



Rýchly Sprievodca C4

Vitajte v ľudskej stránke vašich bezpečnostných systémov!

Po úspešnej inštalácii Systému C4 a registrácii inštalácie môžeme začať s implementáciou systému pre zákazníka. Táto lekcia vás prevedie celým procesom, na konci ktorého je odovzdanie systému zákazníkovi.

Zavedenie dodávateľa

Začneme vytvorením dodávateľského účtu. Pod ním budeme následne vykonávať všetky kroky potrebné k dokončeniu implementácie Systému.

1. Účet technika

Prvý krok zahŕňa pridanie dodávateľskej firmy a osoby do Systému C4, vytvorenie používateľského účtu a zdefinovanie používateľských oprávnení.

Začnite vytvorením dodávateľskej firmy. Následne pod ňu pridajte osobu.

Systém C4 je riešenie typu klient-server, a preto sa všetky zmeny vykonané v C4 Clientovi musia preniesť na server.

A keďže je Systém C4 modulárny, umožňuje spracúvanie údajov vo formulároch vyvinutých nezávislými vývojármi. Preto je pre bezpečné spracovanie údajov potrebné uloženie každého formulára samostatne. To následne generuje veľmi časté požiadavky na ukladanie dát. Z tohto dôvodu Systém C4 ponúka možnosť automatického ukladania dát pri prepínaní medzi jednotlivými časťami klienta. Táto funkcia sa aktivuje zaškrtnutím políčka v každej žiadosti o uloženie. Toto nastavenie je možné kedykoľvek vypnúť v nastaveniach aplikácie.

Teraz vytvoríme používateľský účet a nastavíme preň oprávnenia.

Každá osoba, ktorá bude pracovať v C4 Clientovi, musí mať vytvorený svoj vlastný účet s bezpečným heslom.



Najjednoduchší spôsob definovania oprávnení je priradením roly, ktorá automaticky zadefinuje oprávnenia v rámci Systému C4.

Roly je možné vzájomne kombinovať a výsledné oprávnenia sú súčtom oprávnení jednotlivých rolí.

Technik je rola, ktorá sa udeľuje osobe zaškolenej pre inštaláciu a pripájanie zariadení do Systému C4.

Administrátor je rola pre osobu, ktorá spravuje celkovú inštaláciu Systému C4 a nastavuje oprávnenia pre jednotlivých používateľov.

Kombinácia týchto dvoch rolí dáva osobe najvyššie možné oprávnenia.

Keď je dodávateľský účet vytvorený a sú preň nastavené všetky potrebné oprávnenia, môžete sa odhlásiť zo Support účtu a začať pracovať pod svojim osobným účtom dodávateľa.

2. Prístup do Portálových služieb

V ďalšom kroku povolíme prístup do Portálových služieb.

Aby ste mohli sťahovať Drivery priamo z prostredia C4 Klienta, je potrebné povoliť prístup do Portálových služieb z C4 Klienta.

Systém C4 umožňuje povoliť prístup na Portálové služby pre všetkých používateľov. Pre transparentnejšiu správu Systému C4 sa ale odporúča explicitne definovať osoby s možnosťou prístupu k Portálovým službám.

Zavedenie zariadení

Ďalším krokom je zavedenie zariadení do Systému C4.



1. Inštalácia Drivera

Pre implementáciu zariadenia je najprv potrebné nainštalovať si Driver.

Všetky rozšírenia Systému C4, nazývané Pluginy, sú umiestnené výhradne na Plugin Store spoločnosti Gamanet. Jednou z kategórií Pluginov je Driver, ktorý je určený k integrácii externých systémov do C4. Získať ich je možné dvomi spôsobmi.

V prípade, že nemáte z počítača s C4 Clientom pripojenie k internetu, môžete si stiahnuť balíček pre daný Driver na adrese <https://my.c4portal.com>, v sekcii Plugin Store. Nájdete tu všetky dostupné Drivery, zaradené do kategórií podľa rozsahu funkcionalít, ktoré poskytujú. Kliknutím na Driver sa zobrazia všetky informácie k nemu, a môžete ho odtiaľto aj stiahnuť.

V C4 Clientovi si následne stiahnutý Driver naimportujete a nainštalujete.

