniki do pada.
- 4 – Zaznacz pole **Zdalna aplikacja (Remote application)**, jeżeli urządzenie działa jako takie.
- 5 – Wybierz **Szerokość PEN (Pen width)**.
- 6 – Przy pomocy przycisku Test sprawdź, czy sterowniki działają prawidłowo. Pojawi się okno **Test Pada Podpisów (Signature Pad Test)**.
- 7 – Wybierz zakładkę Wideo, aby ustawić opcje integracji wideo.
 - Opcja Wyłącz DirectX: DirectX to technologia Windows, która umożliwia osiągnięcie lepszej wydajności przy pracy lub przeglądania grafiki albo innej treści multimedialnej, w tym wideo oraz dźwięku. Domyślnie: DirectX jest włączony.
 - Opcja **Kontrola przepustowości wideo (Video bandwidth control)** pozwala ograniczyć/zwiększyć przepustowość wymaganą do strumieniowania wideo na żywo bez wpływania na wydajność sprzętu. Zakres: od 64 KB/s do 8192 KB/s.

Notatka: wartość Kontroli przepustowości wideo nie może przekroczyć wartości serwera EntraPass.



Wybór i konfiguracja drukarki zdarzeń (Printers Selection and Configuration)

Opcje Drukarki pozwalają na wybór drukarki do drukowania zdarzeń oraz do wyboru drukarki raportów lub identyfikatorów.

Wybieranie i ustawianie drukarki logów (Selecting and Setting Up a Log Printer)

Kiedy zdefiniujesz zdarzenia, możesz określić jak oraz kiedy będą one drukowane. Możesz, na przykład, przenieść zdarzenie do aplikacji EntraPass, drukarki albo aktywować przekaźnik.

Notatka: musisz przypisać terminarz „drukowania” do konkretnych zdarzeń, aby wydrukować je o określonym czasie.

1 – Z okienka Drukarka wybierz zakładkę Drukarka logów.

2 – Wybierz opcję drukowania:

- **Brak drukowania logów (No log printer):** żadne zdarzenie nie zostanie wydrukowane, nawet, jeżeli druk jest określony przez terminarz.
- **Użyj Sieciowej/Lokalnej drukarki Windows (Use Network/Local Windows printer):** po wybraniu tej opcji, wszystkie zdarzenia będą buforowane i drukowane, kiedy pełna strona będzie gotowa do wydruku. Zdarzenia będą drukowane na drukarce sieciowej/lokalnej.
- **Użyj Drukuj zdarzenia na lokalnej drukarce igłowej (Use local dot matrix printer):** wszystkie zdarzenie będą drukowane jedno-po-drugim, jedno-za-drugim albo każde na osobnej stronie (zależnie od typu drukarki).

3 – W sekcji Wybór drukarki (Printer selection) określ, czy chcesz drukować wiadomości albo alarmy.

- **Drukuj logi wiadomości:** wszystkie zdarzenia przypisane do terminarza „Wyświetl” w menu parametry zdarzenia zostaną wydrukowane.
- **Drukuj logi alarmów:** wszystkie zdarzenia przypisane do terminarza „Alarm” w menu parametry zdarzenia zostaną wydrukowane.

4 – Z listy Drukarka, wybierz konkretną drukarkę, która będzie wykorzystana, jako drukarka logów.

Wybieranie i ustawianie drukarki raportów (Selecting and Setting Up a Report Printer)

Definiowanie parametrów drukarki do drukowania raportów utworzonych w programie EntraPass.

1 – Z okna Opcje drukarki, wybierz zakładkę Drukarka raportów.

Wybór i konfiguracja drukarki identyfikatorów (Selecting and Setting Up a Badge Printer)

Definiowanie parametrów drukarki do drukowania identyfikatorów utworzonych w programie EntraPass.

1 – Z okna Opcje drukarki, wybierz zakładkę Drukarka identyfikatorów.

2 – Zaznacz opcję Drukarka identyfikatorów (Badge printer), jeżeli drukarka identyfikatorów będzie wykorzystywana – pojawią się nowe przyciski Drukuj identyfikator oraz Podgląd identyfikatora.

3 – Z listy Wybierz drukarkę identyfikatorów, wybierz odpowiednią drukarkę.

4 – Możesz drukować obraz na drugiej stronie identyfikatora – zaznacz **Odwróć na drugą stronę (Invert Reverse Side)/**.

5 – Zaznacz **Użyj kod kreskowy 39, jako czcionki (Use bar code 39 as font)** i wybierz odpowiednią czcionkę.



EntraPass - Instrukcja instalacji i obsługi programu

Opcje



Rejestracja (Registration)

To menu jest wykorzystywane do zarejestrowania nowych komponentów, takich jak KTES, Stacja robocza, Bramka, SmartLink, etc.

Zobacz: **Rejestracja Systemu** ([System Registration](#)), aby zarejestrować i wykorzystać bazę danych systemu oraz aby ustalić komunikację z serwerem.

Wybór i konfiguracja drukarki identyfikatorów (Selecting and Setting Up a Badge Printer)

Definiowanie parametrów drukarki do drukowania identyfikatorów utworzonych w programie EntraPass.

- 1 – Z okna Opcje drukarki, wybierz zakładkę Drukarka identyfikatorów.
- 2 – Zaznacz opcję Drukarka identyfikatorów (Badge printer), jeżeli drukarka identyfikatorów będzie wykorzystywana – pojawią się nowe przyciski Drukuj identyfikator oraz Podgląd identyfikatora.
- 3 – Z listy Wybierz drukarkę identyfikatorów, wybierz odpowiednią drukarkę.
- 4 – Możesz drukować obraz na drugiej stronie identyfikatora – zaznacz **Odwróć na drugą stronę (Invert Reverse Side)**.
- 5 – Zaznacz **Użyj kod kreskowy 39, jako czcionki (Use bar code 39 as font)** i wybierz odpowiednią czcionkę.



Logowanie do trybu serwisowego (Service Login Information)

Informacja wprowadzona tutaj jest wymagana, kiedy serwer działa, jako usługa oraz serwer musi uzyskać dostęp do zasobów sieciowych. **Logowanie do trybu serwisowego (Service Login Information)** jest wymagana dla **Terminarza Kopii zapasowej (Backup Scheduler)** przy wykorzystaniu dysku sieciowego.

- Musisz zaznaczyć pole **Login Server Service**, aby włączyć tą opcję.
- **Musisz** wprowadzić nazwę domeny serwerowej oraz nazwę komputera, login oraz dwukrotnie hasło, dla potwierdzenia.

Notatka: jeśli nie skonfigurowano nazwy domeny ani grupy roboczej, w polu Nazwa domeny musisz wprowadzić Nazwę komputera.

Ustawienie Daty i Czasu (System Date & Time Modification)

Opcja Zmiana systemu (Change system) powinna być wykorzystywana wyłącznie, gdy jest to niezbędne. Może mieć negatywny wpływ na logiczne komponenty systemu dostępu (np. terminarze). Jeżeli z jakiegoś powodu chcesz zmienić datę oraz czas systemu, lepiej to zrobić przy pomocy ustawień parametrów systemu (Opcje > Parametry systemu > Dostosowanie czasu).

- 1 – Z głównego okna Opcji, wybierz Data i Czas.
- 2 – Wprowadź datę w pole Data, albo wybierz datę z kalendarza. Podłączone komponenty również otrzymają informacje o zmianie daty.
- 3 – Wprowadź czas w pole Czas. Podłączone komponenty również otrzymają informacje o zmianie daty.
- 4 – Kliknij OK, żeby wyjść.

Notatka: jeśli chcesz, aby w razie potrzeby system automatycznie zamieniał czas, wykorzystaj zakładkę Dostosowanie czasu w menu Definiowanie parametrów serwera. Zobacz Parametry czasu.

Ważne: nie powinieneś zmieniać czasu przy pomocy ustawień Windows. Rekomenduje się zmianę czasu systemu przez ustawienia parametrów systemu.



Wybór języka (System Language Selection)

EntraPass umożliwia korzystanie z oprogramowania w języku wybranym przez użytkownika. Podstawowe języki to angielski, francuski, hiszpański, niemiecki oraz włoski. **Edytor słownika (Vocabulary Editor)** pozwala dodawać nowe języki.

Zmienianie języka systemu (Changing the System Language)

1 – Z głównego okna EntraPass wybierz pasek narzędzi **Opcje**, a następnie kliknij przycisk **Wybierz język**.

Notatka: jeśli wprowadzasz zmianę głównego języka, operacje na bazie danych zostaną przerwane, a zmiany wejdą w życie po zrestartowaniu systemu. Język bazy danych zostanie zmodyfikowany według wartości ASCII głównego języka. Znaki specjalne w różnych językach mogą mieć wpływa na bazę danych!

2 – Z listy **Wybierz język główny (Select primary language)** wybierz język główny. Z listy **Wybierz drugi język (Select Secondary language)**, wybierz drugi język.

3 – Przełoguj się w EntraPass.



Konfiguracja parametrów systemu (System Parameters Configuration)

Okienko Parametry systemu pozwala Administratorowi Systemu na modyfikowanie parametrów, które określają system EntraPass. Okienko może zostać otworzone ze stacji roboczej albo z serwera. Parametry są pogrupowane razem pod różnymi oznaczeniami, np. Serwer, Bramka, Firmware, Obrazy, etc.

Parametry serwera (Server Parameters)

W zakładce Serwer, możesz zdefiniować pojemność serwera pod kątem logów, możliwości diagnostyczne, parametry bezpieczeństwa, alarmy sieciowe, etc.

Serwer e-mail (E-mail Server)

EntraPass oferuje użytkownikom możliwość wysyłania raportów przy pomocy e-maili. Ta funkcja może zostać wykorzystana przy zgłoszeniu prośby o autentyfikację, przez użytkownika, od serwerów SMTP.

Notatka: połączenia zabezpieczone SSL nie są wspierane.

1 - W polu Serwer Email (Email Server): SMTP albo Serwer Zamienny; wprowadź adres IP serwera, który będzie wykorzystywany do wysyłania wiadomości email.

2 – W polu Port Email (Email Port), wprowadź numer portu, który będzie wykorzystywany do wysyłania wiadomości email (zazwyczaj: 25).

- Unsecured (No SSL/TLS)
- Gmail(SSL/TLS)
- Secured (SSL/TLS)
- Office 365 (STARTTLS)

3 - Wprowadź adres email w pole Nadawca (Email sender). Ten adres będzie wykorzystywany do autentyfikacji serwera email.

4 - Autentyfikacja (Authentication): te opcje mogą być wykorzystane do konfigurowania metody autentyfikacji.

• **Brak autentyfikacji (No authentication)**

• **Autentyfikacja SMTP (SMTP authentication):** autentyfikacja, wysłana na port SMTP, musi zostać potwierdzona zanim wiadomość zostanie wysłana.

• **Autentyfikacja POP3 (POP3 authentication):** autentyfikacja, wysłana na port POP3, musi zostać potwierdzona zanim wiadomość zostanie wysłana.

5 – Wyślij do (Send to): adres odbiorcy.

6 – Test (Test button): wysła wiadomość testową z wybranymi parametrami.

Notatka: domyślna wartość portu email jest ustawiona na 25. Możesz zmienić tę wartość (dostępne wartości: 0-65.535). Aby uzyskać więcej informacji skontaktuj się z administratorem sieci.



Automatyczne wyłączanie operatora

Użyj funkcji automatycznego wyłączania operatora, aby automatycznie dezaktywować operatora, jeśli nie ma aktywności ich konto przez określoną liczbę dni. Wartość domyślna to 90 dni. Po zainstalowaniu EntraPass po raz pierwszy czas lub aktualizacja z poprzedniej wersji, ta funkcja jest wyłączona. Po włączeniu operatora autodeaktywacja o północy EntraPass sprawdza bazę danych pod kątem aktywnych operatorów i pod nieobecność aktywności, automatycznie wysyła e-mail 10 dni przed dezaktywacją, aby powiadomić operatora o ich bezpośrednie rozłączenie.

UWAGA: Operator musi wypełnić swoje pole e-mail, aby otrzymać powiadomienie e-mailem. Jeśli ich e-mail pole nie jest kompletne, dezaktywacja następuje bez powiadomienia e-mail. Funkcja automatycznego wyłączania nie dotyczy operatorów LDAP ani domyślnych operatorów EntraPass: administrator, instalator i operator.

Aby zapobiec dezaktywacji, operator musi zalogować się do EntraPass za pomocą stacji roboczej, sieci lub urządzenia mobilnego przed datą dezaktywacji. Jeśli operator jest dezaktywowany, musi ręcznie włączyć operatora. Do zrob to, kliknij kartę System i kliknij opcję Operator w menu. Wybierz odpowiedniego operatora i wyczyść pole wyboru Operator wyłączony.

W przypadku awarii serwera głównego funkcja nadal działa w pełni na serwerze nadmiarowym. Jeśli serwer i nadmiarowy serwer jest wyłączony w dniu wysłania wiadomości e-mail z powiadomieniem, wiadomość e-mail z powiadomieniem nie jest wysyłana, ale Operator jest dezaktywowany zgodnie z planem.

Ustawianie funkcji automatycznego wyłączania operatora

Aby ustawić funkcję automatycznego wyłączania operatora, wykonaj następujące czynności:

- 1 - Kliknij zakładkę Opcje i kliknij w menu Parametry systemu.
- 2 - W oknie Parametry systemu kliknij opcję Serwer i kliknij kartę Reguły hasła.
- 3 - Zaznacz pole wyboru Automatycznie dezaktywuj operatora.
- 4 - W polu Dni kliknij strzałki, aby wybrać odpowiednią liczbę dni. Kliknij OK. Trzydzieści dni to minimalna ilość dni i 365 dni to maksimum.



Logi serwera (Server Logs)

Możesz określić maksymalną ilość wpisów, które będą przechowywane w logach systemu oraz logach błędów systemu (do 100000). Wpisy zawierają takie transakcje, jak: logowanie do serwera, połączenia/rozłączenia, włączenie/wyłączenie serwera, etc. Te wpisy są przechowywane razem z datą/czasem, informacji o stacji roboczej, informacji o użytkowniku oraz opisem transakcji.

Historia zmian

Aby udostępnić funkcjonalność Historia zmian, zaznacz pole wyboru Historia zmian i wybierz jedną z opcji następujące opcje przechowywania danych:

- Aby zdefiniować liczbę dni na zachowanie danych z audytu, wybierz liczbę. Ustawienie domyślne to 365 dni, minimalna liczba to 30 dni, a maksymalna liczba to pięć lat.
- Aby zdefiniować liczbę rekordów przechowywanych przez system, wybierz liczbę od 1 do 15 w polu Liczba przechowywanych rekordów. Ustawienie domyślne to pięć dni.

W obszarze **Komponenty objęte historią zmian** wybierz komponenty, które chcesz wyświetlić w ścieżce Audytu raport. Po zaznaczeniu pola wyboru Podstawowa nazwa komponentu jest dostępna w ścieżce audytu. Jeśli ty zaznacz pole wyboru Wtórny, informacje o liście komponentów są dostępne w ścieżce audytu.

Przestrzeń dyskowa (Disk Space)

Opcja Przestrzeń dyskowa została opracowana, jako zabezpieczenie przed awarią systemu spowodowaną brakiem miejsca na dysku. Pozwala monitorować ilość wolnego miejsca na dysku dla optymalnego działania systemu oraz generowania raportów. EntraPass daje możliwość przerwania przygotowania raportu, jeżeli zostanie przekroczony próg wolnej przestrzeni dyskowej.

- **Próg wolnej przestrzeni dyskowej (MB) (Disk free space threshold (MB))**: lista: określ maksymalny próg pojemności, po przekroczeniu którego system wyśle wiadomość, że wolna przestrzeń dyskowa spadła poniżej określonej, dopuszczalnej wartości. Wyrażona w mega bajtach. Zakres: od 2000 do 99999 MB.
- **Czas pomiędzy powiadomieniami (Time between notifications (hh:mm))**: wprowadź czas pomiędzy powiadomieniami w momencie, gdy wolna przestrzeń dyskowa spadła poniżej określonej wartości. Na przykład, jeżeli wprowadzisz w polu wartość 00:30, ostrzeżenie systemowe będzie wyświetlane co 30 minut. Zakres: od 10 minut do 24 godzin.
- **Ścieżka archiwum (Archival Path)**: wprowadź ścieżkę do archiwum. Zachowywanie archiwalnych danych na innym dysku zwiększa wydajność systemu.

Serwer redundantny (Redundant Server)

Notatka: Serwer redundantny musi zostać zarejestrowany, aby był dostępny.

Możesz określić **Opóźnienie auto-restartu (m:ss) (Auto-restart delay (m:ss))** dla Zdublowanej bazy danych i Serwera Redundantnego. Zakres: 1:00 do 9:59.

Szybka synchronizacja (**Quick synchronize**): kiedy ta opcja jest zaznaczona, główny serwer nie zamyka tabel podczas synchronizacji ze zdublowaną bazą danych. Wiadomości nadal mogą przychodzić, a baza danych przeglądana. Żółte oznaczenie jest wyświetlane, informując, że system jest w trybie **tylko do odczytu**.

Notatka: program MS/SQL Interface nie jest wspierany przez Mirror Database oraz Serwer redundantny. MS/SQL Interface zbuferuje wszystkie zdarzenia, pomimo że nie może łączyć się z Mirror Database, ani z serwerem redundantnym.

Wylogowanie i stan bezczynności (Logout and Idle)



EntraPass - Instrukcja instalacji i obsługi programu Opcje

W tej zakładce można określić zachowanie aplikacji EntraPass w momencie bezczynności (kiedy użytkownik nie podejmuje działań na klawiaturze).

- **Automatyczne wylogowanie przy bezczynności (Automatic logout on idle):** użytkownik będzie musiał ponownie wprowadzić nazwę użytkownika i hasło, aby uzyskać na nowo dostęp do aplikacji. Maksymalne opóźnienie: 9 minut 59 sekund.
- **Wyślij na pasek przy bezczynności (Send to tray on idle):** aplikacja zostanie zminimalizowana i wysłana na pasek narzędzi, gdy minie określony czas, w którym obecnie zalogowany użytkownik, będzie nieaktywny. Maksimum: 59 minut 59 sekund.
- **Zaloguj, aby zamknąć aplikację serwera (Must login to close a Server application):** jeżeli ta opcja jest wybrana, użytkownik musi się zalogować (nazwa użytkownika i hasło), aby zamknąć aplikację.
- **Powiadom o ostatnim wylogowaniu (Notify last log out):** jeżeli ta opcja jest wybrana, EntraPass powiadomi o wylogowaniu się ostatniego użytkownika.
- **Wyświetl listę logowania (Display Login List):** jeżeli ta opcja jest wybrana, pięciu ostatnich użytkowników, którzy zalogowali się do aplikacji EntraPass, zostanie wyświetlonych w oknie logowania. Ta opcja ułatwia dostęp do systemu dla użytkowników, którzy po prostu mogą wybrać swoją nazwę użytkownika i wprowadzić hasło. Może także ułatwić Administratorowi Systemu kontrolę tego, którzy użytkownicy logowali się w ostatnim czasie na konkretne aplikacje.

Notatka: pomimo zalet zaleca się, aby wyłączyć opcję Wyświetl listę logowania dla zwiększenia bezpieczeństwa systemu.

Terminarz (Schedule)

Zakładka Terminarz to miejsce, w którym będziesz uaktualniać terminarz do poziomu zaawansowanego. EntraPass oferuje użytkownikom więcej elastyczności i ułatwienie obsługi dzięki grupowaniu terminarzy po bramkach, połączeniach albo komponentach systemowych. Przy instalacji EntraPass wersji 3.18 lub nowszej, ta opcja nie jest automatycznie włączona.

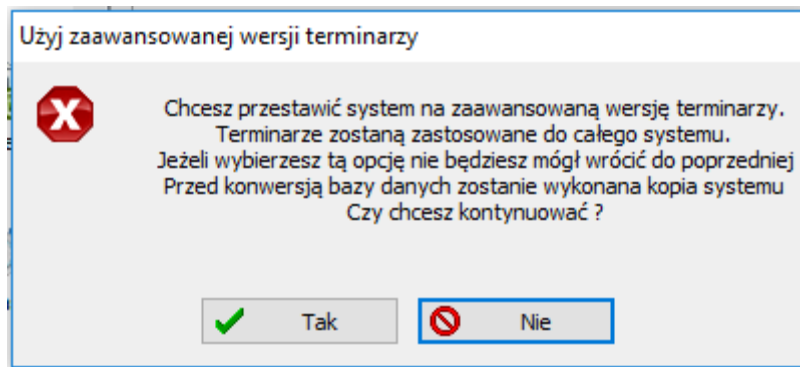
Notatka: zanim zaznaczysz to pole upewnij się, że aktualizacja do zaawansowanego terminarza jest konieczna.

Terminarze są pogrupowane:

- Terminarze systemowe: są stosowane przy komponentach logicznych takich, jak: parametry zdarzeń, terminarze logowania użytkowników, przełączniki wideo, etc. Terminarze systemowe nie są przypisywane dla konkretnych kontrolerów; są przypisywane dla całego systemu. Możesz zaprogramować nieograniczoną ilość terminarzy systemowych.
- Terminarze multi-obiektowe: są definiowane na połączenie. Możesz zdefiniować 100 terminarzy na multi-obiekt, do celów takich jak: nadzór zasilania (kontrolery), odblokowywanie drzwi, przełącznik REX, tryb aktywacji (przełącznik), etc.
- Po zaznaczeniu pola i kliknięciu OK, zostanie wyświetlone ostrzeżenie, że działania jest odwracalne, ale nie bez konsekwencji.
- Przed aktywowanie tej opcji, zalecamy przygotowanie kopii zapasowej danych.



EntraPass - Instrukcja instalacji i obsługi programu Opcje



- Po zatwierdzeniu procesu, zakładka **Terminarz** zniknie z okienka **Parametry systemu**.
- **Włącz terminarz do obejścia REX (Enable schedule to bypass Rex)**, aby włączyć główne i pomocnicze opcje **Terminarza wiadomości pominięcia REX (Rex Bypass Message schedule)** dla drzwi. Zobacz: **Konfigurowanie drzwi (Door Configuration)**.



Status Ikony (Icon Status)

Parametr Opóźnienie statusu limitu czasu (m:ss) (Status time out delay (m:ss)) pozwala określić przedział czasu zanim stacja robocza wyśle zapytanie do serwera o statusy przycisków. Im wyższe opóźnienie, tym mniejsza częstotliwość odświeżania przycisków, co przekłada się na mniejsze obciążenie sieci. Maksymalny czas: 1 min 30 sekund.

Logowanie do trybu serwisowego (Service Login Information)

Informacja wprowadzona tutaj jest wymagana, kiedy serwer działa, jako usługa oraz serwer musi uzyskać dostęp do zasobów sieciowych. **Logowanie do trybu serwisowego (Service Login Information)** jest wymagana dla **Terminarza Kopii zapasowej (Backup Scheduler)** przy wykorzystaniu dysku sieciowego.

- Musisz zaznaczyć pole **Login Server Service**, aby włączyć tą opcję.
- **Musisz** wprowadzić nazwę domeny serwerowej oraz nazwę komputera, login oraz dwukrotnie hasło, dla potwierdzenia.

Notatka: jeśli nie skonfigurowano nazwy domeny ani grupy roboczej, w polu Nazwa domeny musisz wprowadzić Nazwę komputera.

Zasady dotyczące hasła (Password Rules)

Celem tej opcji jest dodawanie parametrów do hasła użytkownika.

1 – Z menu Opcje, wybierz Parametry systemu.

Zasady hasła:

- Ilość znaków (min/max): 8-20.
- Ilość znaków numerycznych (min/max): 0-20.
- Ilość znaków specjalnych (min/max): 0-20.
- Ilość wielkich liter (min/max): 0-20.

Notatka: po wybraniu, wszyscy nowo utworzeni albo zmodyfikowani użytkownicy będą musieli podporządkować się nowym zasadom dotyczącym haseł.



Parametry oprogramowania sprzętowego (Firmware Parameters)

Ta sekcja zawiera wszystkie informacje dotyczące kontrolerów, bramek i module komunikacji IP, oraz sekcje do zaktualizowania oprogramowania sprzętowego (firmware).

Notatka: zakładka KTES będzie dostępna wyłącznie w przypadku, jeżeli kontroler KTES został uprzednio zdefiniowany w systemie. Zobacz Konfigurowanie KTES, aby dowiedzieć się więcej.

KT-100

Zakładka KT-100 określa położenie katalogu zawierającego oprogramowanie dla kontrolerów KT-100. System wykorzysta te dane do zaktualizowania zainstalowanych kontrolerów (nie dostępne w EntraPass KTES Edition).

KT-300

Zakładka KT-300 określa położenie katalogu zawierającego oprogramowanie dla kontrolerów KT-300. System wykorzysta te dane do zaktualizowania zainstalowanych kontrolerów (nie dostępne w EntraPass KTES Edition).

KT-400

Zakładka KT-400 określa położenie katalogu zawierającego oprogramowanie dla kontrolerów KT-400. System wykorzysta te dane do zaktualizowania zainstalowanych kontrolerów.

- Opcja **Włącz Aktualizatora TFTP KT-400 (Enable TFTP KT-400 updater)** umożliwi aktualizację oprogramowania KT-400 z **Operacje > Okienko obiektu w EntraPass (Operation > Site dialog in EntraPass)**.
- **Włącz automatyczne aktualizowanie oprogramowania (Enable automatic firmware update)**: włącz, aby dokonać aktualizacji każdego KT-400 inną wersją oprogramowania.

Notatka: opcja automatycznego aktualizowania oprogramowania odnosi się wyłącznie do KT-400s.



EntraPass - Instrukcja instalacji i obsługi programu Opcje

Notatka: multi obiektowa bramka musi zostać zrestartowana, aby włączyć aktualizację TFTP KT-400.

- Ze względów bezpieczeństwa, jako Administrator Systemu możesz zdecydować, o wyłączeniu tej opcji i niedopuszczeniu użytkowników do aktualizowania oprogramowania we własnym zakresie.

KT-1

Zakładka KT-1 określa położenie katalogu zawierającego oprogramowanie dla kontrolerów KT-1. System wykorzysta te dane do zaktualizowania zainstalowanych kontrolerów.

- Opcja **Włącz Aktualizatora TFTP KT-1 (Enable TFTP KT-1 updater)** umożliwi aktualizację oprogramowania KT-1 z **Operacje > Okienko obiektu w EntraPass (Operation > Site dialog in EntraPass)**.

