HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza alata HealthMonitor

CCERT-PUBDOC-2005-03-113

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

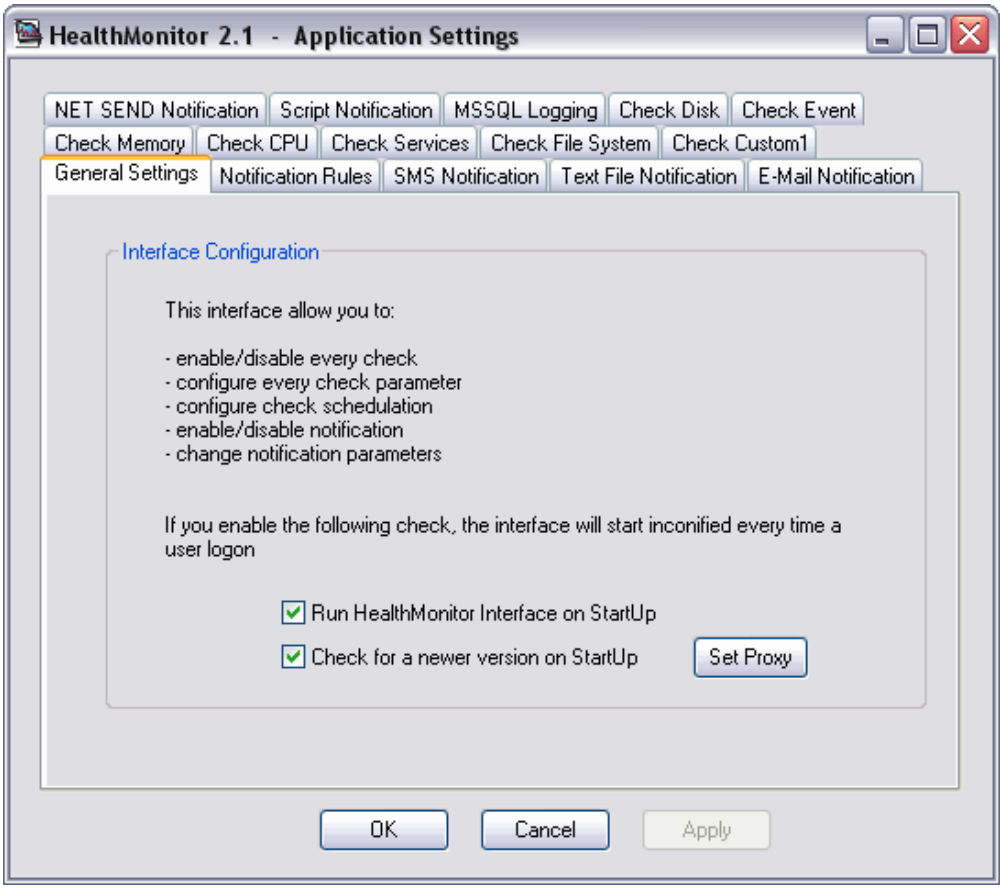
HealthMonitor je besplatan, funkcijama bogat programski alat za nadgledanje računala s Windows operacijskim sustavima. Alat funkcionira kao Windows servis koji nadgleda stanje sustava, odnosno parametre kao što su količina slobodnog diskovnog prostora, datotečni sustav, itd. Alat također posjeduje razne mogućnosti izvješćivanja korisnika kao što su SMS poruke, poruke elektroničke pošte ili nekom drugom metodom, ovisno o željama korisnika.

2. Instalacija alata

Za instalaciju programskog alata potrebno je dohvatiti besplatnu inačicu s referentne adrese http://sourceforge.net/project/showfiles.php?group_id=88973&package_id=93154 te ju pohraniti na lokalni disk. Aktivacijom linka na navedenoj referentnoj adresi korisnik dohvaća datoteku u `.zip` formatu pod imenom `HealthMonitor_2.1Stable.zip`, veličine 392 KB.
U trenutku pisanja dokumenta zadnja dostupna inačica alata je `2.1`.
Za instalaciju programa potrebno je raspakirati `.zip` datoteku i pokrenuti novu datoteku pod imenom `HealthMonitor.msi` čime započinje proces instalacije. Alat funkcionira i na Windows NT platformi, ali preporučljiva konfiguracija je Windows 2000 operacijski sustav ili noviji s instaliranim `.NET Framework 1.1` paketom koji se može pronaći na adresi http://www.microsoft.com/downloads/details.aspx?familyid=262D25E3-F589-4842-8157-034D1E7CF3A3&displaylang=en.

3. Podešavanje alata

Nakon uspješne instalacije, alat se automatski pokreće, a korisnik ima priliku podesiti postavke alata. Slika 1 prikazuje početni prozor alata koji se otvara nakon završenog procesa instalacije.



Slika 1: Početni prozor alata HealthMonitor

Početni prozor alata s aktivnom karticom `General Settings` ima funkciju podešavanja osnovnih parametara alata kao što su način pokretanja i način provjere postojanja nove inačice alata.
Uključivanje opcije `Run HealthMonitor Interface on StartUp` znači da se će alat pokrenuti svaki puta kada se i sustav pokrene.
Opcija `Check for a newer version on StartUp` označava da će prilikom svakog pokretanja sustava prvo slijediti proces provjeravanja postojanja nove inačice alata.
Klikom na dugme `Set Proxy` otvara se dijaloški okvir prikazan na Slici 2, a traženim podacima popunjavaju ga oni korisnici koji za pristup Internetu koriste *proxy* poslužitelj.

