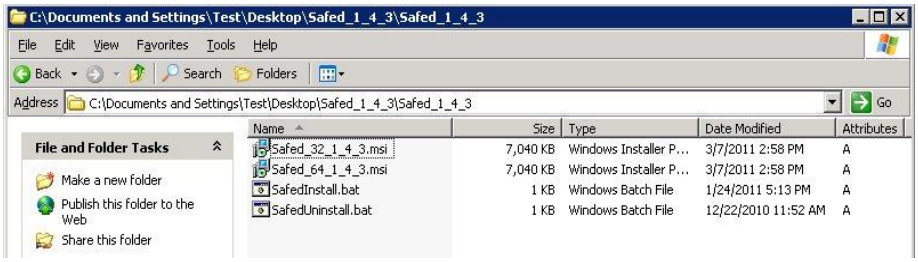
SAFED AGENT INSTALLATION AND CONFIGURATION GUIDE

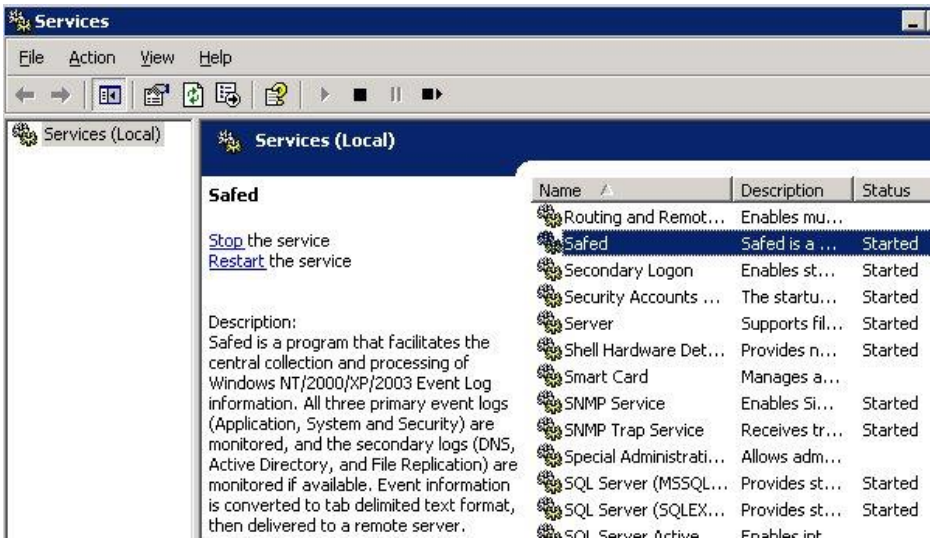
Table of Contents

1 Installation of Safed for Windows

In order to install the Safed agent on Win XP/2003/Vista/2008, please execute SafedInstall.bat

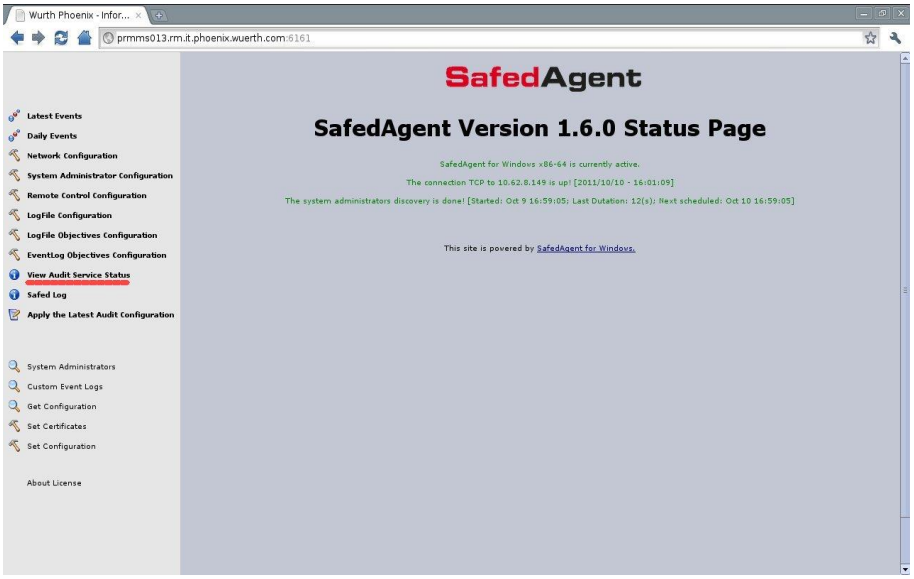


When the installation is terminated the Safed service will be started automatically an it could be controlled with the Windows Services Administrative Tool



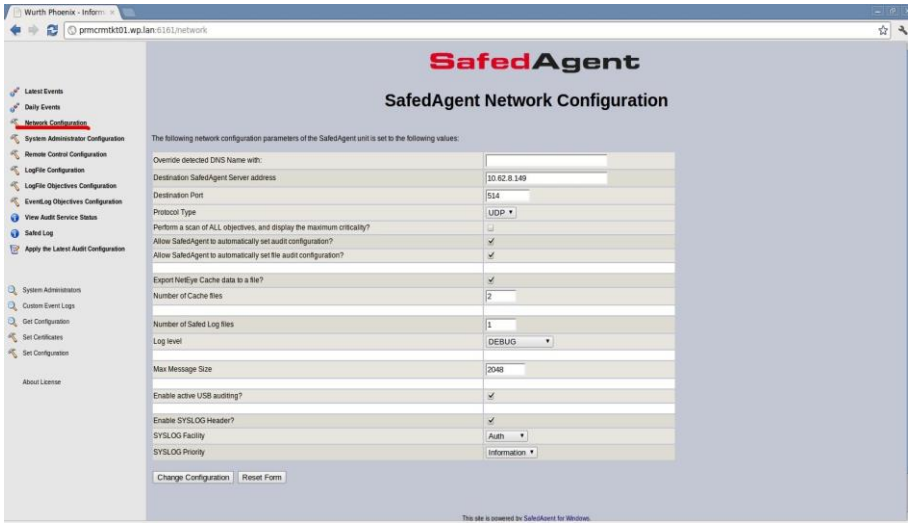
2 Configuration of Safed for Windows

Once the installation is terminated it is possible to connect to the web interface of the agent with your favorite browser at http://host_address:6161/
The version of the Safed agent and the status of the connection to the rsyslog server will be shown. Pay attention, the status of the connection is updated only when a message is sent to the server.
On the left side of the page the menu is displayed.



2.1 Network Configuration

In order to set the network connection it should be selected the 'Network Configuration' item.
Using the Network configuration page it is possible to set the rsyslog host, port (the default is 514) and the desired protocol (tcp or udp). Some interesting features could be enabled, namely the local cache and the numbers of days this cache is rotated.



Brief description of the main fields:

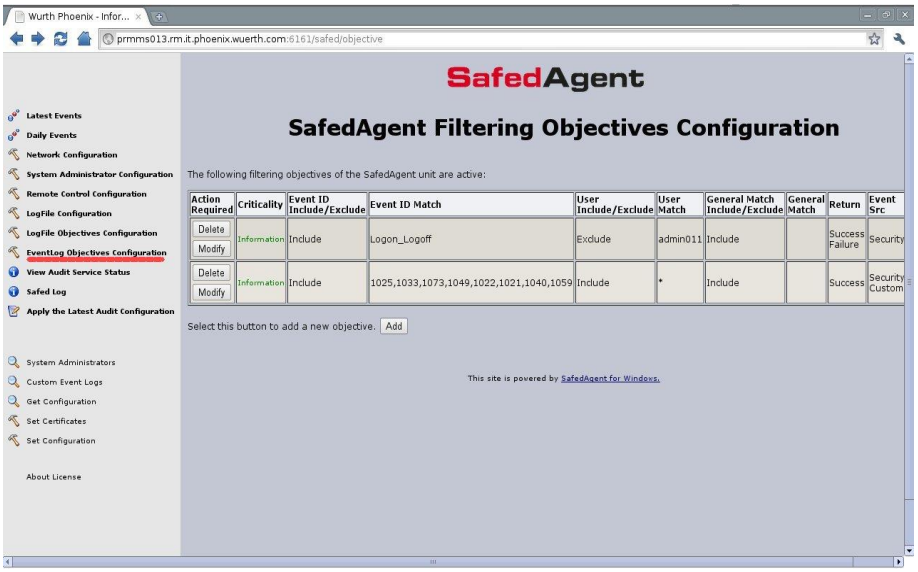
- *Destination NetEye Safed Server address*
  values: maximum of 100 characters
  description: IP address of the log server.
- *Destination Port*
  values: integer between 1 and 65535; default 514
  description: the log server port number.

- *Protocol Type*
  values: UDP, TCP or TLS
  description: determines the used protocol. When selecting UDP the log transmission is connectionless and there is no guarantee about log delivery, and therefore very fast. On the other hand selecting TCP the SAFED transmission is connection - based and the protocol guarantee the log delivery, features that slows down the transmission. Using TLS the communication between Safed and the syslog server is secure.
- *Allow NetEye Safed to automatically set audit configuration?*
  values: yes or not; default NO
  description: set automatically the audit configuration. It is requested to enable the Security Event Log monitoring. Put it to NO only if you have your own policy, otherwise put it always to YES
- *Allow NetEye Safed to automatically set file audit configuration?*
  values: yes or not; default YES
  description: set automatically the file audit configuration. It is requested to enable the monitoring of file and directory access through the Security Event Log. Put it always YES
- *Export NetEye Cache data to a file?*
  values: yes or not; default YES
  description: Safed will write a cache log file to the client system32 path.
- *Number of Cache files*
  values: integer; default 2
  description: Number of daily cache log files of sent events left on the client side .
- *Number of Safed Log files*
  values: integer; default 1
  description: Number of daily safed log files left on the client side .
- *Log level*
  values: NONE, ERROR, WARNING, INFORMATION, DEBUG
  description: log level of Safed. The higher log level is set the larger the log files result on the client side .
- *Max Message Size*
  values: integer; default 2048
  description: max size of the transmitted log message. Using UDP it is not possible to set more than 4K because of UDP stack limitations. The message will be truncated.
  N.B. For message size > 2048, the Configuration Directives $MaxMessageSize should be set with the appropriate value in the /etc/rsyslog.conf
- *Enable active USB auditing?*
  values: yes or not; default No
  description: determines whether a USB port monitoring should be enabled. For Windows Vista and later versions this is done receiving WMI event notifications concerning the target instance "Win32_PnPEntity". All events of classes "__InstanceCreationEvent", "__InstanceDeletionEvent" and "__InstanceModificationEvent"
- *Enable SYSLOG Header?*
  values: yes or not; default YES
  description: determines whether a SYSLOG header will be added to the event record. Put it always YES
- *SYSLOG Facility*
  values: set defined in rfc5424;
  description: determines the SYSLOG Facility.