- **Włącz automatyczne aktualizowanie oprogramowania (Enable automatic firmware update)**: włącz, aby dokonać aktualizacji każdego KT-1 inną wersją oprogramowania.

Notatka: opcja automatycznego aktualizowania oprogramowania odnosi się wyłącznie do KT-1s.

Notatka: multi obiektowa bramka musi zostać zrestartowana, aby włączyć aktualizację TFTP KT-1.

- Ze względów bezpieczeństwa, jako Administrator Systemu możesz zdecydować, o wyłączeniu tej opcji i niedopuszczeniu użytkowników do aktualizowania oprogramowania we własnym zakresie.

- Wybierz **Tryb aktualizacji oprogramowania (Firmware flashing mode)**.

KTES

Zakładka KTES określa położenie katalogu zawierającego oprogramowanie dla kontrolerów KTES. System wykorzysta te dane do zaktualizowania zainstalowanych KTES.

Kantech IP Link

Zakładka IP Link określa położenie katalogu zawierającego oprogramowanie dla modułu Kantech IP Link. System wykorzysta te dane do zaktualizowania zainstalowanego oprogramowania.

- Opcja **Włącz Aktualizatora TFTP IP Link (Enable TFTP IP Link updater)** umożliwi aktualizację oprogramowania IP Link z **Operacje > Okienko obiektu w EntraPass (Operation > Site dialog in EntraPass)**.

Notatka: multi obiektowa bramka musi zostać zrestartowana, aby włączyć aktualizację TFTP IP Link.

- Ze względów bezpieczeństwa, jako Administrator Systemu możesz zdecydować, o wyłączeniu tej opcji i niedopuszczeniu użytkowników do aktualizowania oprogramowania we własnym zakresie.

czytnik ioSmart

- Karta czytnika ioSmart określa folder zawierający oprogramowanie firmware dla czytników. System użyje te dane do aktualizacji zainstalowanych czytników.

ioModules

Zakładka ioModule określa folder zawierający oprogramowanie firmware dla ioModules. System wykorzystuje te dane do aktualizacji zainstalowanego ioModules.

KT-401

Zakładka KT-401 określa położenie katalogu zawierającego oprogramowanie dla kontrolerów KT-401. System wykorzysta te dane do zaktualizowania zainstalowanych kontrolerów.



EntraPass - Instrukcja instalacji i obsługi programu

Opcje

- Opcja **Włącz Aktualizatora TFTP KT-401 (Enable TFTP KT-401 updater)** umożliwi aktualizację oprogramowania KT-401 z **Operacje > Okienko obiektu w EntraPass (Operation > Site dialog in EntraPass)**.
- **Włącz automatyczne aktualizowanie oprogramowania (Enable automatic firmware update)**: włącz, aby dokonać aktualizacji każdego KT-401 inną wersją oprogramowania.

Notatka: opcja automatycznego aktualizowania oprogramowania odnosi się wyłącznie do KT-401s.

Notatka: multi obiektowa bramka musi zostać zrestartowana, aby włączyć aktualizację TFTP KT-401.

- Ze względów bezpieczeństwa, jako Administrator Systemu możesz zdecydować, o wyłączeniu tej opcji i niedopuszczeniu użytkowników do aktualizowania oprogramowania we własnym zakresie.

Parametry obrazu (Image Parameters)

Sekcja **Obraz (Image)** jest miejscem, gdzie możliwe jest określenie parametrów opcji identyfikowania. Można określić jakość obrazu dla obrazów, podpisów i grafik wykorzystywanych, jako tło.

- Jeżeli korzystasz z opcji identyfikowania, zaleca się pozostawić jakość jpeg, jako domyślną. Zmniejszenie jakości może doprowadzić do pogorszenia się jakości obrazu importowanych ze identyfikatorów.
- Jeżeli nie korzystasz z opcji identyfikowania, możesz zredukować jakość jpeg, tak, aby nie zajmowały za dużych przestrzeni bazy danych. Trzeba jednak mieć na uwadze, że zmniejszenie jakości może doprowadzić do pogorszenia się jakości obrazu importowanych ze identyfikatorów.

Parametr pozwala zachować obraz karty i karty gościa, podpisów oraz grafik tła do pliku zamiast bezpośrednio w bazie danych. Opcja może być przydatna dla obiektów o dużym archiwum obrazów i grafik. Bazy danych obrazów, podpisów oraz grafik tła mogą zawierać do 2 Gb danych każda.



Obrazy i identyfikowanie (Picture and Badging)

Opcja Obraz i identyfikowanie pozwala na dopasowanie jakości obrazu i podpisu do wykorzystania przy opcji Identyfikowania (Badging).

- Odznaczenie formatu JPEG, informuje system, że ma zapisywać grafikę w formacie tiff.

Notatka: pamiętaj, że to może mieć wpływ na jakość obrazu. Jeśli nie jesteś zaawansowanym użytkownikiem, nie zmieniaj wartości domyślnych.

- Wartość jakości JPEG dla Tła grafiki (obrazu) wskazuje jakość, z jaką obraz zostanie zapisany. Jeżeli wybierzesz 10, jakość będzie bardzo słaba; 100 oznacza doskonałą jakość.
- Dla obrazów i miniatur wybierz pozycję położenia przezroczystego obrazu. Dostępne są cztery możliwości: górny-prawy, górny-lewy, dolny-prawy oraz dolny-lewy róg. Domyślnie, system wybiera dolny-lewy róg. EntraPass umożliwia użytkownikowi wybór dowolnego koloru.
- Przy zaznaczeniu **Zapisz obrazy i podpis w pliku**, system stworzy foldery Obrazy i Podpisy w lokalizacji: C:\Program Files\Kantech\Server_CE\Data; gdzie zachowywane będą wszystkie obrazy i podpisy.
- Przy zaznaczeniu **Zapisz obrazy i podpis (goście) w pliku**, system stworzy foldery Obrazy i Podpisy w lokalizacji: C:\Program Files\Kantech\Server_CE\Data; gdzie zachowywane będą wszystkie obrazy i podpisy (gości).

Notatka: podczas modyfikowania istniejącego obrazu albo podpisu, EntraPass zapisze zmiany w odpowiednim pliku oraz usunie odpowiedni zapis w bazie danych.



Grafika (Graphic)

Opcja grafiki pozwala dopasować, jakość grafiki dla oprogramowania EntraPass.

- Odznaczenie formatu JPEG, informuje system, że ma zapisywać grafikę w formacie tiff.

Notatka: pamiętaj, że to może mieć wpływ na jakość obrazu. Jeśli nie jesteś zaawansowanym użytkownikiem, nie zmieniaj wartości domyślnych.

- Wartość jakości JPEG dla Tła grafiki (obrazu) wskazuje jakość, z jaką obraz zostanie zapisany. Jeżeli wybierzesz 10, jakość będzie bardzo słaba; 100 oznacza doskonałą jakość.
- Przy zaznaczeniu **Zapisz grafikę w pliku**, system stworzy foldery Grafika w lokalizacji: C:\Program Files\Kantech\Server_CE\Data; gdzie zachowywane będą wszystkie grafiki.

Notatka: podczas modyfikowania istniejącej grafiki, EntraPass zapisze zmiany w odpowiednim pliku oraz usunie odpowiedni zapis w bazie danych.

Parametry raportu (Report Parameters)

Zakładka Raport pozwala użytkownikowi zdefiniowanie separatora pól dla raportów, formatu nazw użytkownika, etc.

CSV

W zakładce CSV, możesz określić separator pól dla twoich raportów.

- Domyślnie, system wykorzystuje przecinek, jako separator. Możesz zmienić na: kropkę, średnik, spację, etc.
- Zaleca się zaznaczenie opcji **Data i czas na osobnych polach**. Domyślnie system umieszcza je na tym samym polu. Po zaznaczeniu, system umieści je na dwóch osobnych polach.



Przestrzeń dyskowa (Disk Space)

Ta opcja służy, jako zabezpieczenie przy, np., żądaniu utworzenie wielkiego raportu. W tym przypadku, system zawiesi wykonywanie raportu oraz wyświetli wiadomość alarmową wskazując powód zawieszenia.

- **Anuluj raport, jeżeli pozostała przestrzeń dyskowa jest mniejsza niż (Abort report if free space lower than (MB)):** z listy możesz wybrać minimalną pojemność wymaganą do przeprowadzenia przygotowania raportu. Zakres: 2000 do 999999 MB.
- **Maksymalna ilość zdarzeń do raportu email (Maximum event for email report):** z listy wybierz maksymalną liczbę zdarzeń, które mogą zostać wysłane w postaci raportu email. Zakres: 100 do 100000 zdarzeń.
- **Maksymalna ilość zdarzeń dla standardowego raportu (Maximum event for standard report):** z listy wybierz maksymalną liczbę zdarzeń, które mogą zostać wysłane w postaci standardowego raportu. Zakres: 1000 do 500000 zdarzeń.
- **Jednoczesne przygotowanie raportów (Simultaneous report process):** określa liczbę raportów, które mogą być przygotowywane w tym samym czasie. Do 10 raportów może być przygotowywane w tym samym czasie bez wpływu na wydajność systemu.

Notatka: kiedy liczba zdarzeń dla raportu przekroczy dopuszczalną wartość maksymalną, niektóre zdarzenia nie zostaną uwzględnione w raporcie. Zostanie utworzone zdarzenie Przekroczono liczbę zdarzeń dla raportu, które zostanie wyświetlone na pulpicie Wiadomości oraz dodane do raportu.

Format nazwy użytkownika karty (User Name Format)

Określenie formatu nazwy użytkownika poinstruuje system, jak nazwa użytkownika karty będzie wyświetlana w EntraPass.

- **Parsuj nazwę użytkownika (Parse user name):** powinno zostać zaznaczone, jeżeli chcesz wybrać metodę parsowania nazwy użytkownika w systemie.
- **Format nazwy użytkownika karty (User Name Format)** pozwala wybrać metodę parsowania. Opcje: Zaczynj od nazwiska; Zaczynj od imienia.
- **Parsuj nazwę użytkownika z (Parse user name with):** pozwala wybrać znak, który zostanie użyty do parsowania pól nazwy użytkownika. Opcje: przecinek, kropka, średnik, dwukropek, spacja.

Notatka: przed wersją EntraPass 3.18, system korzystał z metody wyszukiwania, która wymagała od Administratora wprowadzenia konkretnych wartości granicznych (dolna/górna) do określenia zasad wyszukiwania. Na przykład, aby wygenerować raport, który zawierałby wszystkich użytkowników z nazwiskiem zaczynającym się na A, dolna wartość graniczna powinna zostać określona na „A”, a górna „AZZZZZ”. Teraz system ten sam rezultat po wprowadzenia „A” dla obu wartości granicznych.



Parametry wideo (Video Parameters)

Sekcja wideo wyświetla się wyłącznie wtedy, gdy opcja Integracja wideo jest włączona w systemie EntraPass. Określisz synchronizację czasu, zdalny proces wideo oraz format JPEG dla obrazów wideo.

Parametry (Parameters)

Zakładka Parametry pozwala na określenie parametrów dla procesowania wideo.

- **Wyłącz zdalną synchronizację czasu (Disable manual time synchronization)** powstrzyma serwer EntraPass przed aktualizowaniem daty i czasu serwera wideo po zdalnych modyfikacjach czasu. Opcja przydaje się, kiedy chcesz zachować wszystkie nagrane zdarzenia, które miały miejsce na serwerze wideo niezależnie od czasu „aktualnego” na serwerze EntraPass.

- Sekcja **Parametrów kontroli zdalnego procesowania wideo (Remote video process control parameters)** zawiera parametry, które określają zdalne zarządzanie procesowaniem wideo pomiędzy serwerem EntraPass, a serwerami wideo podłączonymi do EntraPass. Zarządza wszystkimi zadaniami związanymi z: nagrywaniem, zdarzeniami, wzorami, etc.

- Pole aplikacji **Kontrola presetów i trasy (Preset and pattern control)** pozwala na wprowadzenie liczby aplikacji, które zostaną automatycznie uruchomione do procesowania presetów i wzorów. Zakres: od 1 do 8 równoczesnych aplikacji.

Notatka: aplikacja Kontrola presetu oraz trasy jest uruchomiona za każdym razem, kiedy zaczyna się nagranie wideo. Jeśli wprowadzisz „1” jako wartość tej liczby, a – na przykład – posiadasz więcej niż 1 serwer wideo z określonymi presetami i trasami, aplikacja zajmie się presetami na wszystkich tych serwerach wideo. Jeśli zdecydujesz się zwiększyć wprowadzoną liczbę aplikacji pamiętaj, że działanie wielu aplikacji jednocześnie zmniejsza wydajność sprzętu.

- **Resetuj aplikację zdalnego procesowania wideo (Reset remote video process application)** pozwala systemowi przerwać, a następnie automatycznie zresetować aplikację **Zdalne procesowanie wideo (Remote Video Process)**. Ta opcja może zostać użyta, gdy zdarzenia wideo nie są wyświetlane.

- **Resetuj aplikację kontrolującą zdalne procesy wideo (Reset remote video process applications control)** pozwala systemowi przerwać aplikację Kontroli (nagrywanie, zdarzenia, wzory, etc.), a następnie automatycznie zresetować aplikację **Zdalne procesowanie wideo (Remote Video Process)**.

- **Logi błędów procesowania wideo (Log Video process error)** pozwala systemowi zachować rejestr wszystkich błędów procesowania w plikach serwera EntraPass. Lokalizacja: C:\Program files\Kantech\Server_CE\Bin\Log. Każda aplikacja generuje log:

- RVP_LOG_00.txt (błędy wygenerowane przez RVP0.exe)

- RVPPoll_LOG_01.txt (błędy wygenerowane przez RVPPOLL1.exe)

- RVPEvent_LOG_02.txt (błędy wygenerowane przez RVEVENT3.exe)

- RVPRecord_LOG_03.txt (błędy wygenerowane przez RVPRECORD3.exe).

- RVPControl_LOG_04.txt (błędy wygenerowane przez RVPCONTROL4.exe). System wygeneruje tyle logów, ile w danym momencie działa aplikacji (RVPControl_LOG_05 do 08).

Snap:

Opcja Snap pozwala na określenie jakości obrazu, który będzie wyświetlany w miniaturze.

- Snap obrazu wideo (Video image snap) określa jakość obrazu, który zostanie zapisany jako miniatura dla każdego wideo. Jeżeli wybierzesz 10, jakość będzie bardzo słaba; 100 oznacza doskonałą jakość.



EntraPass - Instrukcja instalacji i obsługi programu Opcje



Intellex:

Opcja Intellex pozwala zdefiniować dopuszczalną przepustowość dla procesowania wideo (tylko dla Intellex).

o **Wyłącz DirectX**, wyłączy DirectX, czyli technologię Windows, która umożliwia osiągnięcie lepszej wydajności przy pracy lub przeglądania grafiki albo innej treści multimedialnej, w tym wideo oraz dźwięku. Domyślnie: DirectX jest wyłączony.

Notatka: system wykorzysta więcej zasobów systemowych, kiedy DirectX jest wyłączony.

o Określ przepustowość wideo (**Limit video bandwidth**) pozwala ograniczyć/zwiększyć przepustowość wymaganą do strumieniowania wideo na żywo bez wpływania na wydajność sprzętu. Zakres: od 64 KB/s do 8192 KB/s. Określona wartość będzie się odnosić do wszystkich stacji roboczych, w tym serwera EntraPass. Wartość może zostać zmieniona lokalnie dla poszczególnych stacji roboczych: Opcje > pasek narzędzi > Urządzenia multimedialne > Wideo.

o **Opóźnienie zapisu Video Vault (Video vault save delay)** jest wykorzystywane do określenia opóźnienia czasowego, zanim nagranie z Video Vault zostanie odtworzone.

Notatka: wartość dla stacji roboczej nie może przekraczać wartości dla serwera EntraPass.

HDVR:

o **Opóźnienie zapisu Video Vault (Video vault save delay)** jest wykorzystywane do określenia opóźnienia czasowego, zanim nagranie z Video Vault zostanie odtworzone.

TVR:

o **Opóźnienie zapisu Video Vault (Video vault save delay)** jest wykorzystywane do określenia opóźnienia czasowego, zanim nagranie z Video Vault zostanie odtworzone.

Synchronizacja czasu w systemie (Time Parameters)

Sekcja Czas pozwala określić, która bramka zostanie wykorzystana do automatycznego dopasowania czasu dla wszystkich komputerów podłączonych do serwera EntraPass. Funkcja jest przydatna przy zarządzaniu oddalonymi od siebie obiektami.

Notatka: bramka sprawdza pierwszy kontroler pierwszego obiektu o 5:47 albo 17:47, 1:47 albo 13:47, 7:47 albo 19:47, aby określić czas kontrolera.

• **Brak dopasowania czasu (No time adjustment)** wyłącza opcję.

• **Przez bramkę (By Gateway)** automatycznie zsynchronizuje czas dla wszystkich komputerów przez bramkę wybraną z listy.

• **Przez serwer (By Server)** automatycznie zsynchronizuje czas dla wszystkich komputerów z regularnymi przedziałami. Musisz określić częstotliwość odświeżania. Zakres: 1 do 9999 godzin.



Parametry definiowania kart (Credentials Parameters)

Karta (Card)

Dzięki zakładce Karta, Administrator Systemu będzie miał możliwość przeniesienia swojego systemu EntraPass do zaawansowanego zarządzania użytkownikami, gdzie użytkownicy są zarządzani poprzez swoje nazwy oraz numery kart. Każdy użytkownik karty będzie zarządzany poprzez nazwę użytkownika i przez 5 różnych numerów. Umożliwi to tworzenie kart, bez przypisywania nowym kartom numerów. Zobacz: **Wprowadzanie nowej karty w Zaawansowanym zarządzaniu (Issuing a New Card in Enhanced User Management Environment)**. Ta opcja będzie wykorzystywana razem EntraPass Web. Zobacz: **Pomoc EntraPass Web (EntraPass Web Help)**.

Notatka: umożliwienie przejścia do zaawansowanego zarządzania użytkownikiem jest nieodwracalne przy wykorzystaniu oprogramowania. Jednakże, kiedy system przenosi dane, kopia zapasowa jest utworzona w EntraPass, aby mógł być przywrócony do poprzedniego działania.

- **Przenieś do zaawansowanego zarządzania (Migrate to enhanced user management):** domyślnie – zaznaczona. Zobacz: **Wprowadzanie nowej karty w Zaawansowanym zarządzaniu (Issuing a New Card in Enhanced User Management Environment)**.

Stacja robocza oraz serwer (Workstation and Server)

Przyciski paska narzędzi (Toolbar Buttons)

Rozmiar przycisków paska narzędzi może zostać zwiększony 2,5 krotnie, aby polepszyć czytelność tekstu. Możliwe dla Serwera EntraPass oraz stacji roboczej EntraPass. Przełoguj się, aby wprowadzić zmiany.

Przypisz Nowe Połączenie albo Obiekt (Assign a New Connection to a Site)

Notatka: zobacz Konfigurowanie połączenia, aby dowiedzieć się więcej.

Aby włączyć/wyłączyć funkcję, wybierz:

- **Zgłoszenie (Prompt):** system poprosi użytkownika o określenie obiektu, do którego ma się podłączyć przy tworzeniu nowego połączenia.
- **Obowiązkowy (Mandatory):** system poprosi użytkownika o określenie obiektu, do którego ma się podłączyć (obowiązkowo) przy tworzeniu nowego połączenia.
- **Wyłącz (Disable):** domyślne.

Notatka: nie powstaną żadne odniesienia do stref wirtualnych, o ile przynajmniej jedna nie została utworzona wcześniej (zobacz Konfigurowanie obiektu).



Integracja (Integration)

Zakładka **Integracja** pozwala użytkownikowi na wybranie podzespołów, które zostały zintegrowane z EntraPass przez Kantech.

Rejestracja DLL (DLL registration): Dostępne DLL w tym menu zostaną wykorzystane do określenia, jaki typ podzespołów klient podłączy do EntraPass.

- Kliknij **Dodaj**, aby zintegrować następne DLL. Zobacz: **Konfiguracja integrowanych paneli (Integrated Panel Configuration)**.

Notatka: integracja DLL musi zostać wykonana na serwerze EntraPass, aby skomunikować się z multi obiektową bramką, gdzie fizycznie są podłączone oraz zasilane elementy zewnętrzne.

Wirtualna klawiatura (Virtual keypad): ta zakładka pozwala użytkownikowi dostosować wyświetlanie ekranu wirtualnej klawiatury. Trzy tryby wyświetlania mogą zostać wybrane: **Niezakotwiczony**, **Modalny** albo **Zawsze na wierzchu (Floating, Modal or Stay on top)**.

Interfejs Web (Web Interface)

Zakładka Web (Web tab)

Przy pomocy przycisku **Interfejs Web (Web interface)** możesz skonfigurować parametry EntraPass Web.

- **Podgląd wiadomości w EntraPass Web (Allow messages to EntraPass Web):** zaznacz, aby umożliwić użytkownikowi na podgląd wiadomości w EntraPass Web.
- **Maksymalna ilość wiadomości (Maximum web messages):** wybierz maksimum z licznika.
- **Szerokość PEN pada (Signature pad pen width):** wybierz wartość szerokości dla PEN wykorzystywanego z padem.
- **Maksymalna ilość raportów równoczesnych w sesji (Maximum request simultaneously by session):** wybierz maksymalną liczbę raportów, które mogą być wykonywane jednocześnie.
- **Filtry wiadomości (Message filter for web messages):** z listy wybierz filtr do wyświetlenia.
- **Proporcje identyfikatora obrazu (Badge image ratio for web):** możesz zwiększyć jakość wydruku obrazu (domyślnie: 2). Zwiększenie proporcji zwiększa wielkość pliku.

Zakładka Dostosowania Web (Web Customization tab)

- **Kolor (Custom color):** kliknij, aby zmienić kolor interfejsu.
- **Logo strony (Page logo):** kliknij, aby dodać (lub zmienić) logo w lewym-górnym rogu interfejsu.



EntraPass - Instrukcja instalacji i obsługi programu Opcje

Zakładka go Pass

Jeśli zarejestrujesz aplikację mobilną go Pass, pojawi się karta go Pass. Użyj go Pass ze smartfonem lub zegarkiem Apple, aby zablokować lub odblokować drzwi. Dla wygody można sterować drzwiami z odległej lokalizacji.

Aby zapewnić wyższy poziom bezpieczeństwa, użyj czytnika ioSmart z drzwiami, czytniki ioSmart wykorzystują technologię BLE. Dostosuj się do różnych poziomów bezpieczeństwa, wybierz opcję z listy Ograniczenia zbliżeniowe.

1 - Aby wyświetlić zaszyfrowany profil osobisty posiadacza karty w wiadomościach e-mail z powiadomieniem, wybierz opcję **Wyświetl widoczne informacje powiadomień**. Posiadacze kart wykorzystują dane swojego profilu osobistego lub link w e-mail, aby uzyskać dostęp do aplikacji go Pass.

2 - Aby ponownie wysłać wszystkie wiadomości e-mail z powiadomieniem o przekazaniu do wszystkich ważnych użytkowników karty, kliknij **Prześlij ponownie powiadomienia GoPass dla wszystkich posiadaczy ważnych kart**

3 - Aby kontrolować, jak i kiedy SmartLink reaguje na nieprawidłowe polecenia go Pass, zdefiniuj wszystkie trzy ustawienia w obszarze **ochrona**:

a - Aby ustawić liczbę nieprawidłowych żądań, które wystąpią zanim SmartLink odpowie, wprowadź liczbę w **Odesłanie powiadomienia na niewłaściwe żądanie**.

b - Aby ustawić czas, po upływie którego SmartLink odpowie, wprowadź liczbę w **Opóźnienie dbounce (ss)**.

c - Aby uniemożliwić SmartLink reagowanie na żądanie przejścia przez określony czas, wprowadź wartość w polu **Wyłącz GoPass na powiadomienie (m: ss)**.

Na przykład # niepoprawnych żądań w ciągu # sekund = # sekund przed odpowiedzią SmartLink na przejście request + event Zbyt wiele przejść Wyświetlenie nieudanych żądań.

4 - Wybierz jedną z następujących opcji z listy Ograniczenia zbliżeniowe:

- Brak - nie ma ograniczeń, posiadacz karty go Pass może zablokować i zdalnie odblokować drzwi oraz na drzwi. EntraPass ignoruje technologię BLE.
- Ścisłe (tylko ioSmart BLE) - jeśli posiadacz karty go Pass go przejdzie, przejdź przez czytnik ioSmart, idź Posiadacz karty Pass musi znajdować się w zasięgu drzwi.
- Hybrid (BLE, gdy jest dostępny) - użyj dla posiadaczy kart go Pass, którzy mają dostęp do czytników ioSmart czytniki inne niż ioSmart. Jeśli posiadacz karty go Pass znajduje się przy drzwiach ioSmart, posiadacz karty musi być w środku

zasięg, jeśli jest to drzwi inne niż ioSmart, posiadacz karty może zdalnie sterować drzwiami.

UWAGA: Jeśli nie wybierzesz pola wyboru BLE w szablonie czytnika, którego używa kontroler,

Wybór ograniczeń zbliżeniowych jest zbędny.

Synchronizacja czasu w systemie (Time Parameters)

Sekcja Czas pozwala określić, która bramka zostanie wykorzystana do automatycznego dopasowania czasu dla wszystkich komputerów podłączonych do serwera EntraPass. Funkcja jest przydatna przy zarządzaniu oddalonymi od siebie obiektami.

Notatka: bramka sprawdza pierwszy kontroler pierwszego obiektu o 5:47 albo 17:47, 1:47 albo 13:47, 7:47 albo 19:47, aby określić czas kontrolera.

- **Brak dopasowania czasu (No time adjustment)** wyłącza opcję.
- **Przez bramkę (By Gateway)** automatycznie zsynchronizuje czas dla wszystkich komputerów przez bramkę wybraną z listy.



EntraPass - Instrukcja instalacji i obsługi programu

Opcje

- **Przez serwer (By Server)** automatycznie zsynchronizuje czas dla wszystkich komputerów z regularnymi przedziałami. Musisz określić częstotliwość odświeżania. Zakres: 1 do 9999 godzin.

Format nazwy użytkownika karty (User Name Format)

Określenie formatu nazwy użytkownika poinstruuje system, jak nazwa użytkownika karty będzie wyświetlana w EntraPass.

