

[Problém](#)[Možnosti](#)[Možnosti s CM](#)[Ako na to](#)[Kroky nastavenia v obrázkoch](#)[Čo získal zákazník \(vlastník servera\) ?](#)[Záver a prínosy CM riešenia](#)

PROBLÉM

Ak k vášmu serveru okrem IT správcu pristupujú aj iní subdodávateľa (napríklad pre správu ERP a iných aplikácií), môžete pre nadobudnutie vzájomnej dôvery potrebovať informáciu, čo dodávateľ na danom serveri robí. Externý subdodávateľ má často krát administrátorské oprávnenia pre správu, čo zvyšuje dôvody na kontrolu. Externý dodávateľ má byť informovaný o nahrávaní jeho práce neprehliadnuteľným spôsobom.

MOŽNOSTI

Spôsobov ako kontrolovať prácu na počítači iných administrátorov sa ponúka mnoho. Od nahrávania obrazu, cez odchyt klávesnice, odchyt prístupov k súborom, ukladanie systémových zmien na počítači po bežné nástroje sledovania aktivity.

Výzvy, ktoré treba pri takomto riešení zvládnuť :

- Ľahká obsluha pre používateľa, ktorý má čítať údaje

- Zachytiť údaje v rozsahu pre posúdenie, či nedošlo k zneužitiu role alebo úniku dát

- Ukladať len údaje o sledovanom používateľovi, ostatných používateľov nesledovať

- Rýchla orientácia v údajoch na vyhľadanie citlivého miesta

- Bezpečnosť uchovaných údajov

- Neodstaviť sledovanie bez povšimnutia

- Informovať druhú stranu, že je nahrávaná (keďže nemá ísť o skryté nahrávanie)

- Dlhá doba archivácie

Softvér na internete nám neumožnil splniť všetky tieto požiadavky naraz a rozhodli sme sa implementovať funkciu cez CM.

Dôležité je posúdiť, či je možné subdodávateľovi neprideliť administrátorské práva a tým pádom mu výrazne zúžiť priestor. C-Monitor má na dosiahnutie tohto cieľa potrebné nástroje, v niektorom z ďalších Blog príspevkov sa mu budeme venovať detailnejšie. Zatiaľ si prečítajte [Blog príspevok OpenVPN pre ne-admin používateľa](#) [1] o spúšťaní procesu potrebnú admin oprávnenia u používateľa bez admin oprávnení. Účel sledovania subdodávateľa sa následne zmení len na kontrolu práce v aplikačnom softvéri.

MOŽNOSTI S CM

Keďže nebolo dosiahnuteľné riešenie z internetu, bolo pre splnenie cieľov z predchádzajúceho bodu **vytvorený pomocný programček SaveScreen** (je priložený na konci stránky) a jeho spúšťanie je ovládané pomocou C-Monitora. Tento **program upozorňuje na existenciu nahrávania pri každom prihlásení**, čo je v súlade s politikou CM, ktorý skryto nezbiera žiadne citlivé údaje. Program SaveScreen.exe je naplánovaný v Scheduleri (kvôli autorizácii na sieťovú cestu), spúšťa sa na pokyn (trigger) z Watches v čase aktivity sledovaného konta. Zachytené obrázky sa ukladajú na vami zvolenú cestu, doporučujeme sieťovú cestu bez prístupu sledovanému kontu.

Dosiahnuté vlastnosti riešenia :

- [Ľahká obsluha](#) - používateľ, ktorý dozerá na prácu subdodávateľa, má link na screenshoty

- [Rozsah údajov](#) - v krátkych intervaloch (od 10sec vyššie) aktivity robené screenshoty

- [Údaje len zo sledovaného konta](#) - zabezpečené vďaka C-Monitor, selekcii session

Rýchla orientácia v údajoch - každý screenshot má presný čas a dátum uloženia, uložené sú len obrazovky, keď sa niečo dialo, grafické súbory sa ľahko prehliadajú vďaka náhľadom

Bezpečnosť uchovaných údajov - uloženie na sieť. ceste bez možnosti ich zmazať sledovaným kontom a prístup k súborom riadený cez NTFS oprávnenia

Zabránenie odstavenia sledovania - keďže celý systém je v rámci CM, z ktorého sa ihneď posielajú údaje do CM Portálu, akýkoľvek zásah má zaznamenaný presný čas a je pomocou CM dohľadateľné, ktoré konto vykonalo zmenu.

Informovanie sledovaného konta o nahrávaní - utilita ScreenSaver vždy pri prihlásení oznamuje správu "Your message is recorded"

Dlhá doba archivácie údajov - vďaka ukladaniu screenshotov len v čase aktivity a vami zvolenej perióde, sa šetrí miestom. Ak jeden screenshot má približne 100kB a robíte záznam každých 15sec, za hodinu aktívnej práce sa vytvorí 24MB údajov (to je na 10GB priestoru by ste dostali 416hod). Pre dlhú dobu archivácie utilita nemá mazanie starých údajov, ale to sa ľahko realizuje inými programčekmi, napr. cez forfiles (priamo v distribúcii Windows)

AKO NA TO

1. **Uložte SaveScreen.exe na lokálny disk** (napr. c:\CMonitor\Modules\utilities) a prevezmite si vlastníctvo súboru v rámci NTFS oprávnení na seba a označte súbor len na čítanie (ako preventívny krok pred zmenami od iného administrátora)

2. **V C-MonitorConsole -> Scheduleri pridajte novú úlohu** (bez Sprievodcu) pomenujte ju napríklad Save Screen Task

3. **Vyplňte záložku General novej úlohy**

Pomenujte úlohu, napr. Save Screen Task

Command line vyplňte podľa nápovery programu SaveScreen.exe, kde zadáte cieľovú cestu, formát názvu súboru a grafický formát . Nápoveda sa zobrazí po spustení programu.

