



# **Notification options in SMC 2.6**

Support April 2011



www.avira.de

Technical modifications and errors reserved © Avira GmbH 2011

# Notification options in SMC 2.6

### The following notification options are available in SMC 2.6:

- 1. SMC server informs by email on the basis of product events
- 2. The managed product itself sents emails
- 3. Send product status by email
- 4. Internet Update Manager notification emails

#### 1. SMC server informs by email on the basis of product events

This function is there to ensure that the service of the Security Management Center Server itself informs the administrator about critical events or alerts via email.

This can be set in the SMC Frontend under "Configurations".

The SMTP server, sender address and the login credentials for the SMTP server can be entered under "General Settings".

Email notification	
SMTP Server Sender email address I Use login data SMTP Login SMTP Password Description Enter the user for the SM	10.50.21.34         SMC2_6@testexchange.net         Testexchange\Administrator         •••••         #TP server login here
	Use login data SMTP Login SMTP Password

"Event  $\rightarrow$  Settings" may now be configured to define when an email should be sent to the administrator.

	a Event Settings
General Settings Server Settings Communication	Email notification         Email address       Administrator@testexchange.net         Image: Send after count of 1 ministration warning event(s)         Image: Send after count of 1 ministration warning event(s)         Image: Send after count of 1 ministration warning event(s)         Image: Send after count of 1 ministration warning event(s)         Image: Send after count of 1 ministration warning event(s)         Image: Send after count of 1 ministration warning event(s)         Image: Send after count of 1 ministration warning event(s)         Image: Send after count of 1 ministration warning event(s)         Image: Send after count of 1 ministration warning event(s)         Image: Send after count of 1 ministration warning event(s)         Image: Send after count of 1 ministration warning event(s)         Image: Send after count of 1 ministration warning event(s)         Image: Send after count of 1 ministration warning event(s)         Image: Send after count of 1 ministration warning event(s)         Image: Send after count of 1 ministration warning event(s)         Image: Send after count of 1 ministration warning event(s)         Image: Send after count of 1 ministration warning event(s)         Image: Send after count of 1 ministration warning event(s)         Image: Send after count of 1 ministration warning event(s)         Image: Send after count of 1 ministration warning event(s)         Image: S
	Description

Also, there is the possibility to remove old events automatically from the database that are older than x days.

A warning event would be e.g. if a file could not be scanned, or an update has failed of a managed product.

A critical event would be when a virus has been found.

Here are a few sample emails how the SMC informs in case of such events:

Name	Level	Product	Actor	Message
l vmxpsp2en	Warning	Avira AntiVir Professional 10 (Windows), EN	Guard	Service has been deactivated.
\Lambda vmxpsp2en	Critical	Avira AntiVir Professional 10 (Windows), EN	Guard	Malware 'Eicar-Test-Signature' [virus] was found in file 'C

# Warning Event:

n: Avira Security Management Center [SMC2_6@testexchange.net] Administrator	Sent: Mi 20.04.2011 08
ect: SMC ALERT on VMXPSP2EN (10.50.21.204)[AntiVir checked]	
ost Name: VMXPSP2EN (10.50.21.204)	
odul Name: Guard	
vent Level: Warning	
ssue Time: Wed Apr 20 08:33:45 2011	
essage: Service has been deactivated.	

## Critical Event:

From: Avira Security Management Center [SMC2_6@testexchange.net] To: Administrator Cc:	Sent: Mi 20.04.2011 08:29
Subject: SMC ALERT on VMXPSP2EN (10.50.21.204)[AntiVir checked]	
Host Name: VMXPSP2EN (10.50.21.204) Modul Name: Guard Event Level: Critical Issue Time: Wed Apr 20 08:28:39 2011 Message: Malware 'Eicar-Test-Signature' [virus] was found in file 'C:\Documents and	
Settings\Administrator\Desktop\eicar.com'. Action taken: Allow access.	
	8

#### 2. The managed product itself sents emails

Additionally it can also be configured if it is desired that each managed product sends out an email or when a critical event or warning occurred.

However, it is recommended that only one option is configured, as otherwise the overview may get lost.

AV10 Professional:

Right-click on the product to be managed and then select *Configuration -> Configure* 

In this dialogue there is the possibility to get information via email from the module (Guard, scanner, updater).

1. Step:

The SMTP server information must be provided. In case authentication is needed, it should be mentioned as well.

C 🖸 🖸 🕼 — — — — — — — — — — — — — — — — — —	General > Alerts > Email ? He
Expert mode  Standard configuration  Scanner  Scanner Scanner  Scanner  Scanner  Scanner  Scanner  Scanner  Sca	Email messages         SMTP Server:       10.50.21.34         Segder address:       AVProf@testexchange.net         Authentication       Image: Testexchange\Administrator         Login name:       Testexchange\Administrator         Password:       *****         Send test email         Description         When you click on the button, Avira AntiVir Professional attempts to send a test email to the sender address to check the data entered.

2. Step:

Which modules should inform by email in case an error or a positive event have been recorded.