- **Parsuj nazwę użytkownika (Parse user name):** powinno zostać zaznaczone, jeżeli chcesz wybrać metodę parsowania nazwy użytkownika w systemie.
- **Format nazwy użytkownika karty (User Name Format)** pozwala wybrać metodę parsowania. Opcje: Zaczynij od nazwiska; Zaczynij od imienia.
- **Parsuj nazwę użytkownika z (Parse user name with):** pozwala wybrać znak, który zostanie użyty do parsowania pól nazwy użytkownika. Opcje: przecinek, kropka, średnik, dwukropek, spacja. .

Notatka: przed wersją EntraPass 3.18, system korzystał z metody wyszukiwania, która wymagała od Administratora wprowadzenia konkretnych wartości granicznych (dolna/górna) do określenia zasad wyszukiwania. Na przykład, aby wygenerować raport, który zawierałby wszystkich użytkowników z nazwiskiem zaczynającym się na A, dolna wartość graniczna powinna zostać określona na „A”, a górna „AZZZZ”. Teraz system ten sam rezultat po wprowadzenia „A” dla obu wartości granicznych.



Serwer EntraPass

Aplikacja

Menu **Aplikacja (Application)** pozwala użytkownikowi na podgląd różnych list, które pokazują statusy działań pomiędzy serwerem EntraPass, a stacjami roboczymi podłączonymi do niego.

Podgląd aplikacji podłączonych do serwera (Viewing Applications Connected to the Server)

Użytkownicy mogą sprawdzić status wszystkich aplikacji EntraPass z poziomu interfejsu serwera.

1 – W aplikacji EntraPass wybierz **Aplikacja (Application)**.

2 – Kliknij na strzałkę obok każdej stacji roboczej, aby sprawdzić szczegóły dotyczące stacji roboczej (kody, adres TCP/IP, połączenia, etc.)

Błędy w systemie (Error Log)

Błędy systemowe są wyświetlane z datą i czasem, kodem, nazwą stacji roboczej, na której miał miejsce błąd, kod błędu oraz opisem.

1 – Aby zobaczyć wszystkie błędy, które wystąpiły w systemie wybierz przycisk **Błędy w systemie (Error log)** z menu **Serwer (Server)**.

2 – Kliknij na **Filtr tekstu (Text filter)**, aby wyświetlić okno Filtra tekstu. Wprowadź ciąg tekstu (np. Kantech), a system wyświetli tylko logi zawierające określony tekst.

3 – Kolumny:

- Data i czas: ustawione sekwencyjnie, wprowadzenie innej metody przerywa sekwencyjność.
- Kod: po wybraniu, kolumny będą sortowane według kolumny **Kod (Code)** w porządku alfabetycznym.
- Stacja robocza: po wybraniu, kolumny będą sortowane według kolumny **Stacja robocza (Workstation)** w porządku alfabetycznym.
- Kod błędu: po wybraniu, kolumny będą sortowane według kolumny **Kod błędu (Error Code)** w porządku alfabetycznym.
- Opis: po wybraniu, kolumny będą sortowane według kolumny **Opis (Description)** w porządku alfabetycznym.

4 – Przy pomocy menu prawego przycisku możesz zmienić tło okna oraz usunąć wszystkie wyświetlane dane.

Notatka: możesz eksportować logi do pliku CSV. Aby tego dokonać kliknij prawym w oknie i wybierz Eksportuj CSV z menu skrótów.



Zdarzenia systemowe (Log)

Okno **Zdarzenia systemowe (Log)** zawiera wszystkie zdarzenia logowania (oraz wyjścia) do wszystkich stacji roboczych określonych w systemie. Logi są wyświetlane z datą i czasem, nazwą stacji roboczej, nazwą użytkownika, który korzysta ze stacji roboczej oraz typem logu. Okno **Zdarzenia systemowe (Log)** zawiera wszystkie zdarzenia logowania (oraz wyjścia) do wszystkich stacji roboczych określonych w systemie.

1 – Aby zobaczyć wszystkie logi, wybierz przycisk **Zdarzenia systemowe (log)** z menu **Serwer (Server)**.

2 – Kliknij na **Filtr tekstu (Text filter)**, aby wyświetlić okno Filtra tekstu. Wprowadź ciąg tekstu (np. Kantech), a system wyświetli tylko logi zawierające określony tekst.

3 – Kolumny:

- Data i czas: ustawione sekwencyjnie, wprowadzenie innej metody przerywa sekwencyjność.
- Stacja robocza: po wybraniu, kolumny będą sortowane według kolumny **Stacja robocza (Workstation)** w porządku alfabetycznym.
- Nazwa użytkownika: po wybraniu, kolumny będą sortowane według kolumny **Nazwa operatora (Operator name)** w porządku alfabetycznym.
- Transakcje: po wybraniu, kolumny będą sortowane według kolumny **Transakcje (Transaction)** w porządku alfabetycznym.

4 – Możesz zmienić kolor tła, klikając prawym w oknie i wybierając **Kolor tła (Background colour)** z listy.

5 – Aby usunąć wszystko z okna, wybierz **Usuń wszystko (Delete all)** (menu pojawi się po kliknięciu prawym w oknie)

Notatka: możesz eksportować logi do pliku CSV. Aby tego dokonać kliknij prawym w oknie i wybierz Eksportuj CSV z menu skrótów.



Rejestracja aplikacji (Registration)

To menu jest wykorzystywane do zarejestrowania nowych komponentów, takich jak KTES, Stacja robocza, Bramka, SmartLink, etc.

Zobacz: **Rejestracja Systemu** ([System Registration](#)), aby zarejestrować i wykorzystać bazę danych systemu oraz aby ustalić komunikację z serwerem.

Logi raportów Historia generowania raportów (Report Log)

Okno **Historia generowania raportów (Report Log)** pozwala na podgląd szczegółowej listy całej historii raportów przetworzonych przez system.

1 – Aby zobaczyć wszystkie Logi raportów, wybierz przycisk **Historia generowania raportów (Report log)** z menu **Raport (Report)**.

2 – Kliknij na **Filtr tekstu (Text filter)**, aby wyświetlić okno Filtra tekstu. Wprowadź ciąg tekstu (np. Kantech), a system wyświetli tylko logi zawierające określony tekst.

3 – Kliknij przycisk **Odśwież**, aby zaktualizować wyświetlane dane.

4 - Kolumny:

- **Data zgłoszenia:** ustawione sekwencyjnie, wprowadzenie innej metody przerywa sekwencyjność.
- **Zgłoszone przez:** po wybraniu, kolumny będą sortowane według kolumny **Zgłoszone przez (Requested by)** w porządku alfabetycznym.
- **Nazwa raportu:** po wybraniu, kolumny będą sortowane według kolumny **Nazwa raportu (Report name)** w porządku alfabetycznym.
- **Data od:** po wybraniu, kolumny będą sortowane według kolumny **Data od (Date from)** w porządku alfabetycznym.
- **Data do:** po wybraniu, kolumny będą sortowane według kolumny **Data do (To Date)** w porządku alfabetycznym.

5 – Aby usunąć wszystko z okna, wybierz **Usuń wszystko (Delete all)** (menu pojawi się po kliknięciu prawym w oknie)

6 - Pola:

- **Typ raportu (Report Type):** pokazuje typ raportu.
- **Procesowane przez (Process By):** pokazuje, która aplikacja wykonała raport.
- **Stacja robocza dodana (Workspace applied):** pokazuje, czy stacja robocza została dodana.
- **Przeznaczenie (Destination):** pokazuje, gdzie raport został dostarczony.
- **Wykorzystany szablon (Used Template):** pokazuje wszystkie dll wykorzystane przy raporcie.
- **Tematy w raporcie (Items in report):** ilość tematów w raporcie.
- **Data zgłoszenia (Requested date):** data i czas zgłoszenia potrzeby raportu.
- **Data kolejowania (Queued date):** pokazuje, kiedy raport został dodany do kolejki generowania raportów (data, czas i czas oczekiwania).
- **Data procesowania (Process date):** pokazuje, kiedy proces został rozpoczęty.
- **Data dostarczenia (Delivery date):** pokazuje, kiedy raport został dostarczony.
- **Data zakończenia (Completion date):** pokazuje datę końcową i czas wykonania raportu.
- **Stan zakończenia (Completion State):** pokazuje, czy raport został ukończony z sukcesem, czy nie.



Kopia systemu (Backups)

Kopia systemu to kopia zapasowa bazy danych twojego systemu, która służy jako zastępstwo albo alternatywa w przypadku awarii komputera. Wykonanie kopii zapasowej chroni przez przypadkową utratą danych, kiedy dojdzie do uszkodzenia dysku albo przypadkowego nadpisania lub usunięcia danych. Możesz przywrócić kopię zapasową na innym komputerze, na którym zainstalowany jest serwer EntraPass.

Kopia zapasowa EntraPass pozwala użytkownikowi na wykonanie manualnego utworzenie kopii zapasowej bazy danych: danych systemowych (D), archiwów (A), Wej/Wyj (T) oraz nagrań (V). Przydatne wskazówki:

- Twórz kopię zapasową swoich plików regularnie, przynajmniej raz w tygodniu.
- Rekomendujemy utworzenie dwóch kopii zapasowych twoich plików bazy danych. Zapisz je w osobnych lokalizacjach.
- Aby utworzyć kopię zapasową, możesz wykorzystać:

o menu zakładki Serwer/Kopia zapasowa,

o **Terminarz kopii zapasowej (Backup Scheduler)**,

o inne oprogramowanie lub podzespoły zewnętrzne (nie zalecamy oprogramowania zewnętrznego).

Notatka: domyślnie, kiedy zachowujesz albo odtwarzasz plik, Baza danych EntraPass będzie czasowo wyłączona. W głównym oknie aplikacji EntraPass będziesz mógł zauważyć, że drugi kwadrat w prawej-dolnej części ekranu zmieni kolor na czerwony – oznacza to, że baza danych jest niedostępna. Modyfikacje przeprowadzone na stacjach roboczych nie zostaną wprowadzone do bazy danych, dopóki nie będzie ona znowu dostępna.

Wszystkie dane systemowe są zlokalizowane w C:\Program Files\Kantech\ Server_CE\XXXX. Jeżeli korzystasz z programów zewnętrznych do tworzenia kopii zapasowych, zaleca się utworzenie kopii zapasowych wszystkich katalogów i podkatalogów Kantech. Za każdym razem, gdy tworzona jest kopia zapasowa (nawet automatycznie), nowy podkatalog z danymi jest dodawany.

Tworzenie kopii zapasowych typu D, A, T oraz V (Creating Backups of Type D, A, T and V)

Domyślnie, nazwa folderu, w którym zapisywane są bazy danych: dane/archiwa/wej-wyj/nagrania; jest generowana automatycznie według następującej zasady: X_YYYY_MM_DD_h_mm_ss, gdzie X oznacza typ danych (D – dane, A – archiwa, T – Wej/Wyj, V – nagrania). Poniżej przedstawione są poszczególne kroki, aby stworzyć kopię zapasową.

1 – Wybierz, dla jakiego elementu chcesz wykonać kopię zapasową (D, A, T, V). System wyświetli podkatalog, w którym informacje zostaną zapisane. Możesz zachować folder domyślny albo wybrać dowolne miejsce na dysku.

Notatka: domyślnie, system/stacja robocza zapisuje wszystkie informacje pochodzące z: C:\Program files\Kantech\Server_CE\Data albo Archive albo In/Out pod adresem C:\Program files\Kantech\Server_CE\Backup\X_YYYY_MM_DD_h_mm_ss, gdzie X oznacza typ danych. Następnie określony jest rok, miesiąc, dzień oraz dokładny czas wykonania zapisu.

2 – Wybierz typ kopii zapasowej:



EntraPass - Instrukcja instalacji i obsługi programu Serwer EntraPass

o Osobne pliki: wykonana kopię zapasową bazy danych plik po pliku. Kopia zapasowa zawiera także plik Regdata.ini z informacjami identyfikującymi: oprogramowanie (oraz jego wersja) wykorzystane do tworzenia kopii zapasowej, typ kopii zapasowej, użytkownika zgłaszającego potrzebę utworzenia kopii zapasowej, datę i czas utworzenia kopii zapasowej.

o Samorozpakowujący się skompresowany plik: utworzy plik wykonywalny (*.exe), który skompresuje informacje, aby zredukować ilość miejsca na dysku zajmowaną przez kopię zapasową. System wyświetla informacje identyfikujące kopię zapasową: oprogramowanie (oraz jego wersja) wykorzystane do tworzenia kopii zapasowej, typ kopii zapasowej, użytkownika zgłaszającego potrzebę utworzenia kopii zapasowej, datę i czas utworzenia kopii zapasowej.

Notatka: jeśli samemu chcesz skorzystać z pliku .exe, aby przywrócić samorozpakowującą się kopię zapasową, upewnij się, że kod systemu EntraPass jest taki sam, jak ten w pliku .exe. W innym przypadku rozpakowanie nie powiedzie się. W przypadku awarii systemu, kiedy dane EntraPass oraz aplikacja nie są dostępne, zalecamy przeinstalowanie EntraPass i skorzystanie z funkcjonalności przywracania, zamiast korzystania z pliku .exe.

3 – Z listy Dyski (Drives), wybierz dysk, na którym zostanie przeprowadzona operacja. Wybór jest zależny od ustawień twojego komputera.

4 – Możesz kliknąć Nowy folder (New folder), jeżeli chcesz określić nowy folder przeznaczania.

5 – Kliknij OK, aby rozpocząć procedurę. Proces może być sprawdzany w dolnej części okna.

Notatka: możesz skorzystać z programu terminarza kopii zapasowej (Backup Scheduler), aby ustawić terminarz albo zaplanować automatyczne tworzenie kopii zapasowej. Aby ustawić automatyczne tworzenie kopii zapasowej zobacz Terminarz kopii zapasowej (Backup Scheduler). Kiedy wykonujesz kopię zapasową albo przywracasz plik, bazy danych serwera są niedostępne. Nie możesz modyfikować baz danych, kiedy trwa proces tworzenia kopii zapasowej.

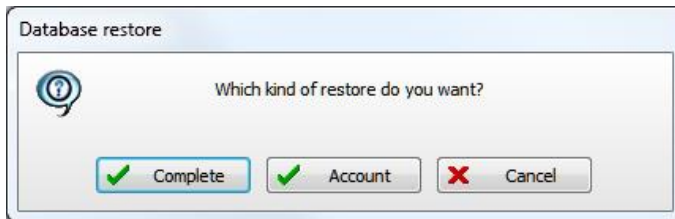


Odtworzenie kopii (Restores)

Jeżeli przywracasz dane, zaleca się wykonanie kopii zapasowej! Jeżeli korzystasz z programów zewnętrznych do tworzenia kopii zapasowych, zaleca się utworzenie kopii zapasowych wszystkich katalogów i podkatalogów Kantech.

1 – Z zakładki **Kopia zapasowa (Backup)**, wybierz przycisk **Przywróć (D, A, T, V) (Restore)**. System wyświetli okno **Przywróć dane (Restore data)**. Zawiera ono adres katalogu kopii zapasowej.

2 – Aby zmienić folder przeznaczenia, sprawdź listę Dysków (Drives). Kliknij OK, aby rozpocząć proces przywracania.



3 – Kiedy klikniesz przycisk Zakończ (Complete), system przywróci wszystkie informacje z wybranego folderu.

Notatka: domyślnie, system przywraca wszystkie informacje pochodzące z: C:\Program files\Kantech\Server_CE\Backup\X_YYYY_MM_DD_h_mm_ss; do C:\Program files\Kantech\Server_CE\Data albo Archive albo In/Out.

Notatka: zaleca się przeładowania bramki po przywróceniu danych (Operacja > Przeładuj dane).



Format wyświetlania numeru karty (Defining a Card Display Format)

System EntraPass może obsługiwać wiele rodzajów czytników. Zależnie od rodzaju czytnika, format wyświetlania karty może się różnić. Okienko **Format wyświetlania (Display format)** pozwoli ci określić format, który będzie automatycznie ustawiany w momencie tworzenia nowej karty.

1 – Na pasku narzędzi Opcje, kliknij przycisk **Format wyświetlania (Display format)**.

Notatka: sekcje Karta #1-5 nie zostaną wyświetlone, o ile opcja Zaawansowanego zarządzania nie jest włączona.

2 – Wybierz format dla **Karty #1**.

- **Dziesiętny (Decimal)**
- **Ósemkowy (Octal)**: każda cyfra ósemkowa odpowiada dokładnie trzem cyfrom binarnym. Format ósemkowy do zapisu używa ośmiu cyfr, od 0 do 7. Programy często wyświetlają dane w tym formacie, ponieważ jest stosunkowo czytelny dla użytkowników i łatwo tłumaczy się na format binarny.
- **Szesnastkowy (Hexadecimal)**: każda cyfra odpowiada czterem cyfrom binarnym. Format szesnastkowy do zapisu używa 16 znaków: cyfr, od 0 do 9; oraz liter od A do F. Na przykład liczba 15 (format dziesiętny) jest wyrażona jako F w szesnastkowym. Programy często wyświetlają dane w tym formacie, ponieważ jest łatwiejszy w odczycie dla użytkownika niż system binarny.
- **FIPS (Federal Information Processing Standard)**, czyli publicznie ogłaszany standard federalnego rządu Stanów Zjednoczonych. Ten format może korzystać z danych > 32 bity.

3 – Zaznacz pole **Użyj formatu wielu kart (Use multiple card format)**, jeżeli twoje środowisko działania zawiera wiele typów czytników i chcesz mieć możliwość wyboru typu czytnika (innego niż domyślny), przy tworzeniu nowej karty.

4 – Wybierz jeden z procesów **Duplikacji numeru PIN (Duplicate PIN)**.

- **Brak powielenia (No duplication)**: błąd wyświetla się na stacji roboczej; pole PIN zostanie zresetowane do wartości domyślnej (00000) oraz zostanie podświetlone. Wprowadź nowy, ważny numer PIN. Tylko PIN 00000 zostanie powielony, niezależnie od ustawień.
- **Powiadom o powieleniu (Notify when duplication)**: serwer sprawdza, czy numer PIN istnieje. Jeżeli istnieje, pojawia się pole z wiadomością, informującą o tym. Przycisk **Szczegóły** pozwoli wyświetlić listę użytkowników karty, którym został przypisany ten PIN.
- **Powielenie (Duplication)**: nie zostanie przeprowadzone żadne sprawdzenie, PIN zostanie zaakceptowany nawet, jeżeli jest powielony.

5 – **Długość numeru PIN (tylko KT-400) (Number of PIN digits)**: możesz wybrać długość: 4, 5 lub 6 znaków (Zobacz: **Definiowanie Opcji Karty (Card Options Definition)**).

Notatka: numer PIN musi zostać ustawiony oraz zachowany, aby uniemożliwić duplikację w przypadku utraty danych lub uzupełnienia przez system.

6 – Gdy wybrano opcję **Zaawansowanego zarządzania (Enhanced User Management)**, wybierz alternatywny format wyświetlania dla **Karty #2**. Powtórz Krok 6 dla **Karty #3**, **Karty #4** oraz **Karty #5**.



EntraPass - Instrukcja instalacji i obsługi programu Serwer EntraPass

7 – Aby określić ogólny format wyświetlania dla KT-100, KT-300 oraz KT-400, wybierz odpowiednią opcję:

- **24-bit Wiegand, 5-cyforwy PIN (domyślnie KT-200):** do 24-bitów dla KT-100, KT-200, KT-300 oraz KT-400.
- **32-bit, 5-cyforwy PIN:** do 32 bitów dla KT-100, KT-300 oraz KT-400.
- **24-bit Wiegand, 6-cyforwy PIN:** do 24-bitów dla KT-100, KT-300 oraz KT-400.
- **Do 16 znaków ABA, 6-cyforwy PIN:** do 16 dla KT-100, KT-300 oraz KT-400.

Notatka: kontrolery KT-100, KT-300 oraz KT-400 wykonają twardy reset przy zmianie formatu karty. Unikaj zmiany formatu karty, ponieważ może się to wiązać z utratą informacji.



Zmiana format wyświetlania kart z 24 bit do 32 bit (Changing from a 24 bit to 32-bit Global Card Format)

Zmiana z 24-bitowego na 32-bitowy format globalnej karty zwiększa ilość kart, które można skonfigurować w EntraPass.

26-bitowy czytnik Wiegand ioProx nie obsługuje zmiany globalnego formatu karty z 24-bitowej na 32-bitową. Jeśli masz połączenie 26-bitowych czytników Wiegand ioProx XSF i ioProx, nie zmieniaj ręcznie formatu lub włącz funkcję automatycznej konwersji. Najpierw musisz zastąpić 26-bitowe czytnikami XSF.

Aby ręcznie zmienić format 24-bitowej na 32-bitową kartę globalną, wykonaj następujące kroki:

- 1 - Kliknij kartę Opcje i wybierz z menu Format wyświetlania.
- 2 - W obszarze Format karty globalnej wybierz kartę 32-bitową, 5-cyfrową opcję PIN.
- 3 - Kliknij OK. Jeśli dokonałeś zmiany z 24-bitowej karty Wiegand, pięć lub sześć cyfr, na kartę 32-bitową, pięć cyfr PIN, monit wyświetlający pytanie, czy karty muszą zostać przekonwertowane na 32-bitowy family code.

- Jeśli klikniesz Tak, wprowadź wartość rozszerzonego kodu obiektu. (HH)
- Po kliknięciu przycisku Nie zostanie wyświetlony monit o włączenie funkcji automatycznej konwersji.

UWAGA: Możliwość zmiany formatu karty globalnej z 24-bitowej na 32-bitową nie jest dostępna, gdy uruchomiony z serwera redundantego. EntraPass nie tworzy kopii zapasowych danych automatycznie po przełączeniu z formatu 24-bitowego na 32-bitowy.

W stacji roboczej EntraPass tworzy kopię zapasową systemu przed konwersją.

Po zmianie formatów KT-100, KT-200 i KT-300 automatycznie wykonują twardy reset. Dla KT-1 i KT-400 zmiana jest płynna.

Automatyczna konwersja

Po zaznaczeniu pola wyboru Użyj auto konwersji dla kart 24-bit wyświetlania okno, EntraPass automatycznie konwertuje wszystkie karty do formatu karty 32-bitowej. Wartość domyślna zostanie wyczyszczona. Aby włączyć to pole wyboru, musisz ustawić format karty globalnej na 32-bitową kartę, 5-cyfrową opcję PIN. Po wybraniu funkcji automatycznej konwersji i użyciu karty która nie ma formatu 32-bitowego, msystem automatycznie modyfikuje numer karty. Wydarzenia muszą być łagodnymi zdarzeniami. Ta funkcja jest dostępna w bramie multi-site gateway, global gateway i brama KT-NCC.

UWAGA: Funkcja automatycznej konwersji jest dostępna podczas uruchamiania serwera nadmiarowego.



Modyfikacja hasła do rejestracji aplikacji (Connection Password Modification)

Hasło połączenia jest wykorzystywane do autentyfikacji stacji roboczej EntraPass przy serwerze EntraPass. Okno hasła połączenia wyświetla się automatycznie, gdzie system nie został jeszcze zarejestrowany.



CAUTION:
Keep in mind that there is no way to reset the connection password if forgotten after its modification.

Notatka: jeśli w celach autentyfikacji nie korzystasz z hasła, użytkownik będzie musiał skorzystać z głównego, domyślnego hasła w celu autentyfikacji stacji roboczej. Domyślne hasło połączenia to kantech (zwróć uwagę na wielką/małą literę).

Zmianie hasła połączenia (Changing the Connection Password)

- 1 – Z głównego okna Opcji, wybierz przycisk **Hasło połączenia (Connection password)**.
- 2 – Wprowadź obecne hasło (wielkość liter ma znaczenie), w polu **Stare hasło (Old authentication password)**. Domyślne: kantech.
- 3 – Wprowadź nowe hasło autentyfikacji w polu **Nowe hasło (New authentication password)**.
- 4 – Potwierdź nowe hasło w polu **Potwierdź hasło (Verify authentication password)**.
- 5 – Kliknij OK. Jeżeli pojawi się wiadomość o błędzie, upewnij się, że dane, które wpisałeś w pola **Nowe hasło** i **Potwierdź hasło** zostały wprowadzone prawidłowo.

Notatka: hasło połączenia jest inne niż hasło użytkownika. Hasło połączenia jest wykorzystywane do autentyfikacji stacji roboczej, podczas, gdy hasło użytkownika jest wykorzystywane do otwarcia sesji.

Wybór języka (System Language Selection)

EntraPass umożliwia korzystanie z oprogramowania w języku wybranym przez użytkownika. Podstawowe języki to angielski, francuski, hiszpański, niemiecki oraz włoski. **Edytor słownika (Vocabulary Editor)** pozwala dodawać nowe języki.

Zmianie języka systemu (Changing the System Language)

- 1 – Z głównego okna EntraPass wybierz pasek narzędzi **Opcje**, a następnie kliknij przycisk **Wybierz język**.

Notatka: jeśli wprowadzasz zmianę głównego języka, operacje na bazie danych zostaną przerwane, a zmiany wejdą w życie po zrestartowaniu systemu. Język bazy danych zostanie zmodyfikowany według wartości ASCII głównego języka. Znaki specjalne w różnych językach mogą mieć wpływ na bazę danych!

- 2 – Z listy **Wybierz język główny (Select primary language)** wybierz język główny. Z listy **Wybierz drugi język (Select Secondary language)**, wybierz drugi język.
- 3 – Przełoguj się w EntraPass.



Ustawienie Daty i Czasu (System Date & Time Modification)

Opcja Zmiana systemu (Change system) powinna być wykorzystywana wyłącznie, gdy jest to niezbędne. Może mieć negatywny wpływ na logiczne komponenty systemu dostępu (np. terminarze). Jeżeli z jakiegoś powodu chcesz zmienić datę oraz czas systemu, lepiej to zrobić przy pomocy ustawień parametrów systemu (Opcje > Parametry systemu > Dostosowanie czasu).

1 – Z głównego okna Opcji, wybierz Data i Czas.

2 – Wprowadź datę w pole Data, albo wybierz datę z kalendarza. Podłączone komponenty również otrzymają informacje o zmianie daty.

3 – Wprowadź czas w pole Czas. Podłączone komponenty również otrzymają informacje o zmianie daty.

4 – Kliknij OK, żeby wyjść.

Notatka: jeśli chcesz, aby w razie potrzeby system automatycznie zamieniał czas, wykorzystaj zakładkę Dostosowanie czasu w menu Definiowanie parametrów serwera. Zobacz Parametry czasu.