Slika 2: Podešavanje postavki proxy poslužitelja

Bitno je naglasiti da svaka promjena u postavkama programa postaje primjenjiva tek nakon odabira gumba `OK` na prozoru prikazanom na slici (Slika 1). Naime, nakon što korisnik podesi postavke i odabere gumb `Apply`, postavke se spremaju, no nisu aktivne. Odabirom gumba `OK`, alat se mora ponovno pokrenuti. Korisniku se pojavljuje dijaloški okvir prikazan na slici Slici 3.

Slika 3: Potvrda za primjenu postavki alata

Odabirom naredbe `Yes`, alat se automatski ponovno pokreće i funkcionira prema zadanim postavkama.

3.1. Provjere stanja sustava

Alat *HealthMonitor* omogućava nekoliko vrsta provjere stanja Windows operacijskog sustava: provjeru zauzeća radne memorije, procesora, servisa, datotečnog sustava, lokalnih diskova, raznih događaja te korisnički definiranih provjera. Navedene provjere podešavaju se kroz odgovarajuće kartice:

- `Check Memory`,
- `Check CPU`,
- `Check Services`,
- `Check File System`,
- `Check Disk`,
- `Check Event`,
- `Check Custom1`.

Zajedničke postavke svim navedenim načinima provjere stanja sustava su opcije:

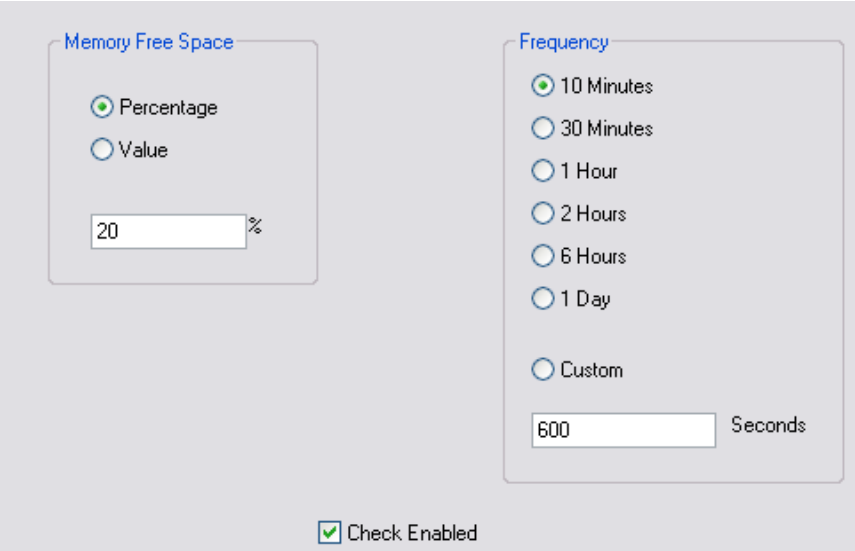
- `Check Enabled` koja označava da li se odgovarajuća provjera sustava izvodi ili ne,

- `Frequency` opcija koja označava vremenski interval izvođenja provjere sustava, a koja može biti odabrana između ponuđenih intervala (od 10 minuta do 1 dana) ili korisnički definirana u sekundama.

Navedenu opciju `Frequency` ne dijele jedino provjera datotečnog sustava i provjera događaja.

3.1.1. Provjera memorije

`Check Memory` kartica omogućava provjeru stanja memorije korištenjem `Memory Free Space` opcije. Ova opcija označava korisnički postavljen prag slobodnog prostora memorije, a može biti iskazana u postocima ili apsolutno u MB. Slika 4 prikazuje karticu `Check Memory`.



Slika 4: Kartica Check Memory

Ukoliko korisnik definira da je se promjena statusa događa kada je 20% memorije slobodno i pokrene provjeravanje memorije, u slučaju zadovoljenja te postavke (slobodno je više od 20% memorije) korisnik će dobiti izvješće da je stanje memorije ispravno, dok će u suprotnom dobiti izvješće o pogrešnom statusu.

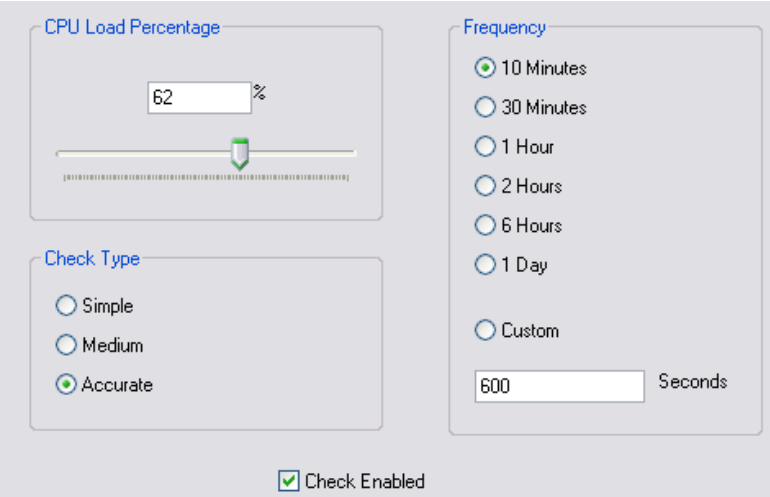
Poruka koja se generira ovom provjerom izgleda ovako:

```
Check Memory Notification at 15.4.2005 18:32:49

Total Memory = 510 Mb
Available Memory = 106 Mb
Percentage Used = 79,1283930032811
```

3.1.2. Provjera procesora

Provjera procesora funkcionira na sličan način kao i provjera memorije. U kartici `Check CPU` podešava se parametar `CPU Load Percentage` (Slika 5).