Vypnite možnosť "Execute by Date and Time"

Zapnite "Execute on Trigger " a zadajte názov Triggeru, napr. savescreen

4. **Vyplňte záložku Advanced novej úlohy**

Zvoľte možnosť Run under logged a nastavte hodnotu Run under one of logged users. Do zoznamu napíšte názov účtu, pod ktorým bude sledovaný používateľ prihlásený.

Ak budete zapisovať na sieťový disk pod inou identitou (silno doporučené), tak zvoľte možnosť Use remote access credentials (connect to network device as another user) a zadajte prihlasovacie údaje pre prístup na daný sieťový disk

5. **Vytvorte nový Watch** (napr. Save Screen Watch). Bude generovať pokyn (trigger) pre stiahnutie obrazovky len v čase aktivity používateľa na obrazovke. Ten bude založený na podmienke Inactivity user time. Odoslanie triggeru bude generované ak Watch bude v stave FAIL, čomu prispôbime znenie podmienky (budeme testovať či neaktivita používateľa je väčšia ako požadovaná perióda)

6. **Vyplňte údaje k podmienke (condition) Inactivity time**

User Name napíšte názov účtu, pod ktorým bude sledovaný používateľ prihlásený

Operátor zvoľte väčší"

Inactivity time nastavte na počet sekúnd zodpovedajúci žiadanej perióde záznamu, napr. 15sec.

Value from this condition ... nastavte na Never. Nepotrebuje vidieť konkrétny čas neaktivity na CM Portáli.

7. **Vyplňte záložku Advanced nového Watchu**

Evaluation and notification of errors on CM server -> For this Watch zmeňte na Blocked notification on CM Server. Zabezpečí to, že z CM servera nebudete SPAMovaný hláseniami z tohto Watchu.

8. **Nastavte prvé poslanie triggeru cez akciu Start**

Nastavenie Start akcie pre prvé zosnímanie obrazovky po začiatku aktivity používateľa.

Stlačte link Add New Start Action z prvej záložky Conditions

Nastavte Activate Trigger a názov musí byť zhodný ako je v naplánovanej úlohe.

9. **Nastavte opakované poslanie triggeru cez akciu Repeat**

Nastavenie Repeat akcie pre snímanie obrazovky v žiadanej perióde (u nás 15sec), kým aktivita používateľa trvá.

V aktuálnom dialógu Start Akcie stlačte link Add New Repeat Action. Pre Repeat akciu už postačí zmeniť len periódu, ostatné je prednastavené zo Start akcie.

Nastavenie na počítači je hotové. Zostávajú voliteľné nastavenia z CM Portálu :

10. Zníženie C-Monitor ticku na 15sec

V ilustračnom príklade je žiadaná perióda nižšia než C-Monitor tick od inštalácie, ktorá je 30sec. Znamenalo by to, že Screenshots by sa ukladali v minimálnej tejto perióde. Pre dosiahnutie kratšej periódy treba skrátiť C-Monitor Tick, čo ide spraviť cez CM Portál v : *Admin. zóna -> C-Monitor klient -> Nastavenia C-Monitor na PC -> výber PC -> položka C-Monitor Tik interval* (v prvej časti Základné nastavenia C-Monitora). Najnižšia dovolená hodnota je 5sec.

11. Zaheslovanie konfigurácie C-Monitoru

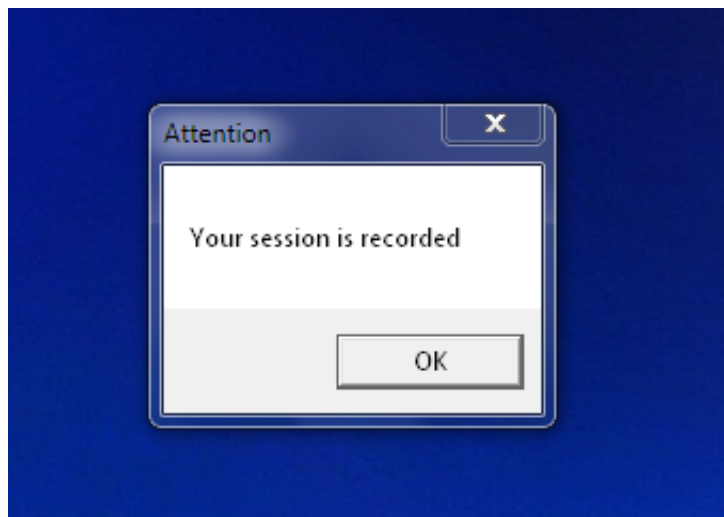
Aby iný administrátor ľahko nezmenil konfiguráciu C-Monitora, je potrebné ju mať zamknutú. Doporučujeme, že by ste mali heslo rovnaké pre celú spoločnosť (Mení sa v nastavení zákazníka), ale ak si to prajete len pre tento počítač, zmeňte to v rovnakom formulári ako v predchádzajúcom bode o položke vyššie Heslo pre prístup do konfigurácie C-Monitor-u.

