

Benachrichtigungsmöglichkeiten in SMC 2.6

Support
April 2011



www.avira.de

Irrtümer und technische Änderungen vorbehalten
© Avira GmbH 2011

Benachrichtigungsmöglichkeiten in SMC 2.6

Folgende Benachrichtigungsmöglichkeiten gibt es in der SMC 2.6:

1. SMC Server informiert per Email anhand von Produktevents
2. Das verwaltete Produkt selbst verschickt Emails
3. Produktstatus per Email verschicken
4. Internet Update Manager Benachrichtigungsemails

1. SMC Server informiert per Email anhand von Produktevents

Diese Funktion dient dazu, dass der Security Management Center Server Dienst selbst den Administrator auf kritische Events oder Warnungen per Email hinweist.

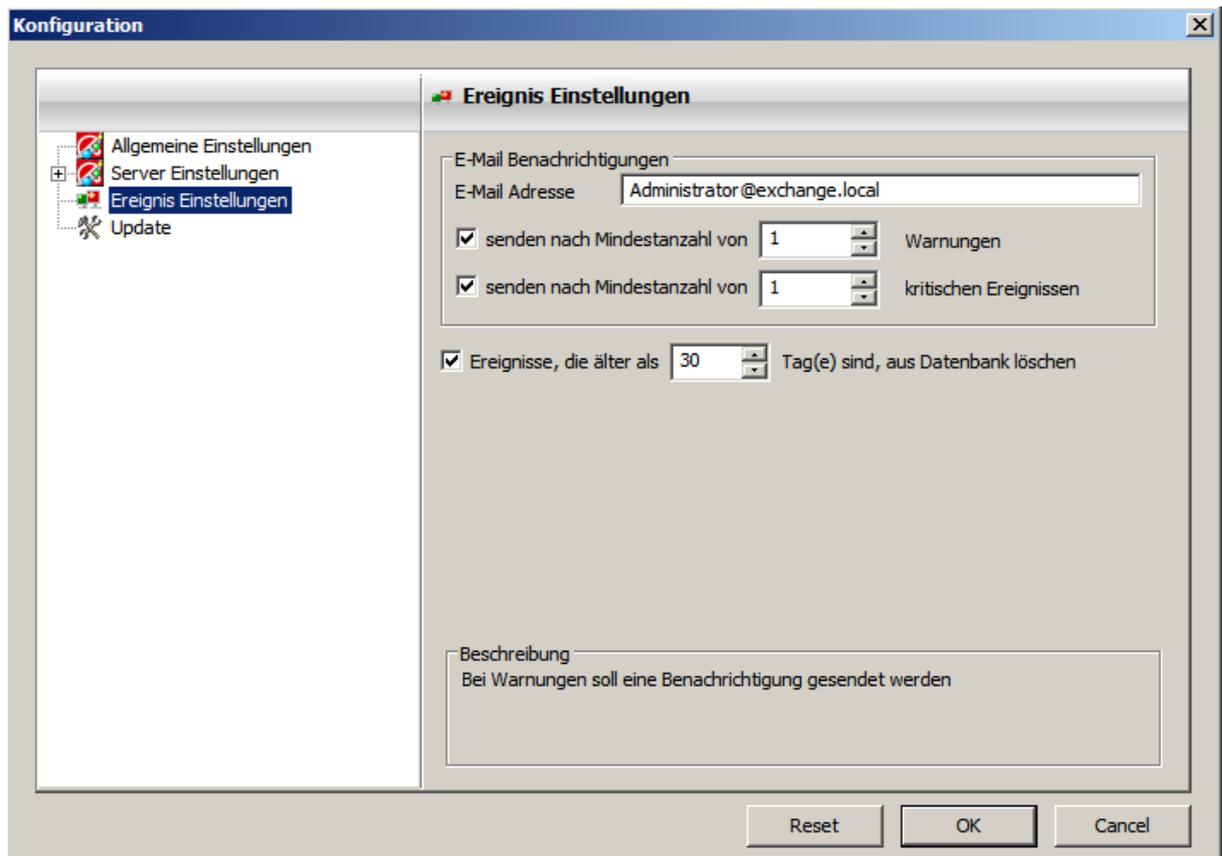
Dies kann im SMC Frontend unter "Konfigurationen" eingestellt werden.

Unter den "Allgemeinen Einstellungen" kann der SMTP Server, Absenderadresse sowie die Logindaten für den SMTP Server eingetragen werden.