Ważne: nie powinieneś zmieniać czasu przy pomocy ustawień Windows. Rekomenduje się zmianę czasu systemu przez ustawienia parametrów systemu.



Konfiguracja parametrów systemu (System Parameters Configuration)

Okienko Parametry systemu pozwala Administratorowi Systemu na modyfikowanie parametrów, które określają system EntraPass. Okienko może zostać otworzone ze stacji roboczej albo z serwera. Parametry są pogrupowane razem pod różnymi oznaczeniami, np. Serwer, Bramka, Firmware, Obrazy, etc.

Parametry serwera (Server Parameters)

W zakładce Serwer, możesz zdefiniować pojemność serwera pod kątem logów, możliwości diagnostyczne, parametry bezpieczeństwa, alarmy sieciowe, etc.

Serwer e-mail (E-mail Server)

EntraPass oferuje użytkownikom możliwość wysyłania raportów przy pomocy e-maili. Ta funkcja może zostać wykorzystana przy zgłoszeniu prośby o autentyfikację, przez użytkownika, od serwerów SMTP.

Notatka: połączenia z certyfikatem SSL nie są wspierane.

1 - W polu Serwer Email (Email Server): SMTP albo Serwer Zamienny; wprowadź adres IP serwera, który będzie wykorzystywany do wysyłania wiadomości email.

2 – W polu Port Email (Email Port), wprowadź numer portu, który będzie wykorzystywany do wysyłania wiadomości email (zazwyczaj: 25).

3 - Wprowadź adres email w pole Nadawca (Email sender). Ten adres będzie wykorzystywany do autentyfikacji serwera email.

4 - Autentyfikacja (Authentication): te opcje mogą być wykorzystane do konfigurowania metody autentyfikacji.

• Brak autentyfikacji (No authentication)

- **Autentyfikacja SMTP (SMTP authentication):** autentyfikacja, wysłana na port SMTP, musi zostać potwierdzona zanim wiadomość zostanie wysłana.

- **Autentyfikacja POP3 (POP3 authentication):** autentyfikacja, wysłana na port POP3, musi zostać potwierdzona zanim wiadomość zostanie wysłana.

5 – Wyślij do (Send to): adres odbiorcy.

6 – Test (Test button): wysła wiadomość testową z wybranymi parametrami.

Notatka: domyślna wartość portu email jest ustawiona na 25. Możesz zmienić tę wartość (dostępne wartości: 0-65.535). Aby uzyskać więcej informacji skontaktuj się z administratorem sieci.



Automatyczne wyłączanie operatora

Użyj operatora. Funkcja automatycznego wyłączania, aby automatycznie dezaktywować operatora, jeśli nie ma aktywności na ich koncie przez określoną liczbę dni. Wartość domyślna to 90 dni. Po zainstalowaniu EntraPass po raz pierwszy aktualizacji z poprzedniej wersji, ta funkcja jest wyłączona. Po włączeniu autodeaktywacji operatora funkcja o północy sprawdza bazę danych pod kątem aktywnych operatorów i pod nieobecność aktywności, automatycznie wysyła e-mail 10 dni przed dezaktywacją, aby powiadomić operatora o ich wyłączeniu.

UWAGA: Operator musi wypełnić swój e-mail, aby otrzymać e-mail z powiadomieniem. Jeśli ich pole e-mail nie jest kompletne, nie otrzyma powiadomienia e-mailem.

Funkcja samoczynnej dezaktywacji nie dotyczy operatorów LDAP ani domyślnych operatorów EntraPass: administrator, instalator i operator.

Aby zapobiec dezaktywacji, operator musi zalogować się do EntraPass za pomocą stacji roboczej, sieci lub urządzenia mobilnego przed datą dezaktywacji. Jeśli operator jest dezaktywowany, trzeba ręcznie włączyć operatora. To zrób to, kliknij kartę System i kliknij opcję Operator w menu. Wybierz odpowiedniego operatora i wyczyść pole wyboru Operator wyłączony.

W przypadku awarii serwera redundantnego. Jeśli serwer i nadmiarowy serwer jest wyłączony, e-mail nie jest wysyłany, ale Operator jest dezaktywowany zgodnie z planem.

Ustawianie funkcji automatycznego wyłączania operatora

Aby ustawić funkcję automatycznego wyłączania operatora, wykonaj następujące czynności:

- 1** - Kliknij zakładkę **Opcje** i kliknij w menu **Parametry systemu**.
- 2** - W oknie **Parametry systemu** kliknij opcję **Serwer** i kliknij kartę **Reguły hasła**.
- 3** - Zaznacz pole wyboru **Automatycznie dezaktywuj operatora**.
- 4** - W polu **Dni** kliknij strzałki, aby wybrać odpowiednią liczbę dni. Kliknij **OK**. Trzydzieści dni to minimalna ilość dni i 365 dni to maksimum.



Logi serwera (Server Logs)

Możesz określić maksymalną ilość wpisów, które będą przechowywane w logach systemu oraz logach błędów systemu (do 100000). Wpisy zawierają takie transakcje, jak: logowanie do serwera, połączenia/rozłączenia, włączenie/wyłączenie serwera, etc. Te wpisy są przechowywane razem z datą/czasem, informacją o stacji roboczej, informacją o użytkowniku oraz opisem transakcji.

Historia zmian (Audit)

Aby udostępnić funkcjonalność Historii zmian, zaznacz pole wyboru **Włącz historię zmian** i wybierz jedną z opcji następujące opcje przechowywania danych:

- Aby zdefiniować liczbę dni na zachowanie danych z Historii zmian, **Liczba dni przechowywania**. Ustawienie domyślne to 365 dni, minimalna liczba to 30 dni, a maksymalna liczba to pięć lat.
- Aby zdefiniować liczbę rekordów przechowywanych przez system, wybierz liczbę od 1 do 15 w polu **Liczba przechowywanych rekordów**. Ustawienie domyślne to pięć dni.

W obszarze **Komponenty objęte historią zmian** wybierz komponenty, które chcesz wyświetlić w ścieżce Audytu. Po zaznaczeniu pola wyboru **Podstawowa** nazwa komponentu jest dostępna w ścieżce audytu. Jeśli ty zaznaczysz pole wyboru **Wtórny**, informacje o liście komponentów są dostępne w ścieżce audytu.

Przestrzeń dyskowa (Disk Space)

Opcja Przestrzeń dyskowa została opracowana, jako zabezpieczenie przed awarią systemu spowodowaną brakiem miejsca na dysku. Pozwala monitorować ilość wolnego miejsca na dysku dla optymalnego działania systemu oraz generowania raportów. EntraPass daje możliwość przerwania przygotowania raportu, jeżeli zostanie przekroczony próg wolnej przestrzeni dyskowej.

- **Próg wolnej przestrzeni dyskowej (MB) (Disk free space threshold (MB))**: lista: określ maksymalny próg pojemności, po przekroczeniu którego system wyśle wiadomość, że wolna przestrzeń dyskowa spadła poniżej określonej, dopuszczalnej wartości. Wyrażona w mega bajtach. Zakres: od 2000 do 99999 MB.
- **Czas pomiędzy powiadomieniami (Time between notifications (hh:mm))**: wprowadź czas pomiędzy powiadomieniami w momencie, gdy wolna przestrzeń dyskowa spadła poniżej określonej wartości. Na przykład, jeżeli wprowadzisz w polu wartość 00:30, ostrzeżenie systemowe będzie wyświetlane co 30 minut. Zakres: od 10 minut do 24 godzin.
- **Ścieżka archiwum (Archival Path)**: wprowadź ścieżkę do archiwum. Zachowywanie archiwalnych danych na innym dysku zwiększa wydajność systemu.

Serwer redundantny (Redundant Server)

Notatka: Serwer redundantny musi zostać zarejestrowany, aby był dostępny.

Możesz określić **Opóźnienie auto-restartu (m:ss) (Auto-restart delay (m:ss))** dla zdublowanej bazy danych i Serwera Redundantnego. Zakres: 1:00 do 9:59.

Szybka synchronizacja (**Quick synchronize**): kiedy ta opcja jest zaznaczona, główny serwer nie zamyka tabel podczas synchronizacji ze zdublowaną bazą danych. Wiadomości nadal mogą przychodzić, a baza danych przeglądana. Żółte oznaczenie jest wyświetlane, informując, że system jest w trybie **tylko do odczytu**.

Notatka: program MS/SQL Interface nie jest wspierany przez Mirror Database oraz Serwer redundantny. MS/SQL Interface zbuforuje wszystkie zdarzenia, pomimo że nie może łączyć się z Mirror Database, ani z serwerem redundantnym.



Wylogowanie i stan bezczynności (Logout and Idle)

W tej zakładce można określić zachowanie aplikacji EntraPass w momencie bezczynności (kiedy użytkownik nie podejmuje działań na klawiaturze).

- **Automatyczne wylogowanie przy bezczynności (Automatic logout on idle):** użytkownik będzie musiał ponownie wprowadzić nazwę użytkownika i hasło, aby uzyskać na nowo dostęp do aplikacji. Maksymalne opóźnienie: 9 minut 59 sekund.
- **Wyślij na pasek przy bezczynności (Send to tray on idle):** aplikacja zostanie zminimalizowana i wysłana na pasek narzędzi, gdy minie określony czas, w którym obecnie zalogowany użytkownik, będzie nieaktywny. Maksimum: 59 minut 59 sekund.
- **Zaloguj, aby zamknąć aplikację serwera (Must login to close a Server application):** jeżeli ta opcja jest wybrana, użytkownik musi się zalogować (nazwa użytkownika i hasło), aby zamknąć aplikację.
- **Powiadom o ostatnim wylogowaniu (Notify last log out):** jeżeli ta opcja jest wybrana, EntraPass powiadomi o wylogowaniu się ostatniego użytkownika.
- **Wyświetl listę logowania (Display Login List):** jeżeli ta opcja jest wybrana, pięciu ostatnich użytkowników, którzy zalogowali się do aplikacji EntraPass, zostanie wyświetlonych w oknie logowania. Ta opcja ułatwia dostęp do systemu dla użytkowników, którzy po prostu mogą wybrać swoją nazwę użytkownika i wprowadzić hasło. Może także ułatwić Administratorowi Systemu kontrolę tego, którzy użytkownicy logowali się w ostatnim czasie na konkretne aplikacje.

Notatka: pomimo zalet zaleca się, aby wyłączyć opcję Wyświetl listę logowania dla zwiększenia bezpieczeństwa systemu.



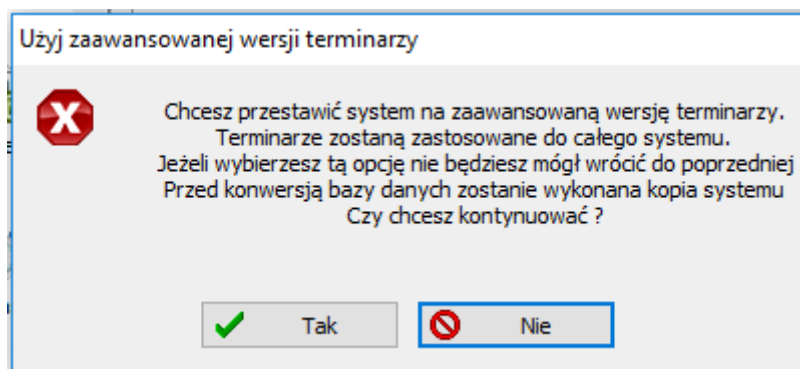
Terminarz (Schedule)

Zakładka Terminarz to miejsce, w którym będziesz uaktualnić terminarz do poziomu zaawansowanego. EntraPass oferuje użytkownikom więcej elastyczności i ułatwienie obsługi dzięki grupowaniu terminarzy po bramkach, połączeniach albo komponentach systemowych. Przy instalacji EntraPass wersji 3.18 lub nowszej, ta opcja nie jest automatycznie włączona.

Notatka: zanim zaznaczysz to pole upewnij się, że aktualizacja do zaawansowanego terminarza jest konieczna.

Terminarze są pogrupowane:

- Terminarze systemowe: są stosowane przy komponentach logicznych takich, jak: parametry zdarzeń, terminarze logowania użytkowników, przełączniki wideo, etc. Terminarze systemowe nie są przypisywane dla konkretnych kontrolerów; są przypisywane dla całego systemu. Możesz zaprogramować nieograniczoną ilość terminarzy systemowych.
- Terminarze multi-obiektowe: są definiowane na połączenie. Możesz zdefiniować 100 terminarzy na multi-obiekt, do celów takich jak: nadzór zasilania (kontrolery), odblokowywanie drzwi, przełącznik REX, tryb aktywacji (przełącznik), etc.
- Po zaznaczeniu pola i kliknięciu OK, zostanie wyświetlone ostrzeżenie, że działania jest odwracalne, ale nie bez konsekwencji.
- Przed aktywowanie tej opcji, zalecamy przygotowanie kopii zapasowej danych.



- Po zatwierdzeniu procesu, zakładka **Terminarz** zniknie z okienka **Parametry systemu**.
- **Włącz terminarz do obejścia REX (Enable schedule to bypass Rex)**, aby włączyć główne i pomocnicze opcje **Terminarza wiadomości pominięcia REX (Rex Bypass Message schedule)** dla drzwi. Zobacz: **Konfigurowanie drzwi (Door Configuration)**.

Status Ikony (Icon Status)

Parametr Opóźnienie statusu limitu czasu (m:ss) (Status time out delay (m:ss)) pozwala określić przedział czasu zanim stacja robocza wyśle zapytanie do serwera o statusy przycisków. Im wyższe opóźnienie, tym mniejsza częstotliwość odświeżania przycisków, co przekłada się na mniejsze obciążenie sieci. Maksymalny czas: 1 min 30 sekund.



Logowanie do trybu serwisowego (Service Login Information)

Informacja wprowadzona tutaj jest wymagana, kiedy serwer działa, jako usługa oraz serwer musi uzyskać dostęp do zasobów sieciowych. **Logowanie do trybu serwisowego (Service Login Information)** jest wymagana dla **Terminarza Kopii zapasowej (Backup Scheduler)** przy wykorzystaniu dysku sieciowego.

- Musisz zaznaczyć pole **Login Server Service**, aby włączyć tą opcję.
- **Musisz** wprowadzić nazwę domeny serwerowej oraz nazwę komputera, login oraz dwukrotnie hasło, dla potwierdzenia.

Notatka: jeśli nie skonfigurowano nazwy domeny ani grupy roboczej, w polu Nazwa domeny musisz wprowadzić Nazwę komputera.

Zasady dotyczące hasła (Password Rules)

Celem tej opcji jest dodawanie parametrów do hasła użytkownika.

1 – Z menu **Opcje**, wybierz **Parametry systemu**.

Zasady hasła:

- Ilość znaków (min/max): 8-20.
- Ilość znaków numerycznych (min/max): 0-20.
- Ilość znaków specjalnych (min/max): 0-20.
- Ilość wielkich liter (min/max): 0-20.

Notatka: po wybraniu, wszyscy nowo utworzeni albo zmodyfikowani użytkownicy będą musieli podporządkować się nowym zasadom dotyczącym haseł.



Parametry oprogramowania sprzętowego (Firmware Parameters)

Ta sekcja zawiera wszystkie informacje dotyczące kontrolerów, bramek i module komunikacji IP, oraz sekcje do zaktualizowania oprogramowania sprzętowego (firmware).

Notatka: zakładka KTES będzie dostępna wyłącznie w przypadku, jeżeli kontroler KTES został uprzednio zdefiniowany w systemie. Zobacz Konfigurowanie KTES, aby dowiedzieć się więcej.

KT-100

Zakładka KT-100 określa położenie katalogu zawierającego oprogramowanie dla kontrolerów KT-100. System wykorzysta te dane do zaktualizowania zainstalowanych kontrolerów (nie dostępne w EntraPass KTES Edition).

KT-300

Zakładka KT-300 określa położenie katalogu zawierającego oprogramowanie dla kontrolerów KT-300. System wykorzysta te dane do zaktualizowania zainstalowanych kontrolerów (nie dostępne w EntraPass KTES Edition).

KT-400

Zakładka KT-400 określa położenie katalogu zawierającego oprogramowanie dla kontrolerów KT-400. System wykorzysta te dane do zaktualizowania zainstalowanych kontrolerów.

- Opcja **Włącz Aktualizatora TFTP KT-400 (Enable TFTP KT-400 updater)** umożliwi aktualizację oprogramowania KT-400 z **Operacje > Okienko obiektu w EntraPass (Operation > Site dialog in EntraPass)**.
- **Włącz automatyczne aktualizowanie oprogramowania (Enable automatic firmware update)**: włącz, aby dokonać aktualizacji każdego KT-400 inną wersją oprogramowania.

Notatka: opcja automatycznego aktualizowania oprogramowania odnosi się wyłącznie do KT-400s.

Notatka: multi obiektowa bramka musi zostać zrestartowana, aby włączyć aktualizację TFTP KT-400.

- Ze względów bezpieczeństwa, jako Administrator Systemu możesz zdecydować, o wyłączeniu tej opcji i niedopuszczeniu użytkowników do aktualizowania oprogramowania we własnym zakresie.

KT-1

Zakładka KT-1 określa położenie katalogu zawierającego oprogramowanie dla kontrolerów KT-1. System wykorzysta te dane do zaktualizowania zainstalowanych kontrolerów.

- Opcja **Włącz Aktualizatora TFTP KT-1 (Enable TFTP KT-1 updater)** umożliwi aktualizację oprogramowania KT-1 z **Operacje > Okienko obiektu w EntraPass (Operation > Site dialog in EntraPass)**.
- **Włącz automatyczne aktualizowanie oprogramowania (Enable automatic firmware update)**: włącz, aby dokonać aktualizacji każdego KT-1 inną wersją oprogramowania.

Notatka: opcja automatycznego aktualizowania oprogramowania odnosi się wyłącznie do KT-1s.

Notatka: multi obiektowa bramka musi zostać zrestartowana, aby włączyć aktualizację TFTP KT-1.

- Ze względów bezpieczeństwa, jako Administrator Systemu możesz zdecydować, o wyłączeniu tej opcji i niedopuszczeniu użytkowników do aktualizowania oprogramowania we własnym zakresie.



EntraPass - Instrukcja instalacji i obsługi programu Serwer EntraPass

- Wybierz **Tryb aktualizacji firmware (Firmware flashing mode)**.

KTES

Zakładka KTES określa położenie katalogu zawierającego oprogramowanie dla kontrolerów KTES. System wykorzysta te dane do zaktualizowania zainstalowanych KTES.

Kantech IP Link

Zakładka IP Link określa położenie katalogu zawierającego oprogramowanie dla modułu Kantech IP Link. System wykorzysta te dane do zaktualizowania zainstalowanego oprogramowania.

- Opcja **Włącz Aktualizatora TFTP IP Link (Enable TFTP IP Link updater)** umożliwi aktualizację oprogramowania IP Link z **Operacje > Okienko obiektu w EntraPass (Operation > Site dialog in EntraPass)**.

Notatka: multi obiektowa bramka musi zostać zrestartowana, aby włączyć aktualizację TFTP IP Link.

- Ze względów bezpieczeństwa, jako Administrator Systemu możesz zdecydować, o wyłączeniu tej opcji i niedopuszczeniu użytkowników do aktualizowania oprogramowania we własnym zakresie.

czytnik ioSmart

- Karta czytnika ioSmart określa folder zawierający oprogramowanie firmware dla czytników. System użyje te dane do aktualizacji zainstalowanych czytników.

ioModules

Zakładka ioModule określa folder zawierający oprogramowanie firmware dla ioModules. System wykorzystuje te dane do aktualizacji zainstalowanego ioModules.

KT-401

Zakładka KT-401 określa położenie katalogu zawierającego oprogramowanie dla kontrolerów KT-401. System wykorzysta te dane do zaktualizowania zainstalowanych kontrolerów.

- Opcja **Włącz Aktualizatora TFTP KT-401 (Enable TFTP KT-401 updater)** umożliwi aktualizację oprogramowania KT-401 z **Operacje > Okienko obiektu w EntraPass (Operation > Site dialog in EntraPass)**.

- **Włącz automatyczne aktualizowanie oprogramowania (Enable automatic firmware update):** włącz, aby dokonać aktualizacji każdego KT-401 inną wersją oprogramowania.

Notatka: opcja automatycznego aktualizowania oprogramowania odnosi się wyłącznie do KT-401s.

Notatka: multi obiektowa bramka musi zostać zrestartowana, aby włączyć aktualizację TFTP KT-401.

- Ze względów bezpieczeństwa, jako Administrator Systemu możesz zdecydować, o wyłączeniu tej opcji i niedopuszczeniu użytkowników do aktualizowania oprogramowania we własnym zakresie.



Parametry obrazu (Image Parameters)

Sekcja **Obraz (Image)** jest miejscem, gdzie możliwe jest określenie parametrów opcji identyfikowania. Można określić jakość obrazu dla obrazów, podpisów i grafik wykorzystywanych, jako tła.

- Jeżeli korzystasz z opcji identyfikowania, zaleca się pozostawić jakość jpeg, jako domyślną. Zmniejszenie jakości może doprowadzić do pogorszenia się jakości obrazu importowanych ze identyfikatorów.
- Jeżeli nie korzystasz z opcji identyfikowania, możesz zredukować jakość jpeg, tak, aby nie zajmowały za dużych przestrzeni bazy danych. Trzeba jednak mieć na uwadze, że zmniejszenie jakości może doprowadzić do pogorszenia się jakości obrazu importowanych ze identyfikatorów.

Parametr pozwala zachować obraz karty i karty gościa, podpisów oraz grafik tła do pliku zamiast bezpośrednio w bazie danych. Opcja może być przydatna dla obiektów o dużym archiwum obrazów i grafik. Bazy danych obrazów, podpisów oraz grafik tła mogą zawierać do 2 Gb danych każda.

Obrazy i identyfikowanie (Picture and Badging)

Opcja Obraz i identyfikowanie pozwala na dopasowanie jakości obrazu i podpisu do wykorzystania przy opcji Identyfikowania (Badging).

- Odnaczenie formatu JPEG, informuje system, że ma zapisywać grafikę w formacie tiff.

Notatka: pamiętaj, że to może mieć wpływ na jakość obrazu. Jeśli nie jesteś zaawansowanym użytkownikiem, nie zmieniaj wartości domyślnych.

- Wartość jakości JPEG dla Tła grafiki (obrazu) wskazuje jakość, z jaką obraz zostanie zapisany. Jeżeli wybierzesz 10, jakość będzie bardzo słaba; 100 oznacza doskonałą jakość.

- Dla obrazów i miniatur wybierz pozycję położenia przezroczystego obrazu. Dostępne są cztery możliwości: górny-prawy, górny-lewy, dolny-prawy oraz dolny-lewy róg. Domyślnie, system wybiera dolny-lewy róg. EntraPass umożliwia użytkownikowi wybór dowolnego koloru.

- Przy zaznaczeniu **Zapisz obrazy i podpis w pliku**, system stworzy foldery Obrazy i Podpisy w lokalizacji: C:\Program Files\Kantech\Server_CE\Data; gdzie zachowywane będą wszystkie obrazy i podpisy.

- Przy zaznaczeniu **Zapisz obrazy i podpis (goście) w pliku**, system stworzy foldery Obrazy i Podpisy w lokalizacji: C:\Program Files\Kantech\Server_CE\Data; gdzie zachowywane będą wszystkie obrazy i podpisy (gości).

Notatka: podczas modyfikowania istniejącego obrazu albo podpisu, EntraPass zapisze zmiany w odpowiednim pliku oraz usunie odpowiedni zapis w bazie danych.



Grafika (Graphic)

Opcja grafiki pozwala dopasować, jakość grafiki dla oprogramowania EntraPass.

- Odznaczenie formatu JPEG, informuje system, że ma zapisywać grafikę w formacie tiff.

Notatka: pamiętaj, że to może mieć wpływ na jakość obrazu. Jeśli nie jesteś zaawansowanym użytkownikiem, nie zmieniaj wartości domyślnych.

- Wartość jakości JPEG dla Tła grafiki (obrazu) wskazuje jakość, z jaką obraz zostanie zapisany. Jeżeli wybierzesz 10, jakość będzie bardzo słaba; 100 oznacza doskonałą jakość.
- Przy zaznaczeniu **Zapisz grafikę w pliku**, system stworzy foldery Grafika w lokalizacji: C:\Program Files\Kantech\Server_CE\Data; gdzie zachowywane będą wszystkie grafiki.

Notatka: podczas modyfikowania istniejącej grafiki, EntraPass zapisze zmiany w odpowiednim pliku oraz usunie odpowiedni zapis w bazie danych.



Parametry raportu (Report Parameters)

Zakładka Raport pozwala użytkownikowi zdefiniowanie separatora pól dla raportów, formatu nazw użytkownika, etc.

CSV

W zakładce CSV, możesz określić separator pól dla twoich raportów.

- Domyślnie, system wykorzystuje przecinek, jako separator. Możesz zmienić na: kropkę, średnik, spację, etc.
- Zaleca się zaznaczenie opcji **Data i czas na osobnych polach**. Domyślnie system umieszcza je na tym samym polu. Po zaznaczeniu, system umieści je na dwóch osobnych polach.

Przestrzeń dyskowa (Disk Space)

Ta opcja służy, jako zabezpieczenie przy, np., żądaniu utworzenie wielkiego raportu. W tym przypadku, system zawiesi wykonywanie raportu oraz wyświetli wiadomość alarmową wskazując powód zawieszenia.

- **Anuluj raport, jeżeli pozostała przestrzeń dyskowa jest mniejsza niż (Abort report if free space lower than (MB))**: z listy możesz wybrać minimalną pojemność wymaganą do przeprowadzenia przygotowania raportu. Zakres: 2000 do 999999 MB.
- **Maksymalna ilość zdarzeń do raportu email (Maximum event for email report)**: z listy wybierz maksymalną liczbę zdarzeń, które mogą zostać wysłane w postaci raportu email. Zakres: 100 do 100000 zdarzeń.
- **Maksymalna ilość zdarzeń dla standardowego raportu (Maximum event for standard report)**: z listy wybierz maksymalną liczbę zdarzeń, które mogą zostać wysłane w postaci standardowego raportu. Zakres: 1000 do 500000 zdarzeń.
- **Jednoczesne przygotowanie raportów (Simultaneous report process)**: określa liczbę raportów, które mogą być przygotowywane w tym samym czasie. Do 10 raportów może być przygotowywane w tym samym czasie bez wpływu na wydajność systemu.