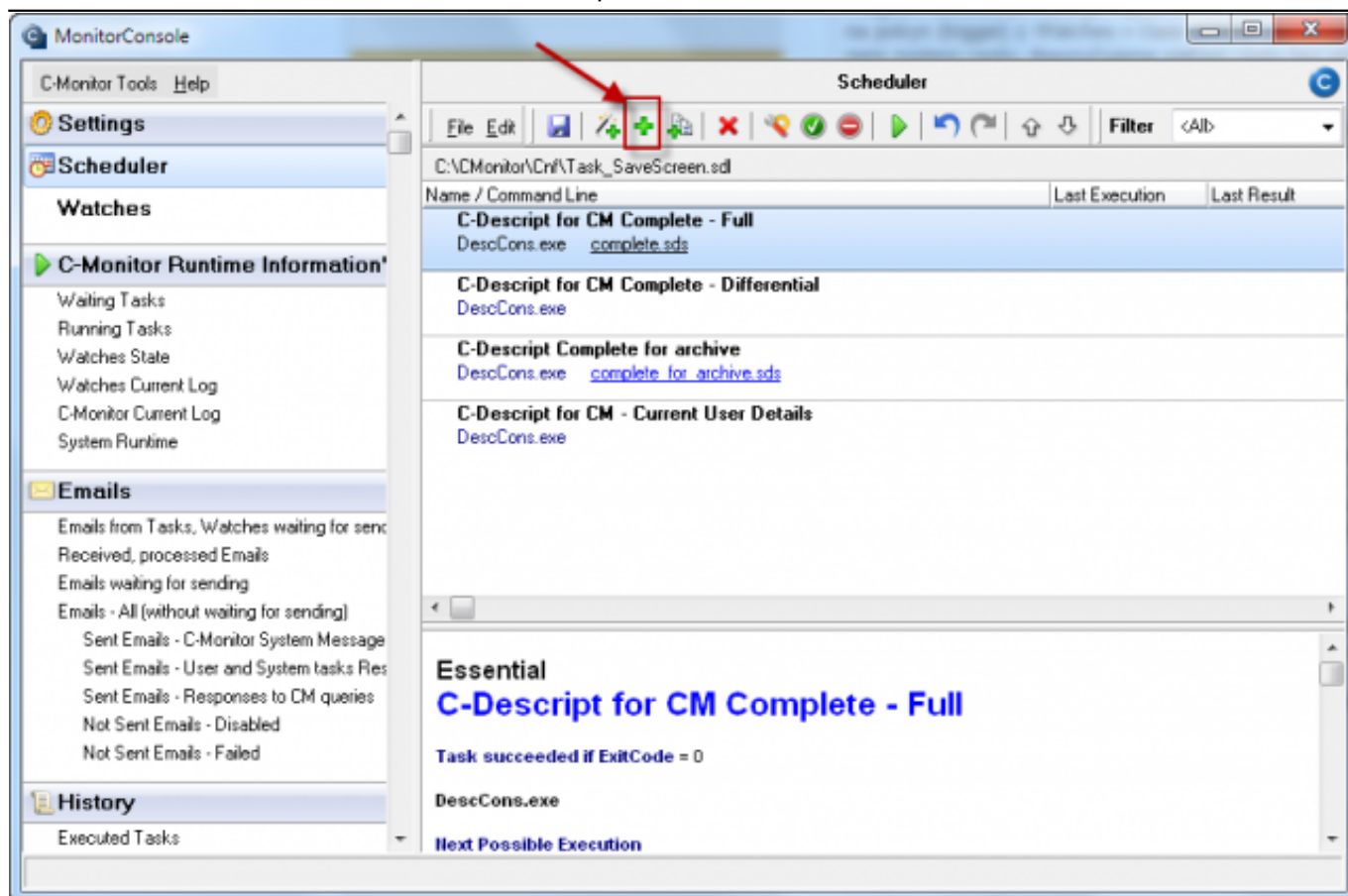
12. Zapnutie hlásenia výpadku Online spojenia s monitorovaným serverom.

Ako dostupný spôsob na znefunkčnenie sledovacieho systému iným administrátorom by sa mohlo javiť, že sa zastaví C-Monitor. Preto treba mať na daný server monitorované [Online spojenie medzi CM Serverom a C-Monitor klientom](#) [2]. Iné spôsoby znefunkčnenia sa dajú odhaliť, nakoľko to nejde bez stôp. Ale ako bolo na začiatku povedané, tento spôsob monitorovania je určený do prostredia, kde subdodávateľ rešpektuje takúto kontrolu a narušiť tento systém by znamenalo zbytočnú stratu dôvery. Ak by ste mali pocit, že vám screenshoty chýbajú, kontaktujte nás čím skôr, na základe logov zistíme, že kedy a akým spôsobom sa systém niekto snažil odstaviť.

KROKY NASTAVENIA V OBRÁZKOCH

(Upozornenie : bod 12 nie je v obrázkoch)





Obrázek: Pridanie novej úlohy pre spúšťanie ScreenSaver aplikácie

Modify Task

Do Before Execution Result File(s) On Task Finish E-Mail

General Accounts Advanced Conditions for Execution Security

Name (Description)
Save screen task

Category
Monitoring

☒ **Scheduling Enabled** ☐ Show in Info Panel

Command Line
\\modules\\utilities\\savescreen.exe \\server2\\D\\screenshots\\@user@_@datetimelong@.jpg

Startup Directory

☐ **Execute by Date and Time**

☒ **Execute on (Trigger, OS start, ...)**

Trigger savescreen

☐ **User must confirm execution**

OK Cancel

Obrázek: Nastavenie záložky General v úlohe

Modify Task [X]

Do Before Execution	Result File(s)	On Task Finish	E-Mail
General	Accounts	Advanced	Conditions for Execution
			Security

☐ Run under same user account as is running C-Monitor

☐ Run as another user (user must exist on this computer or in your domain)

User Name: Domain:

Password: Password Confirmation:

☒ Run under logged on users

Run under one of logged on users [v]

List of users (user login names), separated by , or ;

account-for-monitoring

☒ Run with highest privileges (used only for Windows Vista, 2008,...)