Slika 5: Kartica Check CPU

Postoje tri tipa provjere:

- `Simple`,
- `Medium`,
- `Accurate`.

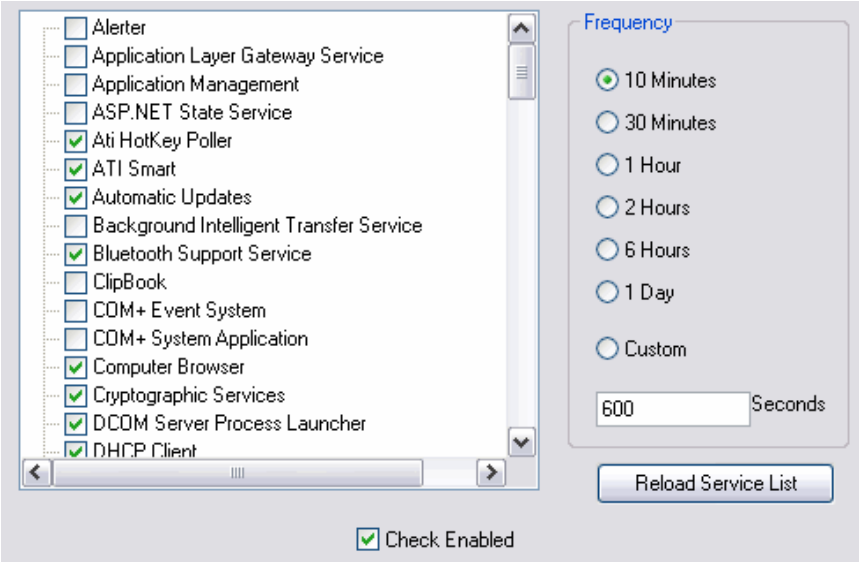
Nakon provjere, ovisno o statusu procesora, korisnik dobiva odgovarajuću poruku. Poruka koja se generira ovom provjerom izgleda ovako:

```
COMPUTERNAME - Priority: High
Check CPU Error at 13.4.2005 13:28:33
Load Percentage: 21%

Description: x86 Family 15 Model 2 Stepping 9
Processor ID: BFEBFBFF00000F29
Status: OK
Manufacturer: GenuineIntel
Availability: Running/Full Power
Current Clock Speed: 2799 MHz
Maximum Clock Speed: 2799
Level 2 Cache Size: 0
Level 2 Cache Speed:
Power Management Supported: False
```

3.1.3. Provjera servisa

Broj servisa koji se mogu provjeravati pomoću ovog alata je oko 100. Prilikom instalacije alata, nekoliko servisa je već predefinirano kao servisi koji se provjeravaju. Korisnik na kratici `Check Services` izvodi promjene postavki servisa koji će se, a koji neće provjeravati. Slika 6 prikazuje postavke na navedenoj kartici.



Slika 6: Kartica Check Services

Da bi se neki servis isključio odnosno uključio za provjeravanje potrebno je kliknuti u kvadratić pored naziva servisa.

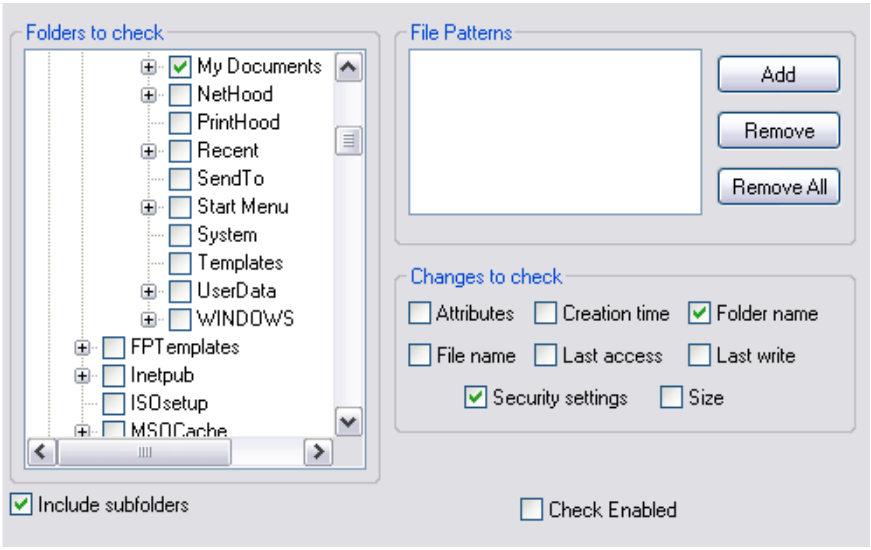
Poruka koja se generira ovom provjerom izgleda ovako:

```
Check Service Notification at 15.4.2005 18:32:49

Service Name: ATI Smart
Status: Stopped
-----------------------------------------------
Service Name: Security Center
Status: Stopped
```

3.1.4. Provjera datotečnog sustava

Datotečni sustav korisnika također se može podvrgnuti provjeri. Kartica `Check File System` namijenjena je podešavanju postavki ovog tipa provjeravanja i prikazana je na slici (Slika 7).