Notatka: kiedy liczba zdarzeń dla raportu przekroczy dopuszczalną wartość maksymalną, niektóre zdarzenia nie zostaną uwzględnione w raporcie. Zostanie utworzone zdarzenie Przekroczono liczbę zdarzeń dla raportu, które zostanie wyświetlone na pulpicie Wiadomości oraz dodane do raportu.



Format nazwy użytkownika karty (User Name Format)

Określenie formatu nazwy użytkownika poinstruuje system, jak nazwa użytkownika karty będzie wyświetlana w EntraPass.

- **Parsuj nazwę użytkownika (Parse user name):** powinno zostać zaznaczone, jeżeli chcesz wybrać metodę parsowania nazwy użytkownika w systemie.
- **Format nazwy użytkownika karty (User Name Format)** pozwala wybrać metodę parsowania. Opcje: Zaczynij od nazwiska; Zaczynij od imienia.
- **Parsuj nazwę użytkownika z (Parse user name with):** pozwala wybrać znak, który zostanie użyty do parsowania pól nazwy użytkownika. Opcje: przecinek, kropka, średnik, dwukropek, spacja. .

Notatka: przed wersją EntraPass 3.18, system korzystał z metody wyszukiwania, która wymagała od Administratora wprowadzenia konkretnych wartości granicznych (dolna/górna) do określenia zasad wyszukiwania. Na przykład, aby wygenerować raport, który zawierałby wszystkich użytkowników z nazwiskiem zaczynającym się na A, dolna wartość graniczna powinna zostać określona na „A”, a górna „AZZZZ”. Teraz system ten sam rezultat po wprowadzenia „A” dla obu wartości granicznych.

Parametry wideo (Video Parameters)

Sekcja wideo wyświetla się wyłącznie wtedy, gdy opcja Integracja wideo jest włączona w systemie EntraPass. Określisz synchronizację czasu, zdalny proces wideo oraz format JPEG dla obrazów wideo.



Parametry (Parameters)

Zakładka Parametry pozwala na określenie parametrów dla procesowania wideo.

- **Wyłącz zdalną synchronizację czasu (Disable manual time synchronization)** powstrzyma serwer EntraPass przed aktualizowaniem daty i czasu serwera wideo po zdalnych modyfikacjach czasu. Opcja przydaje się, kiedy chcesz zachować wszystkie nagrane zdarzenia, które miały miejsce na serwerze wideo niezależnie od czasu „aktualnego” na serwerze EntraPass.

- Sekcja **Parametrów kontroli zdalnego procesowania wideo (Remote video process control parameters)** zawiera parametry, które określają zdalne zarządzanie procesowaniem wideo pomiędzy serwerem EntraPass, a serwerami wideo podłączonymi do EntraPass. Zarządza wszystkimi zadaniami związanymi z: nagrywaniem, zdarzeniami, wzorami, etc.

- Pole aplikacji **Kontrola presetów i wzorów (Preset and pattern control)** pozwala na wprowadzenie liczby aplikacji, które zostaną automatycznie uruchomione do procesowania presetów i wzorów. Zakres: od 1 do 8 równoczesnych aplikacji.

Notatka: aplikacja Kontrola presetu oraz trasy jest uruchomiona za każdym razem, kiedy zaczyna się nagranie wideo. Jeśli wprowadzisz „1” jako wartość tej liczby, a – na przykład – posiadasz więcej niż 1 serwer wideo z określonymi presetami i trasami, aplikacja zajmie się presetami na wszystkich tych serwerach wideo. Jeśli zdecydujesz się zwiększyć wprowadzoną liczbę aplikacji pamiętaj, że działanie wielu aplikacji jednocześnie zmniejsza wydajność sprzętu.

- **Resetuj aplikację zdalnego procesowania wideo (Reset remote video process application)** pozwala systemowi przerwać, a następnie automatycznie zresetować aplikację **Zdalne procesowanie wideo (Remote Video Process)**. Ta opcja może zostać użyta, gdy zdarzenia wideo nie są wyświetlane.

- **Resetuj kontrolę aplikacji zdalnego procesowania wideo (Reset remote video process applications control)** pozwala systemowi przerwać aplikację Kontroli (nagrywanie, zdarzenia, wzory, etc.), a następnie automatycznie zresetować aplikację **Zdalne procesowanie wideo (Remote Video Process)**.

- **Logi błędów procesowania wideo (Log Video process error)** pozwala systemowi zachować rejestr wszystkich błędów procesowania w plikach serwera EntraPass. Lokalizacja: C:\Program files\Kantech\Server_CE\Bin\Log. Każda aplikacja generuje log:

- RVP_LOG_00.txt (błędy wygenerowane przez RVP0.exe)

- RVPPoll_LOG_01.txt (błędy wygenerowane przez RVPPOLL1.exe)

- RVPEvent_LOG_02.txt (błędy wygenerowane przez RVEVENT3.exe)

- RVPRecord_LOG_03.txt (błędy wygenerowane przez RVPRECORD3.exe).

- RVPControl_LOG_04.txt (błędy wygenerowane przez RVPCONTROL4.exe). System wygeneruje tyle logów, ile w danym momencie działa aplikacji (RVPControl_LOG_05 do 08).

Snap:

Opcja Snap pozwala na określenie jakości obrazu, który będzie wyświetlany w miniaturze.

- Snap obrazu wideo (Video image snap) określa jakość obrazu, który zostanie zapisany jako miniatura dla każdego wideo. Jeżeli wybierzesz 10, jakość będzie bardzo słaba; 100 oznacza doskonałą jakość.



Intellex:

Opcja Intellex pozwala zdefiniować dopuszczalną przepustowość dla procesowania wideo (tylko dla Intellex).

o **Wyłącz DirectX**, wyłączy DirectX, czyli technologię Windows, która umożliwia osiągnięcie lepszej wydajności przy pracy lub przeglądania grafiki albo innej treści multimedialnej, w tym wideo oraz dźwięku. Domyślnie: DirectX jest włączony.

Notatka: system wykorzysta więcej zasobów systemowych, kiedy DirectX jest wyłączony.

o Określ przepustowość wideo (**Limit video bandwidth**) pozwala ograniczyć/zwiększyć przepustowość wymaganą do strumieniowania wideo na żywo bez wpływania na wydajność sprzętu. Zakres: od 64 KB/s do 8192 KB/s. Określona wartość będzie się odnosić do wszystkich stacji roboczych, w tym serwera EntraPass. Wartość może zostać zmieniona lokalnie dla poszczególnych stacji roboczych: Opcje > pasek narzędzi > Urządzenia multimedialne > Wideo.

o **Opóźnienie zapisu Video Vault (Video vault save delay)** jest wykorzystywane do określenia opóźnienia czasowego, zanim nagranie z Video Vault zostanie odtworzone.

Notatka: wartość dla stacji roboczej nie może przekraczać wartości dla serwera EntraPass.

HDVR:

o **Opóźnienie zapisu Video Vault (Video vault save delay)** jest wykorzystywane do określenia opóźnienia czasowego, zanim nagranie z Video Vault zostanie odtworzone.

TVR:

o **Opóźnienie zapisu Video Vault (Video vault save delay)** jest wykorzystywane do określenia opóźnienia czasowego, zanim nagranie z Video Vault zostanie odtworzone.

Synchronizacja czasu w systemie (Time Parameters)

Sekcja Czas pozwala określić, która bramka zostanie wykorzystana do automatycznego dopasowania czasu dla wszystkich komputerów podłączonych do serwera EntraPass. Funkcja jest przydatna przy zarządzaniu oddalonymi od siebie obiektami.

Notatka: bramka sprawdza pierwszy kontroler pierwszego obiektu o 5:47 albo 17:47, 1:47 albo 13:47, 7:47 albo 19:47, aby określić czas kontrolera.

- **Brak dopasowania czasu (No time adjustment)** wyłącza opcję.

- **Przez bramkę (By Gateway)** automatycznie zsynchronizuje czas dla wszystkich komputerów przez bramkę wybraną z listy.

- **Przez serwer (By Server)** automatycznie zsynchronizuje czas dla wszystkich komputerów z regularnymi przedziałami. Musisz określić częstotliwość odświeżania. Zakres: 1 do 9999 godzin.



Parametry definiowania kart (Credentials Parameters)

Karta (Card)

Dzięki zakładce Karta, Administrator Systemu będzie miał możliwość przeniesienia swojego systemu EntraPass do zaawansowanego zarządzania użytkownikami, gdzie użytkownicy są zarządzani poprzez swoje nazwy oraz numery kart. Każdy użytkownik karty będzie zarządzany poprzez nazwę użytkownika i przez 5 różnych numerów. Umożliwi to tworzenie kart, bez przypisywania nowym kartom numerów. Zobacz: **Wprowadzanie nowej karty w Zaawansowanym zarządzaniu (Issuing a New Card in Enhanced User Management Environment)**. Ta opcja będzie wykorzystywana razem EntraPass Web. Zobacz: **Pomoc EntraPass Web (EntraPass Web Help)**.

Notatka: umożliwienie przejścia do zaawansowanego zarządzania użytkownikami jest nieodwracalne przy wykorzystaniu oprogramowania. Jednakże, kiedy system przenosi dane, kopia zapasowa jest utworzona w EntraPass, aby mógł być przywrócony do poprzedniego działania.

- **Przenieś do zaawansowanego zarządzania (Migrate to enhanced user management):** domyślnie – zaznaczona. Zobacz: **Wprowadzanie nowej karty w Zaawansowanym zarządzaniu (Issuing a New Card in Enhanced User Management Environment)**.



Stacja robocza oraz serwer (Workstation and Server)

Przyciski paska narzędzi (Toolbar Buttons)

Rozmiar przycisków paska narzędzi może zostać zwiększony 2,5 krotnie, aby polepszyć czytelność tekstu. Możliwe dla Serwera EntraPass oraz stacji roboczej EntraPass. Przełoguj się, aby wprowadzić zmiany.

Przypisz Nowe Połączenie albo Obiekt (Assign a New Connection to a Site)

Notatka: zobacz Konfigurowanie połączenia, aby dowiedzieć się więcej.

Aby włączyć/wyłączyć funkcję, wybierz:

- **Zgłoszenie (Prompt):** system poprosi użytkownika o określenie obiektu, do którego ma się podłączyć przy tworzeniu nowego połączenia.
- **Obowiązkowy (Mandatory):** system poprosi użytkownika o określenie obiektu, do którego ma się podłączyć (obowiązkowo) przy tworzeniu nowego połączenia.
- **Wyłącz (Disable):** domyślne.

Notatka: nie powstaną żadne odniesienia do stref wirtualnych, o ile przynajmniej jedna nie została utworzona wcześniej (zobacz Konfigurowanie obiektu).

Integracja (Integration)

Zakładka **Integracja** pozwala użytkownikowi na wybranie podzespołów, które zostały zintegrowane z EntraPass przez Kantech.

Rejestracja DLL (DLL registration): Dostępne DLL w tym menu zostaną wykorzystane do określenia, jaki typ podzespołów klient podłączy do EntraPass.

- Kliknij Dodaj, aby zintegrować następne DLL. Zobacz: **Konfiguracja integrowanych paneli (Integrated Panel Configuration)**.

Notatka: integracja DLL musi zostać wykonana na serwerze EntraPass, aby skomunikować się z multi obiektową bramką, gdzie fizycznie są podłączone oraz zasilane elementy zewnętrzne.

Wirtualna klawiatura (Virtual keypad): ta zakładka pozwala użytkownikowi dostosować wyświetlanie ekranu wirtualnej klawiatury. Trzy tryby wyświetlania mogą zostać wybrane: **Niezakotwiczony**, **Modalny** albo **Zawsze na wierzchu** (Floating, Modal or Stay on top).



Interfejs Web (Web Interface)

Zakładka Web (Web tab)

Przy pomocy przycisku **Interfejs Web (Web interface)** możesz skonfigurować parametry EntraPass Web.

- **Podgląd wiadomości w EntraPass Web (Allow messages to EntraPass Web):** zaznacz, aby umożliwić użytkownikowi na podgląd wiadomości w EntraPass Web.
- **Maksymalna ilość wiadomości (Maximum web messages):** wybierz maksimum z licznika.
- **Szerokość PEN pada (Signature pad pen width):** wybierz wartość szerokości dla PEN wykorzystywanego z padem.
- **Maksymalna ilość raportów równoczesnych w sesji (Maximum request simultaneously by session):** wybierz maksymalną liczbę raportów, które mogą być wykonywane jednocześnie.
- **Filtry wiadomości (Message filter for web messages):** z listy wybierz filtr do wyświetlenia.
- **Proporcje identyfikatora obrazu (Badge image ratio for web):** możesz zwiększyć jakość wydruku obrazu (domyślnie: 2). Zwiększenie proporcji zwiększa wielkość pliku.

Zakładka Dostosowania Web (Web Customization tab)

- **Kolor (Custom color):** kliknij, aby zmienić kolor interfejsu.
- **Logo strony (Page logo):** kliknij, aby dodać (lub zmienić) logo w lewym-górnym rogu interfejsu.

Zakładka go Pass

Jeśli zarejestrujesz aplikację mobilną go Pass, pojawi się karta go Pass. Użyj go Pass ze smartfonem lub zegarkiem Apple, aby zablokować lub odblokować drzwi. Dla wygody można sterować drzwiami z odległej lokalizacji.

Aby zapewnić wyższy poziom bezpieczeństwa, użyj czytnika ioSmart z drzwiami, czytniki ioSmart wykorzystują technologię BLE. Dostosuj się do różnych poziomów bezpieczeństwa, wybierz opcję z listy Ograniczenia zbliżeniowe.

1 - Aby wyświetlić zaszyfrowany profil osobisty posiadacza karty w wiadomościach e-mail z powiadomieniem, wybierz opcję **Wyświetl widoczne informacje powiadomień**. Posiadacze kart wykorzystują dane swojego profilu osobistego lub link w e-mail, aby uzyskać dostęp do aplikacji go Pass.

2 - Aby ponownie wysłać wszystkie wiadomości e-mail z powiadomieniem o przekazaniu do wszystkich ważnych użytkowników karty, kliknij **Prześlij ponownie powiadomienia GoPass dla wszystkich posiadaczy ważnych kart**

3 - Aby kontrolować, jak i kiedy SmartLink reaguje na nieprawidłowe polecenia go Pass, zdefiniuj wszystkie trzy ustawienia w obszarze **ochrona**:

a - Aby ustawić liczbę nieprawidłowych żądań, które wystąpią zanim SmartLink odpowie, wprowadź liczbę w **Odesłanie powiadomienia na niewłaściwe żądanie**.

b - Aby ustawić czas, po upływie którego SmartLink odpowie, wprowadź liczbę w **Opóźnienie dbounce (ss)**.

c - Aby uniemożliwić SmartLink reagowanie na żądanie przejścia przez określony czas, wprowadź wartość w polu **Wyłącz GoPass na powiadomienie (m: ss)**.

Na przykład # niepoprawnych żądań w ciągu # sekund = # sekund przed odpowiedzią SmartLink na przejście request + event Zbyt wiele przejść Wyświetlenie nieudanych żądań.



EntraPass - Instrukcja instalacji i obsługi programu Serwer EntraPass

4 - Wybierz jedną z następujących opcji z listy Ograniczenia zbliżeniowe:

- Brak - nie ma ograniczeń, posiadacz karty go Pass może zablokować i zdalnie odblokować drzwi oraz na drzwi. EntraPass ignoruje technologię BLE.
- Ścisłe (tylko ioSmart BLE) - jeśli posiadacz karty go Pass go przejdzie, przejdź przez czytnik ioSmart, idź. Posiadacz karty Pass musi znajdować się w zasięgu drzwi.
- Hybrid (BLE, gdy jest dostępny) - użyj dla posiadaczy kart go Pass, którzy mają dostęp do czytników ioSmart czytniki inne niż ioSmart. Jeśli posiadacz karty go Pass znajduje się przy drzwiach ioSmart, posiadacz karty musi być w środku

zasięg, jeśli jest to drzwi inne niż ioSmart, posiadacz karty może zdalnie sterować drzwiami.

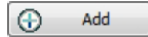
UWAGA: Jeśli nie wybierzesz pola wyboru BLE w szablonie czytnika, którego używa kontroler,

Wybór ograniczeń zbliżeniowych jest zbędny.

Informacje dotyczące dystrybutora (Dealer Information)

Szczegóły pola Informacje (About Box Details)

Aby dodać Informacje dotyczące dystrybutora w oknie **Informacje (About)**, wybierz **Wyświetl szczegóły w polu Informacji (Display details in About box)**

1 – Wypełnij Informacje dotyczące dystrybutora i dodaj logo przy pomocy przycisku .

2 – Wypełnij dane Informacje o obiekcie (**Site information**)

3 – Kliknij OK, aby zakończyć.

Przypomnienie KAP (Kap Reminder)

Wiadomość z przypomnieniem pojawi się, aby poinformować użytkownika, że okres KAP dobiega końca. Przypomnienie może zostać przesłane jako: wiadomość pop-up (wyskakująca), albo email.



Wyskakujące wiadomości (Pop-up Message)

Wiadomość wyskakująca jest automatycznie generowana przez EntraPass, aby przypomnieć użytkownikowi o tym, że okres KAP dobiega końca:

- 60 dni przed końcem.
- 30 dni przed końcem.
- W dniu upłynięcia terminu ważności.
- 30 dni po terminie ważności.

Wiadomość z przypomnieniem musi zostać potwierdzona przez użytkownika. Zostanie odnotowana w bazie danych zdarzeń oraz zostanie umieszczona w raportach.

Email

Okno Informacji dotyczących dystrybutora (Dealer Information) zostało zmodyfikowane, aby umożliwić konfigurację przypomnienia email. Do 4 adresatów może zostać dodanych. Kliknięcie **Wyślij przypomnienie teraz (Send reminder now)** zapisze informacje i wyśle przypomnienie natychmiast.

Nowe zdarzenie zostanie zapisane na liście zdarzeń.

Każda stacja robocza otrzyma 60 sekundową wiadomość wyskakującą (pop-up).

Notatka: opcja Przypomnienie KAP (Kap Reminder) może zostać również wywołana z okna Pomoc (About).



Terminarz kopii systemu (Backup Scheduler)

Kopia zapasowa to kopia zapasowa bazy danych systemu, która służy, jako zastępstwo albo alternatywa w przypadku awarii komputera. W przypadku awarii twojego komputera systemowego, możesz przywrócić kopię zapasową na inny komputer (na którym zainstalowana jest aplikacja EntraPass).

- Twórz kopię zapasową swoich plików regularnie, przynajmniej raz w tygodniu.
- Rekomendujemy utworzenie dwóch kopii zapasowych twoich plików bazy danych. Zapisz je w osobnych lokalizacjach.

- Aby utworzyć kopię zapasową, możesz wykorzystać:

- o menu zakładki Serwer/Kopia zapasowa,

- o **Terminarz kopii zapasowej (Backup Scheduler)**,

- o Aplikację **Dublowania bazy danych (Mirror Databas)**,

- o inne oprogramowanie lub podzespoły zewnętrzne (nie zalecamy oprogramowania zewnętrznego).

Notatka: domyślnie, kiedy zachowujesz albo odtwarzasz plik, Bazy danych serwera będą czasowo wyłączone (nie będą dostępne). Stacje robocze nie będą w stanie modyfikować baz danych.

Program **Terminarz kopii zapasowej (Backup Scheduler)** jest wykorzystany do automatycznego tworzenia kopii zapasowych twoich danych, archiwów, bazy danych wej./wyj. Określ ustawienia domyślne, a system sam zrobić resztę.



Konfigurowanie kopii zapasowej, kiedy serwer EntraPass działa jako usługa (Configuring the Backup when the EntraPass Server is Running as a Service)

Poniższe kroki są wymagane, kiedy serwer EntraPass działa, jako usługa i musisz utworzyć kopię zapasową do innego komputera **wewnątrz tej samej grupy roboczej albo domeny**.

Notatka: aby wykonać następujące czynności musisz posiadać pełne przywileje administratora. Jeżeli takowych nie posiadasz albo nie znasz Windows Administrative Tools, skontaktuj się ze swoim administratorem sieci.

1 – Z serwera EntraPass, idź to Opcje > Parametry systemu > Serwer > Informacje logowania usługi.

2 – Wypełnij wszystkie wymagane pola: nazwa domeny, login, hasło, potwierdzenie hasła.

Notatka: Nazwa domeny albo Grupa robocza musi być taka sama zarówno dla serwera EntraPass, jak i komputera zapasowego.

3 – Kliknij OK.

Ustawienie terminarza Automatycznego tworzenia kopii zapasowych systemowej bazy danych (Scheduling Automatic Backups of the System Database).

1 – Z paska narzędzi Opcje, wybierz **Terminarz kopii zapasowej (Backup Scheduler)**.

2 – Wybierz zakładkę korespondującą do informacji, które chcesz zabezpieczyć: Dane, Archiwum, Wej/Wyj albo Zdarzenia Wideo.

Notatka: domyślnie, każdej niedzieli o 4:00 system automatycznie wykona kopię zapasową wszystkich plików dla wszystkich nowych instalacji. Ustawienie godziny na 4:00 wiąże się z tym, że inne zadania nie będą miały wpływu na wykonanie zapisu.

3 – Wybierz opcję **Automatyczne tworzenie kopii zapasowej (Automatic backup option)**.

4 – Wybierz **folder Kopii zapasowej**:

- Domyślny folder: nazwa folderu jest generowana automatycznie według następującej zasady: X_YYYY_MM_DD_HH_MM_SS, gdzie X = dane albo archiwa albo wej/wyj (D, A, T), Y = rok, M = miesiąc, D = dzień, H = godzina, MM = minuty, S = sekundy.

Notatka: domyślnie, system zapisuje wszystkie informacje pochodzące z: C:\Program files\Kantech\Server\Data albo Archive albo Time on video albo V. Informacje są wysyłane do: C:\Program files\Kantech\Server\Backup\X_YYYY_MM_DD_HH_MM_SS .

- Konkretny folder: zachowa pliki w folderze według domyślnego nazewnictwa w folderze XXX.

5 – Wybierz typ kopii zapasowej: opcje zależą od rodzaju danych, które chcesz zapisać.

• Dane (Data):

- Osobne pliki: wykonana kopię zapasową bazy danych plik po pliku.

- Samorozpakowujący się skompresowany plik: utworzy plik wykonywalny (*.exe), który skompresuje informacje1, aby zredukować ilość miejsca na dysku zajmowaną przez kopię zapasową.

• Archiwalne, Czasu pracy oraz Zdarzenia Wideo (Archive, In/Out and Video Event):

- Osobne pliki (pełna kopia zapasowa): wykona kopię zapasową całej bazy danych.

- Samorozpakowujący się skompresowany plik (pełna kopia zapasowa): utworzy plik wykonywalny (*.exe), który skompresuje informacje1, aby zredukować ilość miejsca na dysku zajmowaną przez kopię zapasową.

- Osobne pliki (przyrostowa kopia zapasowa): wykona kopię zapasową całej bazy danych. Tylko informacje zmodyfikowane od ostatniej kopii zapasowej zostaną zachowane.



EntraPass - Instrukcja instalacji i obsługi programu Serwer EntraPass

o Samorozpakowujący się skompresowany plik (przyrostowa kopia zapasowa): utworzy plik wykonywalny (*.exe), który skompresuje informacje¹, aby zredukować ilość miejsca na dysku zajmowaną przez kopię zapasową. Tylko informacje zmodyfikowane od ostatniej kopii zapasowej zostaną zachowane.

Notatka: przywracanie Samorozpakowującej się kopii zapasowej po aktualizacji EntraPass może być wykonane tylko z serwera, na którym została utworzona Samorozpakowująca się kopia zapasowa.

Notatka: jeśli wybierzesz Pełna kopia zapasowa, za każdym razem, kiedy kopia zapasowa zostanie utworzona, powstanie również nowy podfolder z danymi albo samorozpakowującym się plikiem. Jeśli korzystasz z przyrostowych kopii zapasowych zapisane zostaną tylko informacje, które zostały zmodyfikowane od ostatniego zapisu. Jeśli będziesz chciał przywrócić informacje, będziesz musiał przywracać wszystkie podfoldery, jeden po drugim.

6 – Wybierz częstotliwość tworzenia kopii zapasowej:

- Cotygodniowa: kopia zapasowa zostanie utworzona raz w tygodniu, co tydzień; określ dzień na wykonanie kopii zapasowej (np. każdy czwartek).
- Comiesięczna: kopia zapasowa zostanie utworzona raz w miesiącu, co miesiąc; określ dzień na wykonanie kopii zapasowej (np. każdy pierwszy dzień miesiąca)
- Codzienna: kopia zapasowa zostanie utworzona raz w miesiącu.

7 – Określ czas, o której zostanie wykonana kopia zapasowa (format 24 godzinny).

8 – Wybierz **Teraz (Now), jeżeli chcesz wykonać kopię zapasową natychmiast po zachowaniu parametrów.**

Notatka: dla Mirror Database oraz Serwera Redundantnego opcja Konfiguruj automatyczne tworzenie kopii zapasowej jest niedostępna.

9 – Powtórz kroki od 1 do 8 dla wszystkich zakładek.

10 – Kliknij OK, aby zapisać.



Zdarzenia definiowane przez klienta (Custom Messages)

Ta opcja pozwala użytkownikowi z odpowiednim poziomem dostępu na definiowanie **Zdarzeń definiowanych przez klienta**, które mogą wygenerować zdarzenie w oparciu o terminarz. Do 10 niestandardowych komunikatów może zostać zaprogramowanych do uruchomienia zdarzenia w określonym czasie. A każdy komunikat może zostać uruchomiony, kiedy terminarz stanie się ważny, nieważny, etc. Inaczej: możesz uruchomić do 20 zdarzeń, jeżeli weźmiesz pod uwagę początek/koniec przedziału terminarza. Każde zdarzenie będzie wyświetlone na **Liście wiadomości** na **Pulpicie**.