☐ Connect persistently mapped network drives (with created process user)

☒ Use remote access credentials (connect to network device as another user)

User Name: Domain / Network name of device:

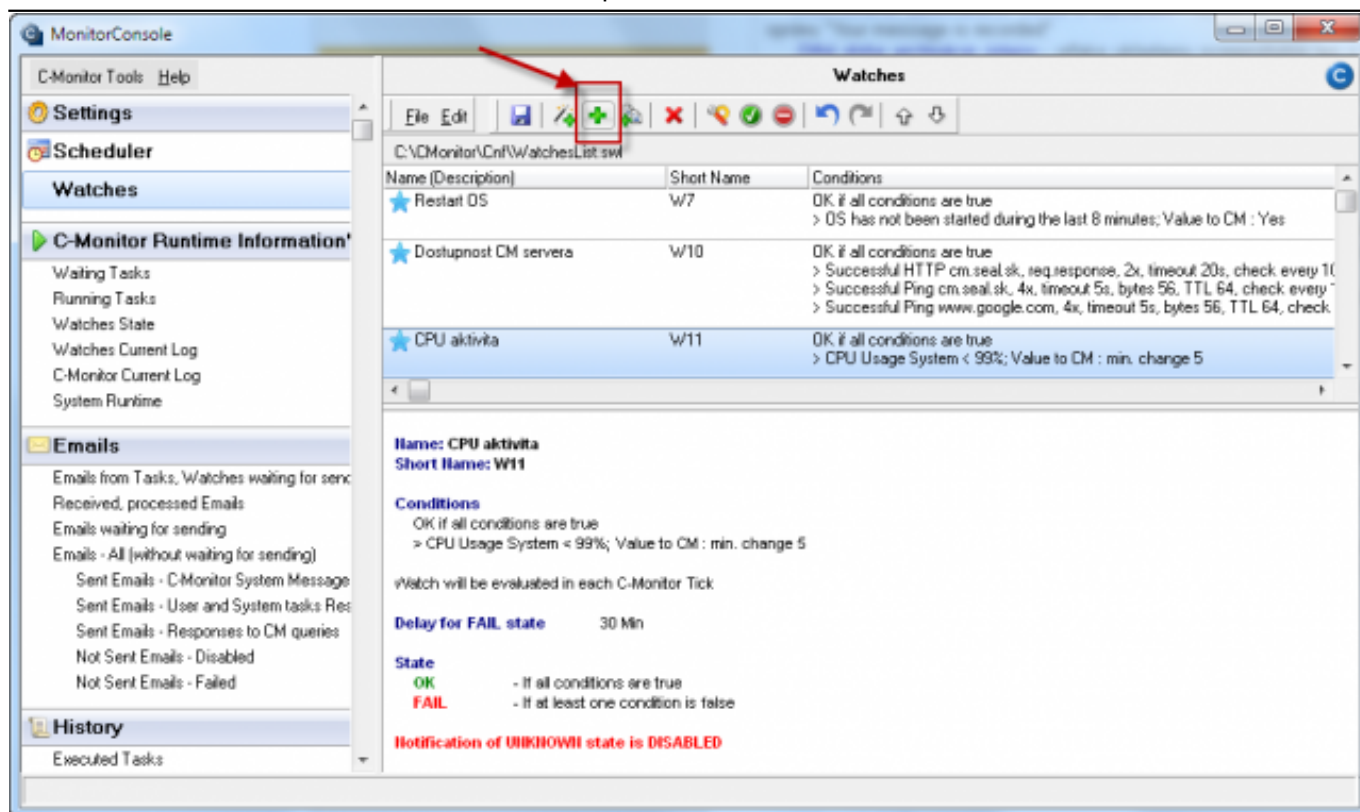
user-only-for-network-access SERVER2

Password: Password Confirmation:

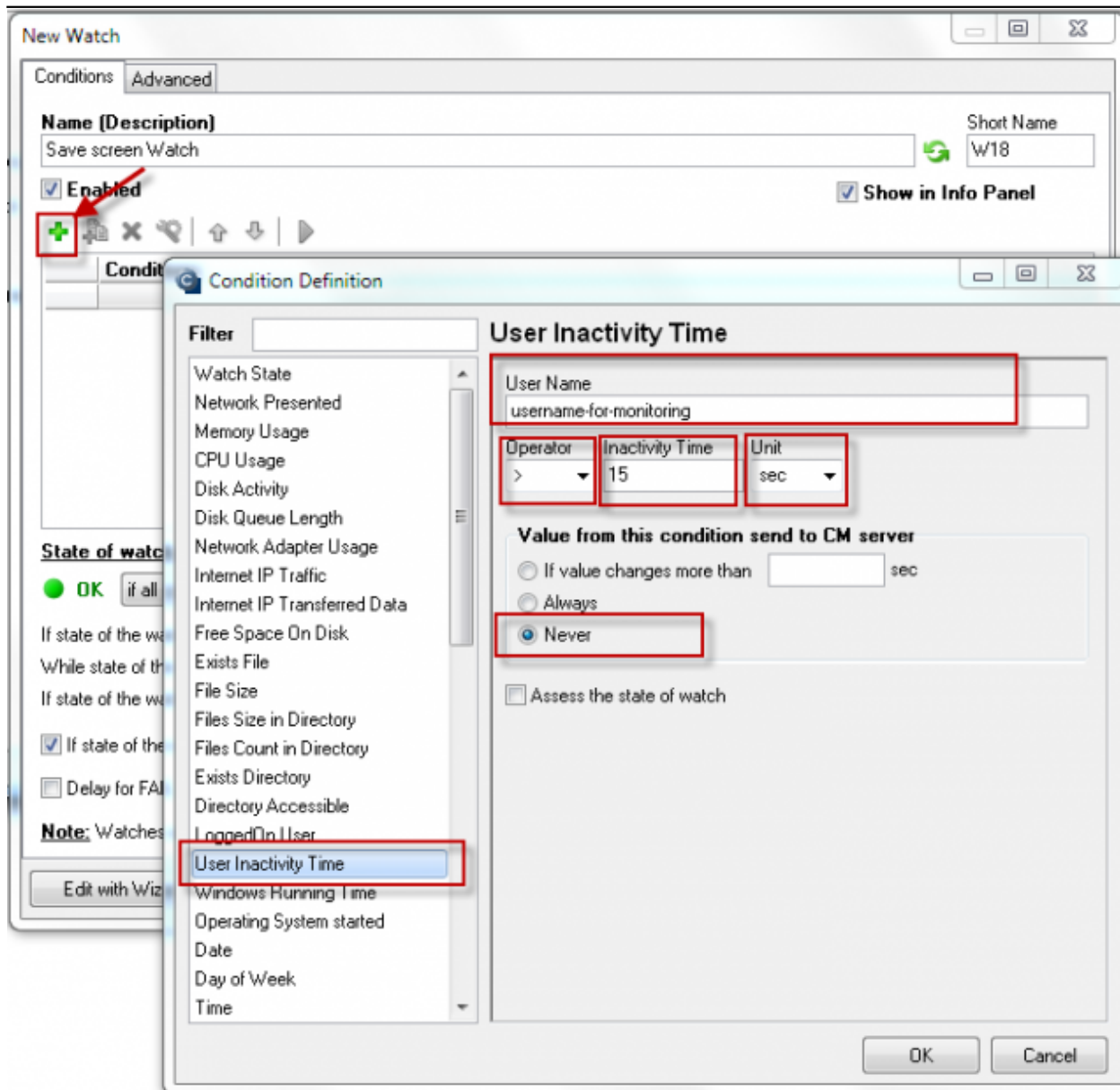
XXXXXXXXXX XXXXXXXXXXXX

OK Cancel

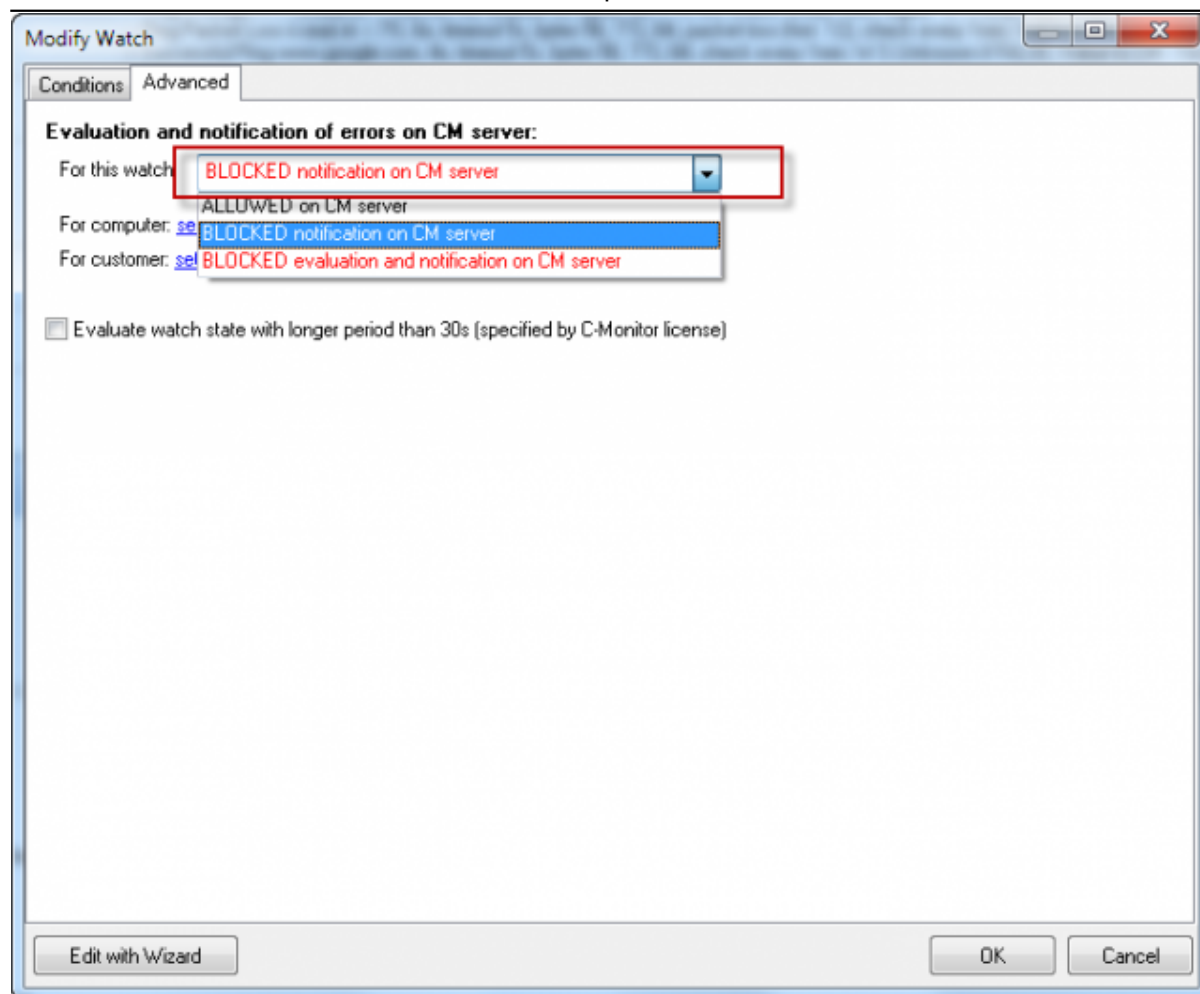
Obrázek: Nastavenie záložky Advanced v úlohe