Druhou možnosťou ako získať Driver je priamo z prostredia C4 Klienta. Dostupné Drivery sa zobrazia po začiatku možnosti Show Available. Aby ste mohli sťahovať Drivery týmto spôsobom, musíte mať nastavené prihlasovanie do Portálových služieb, tak ako sme si vysvetlili na začiatku tejto lekcie.

Ak chcete byť do Portálových služieb prihlasovaní automaticky, môžete si spárovať účet v Portálových službách so svojim účtom v Systéme C4. Takto nebudete pri každom pristupovaní do Portálových služieb vyzvaní zadať svoje prihlasovacie údaje. Jedinou výnimkou je Support účet, ku ktorému nie je možné pristupovať cez automatické prihlasovanie.

Teraz vyberte požadovaný Driver a kliknite na možnosť Install.

Osoba, ktorá bude inštalovať Driver musí byť zaškolená pre konkrétne zariadenie.

Ak vás systém vyzve, reštartujte C4 Klienta.

2. Zavedenie konfigurácie zariadenia

Po stiahnutí Drivera môžeme pokračovať ďalším krokom, ktorým je pridanie konfigurácie zariadenia do Systému C4.

Pre každé zariadenie, ktoré chceme spravovať je potrebné zadefinovať jeho konkrétnu konfiguráciu u daného zákazníka. V Systéme C4 je táto konfigurácia reprezentovaná vo forme stromu. Niektoré Drivery umožňujú automatický import



konfigurácie zo zariadenia a strom sa vytvorí automaticky. V ostatných prípadoch je potrebné strom vytvoriť manuálne.

Začneme pridaním Bus Controllera, ktorý reprezentuje prípojný bod zariadenia. Vyplňte požadované informácie, ako názov zariadenia, IP adresu a nastavte správny port.

Následne pridáme podsystémy, ktorými sú v našom prípade prístupový panel, dvere a čítačka kariet. Pre každý z nich zadajte HW adresu. Táto adresa jednoznačne identifikuje podsystém v rámci topológie zariadenia. Väčšinou ide o fyzickú adresu definovanú priamo na podsystéme. V niektorých prípadoch slúži ako adresa logická adresa vygenerovaná v rámci konfigurácie zariadenia v softvéri výrobcu.

Systém C4 umožňuje definovať rôzne parametre v závislosti od podsystému a možností komunikačného protokolu dodávaného výrobcom zariadenia. Názvy pripojovacích a konfiguračných parametrov sa väčšinou zhodujú s názvami obsiahnutými v manuáli zariadenia dodávaného výrobcom, prípadne v jeho integračnom manuáli dodávaného vývojárom Driveru.

Týmto spôsobom si zavediete všetky zariadenia z vašej inštalácie do Systému C4. V našom prípade inštalácia pozostáva z dvoch demo zariadení, jedno je vstupno-výstupné zariadenie a druhé je prístupové zariadenie.

V prípade prístupových a zabezpečovacích zariadení, ktoré spravujú identifikátory je v tejto fáze potrebné vypnúť parameter *Credential Upload Enabled*, čím sa vypne nahrávanie identifikátorov do zariadenia. Tento parameter sa nachádza buď v nastaveniach Control Panelu prístupového systému alebo v nastaveniach Bus Controllera. Umiestnenie parametra závisí od typu zariadenia a jeho implementácie vývojárom.

Pri prvotnom spustení komunikácie so zariadením – zadaním príkazu Start, Systém C4 prevezme kontrolu nad zariadením v pridelenom rozsahu pamäte zariadenia. Ako úplne prvý krok nahrá do zariadenia všetky identifikátory zadefinované v Systéme C4 pre dané zariadenie. Zvyšok pamäťového priestoru ktorý má Systém C4 v správe, samozrejme vyčistí od starých záznamov. To zabezpečí transparentnosť v informáciách, ktoré následne Systém C4 dostáva zo zariadenia vo forme logov. V prípade zavedenia nového zariadenia je preto potrebné pred



nahratím identifikátorov tieto najskôr vytvoriť, priradiť ich príslušným osobám, prideliť im oprávnenia a až následne ich môžeme nahráť do zariadenia.

Nahrávanie identifikátorov preto povolíme až po ukončení nastavení zamestnancov v nasledujúcom kroku.