The screenshot shows the 'Konfiguration' window with the 'Allgemeine Einstellungen' tab active. The configuration details are as follows:

Field	Value
SMTP Server Name	10.50.21.103
Absender E-Mail Adresse	SMC2_6@exchange.local
Login Daten vorhanden	<input checked="" type="checkbox"/>
SMTP Login	EXCHANGE\administrator
SMTP Passwort
Beschreibung	

Unter "Ereignis → Einstellungen" kann nun konfiguriert werden, wann eine Email an den Administrator verschickt werden soll.



Ebenfalls gibt es die Möglichkeit, alte Events, die älter als x Tage sind, aus der Datenbank automatisch entfernen zu lassen.

Ein Warnungsevent wäre zum Beispiel, wenn eine Datei nicht gescannt werden konnte oder ein Update von einem verwalteten Produkt fehlgeschlagen ist.

Ein kritisches Event wäre ein Virenfund.

Anbei ein paar Beispiel-E-mails wie die SMC im Falle solcher Events informiert:

Name	Level	Anwendung	Aktor	Nachricht
 vmxpsp2de	Warnung	Avira AntiVir Professional 1...	Guard	Service wurde deaktiviert.
 10.50.21.249	Kritisch	Avira AntiVir Server 10 (Wi...	Guard	Malware 'Eicar-Test-Signature' [virus] wurde in Datei '...

Warnungsevent:

Von: Avira Security Management Center [SMC2_6@exchange.local] Gesendet: Di 29.03.2011 14:34
An: Administrator
Cc:
Betreff: SMC ALERT on vmxpsp2de (10.50.21.208)[Virus checked]

Host Name: vmxpsp2de (10.50.21.208)
Modul Name: Guard
Event Level: Warning
Issue Time: Tue Mar 29 14:33:40 2011
Message: Service wurde deaktiviert.

Kritisches Event:

Von: Avira Security Management Center [SMC2_6@exchange.local] Gesendet: Di 29.03.2011 13:58
An: Administrator
Cc:
Betreff: SMC ALERT on SN2k8R2DESMC26 (10.50.21.202)[Virus checked]

Host Name: SN2k8R2DESMC26 (10.50.21.202)
Modul Name: Guard
Event Level: Critical
Issue Time: Tue Mar 29 13:57:22 2011
Message: Malware 'Eicar-Test-Signature' [virus] wurde in Datei 'C:\Users\Administrator\Downloads\eicar.com' gefunden. Durchgeführte Aktion: Datei in Quarantäne verschieben.

2. Das verwaltete Produkt selbst verschickt Emails

Wenn gewünscht wird, daß jedes verwaltete Produkt eine Email verschickt oder wenn ein kritisches Event oder eine Warnung aufgetreten ist, kann dies natürlich noch zusätzlich konfiguriert werden.

Es ist aber empfehlenswert, daß nur eine Möglichkeit konfiguriert wird, da sonst eventuell der Überblick verloren geht.

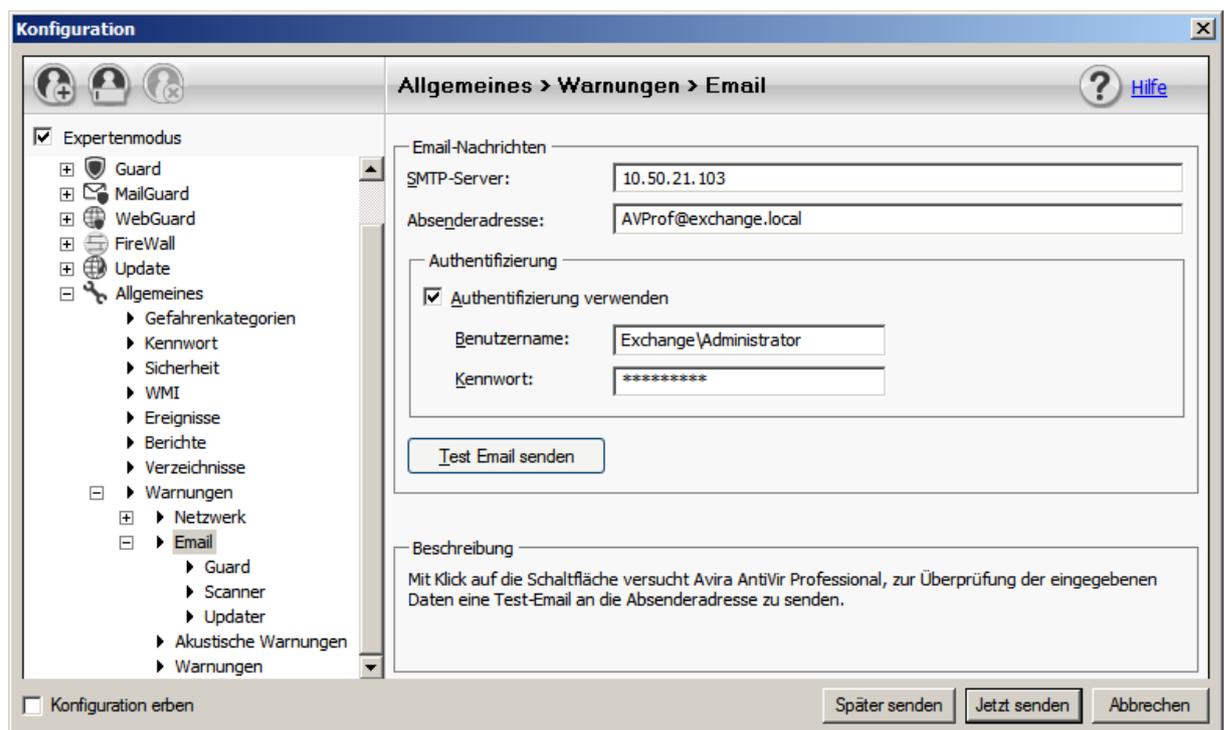
AV10 Professional:

Rechten Mausklick auf das zu verwaltende Produkt, dann *Konfiguration --> Konfigurieren*

In diesem Dialog besteht die Möglichkeit sich vom Modul (Guard, Scanner, Updater) per Email informieren zu lassen.

1. Schritt:

Die SMTP Serverdaten müssen hinterlegt werden. Falls eine Authentifizierung erforderlich ist, muss diese ebenfalls eingetragen werden



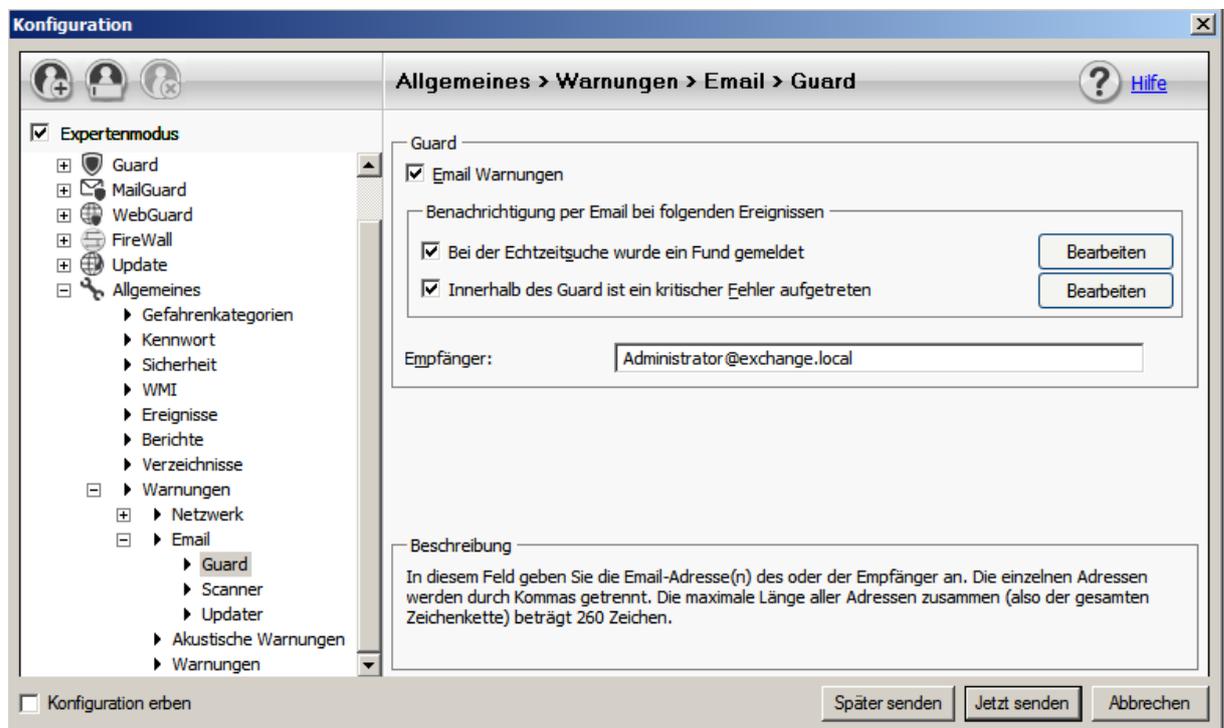
2. Schritt:

Welche Module sollen per Email informieren, wenn ein Fehlerfall oder ein positives Ereignis eingetragen ist.