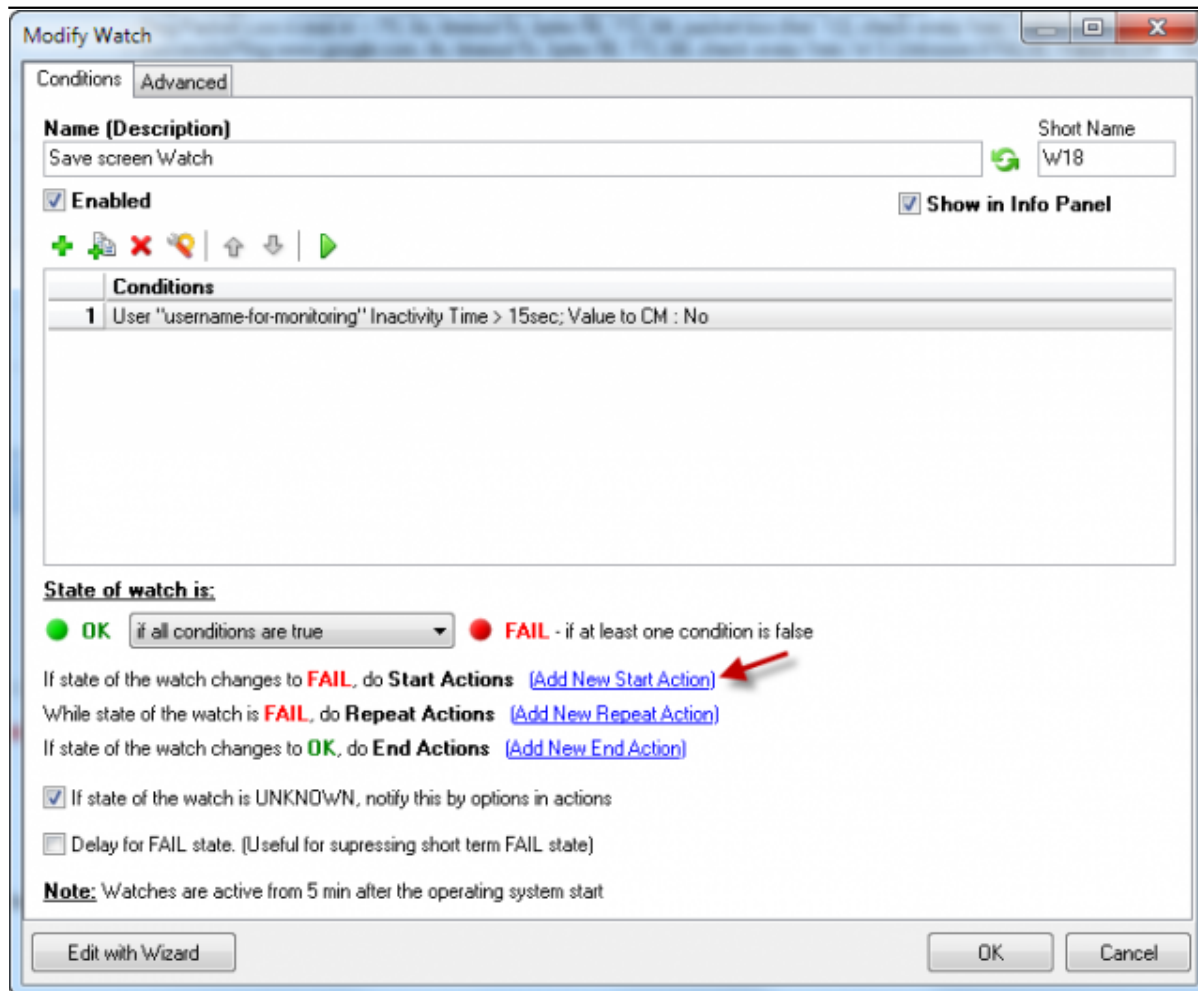
Obrázek: Pridanie nového Watchu pre vydávanie pokynu na odchyt obrazovky (trigger na naplánovanú úlohu)



Obrázek: Vytvorenie podmienky User Inactivity Time a jej nastavenia



Obrázek: Zablokovanie posielania (nežiadúcej) notifikácie pri zmenách Watchu - záložka Advanced vo Watch-i.