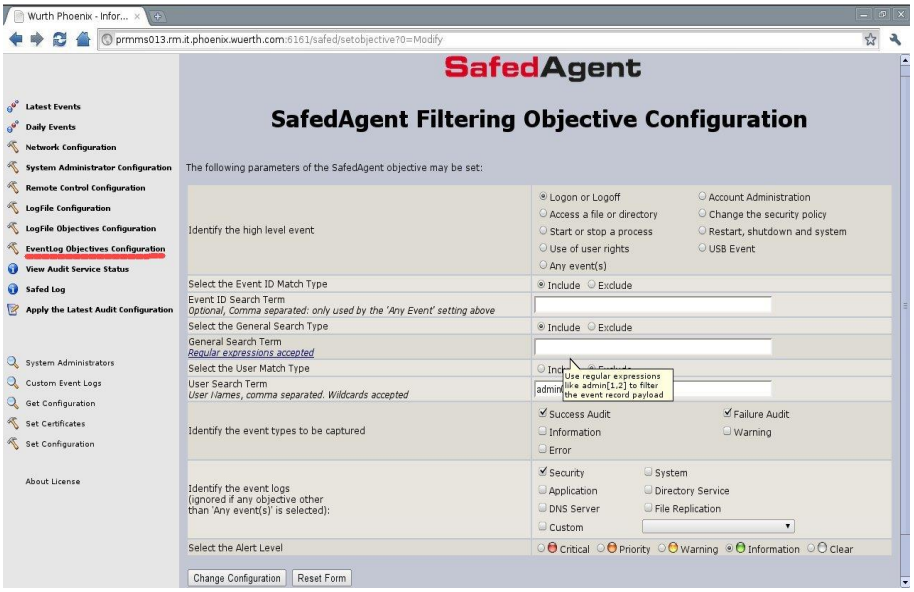
- SYSLOG Priority
  values: et defined in rfc5424;
  description: determines the SYSLOG severity.

2.2 Objective Configuration

In order to set the Event Log monitoring configuration it should be selected the 'EventLogObjective Configuration' item



Here it is possible to add a new windows group of events to be monitored through the add button.



In this page it is possible to select the group of Windows events that should be monitored or selecting 'Any events' it is possible to specify only events one is interested in. In the last case it is necessary to provide a list of comma separated event ids in the 'Event ID Search Term' field, and select the include or exclude radio button.
The second filter on the Windows events that could be selected is based on the User field of the event. The include/exclude radio button should be selected and the list of comma separated users should be inserted in the User Search Term field. Pay attention, in some cases the Windows Log Events don't fill that field and the string SYSTEM is put instead. In that cases it is possible to filter the payload part of the Windows Event Log selecting the include/exclude radio button and inserting the filtering regular expression in the General Search Term field. When SAD is used, in the later field it is possible to use the macro @SYSADMINS@ in order to create a filter with the piped string formed by the discovered system administrators.
In this page Event Type and Alert Level could be selected as well.
Brief description of the main fields:

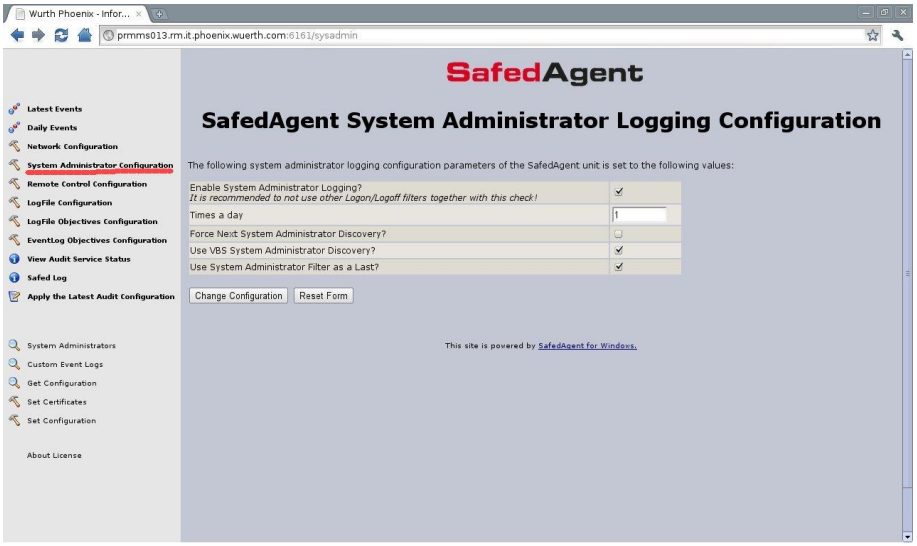
- *High level event*
  values: Logon_Logoff, File_Events, Process_Events, User_Right_Events, User_Group_Management_Events, Security_Policy_Events, Reboot_Events or Any_Event
  description: some high level groups of events to be captured are available. When customized list of events is required select Any_Event
- *Event ID Match Type*
  values: include or exclude ; default include
  description: only used by the 'Any Event' setting above.
- *Event ID Search Term*
  values: max of 256 characters
  description: Comma separated list of events to be captured (528,533 - A user is/is not logged on to a computer). Only used by the 'Any Event' setting above.
- *General Search Term*
  values: max of 512 characters
  description : an additional filter for captured events applied to the event payload. Regular expressions are accepted. For example admin(0|1).*|.?dministrator|pb00164|oms accepts admin023, admin123, administrator, Administrator, oms.
- *User Match Type*
  values: include or exclude ; default include
  description: Filter on UserId is included/excluded
- *User Search Term*
  values: max of 512 characters
  description: comma separated list of UserId . An event may be selected or discarded based on these UserIds, or partial match of an UserId (wildcards are accepted)
- *Event types to be captured*
  values: Success Audit, Failure Audit, Information, Warning and Error
  description: Windows allows for five different audit event types. Select the type or types of interest.
- *Event logs*
  values: Security, System, Application, Directory Service, File Replication, DNS Server and Custom
  description: On Windows Servers, all six event logs may be found, however on Workstation installations only three of these event logs (Security, System and Application) are available Custom could be used if 'Any event(s)' is selected. In the latest case the combo-box will be

filled with the customer event logs found in the registry.
Ignored if any objective other than 'Any event(s)' is selected.

- *Alert Level*
  values: Critical, Priority, Warning, Information and Clear
  description: Indicates the severity of the event.

2.3 System Administrator Configuration

It is possible to monitor the Logon/Logoff of Administrators (Local, Domain and Enterprise) using the 'System Administrator Configuration' item. Here it is possible to set all the necessary for the EventLog Objective, described in the section above, simply by checking a flag.

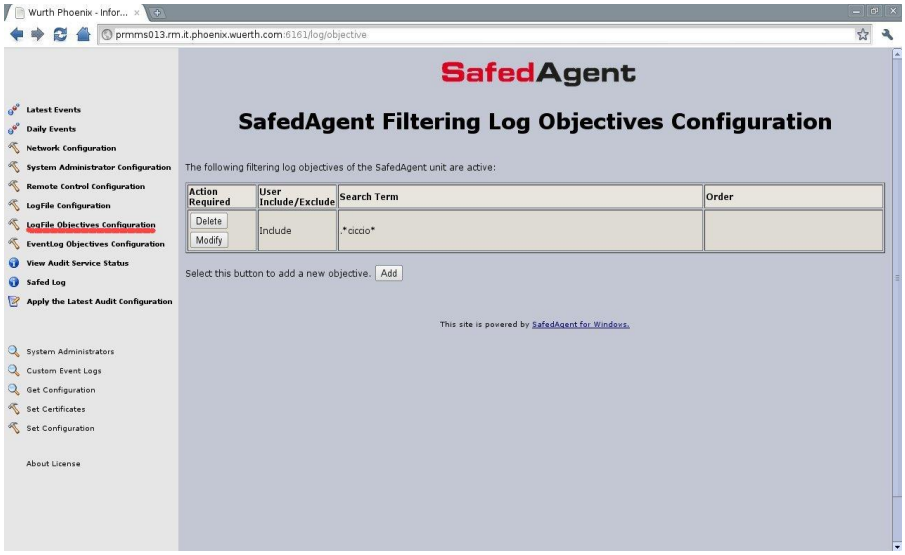


Brief description of the main fields:

- *Enable System Administrator Logging?*
  values: yes or not; default NOT
  description: Enable the System Administrator logging. Checking this flag a SA discovery script is executed and the list of SA is retrieved. Afterward the appropriate filter is created and the EventLog object for SA Logon/Logoff is set
- *Times a day*
  values: integer; default 1
  description: the frequency of the SA discovery script execution.
- *Force Next System Administrator Discovery?*
  values: yes or not; default NOT
  description: Force the execution of the SA discovery after the next 'Apply the Latest Audit Configuration'
- *Use VBS System Administrator Discovery?*
  values: yes or not; default NOT
  description: Select the VBScript or C++ executable for the SA Discovery
- *Use System Administrator Filter as a Last?*
  values: yes or not; default NOT
  description: Select if the SA Discovery Filter should be applied as first or last one.