Guard:

Es besteht die Möglichkeit sich per Email informieren zu lassen, wenn bei der Echtzeitsuche ein Fund gemeldet wurde und wenn innerhalb des Guards ein kritischer Fehler aufgetreten ist.

Die Emailtemplates lassen sich mittels dem Button "Bearbeiten" anpassen, falls eine Erweiterung erwünscht ist.

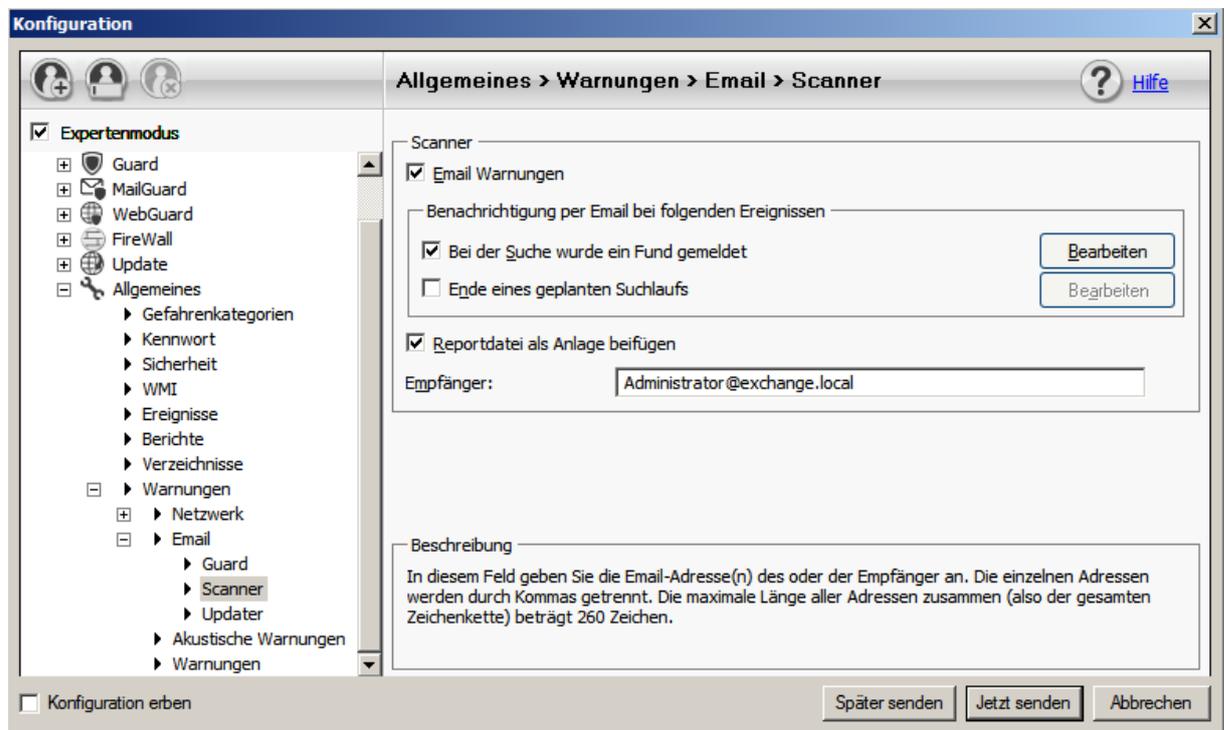


Scanner:

In diesem Dialog besteht die Möglichkeit das Modul Scanner so zu konfigurieren, dass eine Email verschickt wird, wenn bei der Suche des Scanners ein Fund gemeldet wird. Ebenfalls kann eine Email verschickt werden, wenn das Ende eines geplanten Suchlaufes erreicht wurde.

Vorteil von dieser Benachrichtigungsmethode:

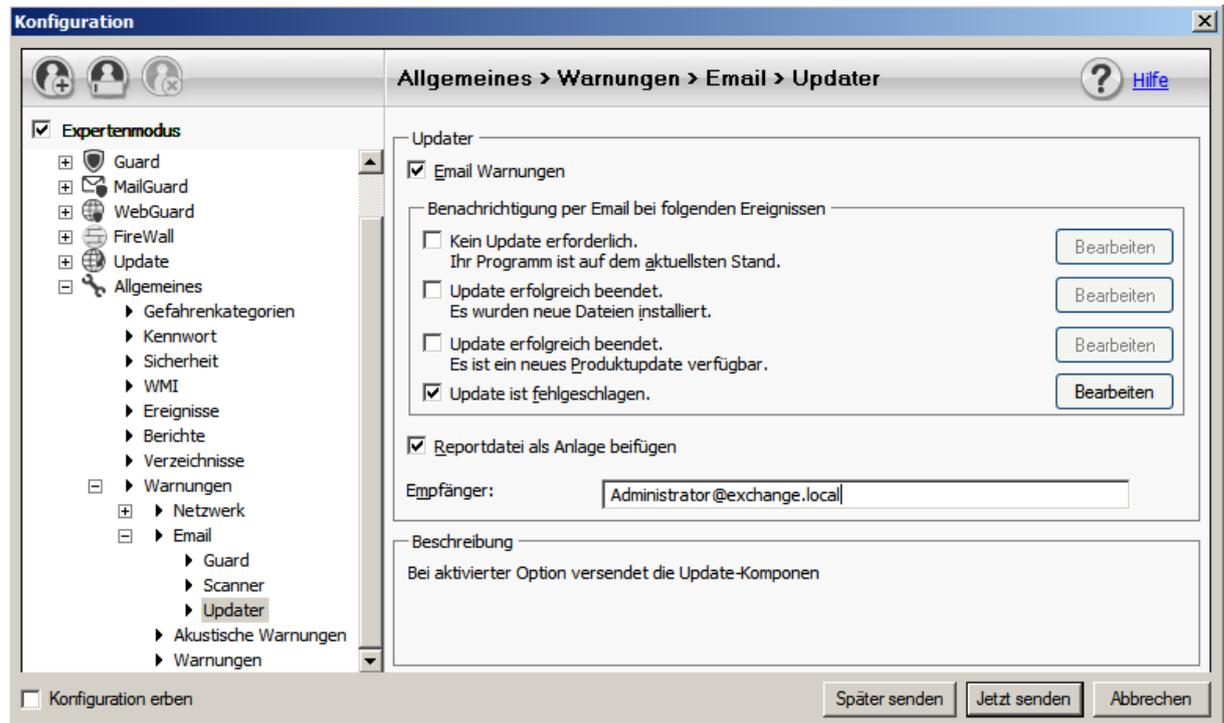
Es kann an der mitgeschickten Logdatei des Suchlaufes sofort nachvollzogen werden, welche Datei als Fund gemeldet wurde und welche Objekte durchsucht wurden.



Updater:

Im Dialog "Updater" kann die Email Warnung ebenfalls aktiviert werden. Hier besteht die Möglichkeit, entweder nur bei einem negativen Ergebnis (Update fehlgeschlagen) eine Emailbenachrichtigung auszulösen oder nur bei einem positiven Ergebnis (Kein Update erforderlich, Update erfolgreich beendet, etc.).

Auch hier besteht wieder die Möglichkeit, daß die Logdatei in einem Fehlerfall mit verschickt wird.



3. Produktstatus per Email verschicken

Dieses Feature lässt sich aktivieren, wenn in der Benutzerverwaltung für die angelegten User eine gültige Emailadresse hinterlegt ist und der SMC Server Dienst gültige SMTP-Daten hinterlegt hat.

Um eine Anpassung eines bestehenden User/Admin Accounts im SMC Frontend durchzuführen, muss die Benutzerverwaltung verwendet werden.

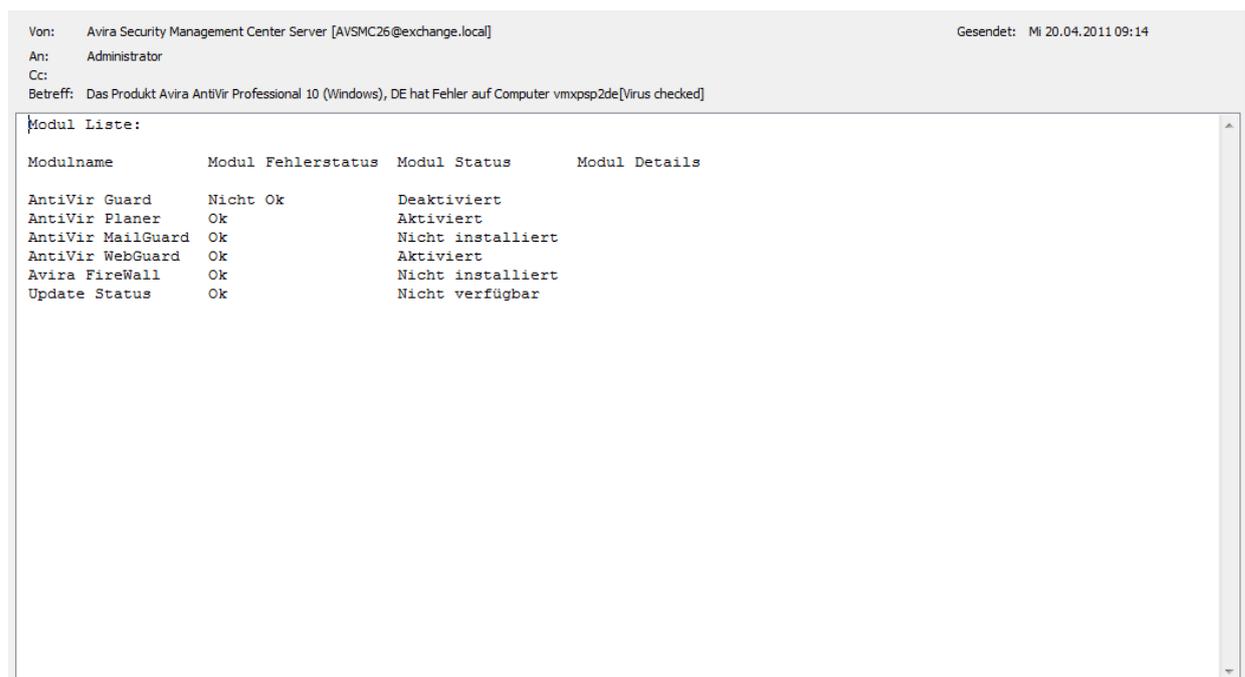
Mittels eines rechten Mausklicks auf den bestehenden User kann der Punkt Eigenschaften gewählt werden.