Modify Watch

Conditions: **Advanced**

Name (Description)
Save screen Watch

Short Name
W18

☒ **Enabled** ☒ **Show in Info Panel**

+ + - X ? | ↑ ↓ | ▶

Conditions	
1	User "username-for-monitoring" Inactivity Time > 15sec; Value to CM : No

State of watch is:

☒ **OK** if all conditions are true ☐ **FAIL** - if at least one condition is false

If state of the watch changes to **FAIL**, do **Start Actions** [\(Add New Start Action\)](#)

While state of the watch is **FAIL**, do **Repeat Actions** [\(Add New Repeat Action\)](#)

If state of the watch changes to **OK**, do **End Actions** [\(Add New End Action\)](#)

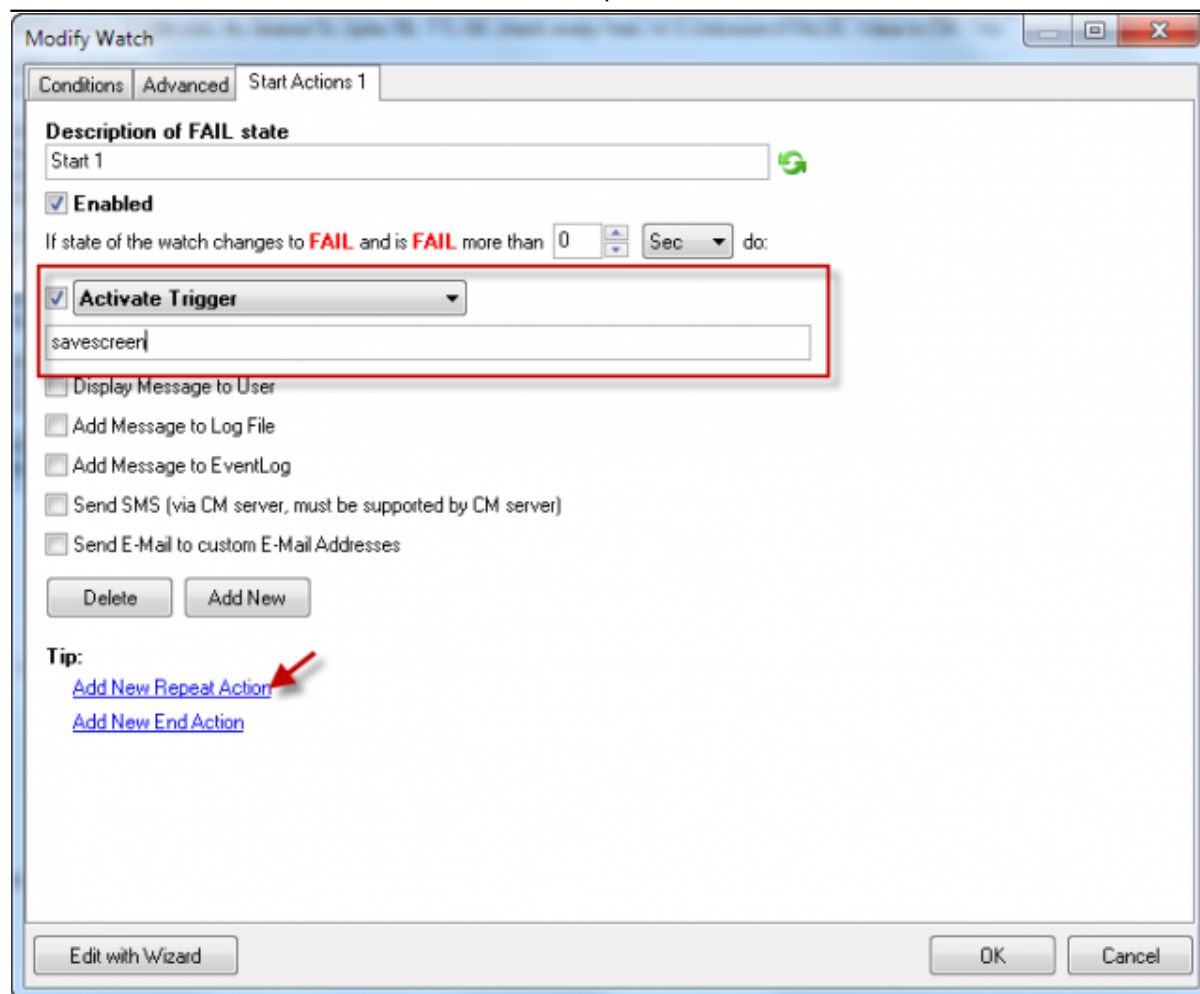
☒ If state of the watch is UNKNOWN, notify this by options in actions

☐ Delay for FAIL state. (Useful for suppressing short term FAIL state)

Note: Watches are active from 5 min after the operating system start

Edit with Wizard OK Cancel

Obrázek: Pridanie akcie Start



Obrázek: Nastavenie akcie Start pre prvé spustenie odchytenia obrazovky

Modify Watch

Conditions | Advanced | Start Actions 1 | Repeat Actions 1

Description of still FAIL state

Repeat 1

☒ **Enabled**

While state of the watch is **FAIL**, repeat each 15 Sec

☐ Interval prolonging x2

☒ **Activate Trigger**

savescreen

☐ Display Message to User

☐ Add Message to Log File

☐ Add Message to EventLog

☐ Send SMS (via CM server, must be supported by CM server)

☐ Send E-Mail to custom E-Mail Addresses

Delete Add New

Tip:
[Add New End Action](#)

Edit with Wizard OK Cancel

Obrázek: Nastavenie akcie Repeat pre opakované odchytávanie obrazovky

Nastavenie C-Monitora na PC

Spoločnosť Počítač & Umiestnenie Používateľ Email Hľadať

Licencia OS

Povolit automatickú aktualizáciu C-Monitor-a ☒ Zobraziť históriu aktualizácií

Heslo pre prístup do konfigurácie C-Monitor-a Vyžadovať heslo vždy Heslo: heslo-do-cmonitora

Heslo sa vyžaduje pre prístup do konfigurácie C-Monitora, úpravu C-Schedulera a Watches, zastavenie a skončenie C-Monitora.