Slika 7: Kartica Check File System

U kartici namijenjenoj provjeri datotečnog sustava moguće je podesiti sljedeće parametre:

- `Folders to check` omogućava korisniku da izabere odnosno označi one lokalne diskove i mape koje želi provjeravati,
- `Include subfolders` opcija, ako je uključena, znači da će se provjeravati i sve podmape unutar označenih mapa.

- `Changes to check` omogućava definiranje koje promjene u datotečnom sustavu će se pratiti (moguće je provjeravati promjenu atributa, vremena kreiranja, imena mape, imena datoteke, posljednjeg pristupa, posljednje promjene, sigurnosnih parametara i veličine).

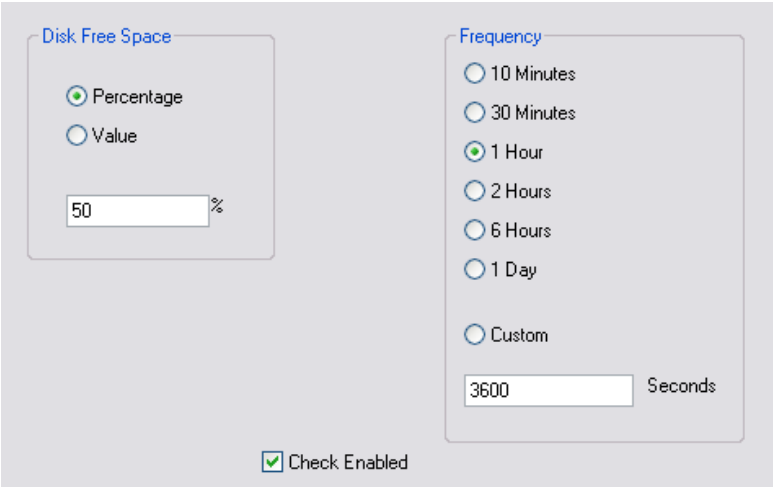
Poruka koja se generira ovom provjerom izgleda ovako:

```
Check File Notification at 15.4.2005 17:18:50

File/Folder: C:\\Documents and Settings\username\My
Documents\private\timo\~wrd2719.tmp
Change Type: Object changed (changes to size, attributes, security settings,
last write, or last access time)
```

3.1.5. Provjera lokalnih diskova

Provjera lokalnih diskova služi provjeri slobodnog prostora na lokalnom disku ili diskovima. Potrebno je unijeti količinu diskovnog prostora koja se iskazuje vrijednošću u postocima ili apsolutnom veličinom u MB, a definira se u polju `Disk Free Space`. Slika 8 prikazuje karticu `Check Disk`.



Slika 8: Kartica Check Disk

Kao i kod provjere memorije i procesora, nakon što je proces provjere diska završio, ovisno o statusu slobodnog prostora, korisnik dobiva odgovarajuće poruke.

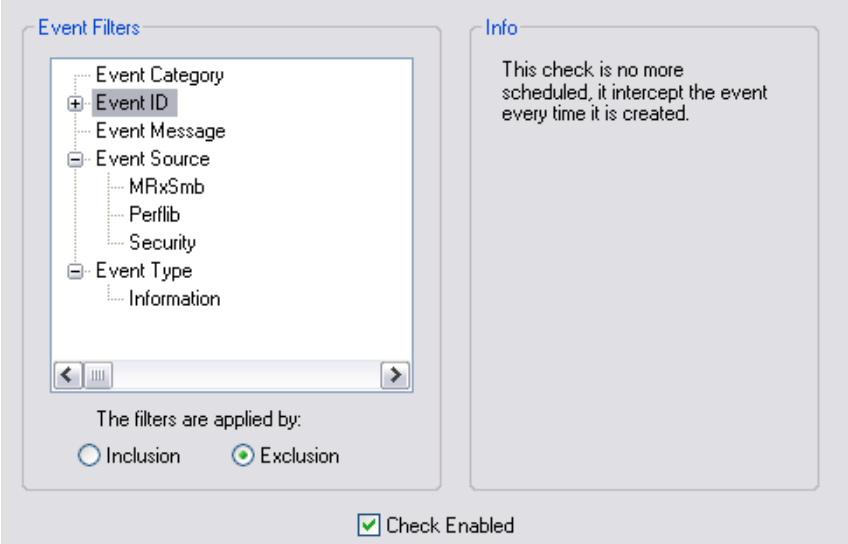
Poruka koja se generira ovom provjerom izgleda ovako:

```
COMPUTERNAME - Priority: High
Check Disk Notification at 16.4.2005 16:11:31

DriveType:     Local hard disk.
Drive C:
File System:   NTFS
Drive Size = 39997Mb
Current free space = 17609 Mb
Volume Name =
Percentage Used = 55,9738289889633
```

3.1.6. Provjera događaja

Provjera događaja korisna je opcija. Podešavanje postavki obavlja se na kartici `Check Event` (Slika 9). Ova vrsta provjere rabi filtar opcije koje omogućuju korisniku da dobije poruku tek kada se dogodi neki događaj koji odgovara podešenom filtru ili filtrima.