Nun muss eine gültige Emailadresse hinterlegt werden.

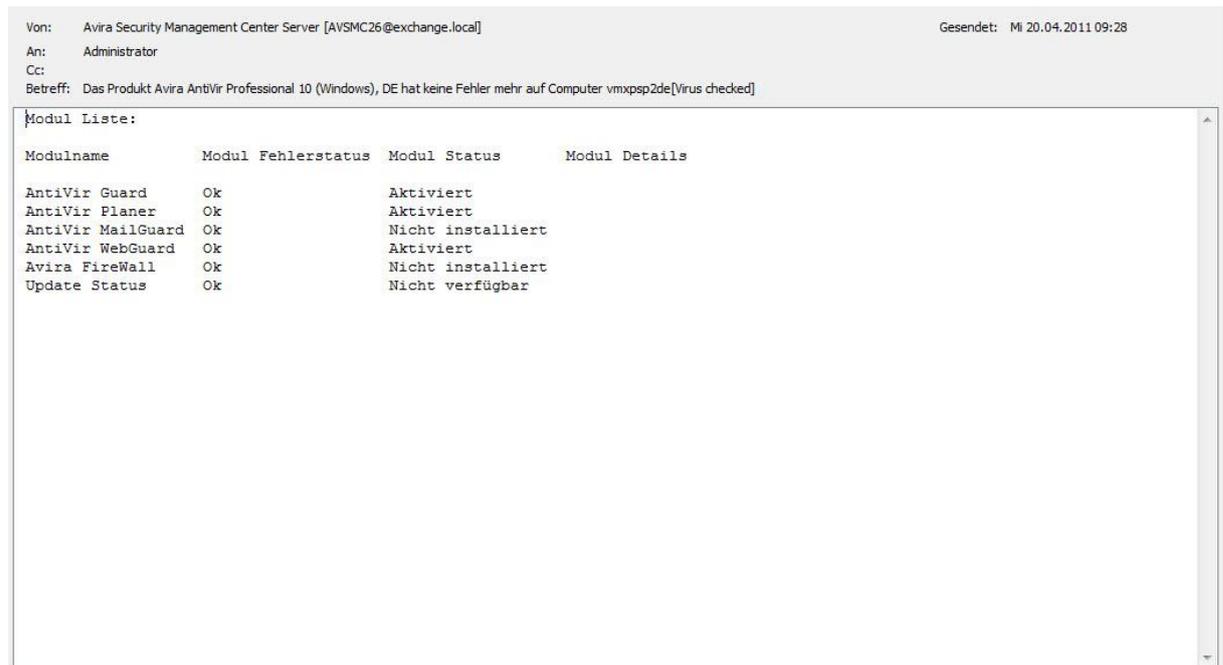
Wenn dies erfolgt ist, wird man ab sofort informiert, wenn an einem Client oder Server die Services deaktiviert wurden.

Auch im Falle einer Reaktivierung wird man über das positive Ergebnis informiert.