Guard:

It is possible to get information by email if a find has been reported in real-time search and if a critical error has occurred within the guard.

The email templates can be adapted using the "Edit" option in case an extension is desired.

	General > Alerts > Email > Guard ? He
<ul> <li>Expert mode</li> <li>Standard configuration</li> <li>Scanner</li> <li>Guard</li> <li>MailGuard</li> <li>WebGuard</li> <li>FireWall</li> <li>FireWall</li> <li>Update</li> <li>General</li> <li>Threat categories</li> <li>Password</li> <li>Security</li> <li>WMI</li> <li>Events</li> <li>Reports</li> <li>Directories</li> <li>Alerts</li> <li>Network</li> <li>Email</li> <li>Guard</li> <li>Scanner</li> <li>Updater</li> </ul>	Guard         ✓ Email alerts         ✓ The on-access scan detected a virus or unwanted program         ✓ A critical error occurred in Guard         ✓ A critical error occurred in Guard         Edit         Recipient(s):         Administrator@testexchange.net

Scanner:

In this dialogue it is also possible to configure the scanner module in such a way that an email is sent out in case of a find during the scan search. Also, an email can be sent when the end of a planned search operation has been reached.

Advantage of this notification method:

The files that have been reported as finds and the searched objects can be traced immediately with the help of the log file of the search operation.

	General > Alerts > Email > Scanner	? Help
<ul> <li>Expert mode</li> <li>Standard configuration</li> <li>Scanner</li> <li>Guard</li> <li>MailGuard</li> <li>WebGuard</li> <li>FireWall</li> <li>Update</li> <li>General</li> <li>Threat categories</li> <li>Password</li> <li>Security</li> <li>WMI</li> </ul>	<ul> <li>Scanner</li> <li>✓ Email alerts</li> <li>Email messages for the following events</li> <li>✓ Ine on-demand scan detected a virus or unwanted program</li> <li>□ End of scheduled scan</li> <li>✓ Add report file as attachment</li> <li>Recipient(s): Administrator@testexchange.net</li> </ul>	Edit Edit
<ul> <li>Writh</li> <li>Events</li> <li>Reports</li> <li>Directories</li> <li>Alerts</li> <li>Metwork</li> <li>Email</li> <li>Guard</li> <li>Scanner</li> <li>Updater</li> </ul>	Description Enter the email address(es) of the recipient(s) in this box. The individual addre commas. The maximum length of all addresses together (i.e. the total character characters.	

Updater:

The email alert will also be activated in the dialogue "Updater". Here you have the option to trigger an email alert only in case of a negative result (update failed) or only in case of a positive result (no update required, update completed successfully, etc.)

Again you have the option to include the log file in case of an error.

onfiguration		
	General > Alerts > Email > Updater	? Help
<ul> <li>Expert mode</li> <li>Scanner</li> <li>Guard</li> <li>HailGuard</li> <li>HebGuard</li> <li>FireWall</li> <li>Update</li> <li>General</li> <li>Threat categories</li> <li>Password</li> <li>Security</li> <li>WMI</li> <li>Events</li> <li>Reports</li> <li>Directories</li> <li>Alerts</li> <li>Network</li> <li>Email</li> <li>Guard</li> <li>Scanner</li> <li>Updateria</li> </ul>	▲     Updater     ✓ Email alerts     Email messages for the following events     □ No update necessary,     Your program is up to date.     □ Update completed successfully.     New files were installed     □ Update finished successfully.     A new groduct update is available.     ✓ Update failed.     ✓ Add report file as attachment     Recipient(s): Administrator@testexchange.net     Description	E dit E dit E dit E dit
Acoustic alerts     Inherit configuration	Send later Send	d now Cancel

#### 3. Send product status by email

This feature can be activated if a valid email address has been stored within the user administration for the created user and the service of the SMC server has registered valid SMTP-data.

The user administration must be used to perform an adaptation of an existing user / admin account within the SMC Frontend.

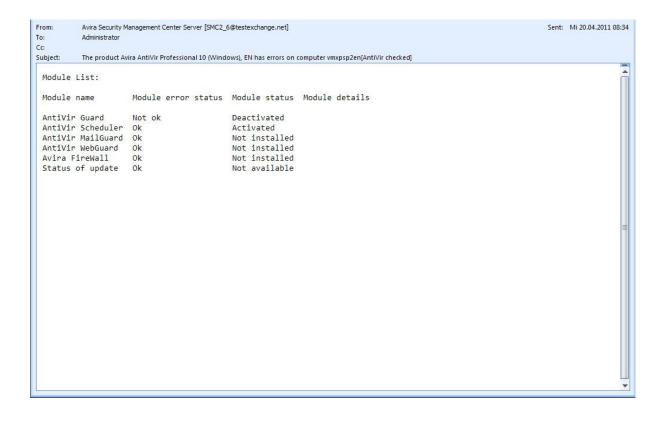
Using a right mouse-click on existing users, the option features can be selected.

Now a valid email address should be provided.

Once this is done, you will be informed immediately if the services have been deactivated at a client or server.