2.4 Log Configuration

If the Safed agent is used to monitor files the 'Log Configuration' and the 'Log Objective Configuration' item of the left menu should be used.

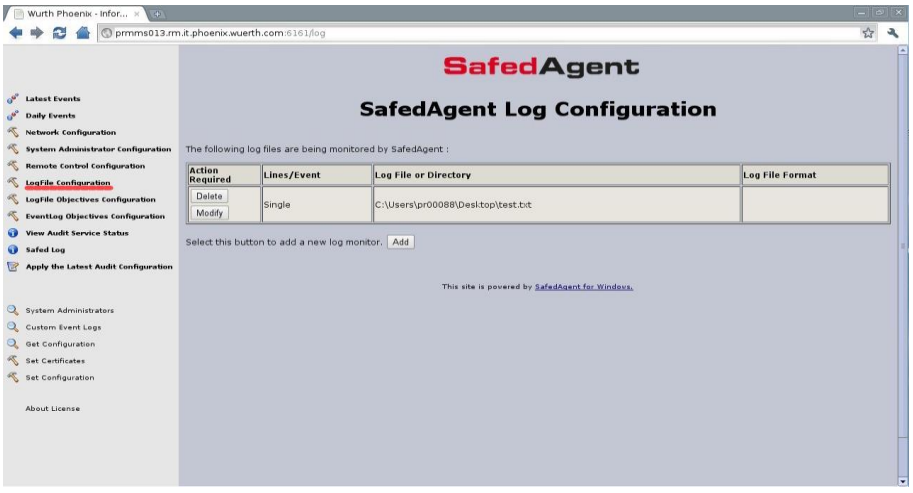


In the 'Log Objective Configuration' page it is possible to specify the search term for the filter. It should be a regular expression. Pressing the add button it is possible to add new filtering rules.
Brief description of the main fields:

- *General Search Term*
  values: max of 512 characters
  description : This is the filter expression. Regular expressions are accepted.

  For example **.*root.*** filters rows containing the root user from the monitored file
- *Select the Match Type*
  values: include or exclude ; default include
  description: filtered lines are included/excluded

In the 'Log Configuration' page it is possible to specify the file to be monitored. Here it is possible the include/exclude comment lines and to specify line separators. Pressing the add button it is possible to add new monitored files.



Brief description of the main fields:

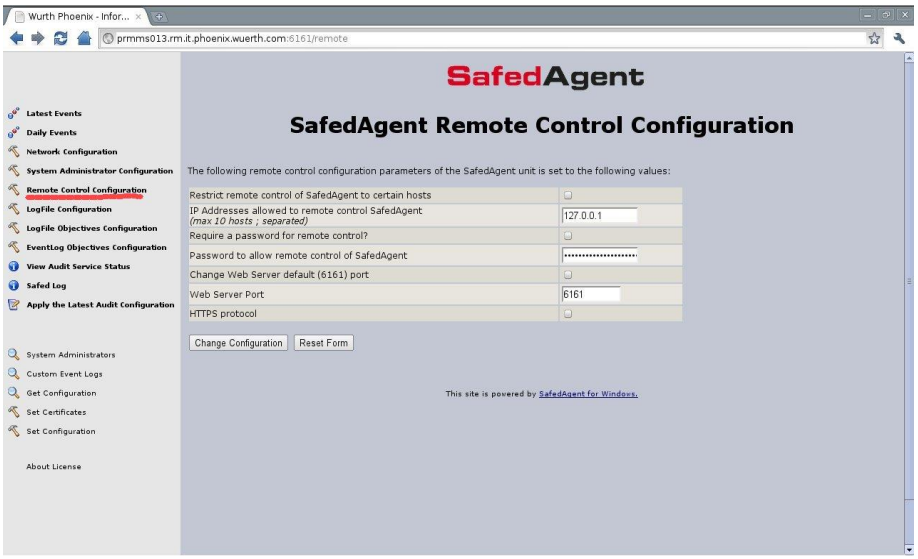
- Log Type
  values: an enumeration; default “Generic log file”
  description : It is optional and it is used to inform the server how to process the data stream.
- *Log Path*
  values: max 260 characters;
  description: The LogPath is the fully qualified path to the log file that needs to be monitored OR the fully qualified path to the directory containing date stamped log files of the form *YYMMDD* (in this case a trailing backslash ('\') is required). Spaces are valid, except at the start of the term.
- *Log Format*
  values: max 260 characters;
  description: A percent sign (%) is used the represent the date format YYMMDD. Wildcards are acceptable.
  e.g. log names like ISALOG_20060913_WEB_000.w3c would be represented as ISALOG_20%_WEB_*.w3c. If this field is not defined, the first matching entry will be used (this is fine in most cases).
- *Send Comment*

values yes or not; default NOT
description: Select whether to include ore exclude commented lines. By default, lines starting with '#' will be ignored;

- *Multi-Line Format*
  values: max 32 characters
  description: Describe the line separator. By default \n is considered. It is possible also to consider a fixed number of lines.

2.5 Remote Control Configuration

Through the “Remote Control Configuration” web page it is possible to configure some features of the integrated web server inside the Safed Agent.



Brief description of the main fields:

- *Restrict remote control of NetEye Safed agent to certain hosts*
  values: yes or not; default NOT
  description : It is possible to restrict the access to the web server to a list of ip addresses.
- *IP Addresses allowed to remote control NetEye Safed*
  values: max 256 characters;
  description: remote control actions may be limited to a list of hosts; this list is entered as a semicolon separated list of ip addresses, and the web server will accept only remote connections coming from these ip addresses
- *Require a password for remote control?*
  values: yes or not; default NOT
  description: a password may be set so that only authorized individuals may access the remote control functions
- *Password to allow remote control of NetEye Safed*

values: max 256 characters;
description: the password which will be encrypted using the MD5 hashing algorithm

- *Change Web Server default (6161) port*

values: yes or not; default NOT
description: signal whether the web port should be changed or not.

- *Web Server Port*

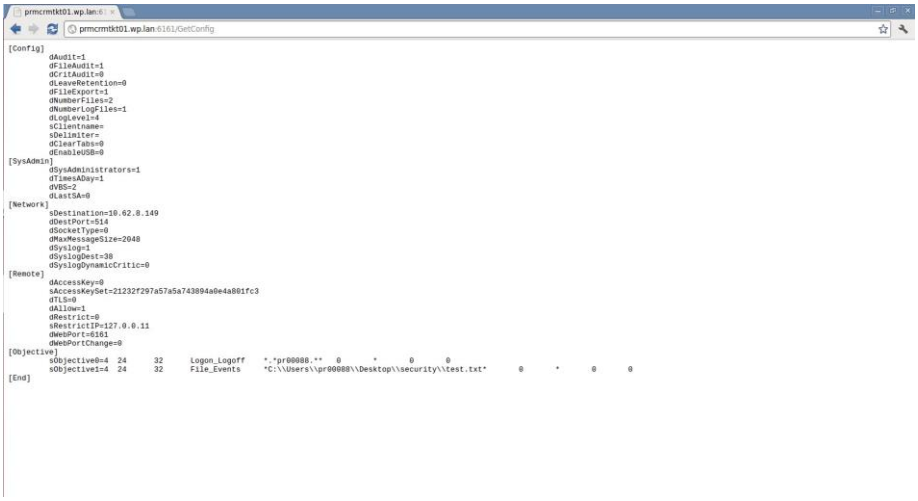
values: integer; default 6161
description: the port on which the embedded web server is listening for connections.

- *HTTPS Protocol*

values: yes or not; default NOT
description: enable the HTTPS protocol.

2.6 Get and Set Configuration

Using the 'Get Configuration' and 'Set Configuration' items of the left menu it is possible to receive/submit the entire configuration of the agent



[Config]
dAudit=1

```
        dFileAudit=1
        dCritAudit=0
        dLeaveRetention=0
        dFileExport=1
        dNumberFiles=2
        dNumberLogFiles=1
        dLogLevel=4
        sClientname=
        sDelimiter=
        dClearTabs=0
        dEnableUSB=0
[SysAdmin]
        dSysAdministrators=1
        dTimesADay=1
        dVBS=2
        dLastSA=0
[Network]
        sDestination=10.62.8.149
        dDestPort=514
        dSocketType=0
        dMaxMessageSize=2048
        dSyslog=1
        dSyslogDest=38
        dSyslogDynamicCritic=0
[Remote]
        dAccessKey=0
        sAccessKeySet=21232f297a57a5a743894a0e4a801fc3
        dTLS=0
        dAllow=1
        dRestrict=0
        sRestrictIP=127.0.0.11
        dWebPort=6161
        dWebPortChange=0
[Objective]
        sObjective0=4  24     32     Logon_Logoff    *.*pr00088.**   0      *      0      0
        sObjective1=4  24     32     File_Events     *C:\\Users\\pr00088\\Desktop\\security\\test.txt*       0      *      0      0
[End]
```

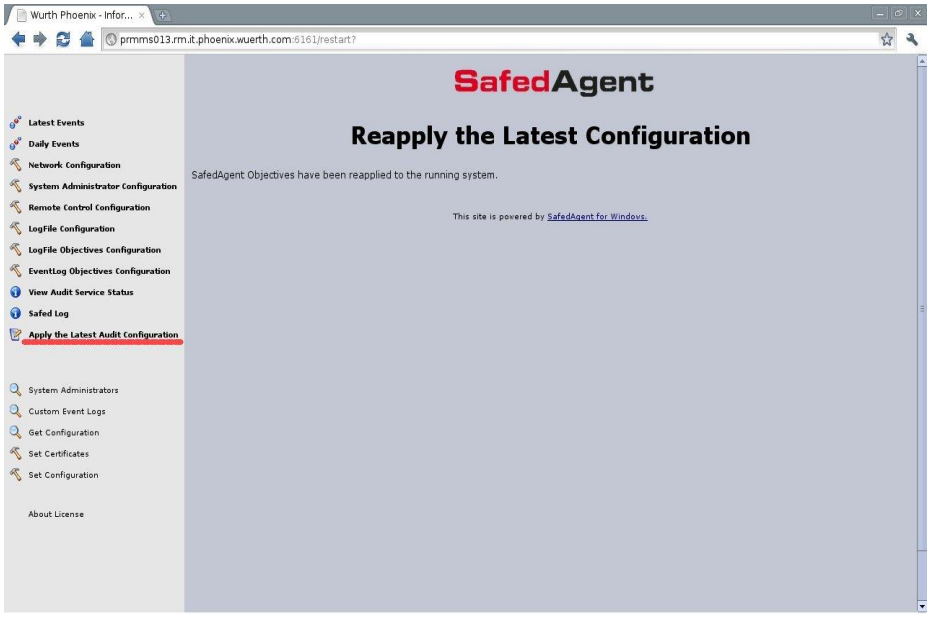
2.7 Custom Event Logs

Using the 'Custom Event Logs' items of the left menu it is possible to receive the piped list of the customer event logs found in "SYSTEM\\CurrentControlSet\\Services\\EventLog” of the windows registry.