Slika 9: Kartica Check Event

Predefinirane filtre nije moguće mijenjati, a korisniku je omogućeno dodavanje novih filtara tako da desnom tipkom miša kliknu na kategoriju filtra (npr. `Evend ID`, `Event Source` ili `Event Type`) i odabere naredbu `Add filter.`

Poruka koja se generira ovom provjerom izgleda ovako:

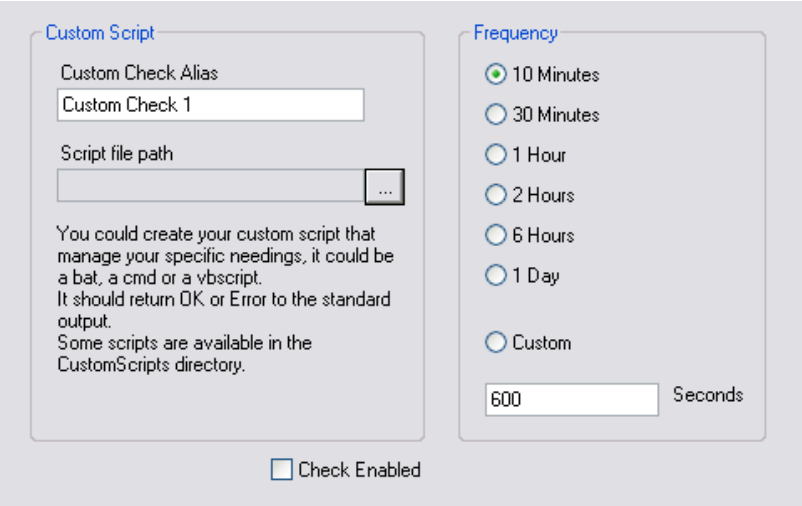
```
Check Event Notification at 15.4.2005 18:56:09

Log File: Application
Record Number: 8917
Type: error
Time Generated: 20050415185609.000000+120
Source: Userenv
Category: None
Category String:
Event: 1030
User: domain\username
Computer: COMPUTERNAME
Message: Windows cannot query for the list of Group Policy objects. A message
that describes the reason for this was previously logged by the policy
engine.


Useful links:
Search Microsoft Support for this Error
Search EventID.net for this Error
Search Google for this Error
```

3.1.7. Korisničko definiranje provjera

Kartica `Check Custom1` namijenjena je naprednim korisnicima koji imaju iskustva u programiranju korištenjem skriptnih jezika (Slika 10).



Slika 10: Kartica Check File System

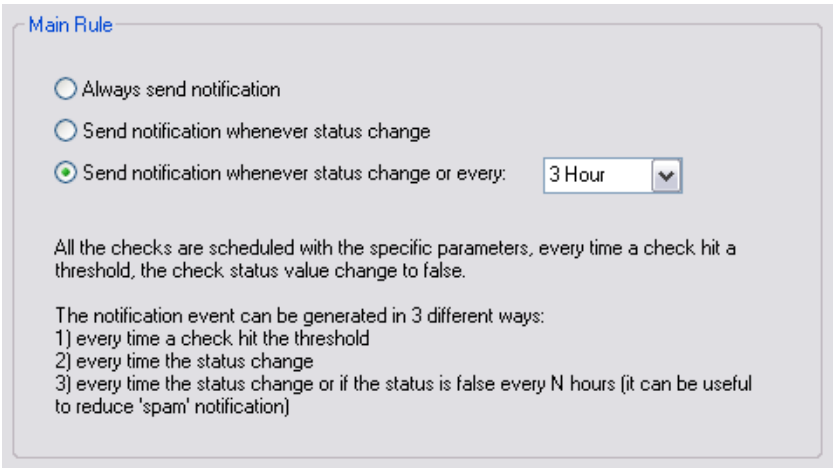
U polju `Custom Check Alias` korisnik upisuje naziv provjere, a u polju `Script file path` definira putanju do skripte koju želi pokrenuti.

3.2. Izvješća

Kartica `Notification Rules` sadrži postavke za slanje izvješća. Korisnik definira koliko često će alat slati izvješća, a moguće je odabrati tri opcije:

- `Always send notification` koja ukazuje da se izvješće šalje odmah po kreiranju,
- `Send notification whenever status change` šalje izvješća samo nakon promjene statusa,
- `Send notification whenever status change or every:` šalje izvješća ili nakon promjene statusa ili nakon definiranog vremenskog intervala, npr. svakih 4 sata.

Osim navedenih osnovnih opcija postoje i dodatne koje su na kartici prikazane samo opisno, a sve opcije prikazane su na slici Slikci 11.



Slika 11: Kartica Notifiction Rules

Osim osnovnih odabira kada će se slati izvješća, korisnik definira i načine slanja, odnosno primanja izvješća. Alat može slati izvješća na sljedeće načine:

1. SMS porukom,
2. zapisivanjem u tekstualnu datoteku (*log* datoteka),
3. slanjem poruke elektronske pošte,
4. slanjem *NET SEND* poruke,

5. izvršavanjem skripte.