Ustawianie Zdarzeń definiowanych przez klienta (Setting up Custom Messages)

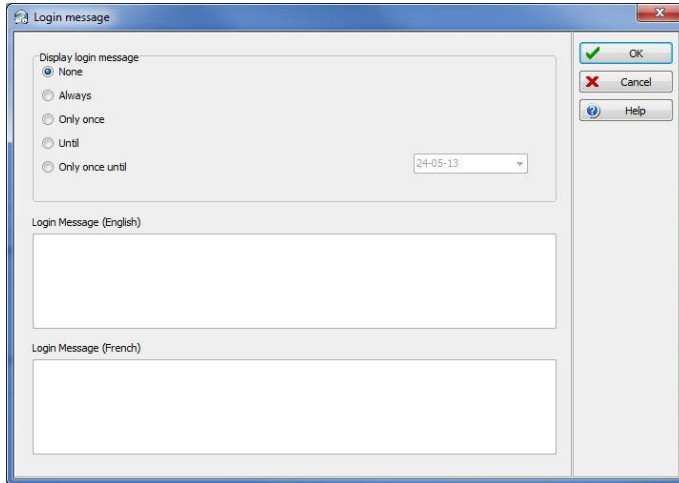
- 1** – Z paska narzędzi **Opcji**, kliknij **Zdarzenia definiowane przez klienta**.
- 2** – W pierwszej zakładce wprowadź pierwszą wiadomość, którą chcesz wyświetlić na Liście wiadomości. Dwa pola są dostępne dla głównego języka i drugiego.
- 3** – Wybierz zdefiniowany wcześniej terminarz, który określi, kiedy zdarzenie będzie uruchomione.
- 4** – Zaznacz czy chcesz, aby zdarzenie było uruchomione przy zmianie statusu terminarza.
- 5** – Przejdź do drugiej zakładki i wprowadź drugą wiadomość; kontynuuj według tego schematu.



Info podczas logowania operatora (Login Messages)

Ta opcja pozwala wprowadzić tekst, który będzie wyświetlany innym użytkownikom, gdy zalogują się na stacjach roboczych.

1 – Z menu *Opcje*, wybierz *Wiadomości przy logowaniu*.



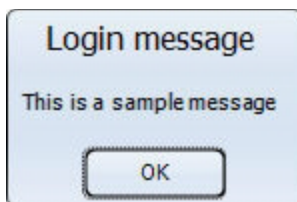
2 – Określ powtarzalność:

- **Brak (None).**
- **Zawsze (Always):** ta wiadomość pojawi się zawsze po logowaniu.
- **Tylko raz (Only once):** ta wiadomość pojawi się tylko raz na użytkownika.
- **Aż do (Until):** ta wiadomość będzie się pojawiać, aż do określonej daty.
- **Tylko raz, aż do (Only once until):** ta wiadomość będzie się pojawiać, aż do określonej daty albo do otrzymania wiadomości przez użytkownika.

3 – Wprowadź wiadomość w polu prawej.

4 – Kliknij OK.

Przykład wyświetlania wiadomości (Message display example):





EntraPass - Instrukcja instalacji i obsługi programu Serwer EntraPass

Spersonalizuj powitalną wiadomość e-mail, którą EntraPass i EntraPass go Pass wysyła do użytkowników i operatorów. Wpisz nagłówek tematu i wybierz opcję wpisywania wiadomości w języku operatora podstawowego lub pomocniczego lub obu języków. Wykonaj następujące czynności:

1-Aby napisać komunikat, że operatorzy widzą, kiedy logują się do dowolnej stacji roboczej, kliknij ikonę login/wiadomość E-mail i kliknij kartę login.

2-Aby napisać wiadomość powitalną dla nowych użytkowników EntraPass, kliknij kartę wiadomość powitalna.

3-Aby napisać wiadomość powitalną dla użytkowników EntraPass go Pass, kliknij kartę Idź do przekazywania wiadomości.

4-aby napisać wiadomość do użytkownika, aby wyjaśnić, dlaczego EntraPass jest wyłączenie konta, kliknij operator Wyłącz wiadomość patka.



Dodatkowe aplikacje i narzędzia programistyczne

Konfiguracja kontrolerów pomocą Instalacji ekspresowej (Configuring a KTES Using Express Setup)

Jeżeli wybierzesz typ połączenia dla nowego obiektu i od razu zapiszesz, system zaproponuje użycie Express Setup do zdefiniowania urządzenia.

- 1 – W oknie **Obiekt**, kliknij **Nowy**, aby określić nowy obiekt. Przypisz mu nazwę.
- 2 – W zakładce **Ogóle (General)**, wybierz **Typ kontrolera (Controller type): Secure IP (KTES)**.
- 3 – Kliknij **Zapisz**, powinna pojawić się wiadomość: Czy chcesz użyć **Programu Ekspresowe ustawienia (Express Setup)** do konfigurowania urządzenia? Kliknij Tak.
 - Jeżeli kliknąłeś Nie, zawsze będziesz mógł wrócić do **Programu Ekspresowe ustawienia (Express Setup)** klikając w przycisk.
- 4 – Zaznacz opcje **Czujnik stanu drzwi (Door contact)** oraz **Czujnik stanu REX (REX contact)**.
- 5 – Zaznacz opcje **Zamka (Postal Lock)**.
- 6 – Kliknij przycisk **Zaawansowane**, aby określić inne urządzenia, takie jak: drzwi, Wejścia linii dozorowej, przekaźniki i wyjścia

Notatka: komponenty są wylistowane w panelu po lewej stronie. Powiązane zakładki są wyświetlone na środku okna. Kiedy wybierzesz komponent, jego domyślna nazwa, numer oraz ustawienia domyślne są wyświetlone w sekcji językowej (language section). Wybierz komponent, aby włączyć jego zakładkę. Komponenty, które są już przypisane są „wyszarzone” i nie mogą być modyfikowane na tym etapie. Jednakże, dzięki menu KTES możesz później modyfikować dowolny opis komponentu (Urządzenia > KTES).

Definiowanie przekaźników (Defining Relays)

Możesz skonfigurować przekaźniki, aby określić ich tryb działania, aktywacji i dezaktywacji terminarzy. Jeżeli chcesz przypisać nazwę do przekaźnika, musisz go wybrać. Jeżeli wybierzesz przycisk Zaznacz wszystkie, nazwy domyślne zostaną zachowane.

- 1 – Wybierz pierwszy przekaźnik, jeżeli chcesz zmienić jego opis. Przekaźnik jest dostępny. Zaznacz pole obok nazwy przekaźnika, aby włączyć sekcję języków.
- 2 – Zaznacz odpowiednią opcję dla **Trybu działania (Operating mode)**.
- 3 – Z listy **Terminarz automatycznych aktywacji (Automatic activation schedule)** wybierz odpowiedni terminarz aktywacji.
- 4 – Z listy **Wyłącz działanie przekaźnika (Disable relay action)**, wybierz odpowiednią akcję.



Definiowanie wejść (Defining Inputs)

Domyślnie, czas odpowiedzi dla REX to 250ms; 500 ms dla innych stref wejść. Czas przywrócenia alarmu to domyślnie 500 ms. Aplikacja Instalacja ekspresowa (**Express Setup**) pozwala określić **Normalny Stan Wejść (Input Normal State)** oraz **Terminarz Monitorowania (Monitoring Schedule)**.

1 – Wybierz pierwsze niezdefiniowane Wejście linii dozorowej. Zaznacz pole, aby włączyć sekcję języków i przypisać nową nazwę.

2 – Wybierz opcje **Normalnego Stanu Wejść (Input Normal State)**

3 – Wybierz Terminarz Monitoringu z listy. Jeżeli chcesz przypisać inny terminarz do wybranego Wejścia linii dozorowej, musisz go określić Definiowanie > Terminarze.

Definiowanie pomocniczych wyjść (LED, brzęczyk) (Defining Auxiliary Outputs (LED and Buzzer))

Jeżeli chcesz zmienić ich przypisanie, możesz to zrobić w trakcie definiowanie kontrolera albo KTES lub w Urządzenia > Wyjścia.

1 - Wybierz pierwsze niezdefiniowane wyjście. Zaznacz pole, aby włączyć sekcję języków i przypisać nową nazwę.

2 – Zaznacz odpowiednią opcję dla **Trybu działania (Operating mode)**.

3 – Przypisz drzwi do wyjścia z listy.

Poniższa tabela przedstawia, jak przez system są wykorzystane strefy wyjść.

Pomocnicze wyjście	Wykorzystanie	Kontrolery
1	LED Drzwi 1	KT-100, KT-200, KT-300 oraz KTES
2	Brzęczyk Drzwi 1	
3	LED Drzwi 2	KT-200 oraz KT-300
4	Brzęczyk Drzwi 2	
3	LED Drzwi 1	KT-400
4	Brzęczyk Drzwi 1	
7	LED Drzwi 2	
8	Brzęczyk Drzwi 2	
11	LED Drzwi 3	
12	Brzęczyk Drzwi 3	
15	LED Drzwi 4	
16	Brzęczyk Drzwi 4	



Narzędzia bazy danych (Database Utility)

Program weryfikuje spójność tabel bazy danych, które są wykorzystywane do gromadzenia zdarzeń, alarmów, alarmów sieciowych oraz grafik. Generalnie, system skanuje wszystkie tabele bazy danych i naprawia błędy (o ile takowe napotka). Zazwyczaj, system weryfikuje spójność bazy danych automatycznie przy uruchomieniu. Jeżeli użytkownik zdecyduje o nieprzeprowadzeniu weryfikacji przy uruchomieniu, może przeprowadzić operację później, przy pomocy programu. Może również pojawić się potrzeba użycia programu, kiedy system ma częste problemy z funkcjonalnością. Operacja powinna być przeprowadzona w momencie, kiedy system nie jest wykorzystywany, ponieważ w trakcie operacji bazy danych nie są dostępne. Niektóre weryfikacje, takie jak przeindeksowywanie plików archiwalnych, aktualizowanie pól bazy danych, weryfikowanie plików archiwalnych albo zmiana języków; wymagają zamknięcia aplikacji EntraPass.

Notatka: serwer EntraPass musi być wyłączony zanim uruchomisz program Narzędzia bazy danych (Database Utility).

Uruchamianie Narzędzia bazy danych (Running the Database Utility)

1 – Możesz uruchomić narzędzie przy pomocy przycisków w zakładce Narzędzia (Utility) w aplikacji Serwer EntraPass albo uruchomić ją z menu Start Windows > Wszystkie programy > EntraPass Corporate Edition > Stacja robocza> Narzędzie bazy danych.

Notatka: po wybraniu Plik > menu stacji roboczej, system wyświetli dwa przyciski: Weryfikuj integralność bazy danych oraz Aktualizuj bazę danych. Plik > menu serwera oferuje większy wybór.

Weryfikowanie spójności bazy danych (Verifying Database Integrity)

1 – Kliknij przycisk **Weryfikuj spójność bazy danych (Verify database integrity)** na pasku narzędzi. Możesz przeprowadzić ekspresowe albo pełne sprawdzenie.

- Szybkie sprawdzenie (Quick check): system skanuje tabele bazy danych, ale nie wyświetla szczegółowego raportu.
- Pełne sprawdzenie (Complete check): system skanuje tabele bazy danych oraz wyświetla szczegółowy raport.

Aktualizowanie pól bazy danych (Updating Database Fields)

Ta funkcja uruchamia się automatycznie przy aktualizacji oprogramowania. Jeżeli użytkownik przeprowadza przywrócenie bazy danych (Serwer, pasek narzędzi Opcje, Przywróć), pola bazy danych są automatycznie zaktualizowane przy przywróceniu informacji.

1 – Z okna Narzędzie bazy danych EntraPass, wybierz Aktualizuj bazę danych.

Notatka: skorzystaj z tej funkcji, jeśli – dla przykładu – masz problemy przy uruchamianiu serwera albo stacji roboczej. Kiedy system nie chce się uruchomić, może to oznaczać problemy z bazą danych.

Weryfikowanie indeksu bazy danych (Verifying Database Index)

Program pozwala na całkowite przebudowanie indeksu bazy danych przy użyciu informacji z głównej bazy danych i pogrupowaniu ich w celu przebudowania bazy danych Registry.DB. Służy do zwiększenia wydajności systemu.

Notatka: program może zostać wykorzystany przy problemach z bazą danych, ponieważ nie została zapisana.

Weryfikowanie linków bazy danych (Verifying Database Links)



EntraPass - Instrukcja instalacji i obsługi programu Dodatkowe aplikacje i narzędzia programistyczne

Jest wykorzystywane do przebudowania wszystkich linków bazy danych. Ponadto, program czyści bazę danych poprzez usuwanie linków, które nie są już aktywne. Na przykład, kiedy zostanie usunięty terminarz, który wcześniej był przypisany do określonej funkcjonalności, system sformatuje pole, w którym był przypisany w głównej bazie danych. Usunie również wszystkie wpisy prowadzące do usuniętego komponentu. Narzędzie umożliwia zarządzanie linkami pomiędzy wszystkimi komponentami i zapewnia, że wyświetlana jest prawidłowa informacja:

- Podczas wyświetlania struktury połączeń/linków pomiędzy komponentami systemu.
- Podczas usuwania wszystkich śladów po danym komponencie wewnątrz bazy danych, kiedy komponent zostanie usunięty.

Notatka: konieczność użycia tego programu może wystąpić w sytuacji, kiedy wiadomo, że linki bazy danych są nieprawidłowe. Ta opcja przydaje się, kiedy system wyłącza się/zawiesza się w niestandardowy sposób.

Weryfikowanie hierarchii bazy danych (Verifying Database Hierarchy)

W EntraPass bazy danych są ustawione hierarchicznie, co oznacza, że wszystkie komponenty mają „nadrzędne” i „podrzędne” komponenty. **Weryfikowanie hierarchii bazy danych** służy do odbudowywania linków nadrzędne-podrzędne wewnątrz bazy danych. Jeżeli uszkodzenia bazy danych są rozległe, program ma ograniczoną możliwość działania.

Notatka: kiedy użytkownik próbuje uzyskać dostęp do kontrolera poprzez wybranie bramki oraz połączenia, a rezultat tych działań odbiega od rzeczywistości, oznacza to, że hierarchia bazy danych jest prawdopodobnie uszkodzona. W takim przypadku opcja Weryfikowania hierarchii bazy danych (Verifying Database Hierarchy) może zostać wykorzystana do rozwiązania problemu. Jeśli problem nie został naprawiony może to oznaczać, że baza danych jest zbyt uszkodzona. Konieczne będzie przywrócenie bazy danych.



Weryfikowanie plików archiwalnych bazy danych (Verifying Database Archive Files)

Ta funkcja służy do weryfikowania plików archiwalnych. Przypisuje nowe, unikalne wartości do wszystkich głównych indeksów plików archiwalnych.

Weryfikowanie plików czasu pracy (Verifying In/Out Files)

Ta funkcja jest używana do weryfikowania plików wej/wyj. Przypisuje nowe, unikalne wartości do wszystkich głównych indeksów plików wej/wyj.

Weryfikowanie plików zdarzeń wideo (Verifying Video Event Files)

Ta funkcja jest używana do weryfikowania plików zdarzeń wideo. Przypisuje nowe, unikalne wartości do wszystkich głównych indeksów plików zdarzeń wideo. Zależnie od ilości plików zacznij od **szybkiego sprawdzenia**. Jeżeli pojawią się błędy, przejdź do **pełnego sprawdzenia**.

Podmiana opisów (Swapping Descriptions)

Ta funkcja jest wykorzystywana do podmienienia opisów bazy danych.

Czyszczenie bazy danych (Cleaning the Database)

Ta opcja służy do skasowania z bazy danych zapisów, które zostały zidentyfikowane przez system, jako usunięte. Większość tych zapisów odnosi się do kart, które są przechowywane w sekcji **Usunięte komponenty**. Użycie tej funkcji zmniejszy przestrzeń zajmowaną przez bazę danych. Zwiększy także wydajność systemu przy wyszukiwaniu informacji o kartach. Nie będzie miała wpływu na Rejestr, ani na archiwalne raporty.

Notatka: zaleca się wykonanie kopii zapasowej systemu przed przeprowadzeniem tej operacji. Opcja Czyszczenie bazy danych zawiesi wszystkie operacje na czas trwania czyszczenia.

Odbudowywanie plików ostatniej transakcji karty (Rebuilding Card Last Transaction Files)

Ta funkcja służy do odbudowywania plików ostatniej transakcji karty.



EntraPass - Instrukcja instalacji i obsługi programu Dodatkowe aplikacje i narzędzia programistyczne



Stacja EntraPass Video (EntraPass Video Vault)

Aplikacja jest odpowiedzią na potrzebę optymalnego przechowywania danych wideo oraz zarządzania archiwami. Umożliwia łatwy sposób na kolekcjonowanie ważnych nagrań do późniejszego wykorzystania. Nagrania wideo mają „krótki czas życia”, zależny od ustawień serwera wideo oraz możliwości. Ponadto, ponieważ nagrania zabierają ogromne przestrzenie powierzchni dyskowej, wykorzystania narzędzia takiego jak EntraPass Video Vault umożliwia lepsze zarządzanie i łatwiejsze odzyskiwanie nagrań wideo. EntraPass Video Vault umożliwia użytkownikom:

- Sprawdzenie statusu żądania archiwizacji wideo.
- Monitorowanie statusu serwera wideo powiązanego z aktywną aplikacją EntraPass Video Vault.
- Monitorowanie pobierania logów nagrań.
- Archiwizowanie segmentów wideo.

EntraPass Video Vault przetworzy następujące typy nagrań segmentów wideo:

- Segmenty, które zostały aktywowane automatycznie
- Segmenty, które zostały aktywowane zdalnie
- Segmenty nagrane po aktywowaniu serwera wideo
- Segmenty wideo oznaczone do archiwizowania

Notatka: aplikacja EntraPass Video Vault wymaga dodatkowej licencji. Można zainstalować więcej niż jedną aplikację EntraPass Video Vault. Każda zainstalowana aplikacja EntraPass Video Vault musi zostać skonfigurowana pod kątem działania z EntraPass (Urządzenia > aplikacja EntraPass).

Instalowanie EntraPass Video Vault (Installing the EntraPass Video Vault)

Do instalacji EntraPass Video Vault wymagany jest Certyfikat. Zobacz: **Dodawanie komponentów systemu (Adding System Components)**.



Uruchamianie EntraPass Video Vault (Launching the EntraPass Video Vault)

Przy uruchamianiu aplikacja EntraPass Video Vault próbuje nawiązać połączenie z serwerem EntraPass. Jeżeli uruchamiasz aplikację po raz pierwszy, musisz wprowadzić adres IP serwera EntraPass. Upewnij się, że najpierw uruchomiłeś serwer EntraPass, zanim uruchomisz EntraPass Video Vault.

1 – Uruchom EntraPass Video Vault z menu Start Windows albo z paska skrótów Pulpitu.

- Główny katalog Video Vault: główny katalog, w którym przechowywane są segmenty wideo. Jest określony w trakcie konfigurowania EntraPass Video Vault (aplikacja stacji roboczej EntraPass > Urządzenia > Aplikacja EntraPass > EntraPass Video Vault). Domyślnie: C:\Kantech Video Vault.
- Obecny proces: określa liczbę segmentów wideo, które są odzyskiwane w celu archiwizacji.
- Archiwizowanie plików (KVI, KVA, AVI, IMG): pokazuje liczbę segmentów wideo odzyskiwanych przez EntraPass Video Vault.
- Domyślny format plików wideo: domyślny format do archiwizowania plików. Jest określony w trakcie konfigurowania EntraPass Video Vault (aplikacja stacji roboczej EntraPass > Wideo > Serwer wideo > zakładka parametry Video Vault).
- Rejestrowanie serwera(ów) wideo: wskazuje liczbę serwerów wideo powiązanych z aktywną aplikacją EntraPass Video Vault. Aplikacja jest powiązana z serwerem wideo w trakcie określania serwera wideo ((aplikacja stacji roboczej EntraPass > Wideo > Serwer wideo > zakładka parametry Video Vault).
- Zliczanie błędów procesowania: wskazuje liczbę procesów archiwizacji nagrań, które nie zakończyły się sukcesem. Aby sprawdzić, dlaczego archiwizacja nie powiodła się, zaloguj się do Video Vault > Menu Akcje > Lista Serwerów Wideo. EntraPass umożliwia ponowną próbę zarchiwizowania nagrań z okna Lista Zdarzeń Wideo: aplikacja stacji roboczej EntraPass > Wideo > Lista Zdarzeń Wideo.

Zarządzanie zarchiwizowanymi segmentami wideo (Managing Archived Video Segments)

1 – Z głównego okna EntraPass Video Vault, wybierz System > Zaloguj się, aby uruchomić EntraPass Video Vault, a następnie zaloguj się.

2 – Wprowadź Nazwę użytkownika i Hasło dla EntraPass Video Vault. Następnie kliknij OK, aby zamknąć okno Operatora. Nie możesz zalogować się do dwóch aplikacji EntraPass jednocześnie przy pomocy tej samej nazwy użytkownika i hasła. Ponieważ musisz używać jednocześnie EntraPass Video Vault i serwera EntraPass, upewnij się, że używasz innej nazwy użytkownika dla EntraPass Video Vault.

Notatka: aby sprawdzić szczegółowe informacje na temat wartości numerycznych wyświetlanych w głównym oknie, zaloguj się do EntraPass Video Vault.

3 – Wybierz Podgląd Serwera wideo z menu, aby sprawdzić listę Serwerów wideo powiązanych z aplikacją EntraPass Video Vault oraz status procesu archiwizacji.



EntraPass - Instrukcja instalacji i obsługi programu Dodatkowe aplikacje i narzędzia programistyczne

- Serwer wideo online, okres archiwizowania ważny: w tym przedziale serwer EntraPass otrzymuje segmenty wideo z serwera Wideo i kolejkuje je do archiwizowania w EntraPass Vault. Wszystkie fragmenty pochodzące z przełącznika (automatycznego lub manualnego) oraz oznaczone do zarchiwizowania są archiwizowane w EntraPass Video Vault.
- Serwer wideo offline, okres archiwizowania ważny: ten status jest oznaczony czerwoną flagą. Oznacza, że serwer EntraPass nie może otrzymywać segmentów z serwera Wideo z różnych powodów. Segmenty wideo nagrane podczas tego okresu nie będą dostępne w EntraPass Video Vault.
- Serwer wideo online, okres archiwizowania nieważny.
- Serwer wideo offline, okres archiwizowania nieważny.

4 – Aby sprawdzić dysk, na którym dane wideo są archiwizowane, wybierz **Sprawdź listę dysków**. Okno pokazuje status wszystkich plików otrzymanych przez EntraPass Video Vault z serwera Wideo.

- Dysk gotowy
- Wolne miejsce na dysku: poniżej 100MB
- Dysk sieciowy niedostępny
- Brak dostępu do dysku

5 – Wybierz **Transakcje (Transaction log)**, aby podejrzeć listę błędów transakcji.

Notatka: okno Transakcje wyświetla wszystkie transakcje, które miały miejsce od ostatniego uruchomienia aplikacji. Filtry umożliwiają użytkownikowi wybór rodzaju transakcji, który ma zostać wyświetlony.



Aplikacja Instalacja ekspresowa (Express Setup Program)

Program oferuje szybki i prosty sposób na konfigurowanie wszystkich komponentów bramek systemu, m.in: typ czytników, liczby połączeń, nazwy połączeń, liczby kontrolerów na połączeniu, etc. Na przykład, umożliwia użytkownikowi zmianę nazwy drzwi poprzez automatyczne przypisanie ustawień domyślnych dla wszystkich przekaźników i wejść kontrolera podłączonego do wybranych drzwi.

Konfigurowanie połączenia bramki multi-obiektowej przy pomocy Express Setup (Configuring a Multi-site Gateway connection Using Express Setup)

1 – Z menu Start Windows: Start > **Wszystkie programy** > EntraPass Corporate Edition > Stacja robocza/serwer > Express Setup. Możesz również uruchomić Express Setup klikając na przycisk Express Setup w oknie rejestracji albo w oknie definiowania bramki.

2 – Z menu Start Windows: Start > **Wszystkie programy** > EntraPass Global Edition > Stacja robocza/serwer > Express Setup. Możesz również uruchomić Express Setup klikając na przycisk Express Setup w oknie rejestracji albo w oknie definiowania bramki.

Notatka: okno Logowanie operatora pojawia się tylko wtedy, kiedy uruchamia się Ustawienia ekspresowa w trybie stand-alone.

3 – Wprowadź swoją nazwę Użytkownika i hasło, po czym kliknij OK.

4 – Wybierz bramkę dla której chcesz skonfigurować połączenie, a następnie kliknij **Nowy**.

5 – Wprowadź nazwę połączenia w polu opisu połączenia, następnie wybierz typ czytnika.

6 – Wybierz typ czytnika dla tego połączenia.

Notatka: opcja KTES jest dostępna tylko dla multi obiektowych bramek.

Notatka: nie można wybrać rodzaju czytnika, ani numeru kontrolera, jeżeli KTES jest wybrany, jako rodzaj kontrolera.



7 – Wybierz Typ czytnika (Reader type).

8 – Ustaw Liczbę kontrolerów (Number of controllers).

9 – Określ Typ połączenia, określając w ten sposób jak połączenie komunikuje się z komputerze,

- Wybierz RS-232 lub USB, jeżeli połączenie jest zintegrowane z komputerem i połączone przez port RS-232. Musisz określić port oraz szybkość transmisji (9600 albo 19200). Domyślnie: 19200.

- Wybierz **RS-232**

- Wybierz **Secure IP (KT-400)**

- Wybierz **Secure IP (KTES)**

- Wybierz **Secure IP (IP Link)**

10 – Kliknij OK.

11 – Określ minimalną konfigurację dla kontrolerów albo KTES zdefiniowanych na obiekcie. Oznacza to przypisanie nazwy do kontrolera/KTES, określenie opcji passback oraz wprowadzenie numeru seryjnego.

Notatka: kolumna numer seryjny pojawia się tylko dla kontrolerów KT-100, KT-300, KT-400 oraz KTES. Kolumna Rodzaj passback pojawia się tylko dla KT-300 oraz KT-400. Opcja passback nie pozwoli na „ponowne” wejście żadnej karcie, które wcześniej nie została wykorzystana do wyjścia. Wymaga to wykorzystanie czytników zarówno na wejściu, jak i wyjściu.

12 – Dla nowych obiektów z KTES, zobacz Punkt 14.



EntraPass - Instrukcja instalacji i obsługi programu Dodatkowe aplikacje i narzędzia programistyczne

13 – Zaznacz **Te same drzwi 1 (Same door 1 and 2)** oraz **2 i Te same drzwi 3 oraz 4 (Same door 3 and 4)**, jeżeli czytnik jest zainstalowany po obu stronach drzwi. Druga opcja dostępna tylko dla KT-400.

14 – Wybierz odpowiedni **Typ Passback (Passback type)** (brak, miękki, twardy). Jeżeli drzwi są zdefiniowane, jako drzwi dostępu, passback nie jest dla nich zdefiniowany. Drzwi wejściowe oraz wyjściowe mogą mieć przypisaną opcję passback.

15 – Przejdź do Punktu 16.