2.8 Apply Configuration

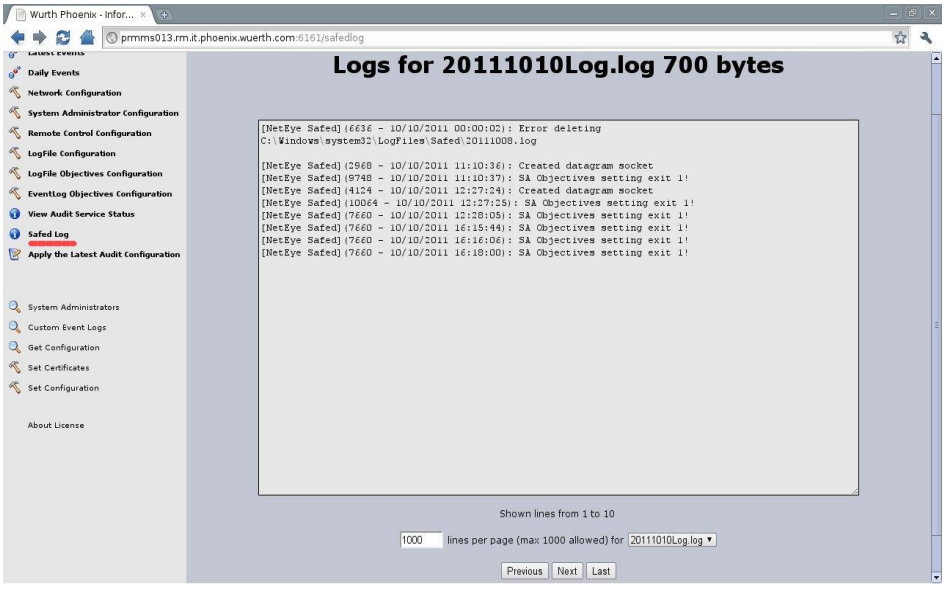
The configuration of the Safed agent, both uploaded via the set configuration function or set by the web server pages should be applied through the 'Apply the Latest Audit Configuration' menu item, in order

to make it effective.



2.9 Safed Log

The daily log of the Safed agent can be visualized using the web interface through the 'Safed Log' menu item. It is possible to select the number of line per page and the specific log to be visualized. The buttons 'Previous' Next' and 'Last' could be used in order to scroll up/down the selected log.



3 Installation of Safed for Linux/Unix

In order to install the Safed agent on Linux use the safed git repo

$ git clone https://github.com/WuerthPhoenix/safed.git

it will create a safed/safed-agent directory; cd to that directory and see all pre - requirements:
$cat README
wolfssl requires autoconf > 2.69 , automake > 1.13, git, gcc, libtool and build-essential (make)
$ ./bootstrap (if you do not need TLS skip this step. No wolfssl is required, skip the pre-requirements too.)
$ ./configure

this generates the Makefile corresponding to your platform and then run

$ make

in order to compile the Safed source code.
To install the agent, you should gain root privileges and the run the script:

./install.sh

which will install the binary, the start/stop script, a basic configuration file in the /etc/safed directory and then runs the agent.
To check if the agent is running, please execute the command **ps -ef|grep safed.**
In order to uninstall Safed use the script **uninstall.sh**

Starting with the version 1.6.0 it is possible to integrate the audit log monitoring for Linux and AIX with safed. Use the safed git repo
$ git clone https://github.com/WuerthPhoenix/safed.git

it will create a safed/safed-audit-ux directory; cd to that directory and run:

$ make

in order to compile the Safed-audit source code.
To install the agent, you should gain root privileges and the run the script:

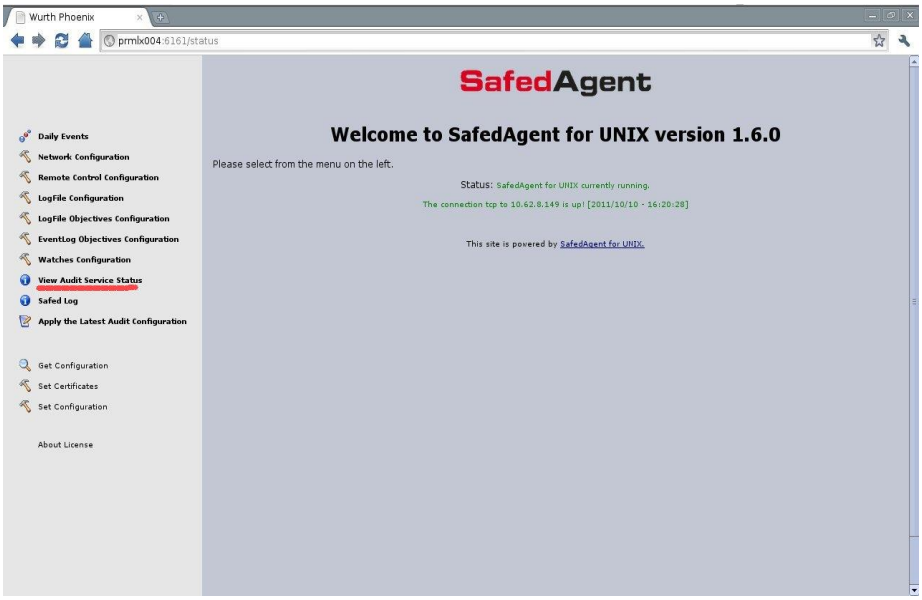
install.sh

which will install the binary, and create the communication pipe/tmp/safedpipe for safed
To check if the agent is running, please execute the command **ps -ef|grep -i safed.**
In order to uninstall Safed use the script **uninstall.sh**

NB. The safed-agent is required in order to use the audit monitoring.

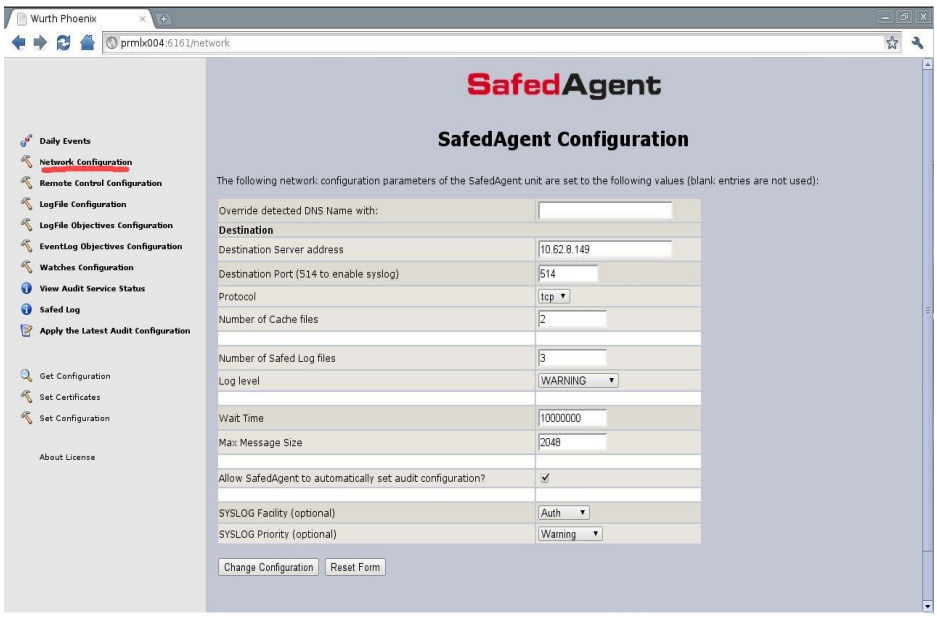
4 Configuration of Safed for Linux

Once the installation is terminated it is possible to connect to the web interface of the agent with your favorite browser at http://host_address:6161/
The version of the Safed agent and the status of the connection to the rsyslog server will be shown. Pay attention, the status of the connection is updated only when a message is sent to the server.
On the left side of the page the menu is displayed.



4.1 Network Configuration

In order to set the network connection it should be selected the 'Network Configuration' item
Using the Network configuration page it is possible to set the rsyslog host, port (the default is 514) and the desired protocol (tcp or udp). Some interesting features could be enabled, namely the local cache and the numbers of days this cache is rotated.