Svaki od navedenih načina slanja izvješća može biti podešen s odgovarajućim parametrima, ali ne mora biti aktivan. Naime, svaka dalje u tekstu opisana kartica ima oznaku `Check Enabled` koja označava da li se neki od navedenih načina izvješćivanja koristi ili ne.
Za svaki od načina slanja izvješća moguće je, uporabom gumba `Test Notification`, testirati postavljene parametre za slanje, odnosno primanja izvješća.

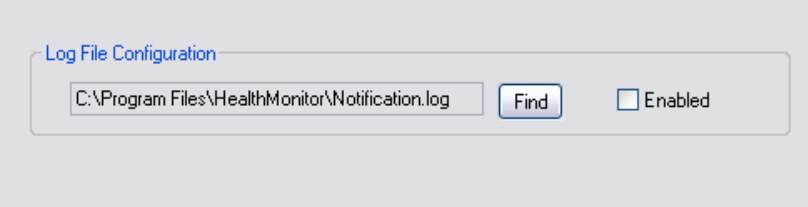
3.2.1. SMS izvješće

Podešavanje slanja izvješća na mobitel korisnika jednostavno je i izvodi se na kartici SMS `Notification`. Potrebno je upisati broj mobitela na koji će se slati izvješća (eng. *Receiver Mobile Phone Number*) te definirati COM *port* na kojem se nalazi mobilni uređaj koji se koristi za slanje izvješća. Slika 12 prikazuje opisane postavke.

Slika 12: Kartica SMS Notification

3.2.2. Izvješće u tekstualnoj datoteci

Drugi način generiranja izvješća jest zapisivanje u tekstualnu datoteku čija je predefinirana putanja `C:\Program Files\HealthMonitor\Notification.log`. Postavke koje sadrži kartica `Text File Notification` ima samo jedno svojstvo koje je potrebno podesiti, a to je lokacija spremanja tekstualne datoteke, što je prikazano na slici (Slika 13).



Slika 13: Kartica Text File Notification

Primjer tekstualne datoteke u kojoj je kreirano izvješće:

```
COMPUTERNAME - Priority: High
Check Event Notification at 12.4.2005 11:13:35

Log File:        Application
Record Number:   8761
Type:            warning
Time Generated:  20050412111335.000000+120
Source:          Userenv
Category:        None
Category String:
Event:           1517
User:            NT AUTHORITY\SYSTEM
Computer:        COMPUTERNAME
Message:         Windows saved user domain\username registry while an application or
```

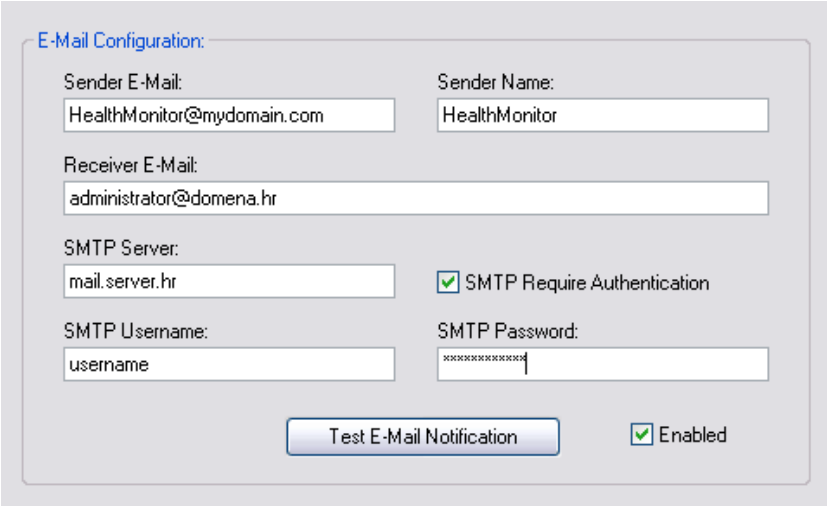
```
service was still using the registry during log off. The memory used by the user's
registry has not been freed. The registry will be unloaded when it is no longer in
use.


This is often caused by services running as a user account, try configuring the
services
to run in either the LocalService or NetworkService account.


Useful links:
<a
href=http://support.microsoft.com/search/default.aspx?Query=event+id+1517&KeywordType=
ALL&maxResults=50&Titles=false>Search Microsoft Support for this Error</a>
<a href=http://www.eventid.net/display.asp?eventid=1517&Source=Userenv>Search
EventID.net
for this Error</a>
<a href=http://groups.google.com/groups?q=event+id+1517+Userenv>Search Google for this
Error</a>
```

3.2.3. Izvješće u poruci elektroničke pošte

Treći način slanja i primanja izvješća je korištenje poruka elektroničke pošte. Podešavanje se obavlja uporabom kartice `E-mail Notification` koja je prikazana na slici (Slika 14).