Po zavedení konfigurácie zariadenia naštartujeme komunikáciu Systému C4 so zariadením. Veľmi detailne preveríme, nakoľko pracujú všetky podsystémy zariadenia správne. Ďalej skontrolujeme, či sa jednotlivé stavy zariadenia zobrazujú správne v Systéme C4 a či prichádzajú zo zariadenia všetky udalosti.

Správa zamestnancov

1. Pridanie osôb

Prvým krokom je pridanie osôb do Systému C4.

Aby ste mohli čerpať z benefitov, ktoré Systém C4 ponúka pri správe prístupových oprávnení, dôrazne sa odporúča zaviesť si do správy osôb organizačnú štruktúru podniku. Z tohto dôvodu zavedeniu osôb predchádza vytvorenie firmy a jednotlivých oddelení. Takto vytvorená štruktúra má zásadný vplyv na transparentnosť správy prístupových oprávnení. Neodporúča sa pridávať zamestnancov priamo pod Root. Takto zavedené osoby nie je možné následne spracúvať hromadne pre pridelovanie prístupov. Organizačná štruktúra výrazne zrýchľuje spracovanie prístupových oprávnení pre nahrávanie do zariadení.

Pri vytváraní organizačnej štruktúry firmy je dôležité, aby ju vytvoril len jeden používateľ. Ak dvaja používatelia jedného systému vytvárajú súčasne vo svojom C4 Clientovi rovnakú firmu alebo oddelenie, tieto sú po uložení evidované v Systéme C4 dvakrát.

Organizačná štruktúra by mala čo najviac zohľadňovať politiku definovania prístupových práv, a teda osoby s rovnakými sadami prístupových práv by mali byť umiestnené v jednej organizačnej jednotke.



Zohľadnenie týchto aspektov nám v budúcnosti umožní výrazne zjednodušiť správu prístupových oprávnení v rámci Systému C4.

V Systéme C4 je možné vytvárať aj skupiny zamestnancov. V tomto prípade sú však nastavenia prístupových práv komplikovanejšie, pretože všetky skupiny sú rovnocenné. Preto sa zásadne odporúča definovať v skupinách výhradne prístupové oprávnenia typu „Povoliť“. Rozdielom v nastaveniach prístupových práv pre osoby v organizačnej štruktúre a pre osoby v skupinách sa budeme bližšie venovať v samostatnej lekcii.

2. Identifikátory

Ďalej pre každého zamestnanca zaregistrujeme jeho identifikátory používané v rámci prístupových práv.

Pred tým si však najskôr musíme do Systému C4 zaviesť zoznam všetkých typov identifikátorov, ktoré budeme v našom systéme používať.

Veľkou výzvou pri správe identifikátorov je rozmanitosť ich typov a formátov, ako aj to, že každý prístupový systém pracuje so svojim špecifickým formátom identifikátorov. Gamanet preto vytvoril centrálnu knižnicu, v rámci ktorej registruje všetky typy podporovaných formátov identifikátorov a ich transformáciu do formátov kompatibilných so zariadeniami integrovanými do Systému C4. Pri importovaní typu identifikátorov sa importujú aj konvertory pre jednotlivé zariadenia.

Pre každého zamestnanca zaregistrujeme všetky jemu pridelené identifikátory používané v rámci správy prístupov. V našom prípade ide o PIN kód typu PIN 4 a kartu typu HID 26.

3. Prístupové oprávnenia

Potom môžeme pristúpiť k zadefinovaniu prístupových práv.



Prístupy môžeme nastaviť zvlášť pre jednotlivé osoby, alebo pre celé oddelenie. Všetky nastavenia definované v rámci organizačnej štruktúry sa automaticky dedia a premietajú na osoby. Ak presunieme osobu z jedného oddelenia do druhého, nadobudne práva zadefinované pre oddelenie, v ktorom sa práve nachádza.

Po zadefinovaní prístupov prejdeme opäť na zariadenie a povolíme možnosť *Credential Upload Enabled*. Akékoľvek zmeny v konfigurácii zariadenia sa vždy prejavia až po reštarte zariadenia.

V prípade prvého spustenia komunikácie so zariadením s povolenou Správou identifikátorov, sa v následnom kroku automaticky spustí proces nahrávania identifikátorov do zariadenia. Tento proces môže trvať dlhšie, v závislosti od rýchlosti siete a počítača, počtu kariet či konfigurácie a typu zariadenia.