Produktstatus-Email im negativen Fall:



Produktstatus-Email im positiven Fall:

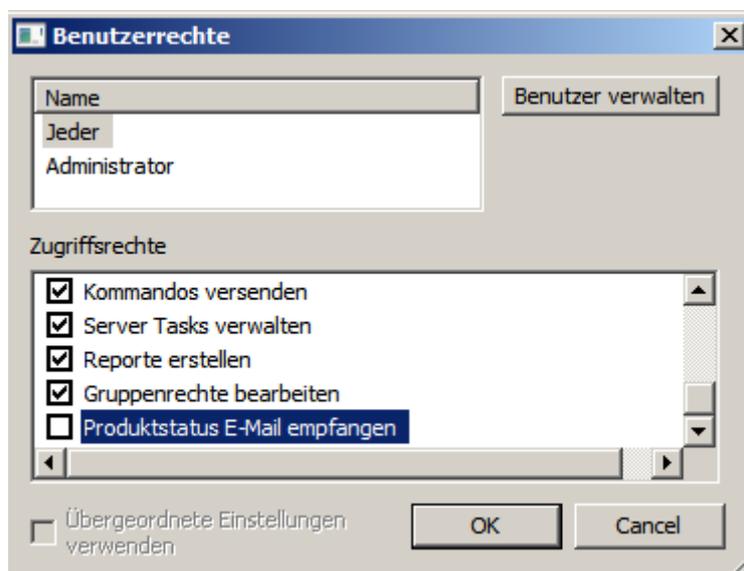


Hinweis:

Die Modulstatusliste kann nur der SMC Agent im Push-Modus abrufen.
Im Pullmodus wird diese Option nicht unterstützt.

Die Produktstatus-Emailbenachrichtigung kann auf 2 verschiedenen Arten abgeschaltet werden.

1. Man entfernt die Emailadresse aus dem SMC Account
2. Man deaktiviert das Benutzerrecht "Produktstatus-Email empfangen" unter den Benutzerrechten in der Sicherheitsumgebung.



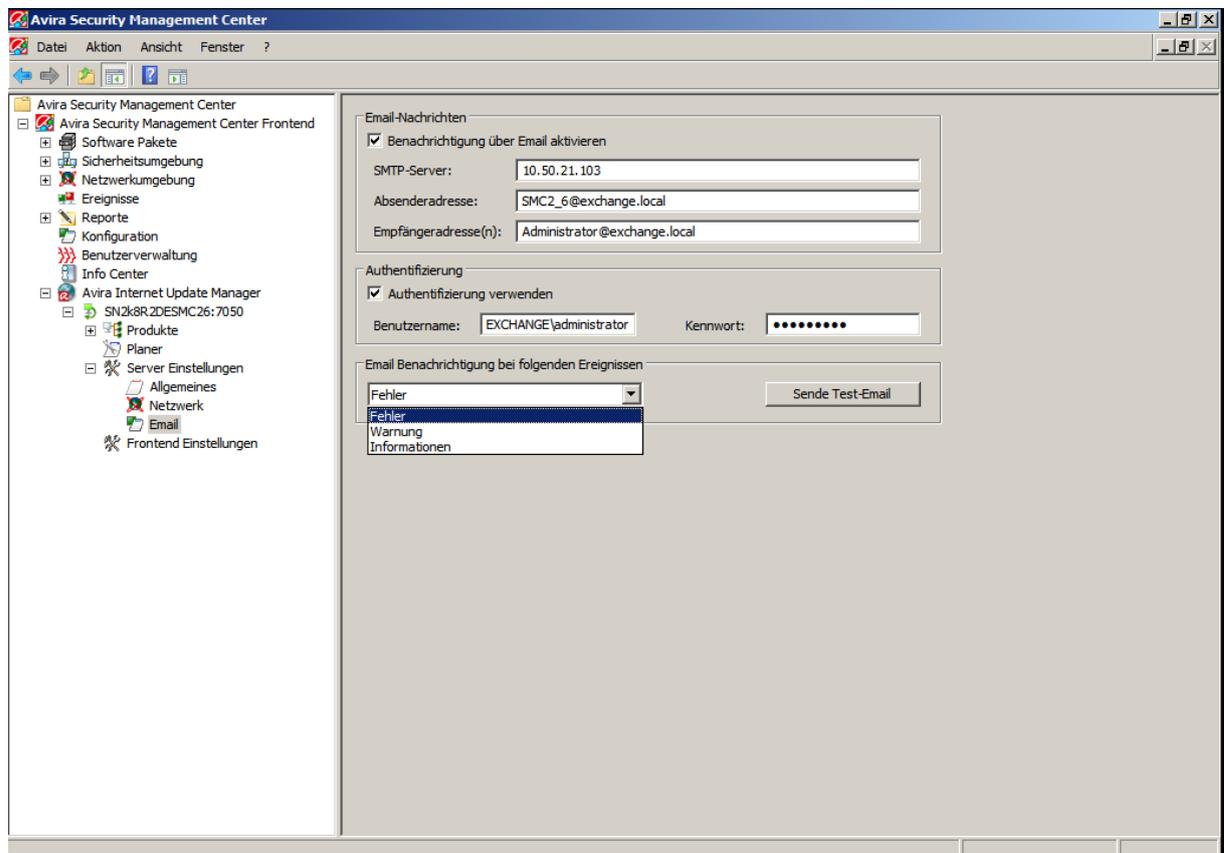
Hinweis:

Das Versenden der Produktstatus-Email erfolgt in einem Intervall von 2 Minuten.