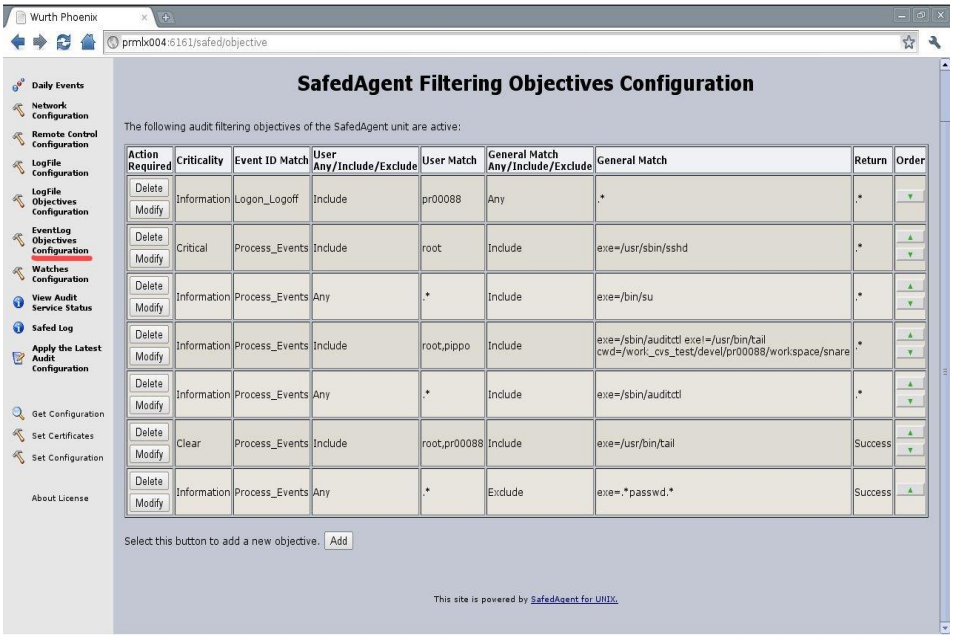


Brief description of the main fields:

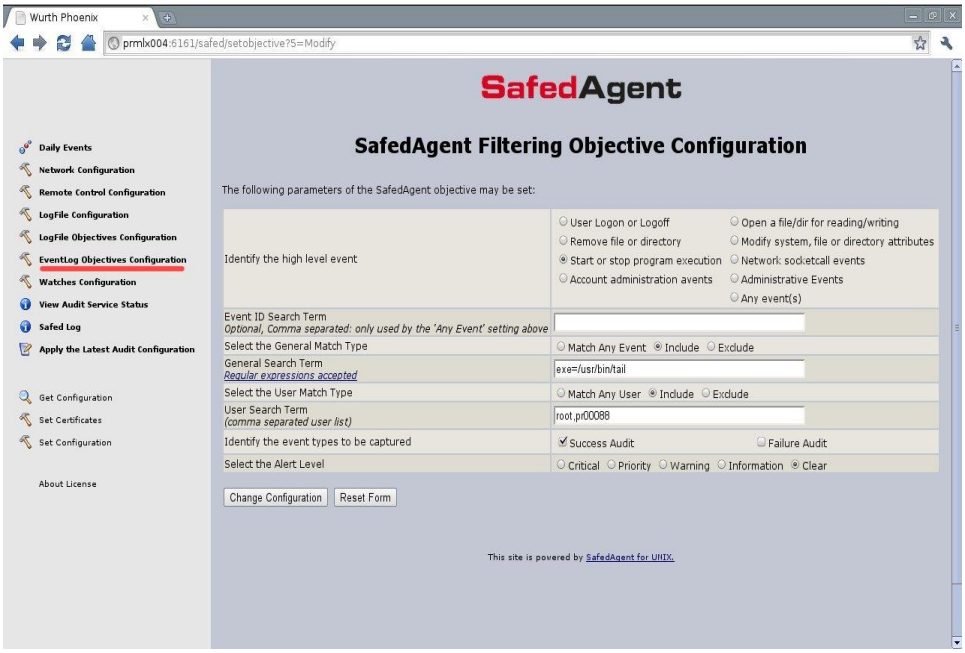
- *Destination Server address*
  values: maximum of 256 characters
  description: IP address of the log server.
- *Destination Port*
  values: integer between 1 and 65535; default 514
  description: the log server port number.
- *Protocol Type*
  values: UDP, TCP or TLS
  description: determines the used protocol. When selecting UDP the log transmission is connectionless and there is no guarantee about log delivery, and therefore very fast. On the other hand selecting TCP the SAFED transmission is connection - based and the protocol guarantee the log delivery, features that slows down the transmission. Using TLS the communication between Safed and the syslog server is secure.
- *Number of Cache files*
  values: integer; default 2
  description: number of daily cache files on client side.
- *Number of Safed Log files*
  values: integer; default 1
  description: number of daily log files left on client side.
- *Log level*
  values: NONE, ERROR, WARNING, INFORMATION, DEBUG
  description: log level of Safed. The higher log level is set the larger the log files result on the client side .
- *Wait Time*
  values: integer; it is the time interval, expressed in nanoseconds, between checks for changes of the log files; default 10.000.000 (100 checks in a second)
  description: The agent will check each"Wait Time" for new matching items.
- *Max Message Size*
  values: integer; default 256
  description: max size of the transmitted log message. Using UDP it is not possible to set more than 4K because of UDP stack limitations. The message will be truncated
  N.B. For message size > 2048, the Configuration Directives $MaxMessageSize should be set with the appropriate value in the /etc/rsyslog.conf
- *SYSLOG Facility*
  values: a set defined in rfc5424;
  description: determines the SYSLOG Facility.
- SYSLOG Priority
  values: a set defined in rfc5424;
  description: determines the SYSLOG severity.

4.2 Objective Configuration

In order to set the System Audit monitoring configuration it should be selected the 'EventLogObjective Configuration' item



In this page it is possible to select the group of Audit events that should be monitored or selecting 'Any events' it is possible to specify only events one is interested in. In the last case it is necessary to provide a list of comma separated Audit event ids in the 'Event ID Search Term' field, and select the include or exclude radio button.



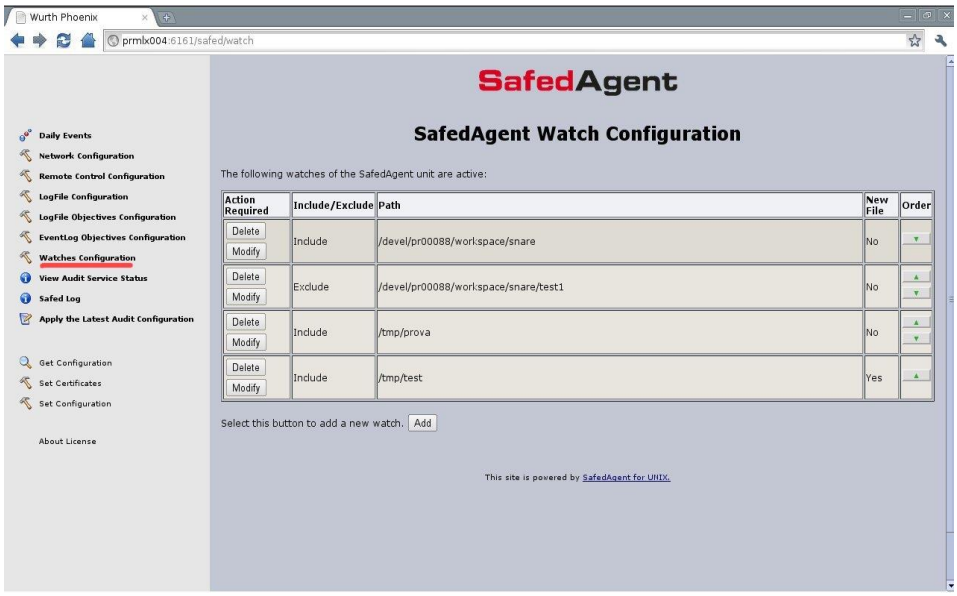
The second filter on the Audit events that could be selected is based on the User field of the event. The include/exclude radio button should be selected and the list of comma separated users should be inserted in the User Search Term field.

In this page Event Type and Alert Level could be selected as well.
Brief description of the main fields:

- *High level event*
  values: User Logon or Logoff, Open a file/dir for reading/writing, Remove file or directory, Modify system, file or directory attributes, Start or stop program execution, Network socketcall events, Account administration avents, Administrative Events or Any_Event
  description: some high level groups of events to be captured are available. When customized list of events is required select Any_Event
- *Event ID Search Term*
  values: max of 256 characters
  description: Comma separated list of events to be captured (528,533 - A user is/is not logged on to a computer). Only used by the 'Any Event' setting above.
- *General Search Term*
  values: max of 512 characters
  description : an additional filter for captured events applied to the event payload. Regular expressions are accepted. For example exe=/usr/bin/tail accepts accepts events regarding the execution of the tail command.
- *User Match Type*
  values: include or exclude ; default include
  description: Filter on UserId is included/excluded
- *User Search Term*
  values: max of 512 characters
  description: comma separated list of UserId . An event may be selected or discarded based on these UserIds
- *Event types to be captured*
  values: Success Audit, Failure Audit
  description: Filter based on the result of the executed command
- *Alert Level*
  values: Critical, Priority, Warning, Information and Clear
  description: Indicates the severity of the event.

4.3 Watches Configuration

Only for Linux it is possible to set watches in order to monitor the manipulation of determinate file/directory (avoiding the overload of the system due to a huge number of audit events generated for file/directory manipulation in general). In order to set the Watches Audit monitoring it should be selected the 'Watches Configuration' item on the left side list.