You will also be informed in case of a reactivation about the positive result.

Product status email in a negative case:



Product status email in a positive case:

Administrator	anagement Center Server [SMC2_	6@testexchange.net]		Sent: Mi 20.04.2011 09:
oject: The product Av	ira AntiVir Professional 10 (Wind	ows) EN reverted to no	rmal operation on computer vmxpsp2en[AntiVir checked]	
Nodule List:				
odule name	Module error status	Module status	Module details	
AntiVir Guard	Ok	Activated		
ntiVir Scheduler		Activated		
ntiVir MailGuard		Not installed		
ntiVir WebGuard	Ok	Not installed		
vira FireWall	Ok	Not installed		
tatus of update	Ok	Not available		

#### Note:

Only the SMC agent in push mode can retrieve the module status list. This option is not supported in pull mode.

There are 2 different ways to switch off the email notifications of the product status.

- 1. You remove the email address from the SMC Account
- 2. You disable the user right "Product status email received" under user rights within the security environment.

Name	Manage user:
Everyone Administrator	
ermissions	
Install products	-
<ul> <li>Uninstall products</li> <li>Configure products</li> </ul>	
Send commands	
Manage server tasks	
Generate reports	
Manage group permissions	
Receive product status E-Mail	
Use parent setting	OK Cancel

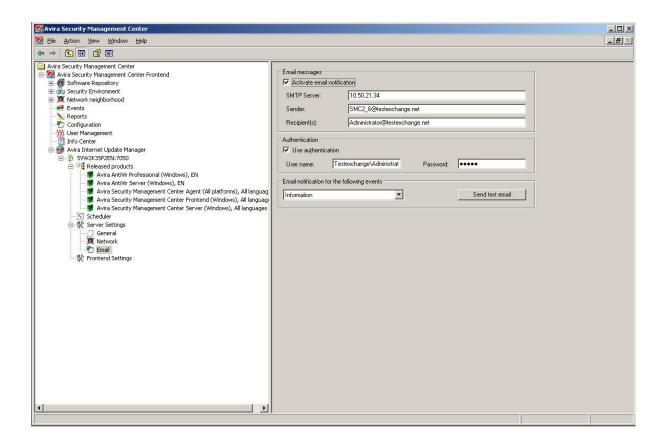
#### Note:

The product status email will be sent out in an interval of 2 minutes.

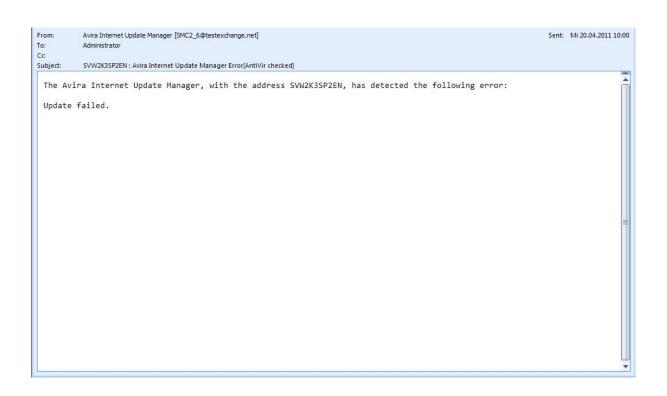
#### 4. Internet Update Manager notification emails

The Internet Update Manager is responsible for the central management of updates and their distribution for the managed products within the Avira SMC environment.

Email alerts can be set here, too.



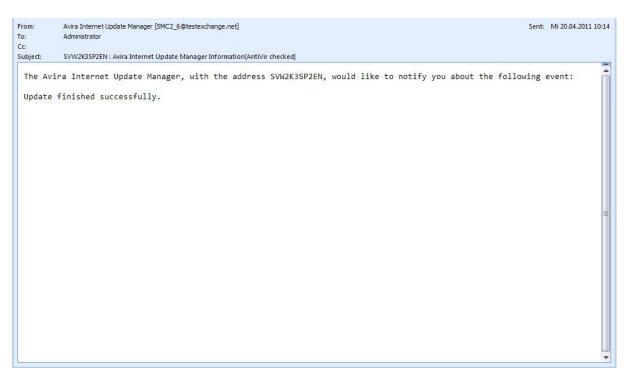
## Example of an error:



#### Example of a warning:

From: To:	Avira Internet Update Manager [SMC2_6@testexchange.net] Administrator	Sent:	Mi 20.04.2011 10:10
Cc: Subject:	SVW2K3SP2EN : Avira Internet Update Manager Warning[AntiVir checked]		
The Av	vira Internet Update Manager, with the address SVW2K3SP2EN, has detected the following warning:		
26	pading files from server <a href="http://dl3.antivir.net">http://dl3.antivir.net</a> was not successful. Error while downloading file idx/master	.idx:	537
			-

#### Example for informations:



The restart of the Internet Update Manager will be done after the SMTP-data has been registered. This causes a temporary deactivation of the Avira Internet Update Manager. The connection will be restored automatically.