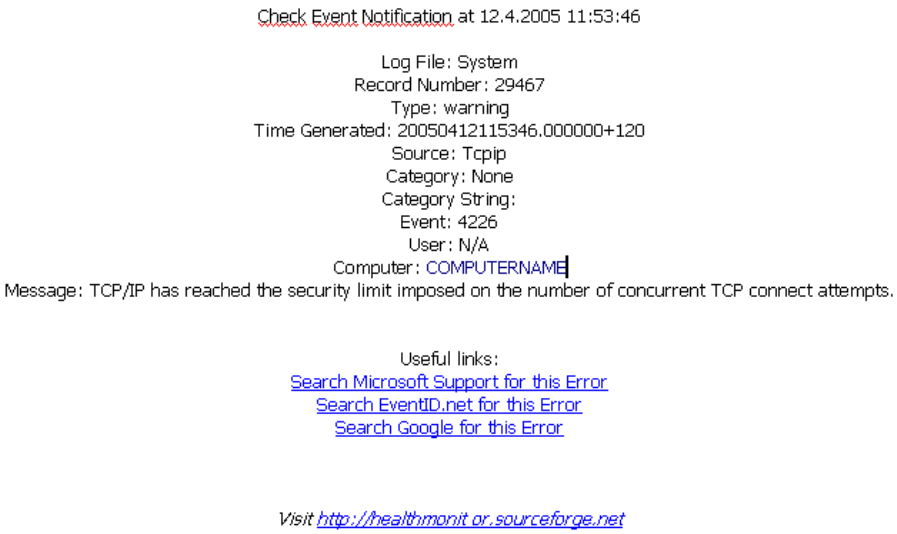


Slika 14: Kartica E-mail Notification

Podešavanje ovih postavki obuhvaća slijedeće:

- `Sender E-Mail` opcija sadrži adresu elektroničke pošte pošiljatelja poruke s izvješćem,
- `Sender name` opcija sadrži naziv pošiljatelja poruke s izvješćem koji će biti prikazan,
- `Receiver E-Mail` opcija sadrži adresu elektroničke pošte primatelja poruke,
- `SMTP server` opcija sadrži DNS ime ili IP adresu poslužitelja koji je zadužen za slanje poruka elektroničke pošte,
- `SMTP Username` sadrži opcionalno korisničko ime koje služi za prijavu na SMTP poslužitelj,
- `SMTP Password` sadrži opcionalnu zaporku koja služi za prijavu na SMTP poslužitelj,

Slika 15 prikazuje primjer izvješća poslanog u poruci elektroničke pošte.

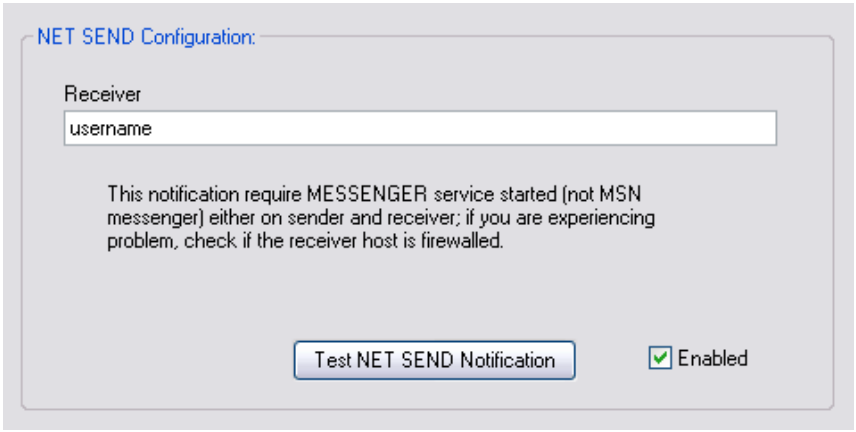


Slika 15: Izvješće u poruci elektroničke pošte

3.2.4. Izvješće putem *NET SEND* poruke

Još jedan način slanja poruka korisniku je uporaba `Messenger` servisa. Servis mora biti pokrenut na lokalnom računalu. Obzirom da je na Windows XP sustavima nakon instalacije *Service pack 2* paketa ovaj servis onemogućen, na tim sustavima potrebno ga je ručno pokrenuti ukoliko se za slanje izvješća želi koristiti NETSEND naredba.

Nakon aktiviranja servisa se uporabom naredbe *NET SEND* moguće je slati poruke definiranom korisniku. Podešavanje ovog načina slanja poruka o promjenama u sustavu izvodi se na kartici NET `SEND Notification`, a koja je prikazana na slici (Slika 16).



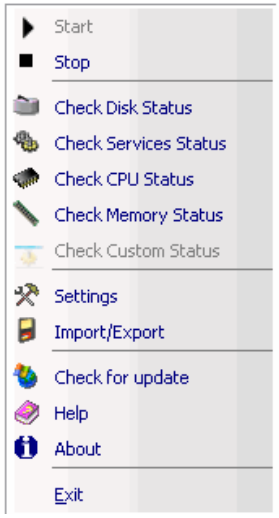
Slika 16: Kartica NET SEND Notification

Za podešavanje ovakvog načina slanja potrebno je upisati korisničko ime primatelja poruka. Poruka koja se korisniku pojavljuje na zaslonu prikazana je na slici (Slika 17).