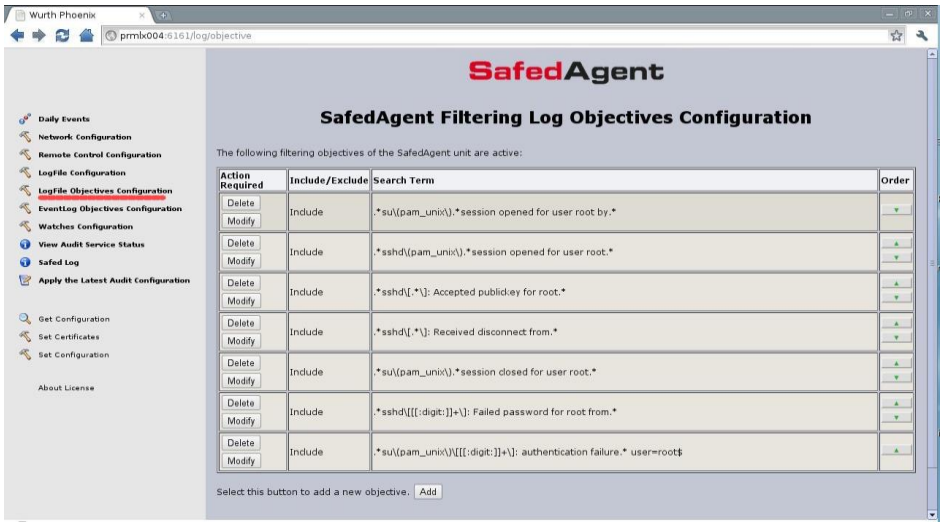


Brief description of the main fields:

- *Select the General Match Type*
  values: include or exclude ; default include
  description: Watch on file is included/excluded
- *Path*
  values: max 512 characters;
  description: The file/directory to be watched.
- *New File*
  values: yes or not; default NOT;
  description: Whether new files in the selected directory should be watched. It is recommended to set it '**not'** due to overload risk

4.4 Log Configuration

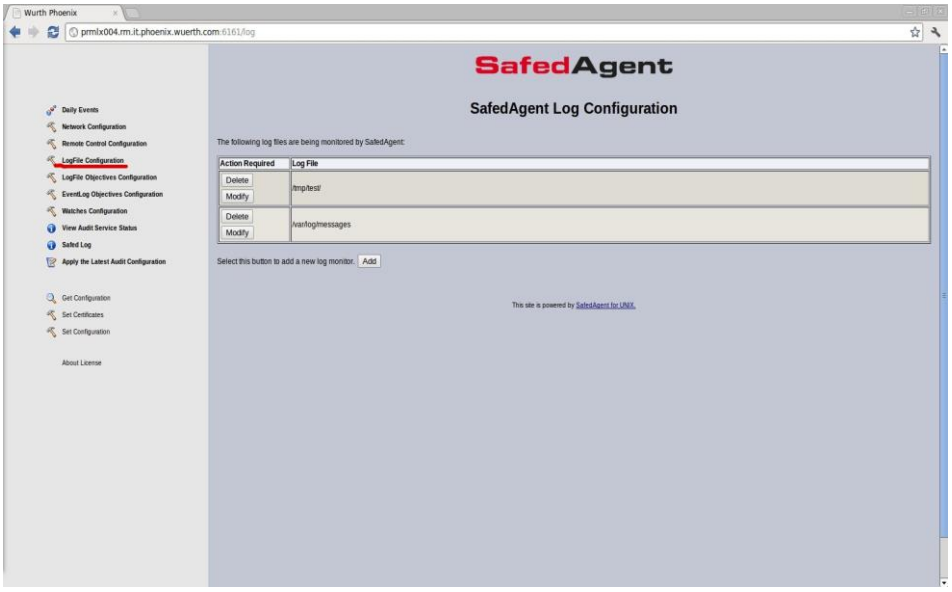
The Safed agent is used to monitor log files and it is possible through the 'LogFile Objectives Configuration' page to specify the search term for the filter. It should be a regular expression.



Here it is possible to add new filtering rules pressing the add button.
Brief description of the main fields:

- *Search Term*
  values: max of 8192 characters
  description : This is the filter expression. Regular expressions are accepted.
  For example **.*root.*** filters rows containing the root user from the monitored file
- *Select the General Match Type*
  values: include , exclude or 'Match Any String'; default ' Match Any String'
  description: Filtered lines are included/excluded. If ' Match Any String' is selected the matching rule is **.***

In the 'LogFile Configuration' page it is possible to specify the file to be monitored. Pressing the add button it is possible to add new monitored files.



Brief description of the main fields:

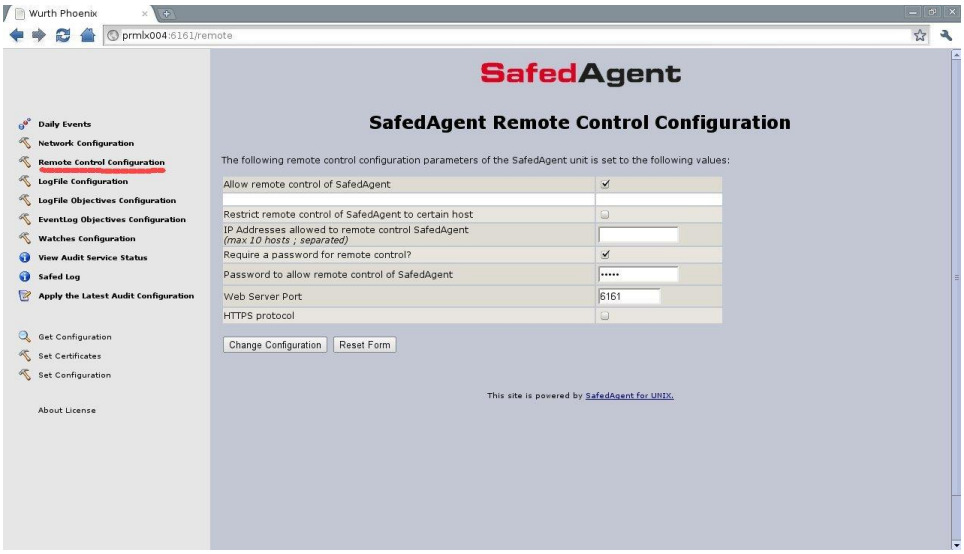
- *Log Type*
  values: an enumeration; default “Generic log file”

description : it is optional and it is used to inform the server how to process the data stream.

- *Log File*
  values: max 1024 characters;
  description: The Log File is the fully qualified path to the log file that needs to be monitored, or a to the directory where a Log Name Format will be applied and the last found file will be monitored. Spaces are valid, except at the start of the term.
- *Log Name Format*
  values: max 260 characters;
  description: A percent sign (%) is used the represent the date format YYMMDD. Regulare expressions are acceptable.
  e.g. log names like ISALOG_20060913_WEB_000.w3c would be represented as ISALOG_20%_WEB_*.w3c. If this field is not defined, the first matching entry will be used (this is fine in most cases).

4.5 Remote Control Configuration

Through the 'Remote Control Configuration' web page it is possible to configure some features of the integrated web server inside the Safed Agent.



Brief description of the main fields:

- *Restrict remote control of NetEye Safed agent to certain hosts*
  values: yes or not; default NOT
  description : It is possible to restrict the access to the web server to a list of ip addresses.
- *IP Addresses allowed to remote control NetEye Safed*
  values: max 256 characters;
  description: remote control actions may be limited to a list of hosts; this list is entered as a semicolon separated list of ip addresses, and the web server will accept only remote connections coming from these ip addresses
- *Require a password for remote control?*

values: yes or not; default NOT
description: A password may be set so that only authorized individuals may access the remote control functions

- *Password to allow remote control of NetEye Safed*

values: max 256 characters;

description: The password which will be encrypted using the MD5 hashing algorithm

- *Web Server Port*

values: integer; default 6161

description: The port of the embedded web server.

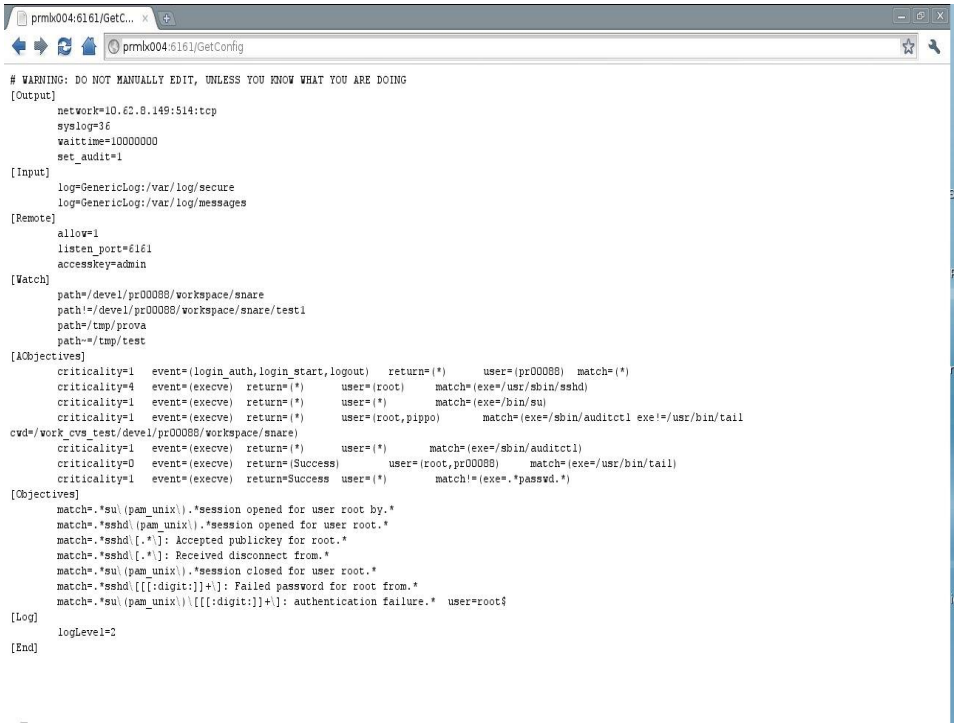
- *HTTPS Protocol*

values: yes or not; default not

description: Enable the HTTPS protocol.