Po ukončení nahrávania vyskúšame, nakoľko sa nahraté záznamy o povolených prístupoch osôb prejavia v reálnej inštalácii. Preto je potrebné preveriť niekoľko identifikátorov, nakoľko nastavenia prístupových oprávnení v C4 zodpovedajú realite. Teda, či osoba na dverách ktoré má v Systéme C4 definované ako povolené, tak aj skutočne prístupový systém tejto osobe povolí vstup. Samozrejme akákoľvek aktivita osoby na prístupovom systéme sa v C4 zobrazí vo forme udalosti v zozname udalostí.

4. Používateľské oprávnenia

Následne zadefinujeme používateľské oprávnenia.

Ak daná osoba bude aktívnym používateľom Systému C4, musíme jej vytvoriť účet, pod ktorým bude pracovať.

Následne každej osobe priradíme rolu na základe toho, aké oprávnenia má mať v Systéme C4.

Prvou osobou s pridelenými oprávneniami Administrátora bude správca inštalácie z pohľadu zákazníka. Priradením roly osobe sa automaticky zadefinujú jej oprávnenia v rámci Systému C4.



Ak chceme nastaviť detailnejšie oprávnenia pre danú osobu pre jednotlivé oblasti, môžeme tak urobiť v záložke Permissions. Tejto téme sa podrobne venuje samostatná lekcia.

Regióny a vizualizácia

Ďalej pokračujeme vytvorením regiónov a vizualizácie.

1. Vytvorenie štruktúry regiónov

Prvým krokom je vytvorenie regiónov a pridanie zariadení do nich.

Regióny sú esenciálnou súčasťou jadra Systému C4. Umožňujú rozšírenie funkcionalít ohľadne prístupových a návštevnych systémov, ako napríklad v prípade počítania osôb, anti-passbacku či dochádzky. Hierarchia regiónov umožňuje inteligentné spracovanie informácií zo zariadení a osôb, ich párovanie a následné vyhodnocovanie na viacerých úrovniach.

Hierarchická štruktúra regiónov je taktiež základom pre vizualizáciu.

Pri vytváraní regiónov začíname vždy regiónom, ktorý reprezentuje celú inštaláciu, či už ide o budovu, mesto, štát alebo kontinent. Jednotlivé regióny by mali odzrkadľovať logickú štruktúru inštalácie. Čím je hierarchia detailnejšia, tým jednoduchšie je pre operátora pohybovať sa v nej a implementovať do nej prípadné zmeny.

Po vytvorení regiónov môžeme do nich jednotlivé zariadenia pridávať potiahnutím myšou.

2. Vizualizácia regiónov a zariadení

Následne vytvoríme vizualizáciu a umiestnime do nej objekty.

Hierarchická štruktúra vizualizácie rozdeľuje celú inštaláciu na malé vizualizačné bloky. Vďaka tomu je v Systéme C4 možné vizualizovať len tú časť budovy, v ktorej potrebujeme pracovať.



Pre vytvorenie jedného bloku začneme vizualizáciou regiónu vo forme podkladového obrázka a pokračujeme vizualizáciou zariadení do pozícií reprezentujúcich ich reálne umiestnenie. Pre obrázky Systém C4 podporuje akýkoľvek verejný rastrový formát.

V prípade požiadavky na vektorové zobrazenie vizualizácie Gamanet poskytuje samostatný vizualizačný modul.

Následne v module pre monitoring môžeme zariadenia monitorovať a ovládať. Akákoľvek zmena na zariadení sa prezentuje vo vizualizácii.

V našom prípade zapnutím detektora simulujeme otvorené okno.

Ak chceme, aby sa v takomto prípade vytvoril incident, môžeme si to nastaviť prostredníctvom Smart Routine.

Incidenty a Workflow

1. Aktivovanie incidentov

Incidenty môžu byť aktivované dvomi spôsobmi. Zákazníci môžu použiť Incident Creator, alebo si môžu vytvoriť svoju vlastnú Smart Routine, ktorá bude generovať incidenty na základe podmienok, ktoré si zadefinujú.

Incident Creator je Smart Routine poskytovaná Gamanetom, ktorá vytvára incidenty zo všetkých udalostí typu alarm, bez ohľadu na typ zariadenia.