Slika 17: Izvješće u obliku NET SEND poruke

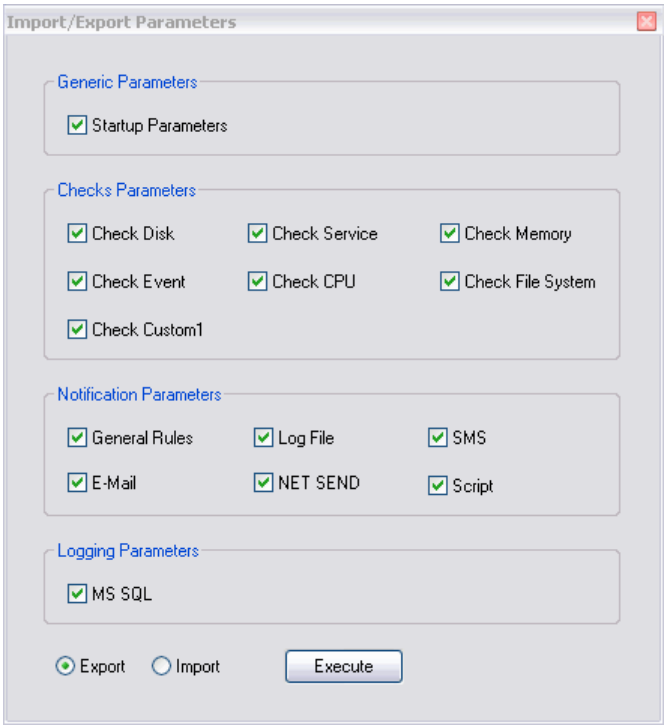
4. Uporaba alata

Nakon što je alat *HealthMonitor* detaljno podešen prema željama i potrebama korisnika, njegova uporaba vrlo je jednostavna. Alat se pokreće prilikom pokretanja računala (ako je tako podešeno u postavkama alata opisanim u točki 3) i njegova aktivnost vidi se u *system tray*-u.
Klikom desne tipke miša na ikonu alata otvara se izbornik odgovarajući izbornik (Slika 18).



Slika 18: Izbornik alata HealthMonitor

Prve dvije naredbe `Start` i `Stop` služe pokretanju (naredba `Start`) te zaustavljanju (naredba `Stop`) alata. Slijede naredbe koje izvršavaju određene provjere, a koje su aktivne samo u slučaju označene opcije `Check Enabled` na svakoj pojedinoj kartici za podešavanje provjeravanja.
Naredba `Settings` otvara početni prozor alata (Slika 1), dok naredba `Import/Export` otvara prozor prikazan na slici (Slika 19) na kojoj se nalaze označene opcije koje će se izvesti (engl. *export*) u obliku `.xml` datoteke koju će korisnik spremiti na željenu lokaciju.



Slika 19: Izbornik alata HealthMonitor

Primjer generirane datoteke:

```
<?xml version="1.0" encoding="utf-8" standalone="yes" ?>
- <!--
Heathmonitor 2.1    - Export Parameters File (16.4.2005 16:20:12)
  -->
- <Configuration>
- <General_Parameters>
- <Startup_Parameters>
  <RunOnStartup>True</RunOnStartup>
  <CheckUpdateOnStartup>True</CheckUpdateOnStartup>
  <ProxyAuthenticated>False</ProxyAuthenticated>
  <ProxyAddress />
  <ProxyPort />
  <ProxyUser />
  <ProxyPassword />
  </Startup_Parameters>
  </General_Parameters>
- <Checks_Parameters>
- <Checks_Disk>
  <DiskThreshold>50</DiskThreshold>
  <DiskCheckTime>3600</DiskCheckTime>
  <DiskCheckEnabled>True</DiskCheckEnabled>
  <DiskCheckType>Percentage</DiskCheckType>
  </Checks_Disk>
- <Checks_Event>
  <EventCheckEnabled>True</EventCheckEnabled>
  <EventFilterLogic>Exclusion</EventFilterLogic>
  <EventFiltersNumber>13</EventFiltersNumber>
  <EventFilters_0_12>Information</EventFilters_0_12>
  <EventFilters_1_12>TY</EventFilters_1_12>
  <EventFilters_0_11>Security</EventFilters_0_11>
  <EventFilters_1_11>SO</EventFilters_1_11>
  <EventFilters_0_10>Perflib</EventFilters_0_10>
  <EventFilters_1_10>SO</EventFilters_1_10>
  <EventFilters_0_9>MRxSmb</EventFilters_0_9>
```

Ostale naredbe su:

- `Check for update` – naredba koja provjerava trenutnu inačicu alata pokrenutog na računalu korisnika s najnovijom izdanom inačicom alata ,
- `Help` – naredba koja otvara referentnu stranicu http://healthmonitor.sourceforge.net/faq.html a ustvari predstavlja najčešće postavljena pitanja (engl. FAQ – *frequently asked questions*),
- `About` – naredba koja otvara prozor koji prikazuje informacije o autoru alata,
- `Exit` – naredba koja zaustavlja rad alata.

5. Zaključak

HealthMonitor je jednostavan i praktičan programski alat koji administratorima Windows operacijskih sustava može pomoći u nadzoru i praćenju rada sustava. S mnoštvom opcija, provjera i slanja izvješća, bitno izmijenjeno stanje sustava odmah će biti uočeno na temelju čega administrator sustava može poduzeti odgovarajuće korektivne mjere. Prednosti alata svakako su mnoštvo opcija koje pomažu u dijagnostici rada sustava te mogućnost vrlo detaljnog podešavanja ponuđenih opcija, a također je za pohvaliti i velik broj načina izvješćivanja korisnika o događajima koje alat generira. Nedostatak alata je nepostojanje pomoći i pojašnjenja opcija pa korisnik u nekim slučajevima mora metodom pokušaja i pogreške testirati alat i njegove mogućnosti.