4.6 Get and Set Configuration

Using the 'Get Configuration' and 'Set Configuration' items of the left menu it is possible to receive/submit the entire configuration of the agent

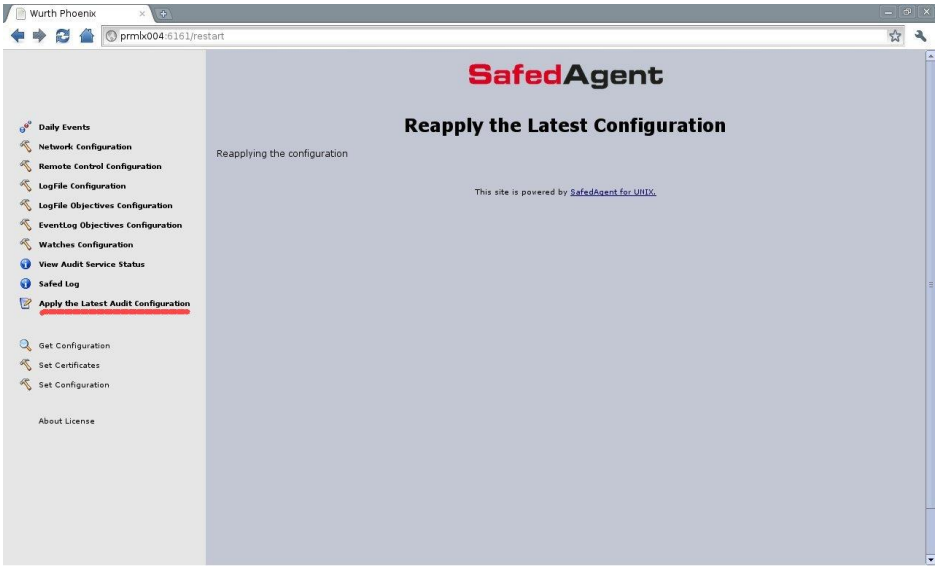



```
# WARNING: DO NOT MANUALLY EDIT, UNLESS YOU KNOW WHAT YOU ARE DOING
[Output]
	network=10.62.8.149:514:tcp
	syslog=36
	waittime=10000000
	set_audit=1
[Input]
	log=GenericLog:/var/log/secure
	log=GenericLog:/var/log/messages
[Remote]
	allow=1
	listen_port=6161
	accesskey=admin
[Watch]
	path=/devel/pr00088/workspace/snare
	path!=/devel/pr00088/workspace/snare/test1
	path=/tmp/prova
```

```
	path~=/tmp/test
[AObjectives]
	criticality=1	event=(login_auth,login_start,logout)	return=(*)	user=(pr00088)	match=(*)
	criticality=4	event=(execve)	return=(*)	user=(root)	match=(exe=/usr/sbin/sshd)
	criticality=1	event=(execve)	return=(*)	user=(*)	match=(exe=/bin/su)
	criticality=1	event=(execve)	return=(*)	user=(root,pippo)	match=(exe=/sbin/auditctl exe!=/usr/bin/tail
cwd=/work_cvs_test/devel/pr00088/workspace/snare)
	criticality=1	event=(execve)	return=(*)	user=(*)	match=(exe=/sbin/auditctl)
	criticality=0	event=(execve)	return=(Success)	user=(root,pr00088)	match=(exe=/usr/bin/tail)
	criticality=1	event=(execve)	return=Success	user=(*)	match!=(exe=.*passwd.*)
[Objectives]
	match=.*su\(pam_unix\).*session opened for user root by.*
	match=.*sshd\(pam_unix\).*session opened for user root.*
	match=.*sshd\[.*\]: Accepted publickey for root.*
	match=.*sshd\[.*\]: Received disconnect from.*
	match=.*su\(pam_unix\).*session closed for user root.*
	match=.*sshd\[[[:digit:]]+\]: Failed password for root from.*
	match=.*su\(pam_unix\)\[[[:digit:]]+\]: authentication failure.*	user=root$
[Log]
	logLevel=2
[End]
```

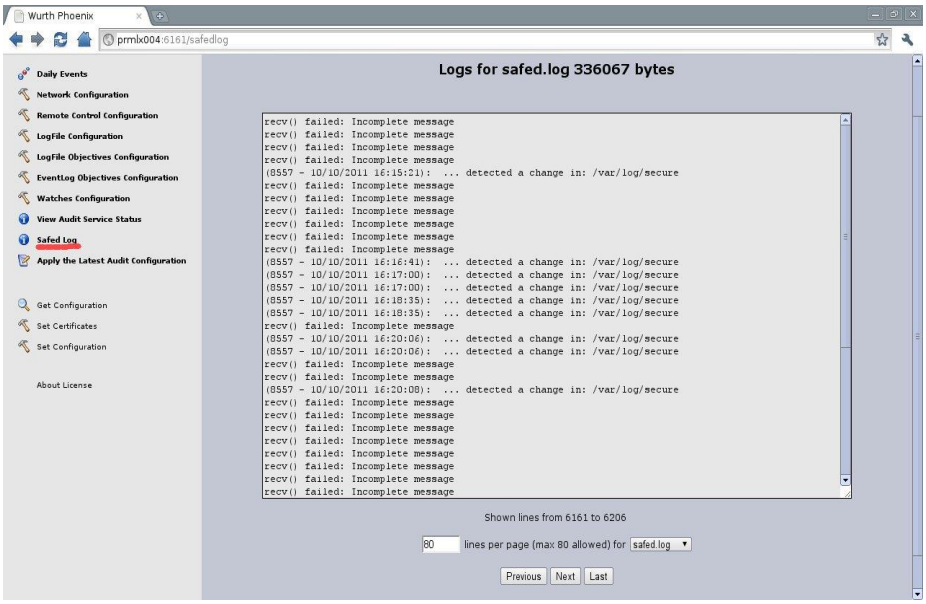
4.7 Apply Configuration

The configuration of the Safed agent, both uploaded via the set configuration function or set by the web server pages should be applied through the 'Apply the Latest Audit Configuration' menu item, in order to make it effective.



4.8 Safed Log

The daily log of the Safed agent can be visualized using the web interface through the 'Safed Log' menu item. It is possible to select the number of line per page and the specific log to be visualized. The buttons 'Previous' Next' and 'Last' could be used in order to scroll up/down the selected log.



5. Generation of certificates for TLS communication between Safed and Syslog server AND for HTTPS enabled Safed web server

Safed uses X.509 certificates for its TLS communication. In the following it is described briefly the generation of those certificates and the Safed configuration. Safed supports TLS 1.2 and TLS 1.3 protocols based on wolfssl >= 3.15.7 library (https://github.com/wolfSSL/wolfssl/)

5.1 X.509 certificates generation

Safed uses Wolfssl (https://github.com/wolfSSL/wolfssl/) for the secure communication though TLS for both 1.between Safed and the syslog server and 2. HTTPS access of to the embedded Safed web server. On each host where Safed is installed it is necessary to have:

- *The Private Key (key.pem)*
- *The relative X.509 certificate (cert.pem)*
- *The certificate of the Certification Authority who released the the above mentioned certificate. It can also be a self-signed certificate.(ca.pem)*

These thee files key.pem, cert.pem and ca.pem have to be copied for each Safed host in :

- ***C:\Program Files\Safed*** *for Windows installations*
- ***/etc/safed/*** *for Ux installations*

GnuTLS supplies the **certtool** tool for the generation of certificates, including the self – signed one.

5.1.1 Self-signed certificates

When a self-signed certificate is used the following steps have to be done on the host used for certificates release:

- **certtool --generate-privkey --outfile ca-key.pem --bits 2048**
- **certtool --generate-self-signed --load-privkey ca-key.pem --outfile ca.pem**

You will be prompted to enter the following data:
Generating a self signed certificate...

Please enter the details of the certificate's distinguished name. Just press enter to ignore a field.

Country name (2 chars): IT
Organization name: SomeOrg

Organizational unit name: SomeOU

Locality name: Somewhere

State or province name: RM

Common name: someName (not necessarily DNS!)

UID:

This field should not be used in new certificates.

E-mail:

Enter the certificate's serial number (decimal):

Activation/Expiration time.

The certificate will expire in (days): 3650

Extensions.

Does the certificate belong to an authority? (Y/N): y

Path length constraint (decimal, -1 for no constraint):

Is this a TLS web client certificate? (Y/N):

Is this also a TLS web server certificate? (Y/N):

Enter the e-mail of the subject of the certificate: someone@example.net

Will the certificate be used to sign other certificates? (Y/N): y

Will the certificate be used to sign CRLs? (Y/N):

Will the certificate be used to sign code? (Y/N):

Will the certificate be used to sign OCSP requests? (Y/N):

Will the certificate be used for time stamping? (Y/N):

Enter the URI of the CRL distribution point:

Is the above information ok? (Y/N): y

- **chmod 400 ca-key.pem**

As mentioned before, ca.pem is the X.509 certificate to be used for further certificate generation for the Safed hosts and ca-key.pem is the private key of who releases certificates – to be put in a secure

place!!!