4. Internet Update Manager Benachrichtigungsemails

Der Internet Update Manager ist für die zentrale Verwaltung der Updates und deren Verteilung für die verwalteten Produkte in der Avira SMC Umgebung verantwortlich.

Auch hier ist eine Emailbenachrichtigung einstellbar.



Beispiel für einen Fehler:

Von: Avira Internet Update Manager [SMC2_6@exchange.local] Gesendet: Mi 30.03.2011 09:41
An: Administrator
Cc:
Betreff: SN2k8R2DESMC26 : Avira Internet Update Manager Fehler[Virus checked]

Der Avira Internet Update Manager, mit der Adresse SN2k8R2DESMC26, hat folgenden Fehler festgestellt:

Aktualisierung schlug fehl.

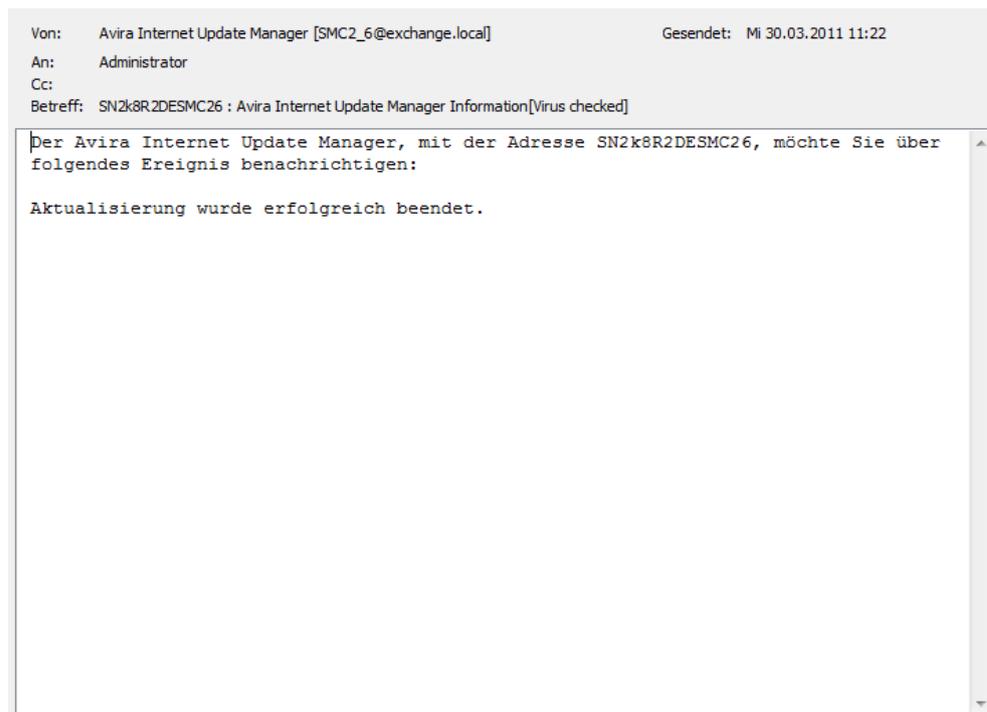
Beispiel für eine Warnung:

Von: Avira Internet Update Manager [AVIUM@exchange.local] Gesendet: Fr 25.03.2011 10:56
An: Administrator
Cc:
Betreff: charly : Avira Internet Update Manager Warnung[Virus checked]

Der Avira Internet Update Manager, mit der Adresse charly, hat folgenden Warnung festgestellt:

Herunterladen von Dateien von Server <http://dl3.antivir.net> war nicht erfolgreich.
Fehler beim Herunterladen von Datei idx/master.idx: 537

Beispiel für Informationen:



Nach dem Hinterlegen der SMTP Daten wird ein Neustart des Internet Update Manager Dienstes durchgeführt, was zu einer kurzzeitigen Deaktivierung des Avira Internet Update Managers führt. Die Verbindung wird automatisch wieder hergestellt.