C-Monitor Tick interval 15 sek

Východzia hodnota je 30 sekúnd. Hodnotu pre C-Monitor Tick interval zadajte len v prípade, ak si prajete použiť inú ako východziu hodnotu.

Parametre pre http komunikáciu medzi C-Monitor klientom a CM serverom

Použiť nastavenia zákazníka

URL Customer Monitora

Použiť Proxy Nie

Proxy server

Proxy port

Proxy používateľ

Proxy heslo

Nastavenia zákazníka

http://

Nie

0

Aktualizovať na počítači

Obrázek: Skrátenie C-Monitor Ticku, ak sú screeny žiadané v intervale kratšom než 30sec, zaheslovanie konfigurácie C-Monitora

ČO ZÍSKAL ZÁKAZNÍK (VLASTNÍK SERVERA) ?

Získal bezpečným spôsobom istotu, čo sa deje na jeho serveri u subdodávateľov. Jednoduchý prístup k uloženým informáciám s relatívne ľahkým vyhľadáváním potrebného momentu. To len za cenu riešenia CM, aplikácia SaveScreen je výrobcom CM uvoľnená bezplatne.

Dohoda môže byť dokonca taká, že sa budú nahrávať aj sami IT správcovia a dokladovať tak, že robili len to čo bolo dohodnuté. Je samozrejme na dôvere, že daný systém sami nebudú vypínať (predsa len, kto systém inštaluje, vie ho aj vypnúť).

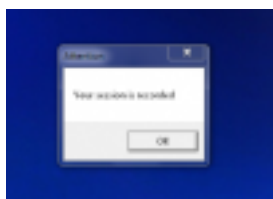
Z CM sa na túto tému kontroly subdodávateľov dajú získať aj ďalšie informácie v XLS forme, napríklad kedy bol prihlásený a kedy aktívne na danom serveri pracoval.

ZÁVER A PRÍNOSY CM RIEŠENIA

Okrem už vyššie spomenutých výhod riešenia, nasaditeľné zbehlým CM technikom vo veľmi krátkom čase, je dôležitý prínos je vo fakte, že takýto odchyt obrazovky je realizovaný serióznym softvérom. Práve odchyt obrazoviek patrí do segmentu, kedy aj platený softvér môže mať úplne iný skrytý účel. To je v softvéri CM vylúčené a všetky činnosti, ktoré vykonáva sú transparentne odkomunikované.

Date:

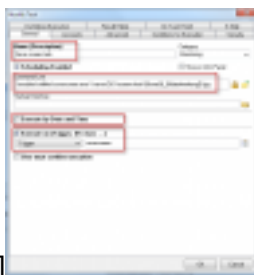
13.1.2013Obrázky:



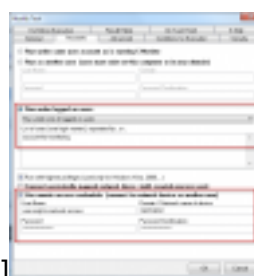
[3]



[4]



[5]



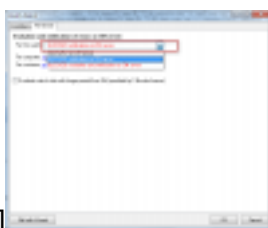
[6]



[7]



[8]



[9]



[10]



[11]



[12]



[13]Documents:



[Program SaveScreen pre screenshoty obrazovky s upozornením nahrávania](#) [14]

Odkazy

[1] <https://customermonitor.cz/news/blog/openvpn-pre-ne-admin-pouzivatela>

-
- [2] <https://customermonitor.cz/ako-funguje-cm/monitoring/monitoring-dostupnosti-serverov/signalizacia-zo-strany-cm-servera>
 - [3] https://customermonitor.cz/sites/default/files/Session_is_recorded_atenttion_dialog.png
 - [4] https://customermonitor.cz/sites/default/files/SaveScreen_zaciatok.png
 - [5] https://customermonitor.cz/sites/default/files/SaveScreen_general.png
 - [6] https://customermonitor.cz/sites/default/files/SaveScreen_advanced.png
 - [7] https://customermonitor.cz/sites/default/files/SaveScreen_novy_Watch.png
 - [8] https://customermonitor.cz/sites/default/files/SaveScreen_condition_Inactivity_time.png
 - [9] https://customermonitor.cz/sites/default/files/SaveScreen_Watch_advanced.png
 - [10] https://customermonitor.cz/sites/default/files/SaveScreen_Akcie_zaciatok.png
 - [11] https://customermonitor.cz/sites/default/files/SaveScreen_Akcia_Start.png
 - [12] https://customermonitor.cz/sites/default/files/SaveScreen_Akcia_Repeat.png
 - [13] https://customermonitor.cz/sites/default/files/SaveScreen_uprava_ticku_a_zaheslovanie_0.png
 - [14] <https://customermonitor.cz/sites/default/files/ScreenSaver.zip>