Taktiež si môžeme rozšíriť incidenty na základe podmienok definovaných prostredníctvom ktorejkoľvek Smart Routiny nainštalovanej v Systéme C4.

V našom prípade si vytvoríme automatickú akciu prostredníctvom Log Routine, ktorá vygeneruje incident v prípade, že sa otvorí okno.

Incident sa môže vytvoriť z akejkoľvek udalosti, zmeny stavu na zariadení, alebo naplánovaného času, v závislosti od špecifických požiadaviek zákazníka.

Keď sú splnené podmienky pre vytvorenie incidentu, zobrazí sa okno Alarm Overview. *Input opened* znamená, že okno bolo otvorené.



2. Ďalšie workflow

Zákazníci si na základe svojich špecifických požiadaviek môžu nadefinovať rôzne ďalšie workflow.

V súčasnej generácii Systému C4 je možné základnú sadu Smart Routine rozširovať o vlastné rutiny vyvinuté na základe požiadaviek zákazníka.

Smart Routiny môžu byť aktivované tromi rôznymi zdrojmi signálov. Prvým je vznik určitej udalosti, druhým je zmena stavu zariadenia, a tretou možnosťou je naplánovanie Smart Routine na určitý čas, kedy bude aktivovaná.

Predchádzajúce generácie Systému C4 obsahovali tzv. automatické akcie. V novej generácii sú tieto obsiahnuté v rutine Log Routine.

Smart Routine sa skladá z dvoch častí.

Prvou časťou je súbor podmienok, ktoré sa vyhodnotia, a na základe výsledku sa systém rozhodne, či má vykonať definovanú akciu.

Pre definovanie podmienok máme k dispozícii sadu parametrov.

Rozsah parametrov, ktoré používateľ môže nastaviť, je definovaný vývojárom. Napr. pre túto Log Routine môžeme konfigurovať parametre týkajúce sa zariadenia, udalosti, osoby či regiónu.

Zadaním podmienok v danej Smart Routine určujeme, na ktoré položky sa bude vzťahovať. Napríklad, v prípade udalosti presne zadefinujeme, či sa vzťahuje len na danú udalosť, alebo aj na podriadené udalosti, prípadne navolíme presný zoznam udalostí, na ktoré sa bude daná Smart Routine vzťahovať.

V rámci jednej sady podmienok je možné kombinovať podmienky pre rôzne typy položiek, ktoré sú v udalosti obsiahnuté. Napríklad môžeme kombinovať alarm s konkrétnym detektorom 3.

Nová generácia Systému C4 umožňuje okrem kombinovania jednoduchých podmienok vytvárať aj zložené podmienky so zátvorkami.



Splnením všetkých zadefinovaných podmienok sa spustí druhá časť Smart Routine, ktorou je akcia alebo súbor akcií.

Systém C4 rozlišuje dva typy akcií, v závislosti od toho, kde sa spúšťajú. Prvým typom sú akcie, ktoré sa vykonávajú na strane servera, napr. poslanie príkazu na zariadenie či poslanie e-mailu.

V tomto prípade zadefinujeme, že e-mail sa má poslať operátorovi, ale je možné poslať ho na akúkoľvek jednotku v rámci organizačnej štruktúry.

K e-mailu je možné pripojiť aj súbor s informáciami o udalosti.

Druhým typom sú akcie, ktoré sa vykonávajú na strane klienta, napr. zobrazenie inštrukčnej sady operátorovi, či zobrazenie živého obrazu z kamery.

Na jednu sadu podmienok je možné nastaviť kombináciu serverových aj klientskych akcií.

Zoznam klientskych aj serverových akcií je otvorený a je možné ho rozširovať podľa požiadaviek zákazníka.

Odovzdanie zákazníkovi

Po vykonaní nastavení popísaných v tejto lekcii bude systém pripravený na odovzdanie zákazníkovi.

Pred samotným odovzdaním je však potrebné ešte urobiť nejaké kroky.

Je potrebné upraviť oprávnenia. Dodávateľovi ostane rola technika. Inštalačný manažér u zákazníka bude mať rolu administrátora.

Nastaví sa nové heslo pre prístup do Support účtu. Heslo si zákazník uschová pre použitie v núdzových prípadoch.

Nakoniec sa podpíše inštalačný protokol a spolu s heslom pre Support účet zalepeným v obálke sa odovzdá zákazníkovi.