5.1.2 Generation of Peer Certificates

In order to generate the private key and certificate for each Safed host the following steps have to be done:

- **certtool --generate-privkey --outfile key.pem --bits 2048**
- **certtool --generate-request --load-privkey key.pem --outfile request.pem**

You will be prompted to enter the following data:
Generating a PKCS #10 certificate request...
Country name (2 chars): IT
Organization name: SomeOrg

Organizational unit name: SomeOU

Locality name: Somewhere

State or province name: RM
Common name: machine.example.net *(This is the name of the host that will use the certificate)*
UID:
Enter a dnsName of the subject of the certificate:
Enter the IP address of the subject of the certificate:
Enter the e-mail of the subject of the certificate:
Enter a challange password:
Does the certificate belong to an authority? (y/N): n
Will the certificate be used for signing (DHE and RSA-EXPORT ciphersuites)? (y/N):
Will the certificate be used for encryption (RSA ciphersuites)? (y/N):
Is this a TLS web client certificate? (y/N): y
Is this also a TLS web server certificate? (y/N): y

- **certtool --generate-certificate --load-request request.pem --outfile cert.pem --load-ca-certificate ca.pem --load-ca-privkey ca-key.pem**

You will be prompted to enter the following data:

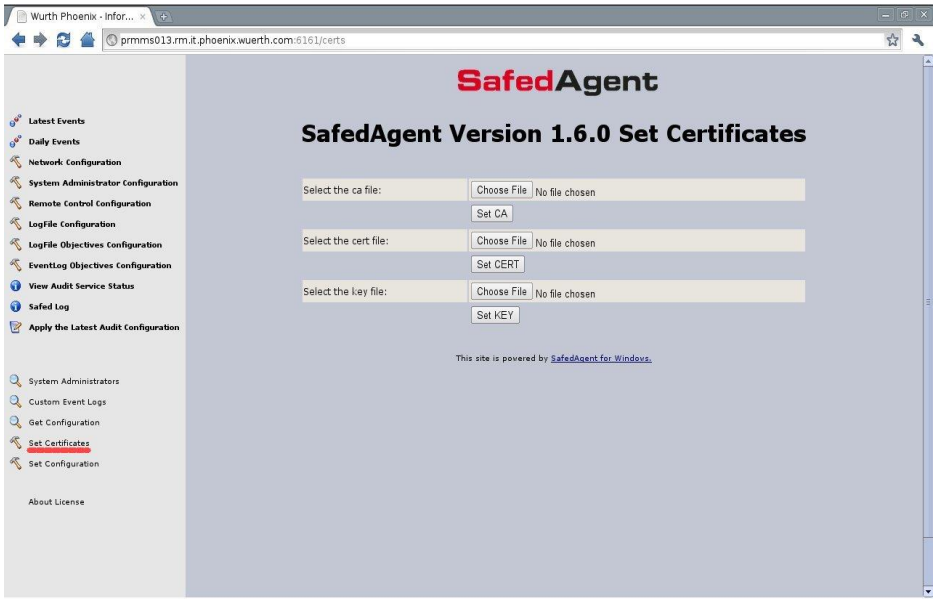
Generating a signed certificate...
Enter the certificate's serial number (decimal):
Activation/Expiration time.
The certificate will expire in (days): 1000
Extensions.
Do you want to honour the extensions from the request? (y/N):
Does the certificate belong to an authority? (Y/N): n
Is this a TLS web client certificate? (Y/N): y
Is this also a TLS web server certificate? (Y/N): y
Enter the dnsName of the subject of the certificate: machine.example.net *(This is the name of the host that will use the certificate)*
Enter the IP address of the subject of certificate:
Will the certificate be used for signing (DHE and RSA-EXPORT ciphersuites)? (Y/N):
Will the certificate be used for encryption (RSA ciphersuites)? (Y/N):
Is the above information ok? (Y/N): y

- **rm -f request.pem**

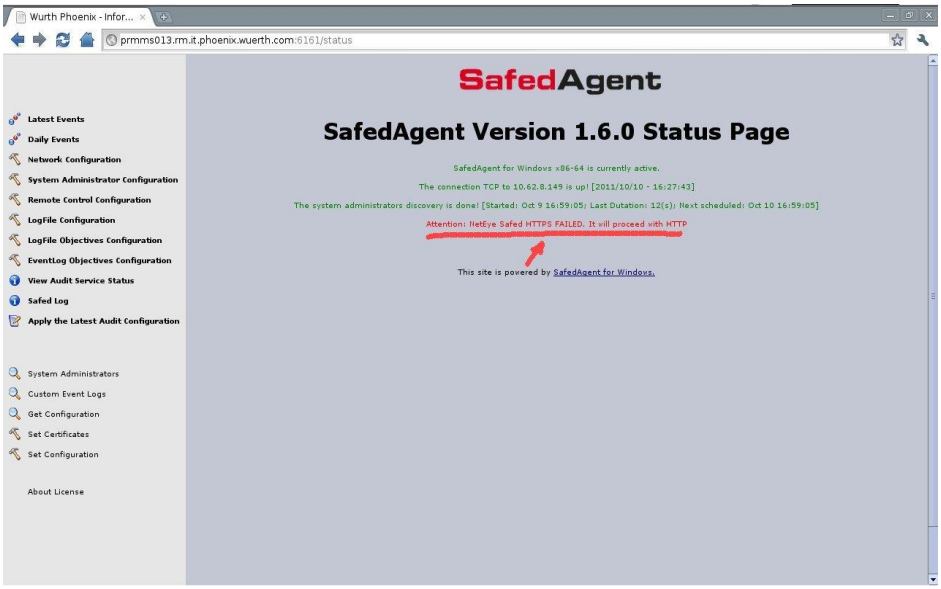
As mentioned before, key.pem is the private key and cert.pem is the X.509 certificate of the Safed host.

5.2 Uploading certificates to Safed

Through the 'Set Certificates' web page it is possible to upload the certificates to Safed.



Using the Browse buttons it is possible to select the ca.pem, key.pem and cert.pem files containing the certificate of the certification authority, the private key of the agent and it's certificate.
Using 'Set CA' button the ca.pem will be uploaded to Safed. An http posts will be done (http://host_address:6161/setca)
Using 'Set CERT' button the cert.pem will be uploaded to Safed. An http posts will be done (http://host_address:6161/setcert)
Using 'Set KEY' button the key.pem will be uploaded to Safed. An http posts will be done (http://host_address:6161/setkey)
Once the certificates have been uploaded it is possible to set the TLS communication for Safed (the communication between Safed and Syslog server or the HTTPS for the enbedded web server or both) .
The configuration of the Safed agent should be applied through the 'Apply the Latest Audit Configuration' menu item, in order to make it effective.
Pay attention, if some error occurs during the certificate loading on Safed side, in case of HTTPS communication an error message will be displayed and a switch to HTTP will be done.

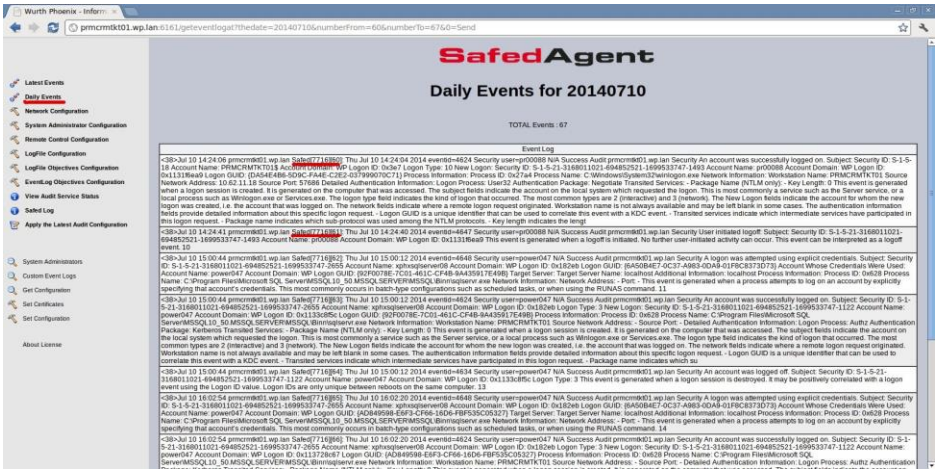


6. Local cache and sent log messages enumeration

The Safed agent is aimed at filtering local machine logs applying configured filters and then transmitting them to a centralized syslog server. Log transmission can be done by both using UDP or TCP protocol with the advantage of latest one to have the acknowledgment and therefore the "certainty" of the transmitted packages. In order to enforce the certainty of the transmitted logs at application level Safed enumerates in a progressive way each transmitted log message. This way it is clear what was sent from the Safed agent and what was received on the syslog server. Moreover Safed has its own local persistent cache where filtered logs are stored. The combination of log message enumeration and local cache make it possible in case of transmission failure to have an automatic retransmission once it becomes possible to do it again (ex. recovery from network failure reported by TCP).
Another possible scenario is the retransmission "on demand" of the missing log messages on the server side. As mentioned before all log messages are enumerated, so it is possible on the syslog server side to identify missing logs and to request Safed to resend them if still hold in the cache. The number of days that the local cache preserves log messages is configurable.
In the following some log message examples are reported. It is highlighted in red the message enumeration set by Safed.

<38>Jul 10 14:24:06 prmcrmtkt01.wp.lan Safed[7716][60]: Thu Jul 10 14:24:04 2014 eventid=4624 Security user=pr00088 N/A Success Audit prmcrmtkt01.wp.lan Security An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: PRMCRMTKT01$ Account Domain: WP Logon ID: 0x3e7 Logon Type: 10 New Logon: Security ID: S-1-5-21-3168011021-694852521-1699533747-1493 Account Name: pr00088 Account Domain: WP Logon ID: 0x1131f6ea9 Logon GUID: {DA54E4B6-5D9C-FA4E-C2E2-037999070C71} Process Information: Process ID: 0x27a4 Process Name: C:\Windows\System32\winlogon.exe …....

<38>Jul 10 14:24:41 prmcrmtkt01.wp.lan Safed[7716][61]: Thu Jul 10 14:24:40 2014 eventid=4647 Security user=pr00088 N/A Success Audit prmcrmtkt01.wp.lan Security User initiated logoff: Subject: Security ID: S-1-5-21-3168011021-694852521-1699533747-1493 Account Name: pr00088 Account Domain: WP Logon ID: 0x1131f6ea9 This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event. 10


Wurth Phoenix - Inform
prmcrmtkt01.wp.lan:6161/geteventlogat?thedate=20140710&numberFrom=60&numberTo=67&0=Send
SafedAgent
Daily Events for 20140710
Latest Events
Daily Events
Network Configuration
System Administrator Configuration
Remote Control Configuration
LogFile Configuration
LogFile Objectives Configuration
EventLog Objectives Configuration
View Audit Service Status
Safed Log
Apply the Latest Audit Configuration
System Administrators
Custom Event Logs
Get Configuration
Set Certificates
Set Configuration
About License
TOTAL Events : 67
Event Log