16 – Zaznacz opcję Czujnik stanu drzwi (Door contact).

17 – Zaznacz opcję Zamek (Postal lock), dostępna wyłącznie dla KTES.

18 – Wprowadź **numer seryjny**. Numer seryjny **S/N** zaczyna się zazwyczaj od **Axxxxxxx**.

19 – Kliknij OK. Komponenty powiązane z kontrolerem i obiektem są utworzone w bazie danych serwera. Poniższa tabela przedstawia domyślne wartości, które są przypisane do kontrolerów.

Notatka: kiedy system aktualizuje bazę danych, fakt, że baza danych jest zablokowana symbolizowany jest czerwonym oznaczeniem (oflagowaniem). Jeśli będziesz próbował uruchomić menu systemowe w trakcie zablokowania bazy danych, pojawi się wiadomość informująca o błędzie. Poczekaj, aż baza danych będzie ponownie dostępna.

Kontroler albo KTES	Drzwi	Przełącznik	Strefa Wejścia linii dozorowej	Pomocnicze wyjście
KT-100	1	4	4	2
KT-200	2	2	16	4
KT-300	2	2	8	4
KT-400	4	4	16	16
KTES	1	3	4	2
KT-1	1	2	5	5



EntraPass - Instrukcja instalacji i obsługi programu
Dodatkowe aplikacje i narzędzia programistyczne

Poniższa tabela podsumowuje, jak strefy Wejścia linii dozorowej są wykorzystywana przez kontrolery.

Strefa Wejścia linii dozorowej	Wykorzystanie	Kontrolery
1	Czujnik stanu drzwi 1	KT-100, KT-200, KT-300, KT-400, KT-1
2	REX Drzwi 1	
3	Czujnik stanu drzwi 2	KT-300
4	REX Drzwi 2	
5	Czujnik stanu drzwi 2	KT-400
6	REX Drzwi 2	
9	Czujnik stanu drzwi 2	KT-200
10	REX Drzwi 2	
9	Czujnik stanu drzwi 3	KT-400
10	REX Drzwi 3	
13	Czujnik stanu drzwi 4	
14	REX Drzwi 4	

Poniższa tabela podsumowuje, jak strefy Wejścia linii dozorowej są wykorzystywana przez system dla KTES.

Strefa Wejścia linii dozorowej	Wykorzystanie	KTES
1	Czujnik stanu drzwi	KTES
2	Zamek	
3	REX Drzwi	
4	Future	

Poniższa tabela podsumowuje, jak strefy wyjścia są wykorzystywane przez system.

Pomocnicze wyjście	Wykorzystanie	Kontrolery
1	LED Drzwi 1	KT-100, KT-200, KT-300 oraz KTES
2	Brzęczyk Drzwi 1	
3	LED Drzwi 2	KT-200 oraz KT-300
4	Brzęczyk Drzwi 2	



EntraPass - Instrukcja instalacji i obsługi programu
Dodatkowe aplikacje i narzędzia programistyczne

Pomocnicze wyjście	Wykorzystanie	Kontrolery
1	WYJ1 (Drzwi 1)	KT-400
2	WYJ2 (Drzwi 1)	
3	LED (Drzwi 1)	
4	Brzęczyk (Drzwi 1)	
5	WYJ1 (Drzwi 2)	
6	WYJ2 (Drzwi 2)	
7	LED (Drzwi 2)	
8	Brzęczyk (Drzwi 2)	
9	WYJ1 (Drzwi 3)	
10	WYJ2 (Drzwi 3)	
11	LED (Drzwi 3)	
12	Brzęczyk (Drzwi 3)	
13	WYJ1 (Drzwi 4)	
14	WYJ2 (Drzwi 4)	
15	LED (Drzwi 4)	
16	Brzęczyk (Drzwi 4)	
1	WYJ1 (Drzwi 1)	KT-1
2	WYJ2 (Drzwi 1)	
3	LED (Drzwi 1)	
4	Brzęczyk (Drzwi 1)	
5	Nieprzenoszalnym	

Notatka: pozostałe komponenty (przełączniki oraz strefy wejść (input)) są niezidentyfikowane, to znaczy, że zostały utworzone, ale jeszcze nie dokonano ich zdefiniowania. Zdefiniowane komponenty są „wyszarzone”. Nie możesz ich wybrać, ani zmienić ich opisu. Możesz tego dokonać w ich menu definiowania (Urządzenia > Przełączniki/Strefy wejść (Input)).

Domyślnie system zakłada, że:

- Czytnik: ioProx Kantech XSF
- Nadzór zasilania jest zawsze ważny.
- Opóźnienie bezpieczeństwa jest ustawione na 45 sekund.
- Typ opornika jest: **żaden** (KT-100, KT-300, KT-400 oraz KTES),
- Opóźnienie oczekiwania na drugą kartę: 30 sekund.



Konfigurowanie kontrolera przy pomocy Express Setup (Configuring a Controller Using Express Setup)

Jeżeli wybierzesz typ połączenia dla nowego obiektu i od razu zapiszesz, system zaproponuje użycie Express Setup do zdefiniowania urządzenia.

1 – W oknie Kontroler, wybierz niezdefiniowany kontroler.

2 – W zakładce **Ogóle (General)**, wybierz **Typ kontrolera (Controller type)**.

3 – Kliknij **Zapisz**, powinna pojawić się wiadomość: Czy chcesz użyć **Programu Ekspresowe ustawienia (Express Setup)** do konfigurowania urządzenia? Kliknij Tak.

- Jeżeli kliknąłeś Nie, zawsze będziesz mógł wrócić do **Programu Ekspresowe ustawienia (Express Setup)** klikając w przycisk.

Notatka: należy pamiętać, że KT-300 jest 2-drzwiowym systemem, a KT-400 4-drzwiowym.

4 – Określ, czy oba czytniki są zainstalowane na tych samych drzwiach (nie dla KTES). Jeżeli są, czujnik REX jest wyłączony.

5 – Kliknij przycisk **Zaawansowane**, aby określić inne urządzenia, takie jak: drzwi, Wejścia linii dozоровej, przekaźniki i wyjścia.

Notatka: komponenty są wylistowane w panelu po lewej stronie. Powiązane zakładki są wyświetlone na środku okna. Kiedy wybierzesz komponent, jego domyślna nazwa, numer oraz ustawienia domyślne są wyświetlone w sekcji językowej (language section). Wybierz komponent, aby włączyć jego zakładkę. Komponenty, które są już przypisane są „wyszarzone” i nie mogą być modyfikowane na tym etapie. Jednakże, później możesz modyfikować dowolny opis komponentu (Urządzenia > Kontroler/Drzwi/Przełącznik/Wejście linii dozоровej (Input)/Wyjście).



Konfiguracja kontrolerów pomocą Instalacji ekspresowej (Configuring a KTES Using Express Setup)

Jeżeli wybierzesz typ połączenia dla nowego obiektu i od razu zapiszesz, system zaproponuje użycie Express Setup do zdefiniowania urządzenia.

1 – W oknie **Obiekt**, kliknij **Nowy**, aby określić nowy obiekt. Przypisz mu nazwę.

2 – W zakładce **Ogóle (General)**, wybierz **Typ kontrolera (Controller type): Secure IP (KTES)**.

3 – Kliknij **Zapisz**, powinna pojawić się wiadomość: Czy chcesz użyć **Programu Ekspresowe ustawienia (Express Setup)** do konfigurowania urządzenia? Kliknij Tak.

- Jeżeli kliknąłeś Nie, zawsze będziesz mógł wrócić do **Programu Ekspresowe ustawienia (Express Setup)** klikając w przycisk.

4 – Zaznacz opcje **Czujnik stanu drzwi (Door contact)** oraz **Czujnik stanu REX (REX contact)**.

5 – Zaznacz opcje **Zamka (Postal Lock)**.

6 - Kliknij przycisk **Zaawansowane**, aby określić inne urządzenia, takie jak: drzwi, Wejścia linii dozorowej, przekaźniki i wyjścia.

Notatka: komponenty są wylistowane w panelu po lewej stronie. Powiązane zakładki są wyświetlone na środku okna. Kiedy wybierzesz komponent, jego domyślna nazwa, numer oraz ustawienia domyślne są wyświetlone w sekcji językowej (language section). Wybierz komponent, aby włączyć jego zakładkę. Komponenty, które są już przypisane są „wyszarzone” i nie mogą być modyfikowane na tym etapie. Jednakże, dzięki menu KTES możesz później modyfikować dowolny opis komponentu (Urządzenia > KTES).



Definiowanie przekaźników (Defining Relays)

Możesz skonfigurować przekaźniki, aby określić ich tryb działania, aktywacji i dezaktywacji terminarzy. Jeżeli chcesz przypisać nazwę do przekaźnika, musisz go wybrać. Jeżeli wybierzesz przycisk Zaznacz wszystkie, nazwy domyślne zostaną zachowane.

1 – Wybierz pierwszy przekaźnik, jeżeli chcesz zmienić jego opis. Przekaźnik jest dostępny. Zaznacz pole obok nazwy przekaźnika, aby włączyć sekcję języków.

2 – Zaznacz odpowiednią opcję dla **Trybu działania (Operating mode)**.

3 – Z listy **Terminarz automatycznych aktywacji (Automatic activation schedule)** wybierz odpowiedni terminarz aktywacji.

4 – Z listy **Wyłącz działanie przekaźnika (Disable relay action)**, wybierz odpowiednią akcję.

Definiowanie wejść (Defining Inputs)

Domyślnie, czas odpowiedzi dla REX to 250ms; 500 ms dla innych stref wejść. Czas przywrócenia alarmu to domyślnie 500 ms. Aplikacja Instalacja ekspresowa (**Express Setup**) pozwala określić **Normalny Stan Wejść (Input Normal State)** oraz **Terminarz Monitorowania (Monitoring Schedule)**.

1 – Wybierz pierwsze niezdefiniowane wejście. Zaznacz pole, aby włączyć sekcję języków i przypisać nową nazwę.

2 – Wybierz opcje **Normalnego Stanu Wejść (Input Normal State)**

3 – Wybierz Terminarz Monitoringu z listy. Jeżeli chcesz przypisać inny terminarz do wybranego Wejścia linii dozorowej, musisz go określić Definiowanie > Terminarze.



Definiowanie pomocniczych wyjść (LED, brzęczyk) (Defining Auxiliary Outputs (LED and Buzzer))

Jeżeli chcesz zmienić ich przypisanie, możesz to zrobić w trakcie definiowania kontrolera albo KTES lub w Urządzenia > Wyjścia.

1 - Wybierz pierwsze niezdefiniowane wyjście. Zaznacz pole, aby włączyć sekcję języków i przypisać nową nazwę.

2 – Zaznacz odpowiednią opcję dla **Trybu działania (Operating mode)**.

3 – Przypisz drzwi do wyjścia z listy.

Poniższa tabela przedstawia, jak przez system są wykorzystane strefy wyjść.

Pomocnicze wyjście	Wykorzystanie	Kontrolery
1	LED Drzwi 1	KT-100, KT-200, KT-300 oraz KTES
2	Brzęczyk Drzwi 1	
3	LED Drzwi 2	KT-200 oraz KT-300
4	Brzęczyk Drzwi 2	
3	LED Drzwi 1	KT-400
4	Brzęczyk Drzwi 1	
7	LED Drzwi 2	
8	Brzęczyk Drzwi 2	
11	LED Drzwi 3	
12	Brzęczyk Drzwi 3	
15	LED Drzwi 4	
16	Brzęczyk Drzwi 4	

Diagnostyka PING (PING Diagnostic)

Osobny program jest wykorzystywany do diagnozowania problemów z przerywaniem połączenia sieci oraz/lub do określenia czy konkretny adres IP jest dostępny. Działa poprzez wysłanie pakietu danych na konkretny adres i oczekiwanie na odpowiedź. Program do diagnostyki PING jest wykorzystywany głównie do rozwiązywania problemów z połączeniami internetowymi.

Notatka: jeśli chcesz, aby ta opcja była dostępna, musisz wybrać Diagnostyka sieci (Allow diagnostic on network) przy definiowaniu parametrów serwera.

1 – Z menu Start Windows, kliknij Start > Wszystkie programy > EntraPass Corporate Edition > Stacja robocza/Serwer > Diagnostyka PING.

2 – Z listy wybierz aplikację, którą chcesz monitorować (Serwer, stacja robocza, bramka, etc.).

3 – Wybierz wielkość pakietu danych z listy. Wielkość: od 1KB do 1024KB (1MB).

4 – W polu adres TCP/IP, wprowadź adres IP komputera, dla którego chcesz sprawdzić połączenie.

Notatka: aby uzyskać adres TCP-IP skontaktuj się ze swoim Administratorem sieci.

5 – Kliknij przycisk Test, aby uruchomić polecenie. Informacja zostanie wysłana 16 razy. System wyświetli ilość bajtów wysłanych i otrzymanych oraz opóźnienie (w milisekundach).



Notatka: opóźnienie pomiędzy podejściami powinno być podobne, za wyjątkiem pierwszego, które może być dłuższe. Jeśli nie otrzymasz odpowiedzi, wiadomość zostanie wyświetlona w następującym formacie: Sent(block) Bytes, No Answer (1717).

Przeglądarka raportów (Quick Report Viewer)

Jest to program, który pozwala użytkownikowi podgląd zapisanych wcześniej raportów bez potrzeby uruchamiania EntraPass. Jest wykorzystywany do podglądu/wyświetlenia/wczytania raportów, które zostały wcześniej zapisane (w formacie .QRP) podczas podglądu wydruku albo Szybkiego raportu. Zobacz: **Żądanie raportu (Requesting Reports)**. Program jest przydatny w momencie, kiedy EntraPass jest offline, a raport musi zostać sprawdzony.

1 – Z menu Start Windows, kliknij Start > Wszystkie programy > EntraPass > Serwer > Przeglądarka Szybkich raportów.

2 – Kliknij Otwórz, aby otworzyć raport.

3 – Domyślnie, kiedy raport jest zapisany w formacie QRP, system automatycznie zapisze go w folderze Moje Dokumenty.

4 – Kliknij Otwórz, aby włączyć podgląd raportu. Wybierz raport.

5 – Przy pomocy przycisków paska narzędzi sprawdź raport:



Przycisk Pomniejsz: „oddala” podglądany raport.

Przycisk Powiększ: „przybliża” raport.



Poprzednia/Następna strona: zmienia strony.



Otwórz: otwiera raport zapisany w dowolnym folderze.



Drukuj: raport zostanie automatycznie wydrukowany; okno wydruku nie zostanie wyświetlone. Aby anulować, kliknij Anuluj.



Wyjdź: zamyka aplikację.



Aplikacja SmartLink Interface (The SmartLink Interface)

Aplikacja SmartLink Interface pozwala użytkownikowi określić wiadomość i typ formatu, który może być wysłany do drugiego portu COM albo do pliku na dysku. Poniżej znajduje się instrukcja, które informuje jak stworzyć ciąg/napis, który może zostać wysłany przez SmartLink. Przy pomocy SmartLink możesz przyłączyć się niemalże każdego inteligentnego urządzenia. Aby to zrobić, utworzony zostaje link RS-232 pomiędzy stacją roboczą EntraPass, a zewnętrznym urządzeniem. Niezbędne polecenia oraz protokoły mogą być łatwo edytowane na połączeniu.

SmartLink ułatwia połączenia z „obcymi” inteligentnymi urządzeniami, ponieważ dostarcza instalatorowi systemu wszystkie niezbędne narzędzia do zbudowania i nadzorowania połączenia bez potrzeby dokupowania „specjalnych” sterowników. W komunikacji, link to linia albo kanał, po których transmitowane są dane z jednego komputera na drugi, albo z jednego urządzenia na drugie. Urządzenia do komunikacji to tym samym urządzenie, które asystuje przy transmisji danych (modem, kabel, part, etc.).

Wymagania (Required Material)

- Komputer spełniający te same wymagania, co stacja robocza EntraPass (zobacz: **Minimalne wymagania systemowe (Minimum System Requirements)**).
- płyta instalacyjna SmartLink z numerem seryjnym.

Instalacja (Installation)

1 – Stwórz nową aplikację w menu **Rejestracja Stacji Roboczej (Workstation Registration)**, aby dowiedzieć się więcej o tym, jak stworzyć nową aplikację, zobacz: **Minimalne wymagania systemowe (Minimum System Requirements)**).

2 – Zainstaluj aplikację SmartLink na komputerze (zobacz: **Instalacja Systemu (System Installation)**).

Notatka: EntraPass Web zostanie automatycznie zainstalowany razem ze SmartLink.

3 – Po zainstalowaniu, skonfiguruj aplikację.

4 – Jeżeli korzystasz z Trybu Wiadomości, będziesz musiał stworzyć zadania. Aby dowiedzieć się więcej o tym, jak stworzyć zadania, zobacz: **Definiowanie Makro-poleceń(Task Builder Definition)**.

Konfigurowanie aplikacji SmartLink (Configuring the SmartLink Application)

Konfiguracja może zostać przeprowadzona na zwykłej stacji roboczej EntraPass. Zależnie od trybu, który będzie wykorzystany do SmartLink (**Wiadomości** albo **Polecenia**), musisz odpowiednia zaprogramować stację roboczą.

Uruchamianie aplikacji SmartLink (Starting the SmartLink Application)

1 – Na komputerze na którym zainstalowany jest SmartLink, kliknij na menu Start Windows: Start > Wszystkie programy > EntraPass > SmartLink > SmartLink. Zostanie uruchomiona aplikacja SmartLink. Aby dowiedzieć się więcej zobacz: *SmartLink Reference Manual DN1327*.

Notatka: ograniczone wsparcie jest udzielane na interfejsie SmartLink.



EntraPass - Instrukcja instalacji i obsługi programu
Dodatkowe aplikacje i narzędzia programistyczne



Edytor słownika (Vocabulary Editor)

Edytor Słownika pozwala użytkownikowi na przetłumaczenie wyświetlanego tekstu na wybrany język. EntraPass umożliwia dodanie do 99 nowych języków. Należy przy tym pamiętać, że program może działać tylko przy dwóch aktywnych językach na raz: głównym i pomocniczym. Jeżeli chcesz używać programu w języku innym niż: angielski, francuski, niemiecki, włoski lub hiszpański; możesz przetłumaczyć bazę danych na dowolny język. Następnie będziesz musiał zintegrować słownik z oprogramowaniem. Tworzenie nowego języka odbywa się w trzech etapach.

- Tłumaczenie tekstu źródłowego.
- Integrowanie nowo utworzonego języka ze słownikiem na serwerze.
- Przesłanie nowego języka do wszystkich aplikacji EntraPass.

Notatka: aby mieć możliwość korzystania z dodatkowego języka, twój system operacyjny musi obsługiwać ten język. Na przykład, twoja klawiatura oraz okno muszą obsługiwać charakterystyczne znaki dla danego języka. Komputery, na których działa EntraPass, również muszą obsługiwać wybrany, dodatkowy język. Aby dowiedzieć się więcej, skontaktuj się ze swoim administratorem systemu.

Instalowanie Edytora słownika (Installing the Vocabulary Editor)

Edytor słownika jest osobnym programem. Możesz go zainstalować i uruchamiać niezależnie. Jeżeli chcesz przetłumaczyć język systemu, musisz zainstalować Edytor, a następnie przetłumaczyć bazę danych słownika.

Notatka: nie potrzebujesz dodatkowej licencji, aby zainstalować Edytor słownika. Musisz go tylko wybrać w menu Ustawienia. Zobacz Instalacja systemu, aby dowiedzieć się więcej.



Tłumaczenie języka systemowego (Translating the System Language)

Edytor słownika EntraPass jest osobnym programem. Możesz go zainstalować i uruchamiać niezależnie bez uruchamiania aplikacji EntraPass. Edytor pomoże przetłumaczyć słownik na nowy język, jeżeli chcesz używać programu w języku innym niż: angielski, francuski, niemiecki, włoski lub hiszpański;

1 – Uruchom Edytor słownika z menu Start Windows: Start > Wszystkie programy > EntraPass Corporate Edition > Edytor słownika > Edytor słownictwa.

2 – Wybierz jeden z **dostępnych języków** i kliknij Nowy. System wyświetli okno **Wybierz język**.

3 – Wybierz język źródłowy dla instalacji i kliknij OK. Wybrany język zostaje przeniesiony na listę **Wybrane języki (Custom Languages)** po prawej.

4 – Kliknij na nowym **Wybranym języku**, a następnie na **Edytuj Wybrany język**, aby rozpocząć tłumaczenie słownictwa oprogramowania. System wyświetli bazę danych słownika.

Notatka: musisz sprawdzać, czy katalogi słowników są regularnie zapisywane/aktualizowane
C:\ProgramFiles\Kantech\Vocabulary Editor\CustomDictionary\files.xxx.ath albo
C:\ProgramFiles\Kantech\„Application type”\CustomDictionary\files.xxx.0

Tabela objaśnia oznaczenia kolorami w Edytorze słownika.

Edytor Słownika – oznaczenie kolorami	Znaczenie
Zielony	Prawidłowy tekst
Niebieski/Zielony	Nowy tekst
Czerwony	Nieaktualny tekst

- Kolumna „Język źródłowy” zawiera tekst w podstawowym języku wybranym podczas tworzenia słownictwa. Ta kolumna służy, jako „źródło” dla tłumaczenia i nie może być modyfikowana przez użytkownika.
- Kliknij prawym, aby wyświetlić menu kontekstowe lub użyć paska narzędzi Edytora języka.



Integrowanie Wybranego języka w EntraPass (Integrating the Custom Language in EntraPass)

Po ukończeniu tłumaczenia, musisz zintegrować nowy słownik ze słownikiem systemowym, aby operatorzy systemu mogli z niego korzystać. Poniżej znajduje się opis akcji w oknie edytora słownika. Te działania są również dostępne w menu **Akcje (Actions)**.



Wprowadź zmiany do słownika operacyjnego: sprawdza zmiany przed zaktualizowaniem wszystkich stacji roboczych.



Przywróć słownik operacyjny: przywraca domyślne języki. Tworzy samorozpakowujący się plik, który przywraca oryginalny słownik.



Skanuj słownik w poszukiwaniu nowych wpisów: sprawdza po aktualizacji.



Stwórz samorozpakowujący się plik do aktualizacji: system tworzy plik Updatedictionary.exe i prosi o wybranie miejsca docelowego zapisu.

1 – Uruchom Edytor słownika. Edytor wyświetla pięć przycisków.

Notatka: Interfejs użytkownika grafiki (Graphic User Interface) wyświetli się w jednym z pięciu języków: angielskim, francuskim, niemieckim, włoskim albo hiszpańskim.

2 – Wybierz nowo przetłumaczony słownik.

- Możesz wybrać **Wprowadź zmiany do słownika operacyjnego (Apply changes to the Operational dictionary)**: sprawdza zmiany przed zaktualizowaniem wszystkich stacji roboczych.
- **Przywróć słownik operacyjny (Restore the operational vocabulary)**: przywraca domyślne języki. Tworzy samorozpakowujący się plik, który przywraca oryginalny słownik
- **Skanuj słownik w poszukiwaniu nowych wpisów (Scan dictionary for new entries)**: sprawdza po aktualizacji.

3 – Jeżeli zdecydujesz się wprowadzić nowy słownik, wybierz menu **Akcje**, a następnie wybierz **Stwórz samorozpakowujący się plik do aktualizacji (Create self-extracting file for update)**. System tworzy plik Updatedictionary.exe i prosi o wybranie miejsca docelowego zapisu.

4 – Wybierz miejsce docelowe Updatedictionary.exe; domyślnie: C:\Program Files\Kantech (aplikacja).

Notatka: zaleca się skopiowanie pliku Updatedictionary.exe do folderu sieciowego, aby operatorzy mieli do niego dostęp i mogli aktualizować aplikację.



Rozpowszechnianie słownika nowego systemowego (Distributing the New System Vocabulary)

Zanim uruchomisz plik, upewnij się, że zamknąłeś aplikację EntraPass; inaczej operacje nie powiedzie się. Aby przeprowadzić aktualizację słownika systemu, najpierw musisz zaktualizować serwer EntraPass. Jeżeli masz zainstalowaną aplikację Dublowania bazy danych, zamknij ją zanim wyłączysz serwer (żeby nie uruchomiła serwera redundantnego). Następnie wyłącz główny serwer, zaktualizuj go i uruchom ponownie. Zaktualizuj zdublowaną bazę danych i serwer redundantny, po czym uruchom zdublowaną bazę danych.

Aktualizowanie słownika systemowego (Updating the System Vocabulary)

- 1 – Wyłącz wszystkie programy EntraPass.
- 2 – Uruchom Windows Explorer > Kantech > (aplikacja EntraPass), po czym skopiuj plik Updatedictionary.exe na serwer.
- 3 – Uruchom Updatedictionary.exe. System wyświetli aplikacje EntraPass zainstalowane na komputerze.
- 4 – Wybierz aplikację, po czym kliknij przycisk **Aktualizuj (Update dictionary)**.
- 5 – Musisz skopiować plik Updatedictionary.exe na każdy komputer, na którym zainstalowany jest EntraPass. Przed uruchomieniem aktualizacji, zamknij wszystkie aplikacje EntraPass.
- 6 – Wybierz aplikację, którą chcesz zaktualizować (jedną na raz) i kliknij przycisk **Aktualizuj**.

Notatka: MUSISZ zaktualizować wszystkie aplikacje w systemie.

Notatka: aby przywrócić słownik do wartości domyślnych wykonaj te same procedury, co przy aktualizacji.

7 – Kiedy ukończysz aktualizowanie bazy danych słownika dla **głównego serwera, zdublowanej bazy danych** oraz **serwera redundantnego**, uruchom **główny serwer**.

8 – Wybierz pasek narzędzi **Opcje**, po czym kliknij przycisk **Wybierz język**.

9 – W oknie Wybierz język, wybierz główny język i drugi język. Nowo zintegrowane języki są wyświetlone na liście. Ważne jest, aby na tym etapie wybrać język, ponieważ w innym przypadku operator systemu nie będzie mógł z niego skorzystać.

Notatka: przy zmianie głównego języka (np. angielskiego) na rosyjski, wszyscy operatorzy „otrzymają” rosyjski, jako nowy język główny. Jeśli natomiast zmienisz język pomocniczy (np. francuski) na rosyjski, a operatorzy korzystają z języka głównego (np. angielskiego) wtedy zmianę na rosyjski trzeba przeprowadzić zdalnie. Aby przypisać dany język do operatora skorzystaj z menu Definiowanie systemu, a następnie menu Definiowanie operatora.

10 – Zanim zaktualizujesz aplikację, zaloguj się na serwerze i zweryfikuj język wyświetlania. Jeżeli wszystko wydaje się w porządku możesz kontynuować z aktualizacją systemu. Pamiętaj, komputer musi wspierać język (wyświetlanie oraz klawiatura).

Notatka: dla każdego instalowanego języka upewnij się, że wybrałeś odpowiednią klawiaturę (Start > Ustawienia > Panel sterowania > Klawiatura). Wybrana klawiatura jest wyświetlona na pasku systemu.

Uaktualnianie słownika systemowego (Upgrading the System Vocabulary)

Kiedy aktualizujesz swój system, nowe albo zmodyfikowane wiersze są automatycznie dodawane do słownika systemowego. Jeżeli dodałeś nowe tłumaczenie do swojego systemu, musisz przetłumaczyć nowe/zmodyfikowane linie po aktualizacji systemu. Tym samym musisz prze-edytować słownik i utworzyć nowy samorozpakowujący się plik. Kiedy ponownie otworzysz tabelę słownika, nowe wiersze są zaznaczone przez zielony punkt. Nieaktualne są zaznaczone na czerwono.

Notatka: dla ułatwienia zarządzania rekomendujemy, aby zawsze edytować słownik z tego samego komputera.



EntraPass - Instrukcja instalacji i obsługi programu
Dodatkowe aplikacje i narzędzia programistyczne



Ikony w programie EntraPass

Animowane ikony wskazują na status fizycznych lub logicznych komponentów w oknach oprogramowania EntraPass. Obrazują status komponentu w czasie rzeczywistym i symulują ruch poprzez wyświetlenie serii obrazów powiązanych z komponentem.

Systemy alarmowe (Alarm Systems)

Ikony systemu alarmowego wskazują status systemu alarmowego w oknie map (Pulpit > Okna map) albo w oknie Operacje (Operation).

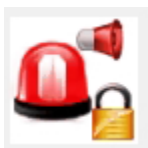
System alarmowy jest w stanie alarmu (Alarm system is in alarm)



Ta animowana ikona wyświetla się, gdy system alarmowy jest w stanie alarmu. Jest wyświetlana w:

- oknie Wiadomości alarmowe, gdy wymagane jest potwierdzenie.
- oknie Operacje (Operation)
- Pulpicie > Okna map.

System alarmowy jest uzbrojony (Alarm system is armed)



Ta animowana ikona wyświetla się, gdy systemu alarmowy jest uzbrojony. Jest wyświetlana w:

- oknie Operacje (Operation)
- Pulpicie > Okna map.

System alarmowy jest uzbrojony z Wejście linii dozorowej w alarmie - wymuszone uzbrojenie (Alarm system is armed with input in alarm (forced arming))



Ta animowana ikona wyświetla się, gdy system alarmowy jest uzbrajany w momencie, gdy obszar monitorowany jest w stanie alarmu. System pozwoli uzbroić system (wymuszone uzbrojenie), a ikony wyświetlą Wejście linii dozorowej w alarmie w:

- oknie Operacje (Operation)
- Pulpicie > Okna map.



Ikony EntraPass

EntraPass - Instrukcja instalacji i obsługi programu Ikony w programie EntraPass

System alarmowy w stanie oczekiwania na zatwierdzenie „żądania uzbrojenia” (Alarm system is in arming request delay)



Ta animowana ikona wyświetla się, gdy system jest w stanie oczekiwania na potwierdzenie „żądania uzbrojenia”. Jest wyświetlana w:

- oknie Operacje (Operation)
- Pulpicie > Okna map.

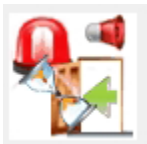
System alarmowy jest wyłączony (Alarm system is disarmed)



Ta animowana ikona wyświetla się, gdy system jest wyłączony. Jest wyświetlana w:

- oknie Operacje (Operation).
- Pulpicie > Okna map.

System alarmowy oczekuje na uruchomienie (Alarm system is in entry delay)



Ta animowana ikona wyświetla się, gdy system alarmowy oczekuje na „wejście”. Jest wyświetlana w:

- oknie Operacje (Operation).
- Pulpicie > Okna map.

System alarmowy oczekuje na zamknięcie (Alarm system is in “Exit” delay)



Ta animowana ikona wyświetla się, gdy system alarmowy oczekuje na „wyjście”. Jest wyświetlana w:

- oknie Zdalne operacje (Manual Operation).
- Pulpicie > Okna map.



Ikony EntraPass

EntraPass - Instrukcja instalacji i obsługi programu Ikony w programie EntraPass

Status systemu alarmowego jest nieznany (Alarm system status is not yet known)



Ta animowana ikona wyświetla się, gdy status systemu alarmowego jest nieznany. Jest wyświetlana w:

- oknie Grafiki (Graphic), Pulpicie > Okna map, kiedy status jest nieznany.

System alarmowy jest w trybie „Wstrzymaj” (Alarm system is in “Postpone” mode)



Ta animowana ikona wyświetla się, gdy system alarmowy jest w trybie „Wstrzymaj”. Kiedy to opóźnienie zostanie zakończone, system ponownie się uzbroi (uruchamiając jednocześnie oczekiwania na zamknięcie). Jest wyświetlana w:

- oknie Operacje (Operation).
- oknie Grafiki (Graphic), Pulpicie > Okna map.

Kontrolery (Controllers)

Animowane ikony kontrolerów wskazują status kontrolerów drzwi w oknie grafiki (Pulpit > Okna map), albo w oknie Operacje (Operation).

Status nieznany (Status unknown)



Ikona pojawia się, gdy aplikacja EntraPass nie otrzymała statusu komponentu po czterech próbach. Jest wyświetlana w:

- oknie Operacje (Operation) (alarmy, obszary, trasy strażników, drzwi, drzwi windy, przekaźniki, etc.)
- Pulpicie > Okna map.

Awaria zasilania kontrolera (Controller AC failure)



Ikona pojawia się, gdy kontroler ma problemy z zasilaniem. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Reset kontrolera



Ikony EntraPass

EntraPass - Instrukcja instalacji i obsługi programu Ikony w programie EntraPass

Błąd w procesie odpytywania kontrolera (Controller Polling Malfunction)



Ikona pojawia się, gdy występują problemy lub błędy w procesie odpytywania kontrolera (np. utrata komunikacji). Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Kontroler

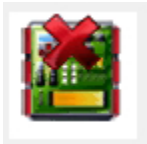
Awaria zasilania kontrolera i przełącznik Czujnika antysabotażowego jest w stanie alarmu (Controller AC failure and Tamper Switch in "alarm")



Ikona pojawia się, gdy kontroler ma problemy z zasilaniem, a przełącznik Czujnika antysabotażowego jest w stanie alarmu. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Reset kontrolera

Brak komunikacji z kontrolerem (Controller is not communicating)



Ikona pojawia się, gdy brak komunikacji z kontrolerem. Jest wyświetlana w:

- oknie operacji – w oknach: obszar, trasa strażnika, reset kontrolera.
- Pulpicie > Okna map.

Komunikacja z kontrolerem w normie – brak problemów (Controller communication is regular (no problem))



Ikona pojawia się, gdy komunikacja z kontrolerem przebiega bez problemów. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Reset kontrolera



Ikony EntraPass

EntraPass - Instrukcja instalacji i obsługi programu Ikony w programie EntraPass

Kontroler w stanie „resetu” oraz awarii zasilania (Controller is in “Reset” and AC failure)



Ikona pojawia się, gdy kontroler jest w stanie „resetu” oraz awarii zasilania. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Reset kontrolera

Kontroler w stanie „resetu”, awarii zasilania oraz Alarm czujnika antysabotażowego (Controller is in “Reset”, “AC failure” and “Tamper in alarm”)



Ikona pojawia się, gdy kontroler jest w stanie „resetu”, awarii zasilania oraz Alarmu czujnika antysabotażowego. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Reset kontrolera

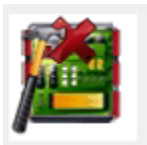
Kontroler w stanie „resetu” oraz Alarmu czujnika antysabotażowego (Controller is in reset and tamper in alarm)



Ikona pojawia się, gdy kontroler jest w stanie „resetu” oraz Alarmu czujnika antysabotażowego. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Reset kontrolera

Kontroler jest w stanie „Alarm czujnika antysabotażowego” (Controller tamper in alarm)



Ikona pojawia się, gdy kontroler jest w stanie Alarmu czujnika antysabotażowego. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Reset kontrolera (w stanie Alarmu czujnika antysabotażowego)



Ikony EntraPass

EntraPass - Instrukcja instalacji i obsługi programu Ikony w programie EntraPass

Kontroler przeładowuje firmware (Controller reloading firmware)



Ikona pojawia się, gdy kontroler przeładowuje firmware. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Reset kontrolera

Problem z kontrolerem KT-400 (KT-400 controller trouble)



Ikona pojawia się, gdy wystąpi problem z kontrolerem KT-400. Jest wyświetlana w:

- Pulpicie > Okna map.
- oknie Operacje > Kontroler

Drzwi

Ikony przedstawiające drzwi wskazują status drzwi w oknie map (Pulpit > Okna map) albo w oknie Operacje (Operation).

Wymuszone otwarcie drzwi (Door forced open)



Animowana ikona pojawia się, gdy zostały otwarte drzwi bez upoważnienia albo nie było zgłoszenia o wyjście. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Drzwi, Drzwi windy

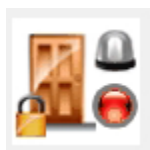
Wymuszony otwarcie drzwi – wyłączony czytnik (Door forced open (reader disabled))



Animowana ikona pojawia się, gdy zostały otwarte drzwi bez upoważnienia albo nie było zgłoszenia o wyjście, a czytnik jest wyłączony. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Drzwi, Drzwi windy

Drzwi zamknięte i zaryglowane (Door closed and locked)



Animowana ikona pojawia się, gdy drzwi są zamknięte i zaryglowane. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Drzwi

Drzwi zamknięte i zaryglowane – wyłączony czytnik (Door closed and locked (reader disabled))



Animowana ikona pojawia się, gdy drzwi są zamknięte i zaryglowane, a czytnik jest wyłączony. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Drzwi

Drzwi otwarte za długo (Door open too long)



Animowana ikona pojawia się, gdy drzwi są otwarte dłużej, niż dopuszczalny czas. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Drzwi, Drzwi windy

Drzwi otwarte za długo – wyłączony czytnik (Door open too long (reader disabled))



Animowana ikona pojawia się, gdy drzwi są otwarte dłużej, niż dopuszczalny czas, a czytnik jest wyłączony. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Drzwi, Drzwi windy



Ikony EntraPass

EntraPass - Instrukcja instalacji i obsługi programu Ikony w programie EntraPass

Drzwi otwarte i odryglowane ręcznie (Door open and unlocked manually)



Animowana ikona pojawia się, gdy drzwi zostały otwarte i odryglowane przez użytkownika. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Drzwi > Drzwi windy

Drzwi otwarte i odryglowane ręcznie – wyłączony czytnik (Door open and unlocked manually (reader disabled))



Animowana ikona pojawia się, gdy drzwi zostały otwarte i odryglowane przez użytkownika, a czytnik jest wyłączony. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Drzwi > Drzwi windy

Drzwi otwarte i odryglowane przez terminarz (Door is opened and unlocked by schedule)



Animowana ikona pojawia się, gdy drzwi zostały otwarte i odryglowane przez terminarz. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Drzwi > Drzwi windy

Drzwi otwarte i odryglowane przez terminarz – wyłączony czytnik (Door is opened and unlocked by schedule (reader disabled))



Animowana ikona pojawia się, gdy drzwi zostały otwarte i odryglowane przez terminarz, a czytnik jest wyłączony. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Drzwi > Drzwi windy

Drzwi otwarte za długo, przed-alarm (Door pre-alarm on open too long)



Animowana ikona pojawia się, gdy drzwi są otwarte ponad połowę dopuszczalnego czasu. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Drzwi > Drzwi windy

Drzwi otwarte za długo, przed-alarm – wyłączony czytnik (Door pre-alarm on open too long (reader disabled))



Animowana ikona pojawia się, gdy drzwi są otwarte ponad połowę dopuszczalnego czasu, a czytnik jest wyłączony. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Drzwi > Drzwi windy

Drzwi nadal otwarte, błędny terminarz (Door still opened schedule invalid)



Animowana ikona pojawia się, gdy drzwi są otwarte, a terminarz jest błędny. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Drzwi > Drzwi windy

Drzwi nadal otwarte, błędny terminarz – wyłączony czytnik (Door still opened schedule invalid (reader disabled))



Animowana ikona pojawia się, gdy drzwi są otwarte, terminarz jest błędny, a czytnik jest wyłączony. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Drzwi > Drzwi windy



Ikony EntraPass

EntraPass - Instrukcja instalacji i obsługi programu Ikony w programie EntraPass

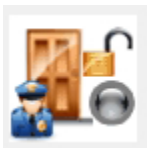
Drzwi odryglowane przez operatora (Door unlocked by an operator)



Animowana ikona pojawia się, gdy drzwi są odryglowane ręcznie przez **operatora**. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Drzwi > Drzwi windy

Drzwi odryglowane przez operatora – wyłączony czytnik (Door unlocked by an operator (reader disabled))



Animowana ikona pojawia się, gdy drzwi są odryglowane ręcznie przez **operatora**, a czytnik jest wyłączony. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Drzwi > Drzwi windy

Drzwi odryglowane przez terminarz (Door unlocked by a schedule)



Animowana ikona pojawia się, gdy drzwi są odryglowane przez terminarz. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Drzwi > Drzwi windy

Drzwi odryglowane przez terminarz – wyłączony czytnik (Door unlocked by a schedule (reader disabled))



Animowana ikona pojawia się, gdy drzwi są odryglowane przez terminarz, a czytnik jest wyłączony. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Drzwi > Drzwi windy



Ikony EntraPass

EntraPass - Instrukcja instalacji i obsługi programu Ikony w programie EntraPass

Drzwi windy odryglowane i zamknięte (Elevator door unlocked and closed)



Animowana ikona pojawia się, gdy drzwi windy są zamknięte i odryglowane. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Drzwi > Drzwi windy

Zamek bezprzewodowy połączony (Wireless Lock Connected)



Animowana ikona pojawia się, gdy zamek bezprzewodowy jest połączony. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Zintegrowane panele/Zamek bezprzewodowy

Błąd zamka bezprzewodowego (Wireless Lock Error)



Animowana ikona pojawia się, gdy wystąpił błąd przy zamku bezprzewodowym. Jest wyświetlana w:

- Oknie map (Pulpit > okno pulpitu Grafiki)
- oknie Operacje > Zintegrowane panele/Zamek bezprzewodowy

Przełączniki

Ikony przedstawiające przełączniki wskazują status przełączników w oknie map (Pulpit > Okna map) albo w oknie Operacje (Operation).

Przełącznik aktywowany przez wydarzenie (Relay activated by an event)



Animowana ikona pojawia się, gdy przełącznik jest aktywowany przez wydarzenie. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Przełącznik



Ikony EntraPass

EntraPass - Instrukcja instalacji i obsługi programu Ikony w programie EntraPass

Przełącznik chwilowo aktywowany przez wydarzenie (Relay temporarily activated by an event)



Animowana ikona pojawia się, gdy przełącznik jest chwilowo aktywowany przez wydarzenie. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Przełącznik

Przełącznik aktywowany przez Wejście linii dozorowej (Relay activated by an input)



Animowana ikona pojawia się, gdy przełącznik jest aktywowany przez Wejście linii dozorowej. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Przełącznik

Przełącznik chwilowo aktywowany przez Wejście linii dozorowej (Relay temporarily activated by an input)



Animowana ikona pojawia się, gdy przełącznik jest chwilowo aktywowany przez Wejście linii dozorowej. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Przełącznik

Przełącznik aktywowany przez operatora (Relay activated by an operator)



Animowana ikona pojawia się, gdy przełącznik jest aktywowany przez **operatora**. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Przełącznik

Przełącznik chwilowo aktywowany przez operatora (Relay temporarily activated by an operator)



EntraPass - Instrukcja instalacji i obsługi programu Ikony w programie EntraPass

Animowana ikona pojawia się, gdy przekaźnik jest chwilowo aktywowany przez **operatora**. Jest wyświetlana w:

Ikony EntraPass

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Przekaznik

Przekaznik aktywowany przez terminarz (Relay temporarily activated by a schedule)



Animowana ikona pojawia się, gdy przekaźnik jest aktywowany przez terminarz. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Przekaznik

Przekaznik wyłączony (Relay deactivated)



Animowana ikona pojawia się, gdy przekaźnik jest wyłączony. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Przekaznik

Wejścia linii dozorowej

Ikony przedstawiające Wejścia linii dozorowej wskazują status wejść w oknie map (Pulpit > Okna map) albo w oknie Operacje (Operation).

Wejście linii dozorowej aktywne – nienadzorowane (Input activated—Not supervised)



Animowana ikona pojawia się, gdy Wejście linii dozorowej jest aktywne, ale brak terminarza monitorowania. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Wejście linii dozorowej

Wejście linii dozorowej aktywne – nadzorowane (Input activated—Supervised)





EntraPass - Instrukcja instalacji i obsługi programu Ikony w programie EntraPass

Animowana ikona pojawia się, gdy Wejście linii dozorowej jest aktywne i działa terminarz monitorowania. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Wejście linii dozorowej



Ikony EntraPass

EntraPass - Instrukcja instalacji i obsługi programu Ikony w programie EntraPass

Wejście linii dozorowej aktywne – nienadzorowane, ręcznie operowane (Input activated—Not supervised manual operation)



Animowana ikona pojawia się, gdy Wejście linii dozorowej jest aktywne, ręcznie operowane i brak terminarza monitorowania. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Wejście linii dozorowej

Wejście linii dozorowej aktywne – nadzorowane, ręcznie operowane (Input activated—Supervised manual operation)



Animowana ikona pojawia się, gdy Wejście linii dozorowej jest aktywne, ręcznie operowane i działa terminarz monitorowania. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Wejście linii dozorowej

Wejście linii dozorowej aktywne – chwilowo nadzorowane, ręcznie operowane (Input activated—Supervised temporarily manual operation)



Animowana ikona pojawia się, gdy Wejście linii dozorowej jest aktywne, ręcznie operowane i chwilowo działa terminarz monitorowania. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Wejście linii dozorowej

Wejście linii dozorowej w stanie alarmu – nienadzorowane (Input in alarm—Not supervised)



Animowana ikona pojawia się, gdy Wejście linii dozorowej jest w stanie alarmu, ale brak terminarza monitorowania. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Wejście linii dozorowej



Ikony EntraPass

EntraPass - Instrukcja instalacji i obsługi programu Ikony w programie EntraPass

Wejście linii dozorowej w stanie alarmu – „wyłączone” przez operatora (Input in alarm—Shunted by operator)



Animowana ikona pojawia się, gdy Wejście linii dozorowej jest w stanie alarmu i jest „przyblokowane” przez **operatora**. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Wejście linii dozorowej

Wejście linii dozorowej w stanie alarmu – nadzorowane (Input in alarm—Supervised)



Animowana ikona pojawia się, gdy Wejście linii dozorowej jest w stanie alarmu i działa terminarz monitorowania. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Wejście linii dozorowej

Wejście linii dozorowej w stanie alarmu – nadzorowane przez operatora (Input in alarm—Supervised by operator)



Animowana ikona pojawia się, gdy Wejście linii dozorowej jest w stanie alarmu i jest nadzorowane przez **operatora** (ciągłe nadzorowanie). Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Wejście linii dozorowej

Wejście linii dozorowej OK – nienadzorowane (Input OK—Not supervised)



Animowana ikona pojawia się, gdy Wejście linii dozorowej działa normalnie, ale brak terminarza monitorowania. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Wejście linii dozorowej



Ikony EntraPass

EntraPass - Instrukcja instalacji i obsługi programu Ikony w programie EntraPass

Wejście linii dozorowej OK – „wyłączone” przez operatora (Input OK—Shunted by operator)



Animowana ikona pojawia się, gdy Wejście linii dozorowej działa normalnie i jest „przyblokowane” przez **operatora**. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Wejście linii dozorowej

Wejście linii dozorowej OK – nadzorowane (Input OK—Supervised)



Animowana ikona pojawia się, gdy Wejście linii dozorowej działa normalnie i działa terminarz monitorowania. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Wejście linii dozorowej

Wejście OK – nadzorowane przez operatora (Input OK—Supervised by operator)



Animowana ikona pojawia się, gdy Wejście linii dozorowej działa normalnie jest nadzorowane przez **operatora** (ciągłe nadzorowanie). Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Wejście linii dozorowej

Połączenie kontrolera

Ikony przedstawiają status połączenia albo bramki w oknie map (Pulpit > Okna map) albo w oknie Operacje (Operation).

Status połączenia jest jeszcze nieznan (Connection status is not yet known)



Animowana ikona pojawia się, gdy status połączenia kontrolera nie jest jeszcze znany. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)



Ikony EntraPass

EntraPass - Instrukcja instalacji i obsługi programu Ikony w programie EntraPass

Połączenie kontrolera – połączone (Controller connection connected)



Animowana ikona pojawia się, gdy połączenie jest prawidłowe i komunikacja przebiega bezproblemowo. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Przeładuj dane (Reload data)

Połączenie kontrolera – połączone, stan „Przeładowywania danych” (Controller connection connected and in “Reload Data”)



Animowana ikona pojawia się, gdy połączenie jest prawidłowe i jest w stanie „przeładowywania danych”. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Przeładuj dane (Reload data)

Połączenie kontrolera – błąd w komunikacji (Controller connection—Communication Failure)



Animowana ikona pojawia się, gdy brak połączenia i występuje błąd w komunikacji. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Przeładuj dane (Reload data)

Bramki

Bramki – błąd w komunikacji (Gateway—Communication Failure)



Animowana ikona pojawia się, gdy wystąpił błąd w komunikacji z bramką. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje (drzwi, drzwi windy, przekaźniki, Wejścia linii dozorowej, etc.)



Ikony EntraPass

EntraPass - Instrukcja instalacji i obsługi programu Ikony w programie EntraPass

Bramka – stan „Przeładowywania danych” (Gateway in “Reload Data”)



Animowana ikona pojawia się, gdy bramka jest „przeładowywana”. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje (drzwi, drzwi windy, przekaźniki, Wejścia linii dozorowej, etc.)

Bramka – błąd w komunikacji podczas „przeładowywania danych” (Gateway—Communication Failure during Reload Data)



Animowana ikona pojawia się, gdy bramka traci połączenie w trakcie „przeładowywania danych”. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Przeładuj dane (Reload data)

Bramka – połączenie w normie (brak problemów (Gateway communication is regular (no problem))



Animowana ikona pojawia się, gdy bramka jest połączona i komunikacja przebiega prawidłowo. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Przeładuj dane (Reload data)

Bramka – problemy (Gateway Trouble)



Animowana ikona pojawia się, gdy brak komunikacji z bramką. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Przeładuj dane (Reload data)



Ikony EntraPass

EntraPass - Instrukcja instalacji i obsługi programu Ikony w programie EntraPass

Bramka – problemy z „przeładowaniem” (Gateway Trouble when Reloading)



Animowana ikona pojawia się, gdy brak komunikacji z bramką w trakcie „przeładowywania danych”. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Przeładuj dane (Reload data)

Gateway (Gateway Software Interface):

Bramka OK – komunikacja bez problemu (Gateway OK—communicating)



Animowana ikona pojawia się, gdy komunikacji z bramką przebiega bez problemu. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Przeładuj dane (Reload data)

Bramka – stan „Przeładowywania danych” (Gateway in “Reload Data”)



Animowana ikona pojawia się, gdy bramka jest „przeładowywana”. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje > Przeładuj dane (Reload data)

Bramki – błąd w komunikacji (Gateway—Communication Failure)



Animowana ikona pojawia się, gdy wystąpił błąd w komunikacji z bramką. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje (drzwi, drzwi windy, przekaźniki, Wejścia linii dozorowej, etc.)

Aplikacja EntraPass



Ikony EntraPass

EntraPass - Instrukcja instalacji i obsługi programu Ikony w programie EntraPass

Status aplikacji nie jest jeszcze znany (Application status is not yet known)



Animowana ikona pojawia się, status aplikacji nie jest jeszcze znany. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)

Aplikacja próbuje nawiązać komunikację (Application attempts communication)



Ta animowana ikona jest wyświetlana w:

- oknie startowym, gdy stacja robocza próbuje nawiązać komunikację z serwerem.

Aplikacja – błąd komunikacji (Application—Communication Failure)



Animowana ikona pojawia się, gdy wystąpił błąd w komunikacji ze stacją roboczą. Jest wyświetlana w:

- oknie Grafiki (pulpit – grafika)
- oknie Operacje (alarm, strefa, trasa strażnika, drzwi, drzwi windy, przekaźniki, Wejścia linii dozоровej, etc.)

Inne

Uruchomienie bazy danych (Database Initialization)



Ta animowana ikona jest wyświetlana w:

- oknie startowym, gdy stacja robocza uruchamia bazę danych.

Brak danych (Data not available)



Ta animowana ikona wskazuje fazę przejściową. Może oznaczać, że poszukiwane informacje nie są obecnie dostępne.



Ikony EntraPass

EntraPass - Instrukcja instalacji i obsługi programu Ikony w programie EntraPass

Brak statusu (No status available)



Ta animowana ikona wskazuje fazę przejściową. Może oznaczać, że poszukiwany status komponentu nie jest obecnie dostępny.

Status wyjścia nie jest jeszcze znany (Output status is not yet known)



Ta animowana ikona jest wyświetlana w:

- oknie Grafiki (pulpit – grafika), gdy status wyjścia nie jest jeszcze znany

Status nieznany (Status unknown)



Animowana ikona pojawia się, gdy stacja robocza nie otrzymała statusu komponentu po czterech próbach. Jest wyświetlana w:

- oknie Operacje (Operation) (alarmy, obszary, trasy strażników, drzwi, drzwi windy, przekaźniki, etc.)
- Pulpicie > Okna map.

Wykryto błąd (Error in proces)



Animowana ikona pojawia się, gdy wykryto konkretny błąd. Jest wyświetlana w:

- oknie Operacje (Operation) (alarmy, obszary, trasy strażników, drzwi, drzwi windy, przekaźniki, etc.)
- Pulpicie > Okna map.

Niezidentyfikowany komponent (Undefined Component)



Animowana ikona pojawia się, gdy komponent nie istnieje. Jest wyświetlana w: