assono

AdminCamp 2012
Track 2, Session 1:

Lotus Protector -
weil sicher sicher sicher ist

Gelsenkirchen, 18. Juni 2012

Innovative Software-Lösungen.

www.assono.de

assono

Thomas Bahn

Diplom-Mathematiker, Universität Hannover

seit 1997 entwickle ich mit Java und relationalen Datenbanken

seit 1999 mit Notes/Domino zu tun: Entwicklung, Administration, Beratung und Schulungen

regelmäßiger Sprecher auf nationalen und internationalen Fachkonferenzen zu IBM Lotus Notes/Domino und Autor für THE VIEW

tbahn@assono.de
http://www.assono.de/blog
04307/900-401

assono
IT-Consulting & Solutions

Agenda

- Lotus Protector – ein Name, zwei Produkte
- Lotus Protector for Mail Security
  - Theorie
  - Praxis
- Lotus Protector for Mail Encryption
  - Theorie
  - Praxis

Lotus Protector – ein Name, zwei Produkte

assono

Lotus Protector

- Einkäufe von IBM
  - LPMS: Proventia (Unternehmen)
  - LPME: PGP Universal Server (Produkt)
- Appliances
- Bedienung über Web-Oberfläche
- auf Linux-Basis
  - LPMS: SuSE Linux Enterprise Server (SLES) 10.2
  - LPME: Red Hat

Lotus Protector for Mail Security

Theorie

Lotus Protector for Mail Security (LPMS)

Lotus® Protector for Mail Security

- Schutz vor:
  - Spams, Phishing, „unerwünschte Sprache“, …
  - Viren, Trojaner, …
  - „Datenabfluss“ (Data Leakage Protection, DLP)
- Steuerung über Richtlinien (Policies) und Regeln (Rules)

assono

Lotus Protector for Mail Security (LPMS)

- mehrere (>20) Verfahren kombinierbar, u.a.
  - Dynamic Host Reputation
  - Bayessche Filter
  - Fuzzy Fingerprints
  - Flow Control
  - Struktur-Analysen
  - Antivirus-Erkennung nach Signaturen und Verhalten
  - URL- und Spam-/Phishing-Datenbanken
  - Whitelists/Blacklists
- Zero Layer Analysis (ZLA): effiziente Vorprüfung des eingehenden Bitstroms mit reduzierter Filtermenge

Lotus Protector for Mail Security (LPMS)

- Virenscanner per Web-Service via ICAP für
  - jetzt: IBM Connections, Lotus Quickr(J), Squid
  - später: Lotus Quickr(D), IBM Sametime
- Selbstschutz z.B. vor Denial-of-Service-Angriffen mit Intrusion Prevention System (IPS)
- Integration in den Notes-Client „out-of-the-box“ (seit Notes 8.5.1-Mail-Schablone)
- vordefinierte Berichte

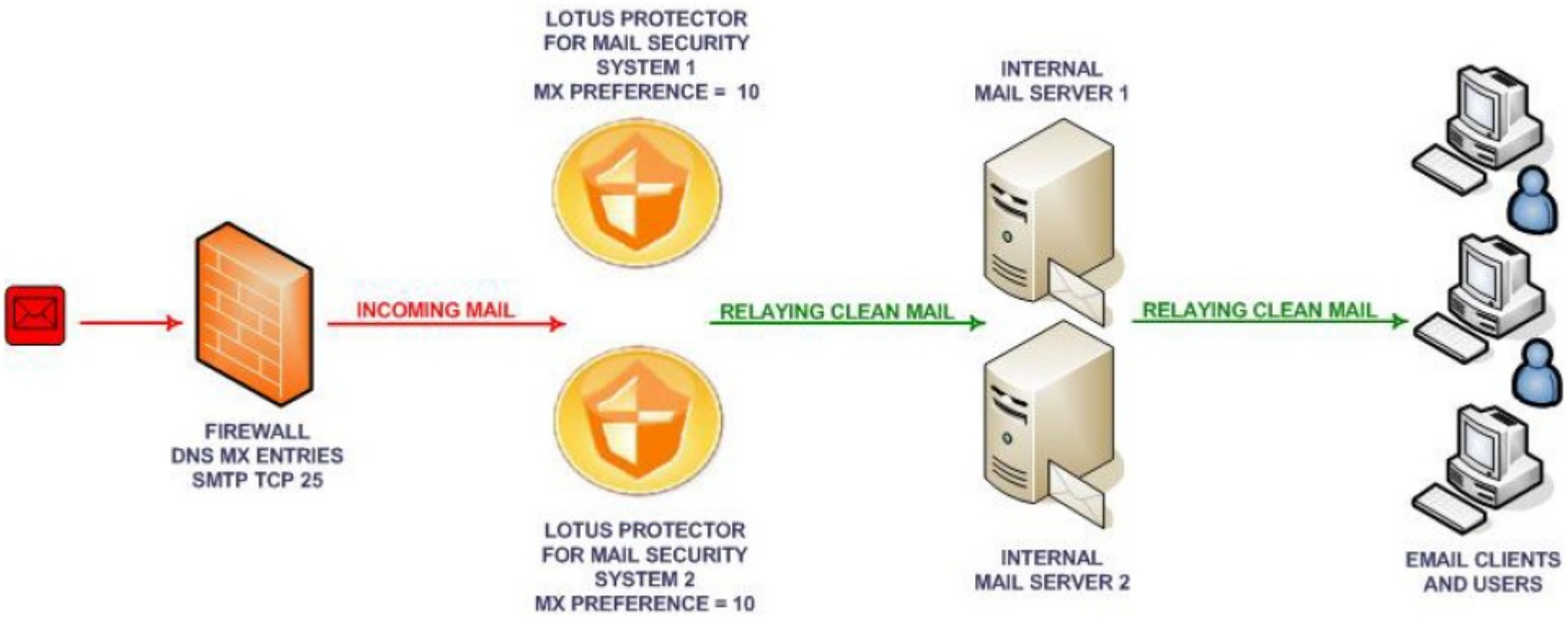
Lotus Protector for Mail Security

Praxis

MX-Einträge (DNS)

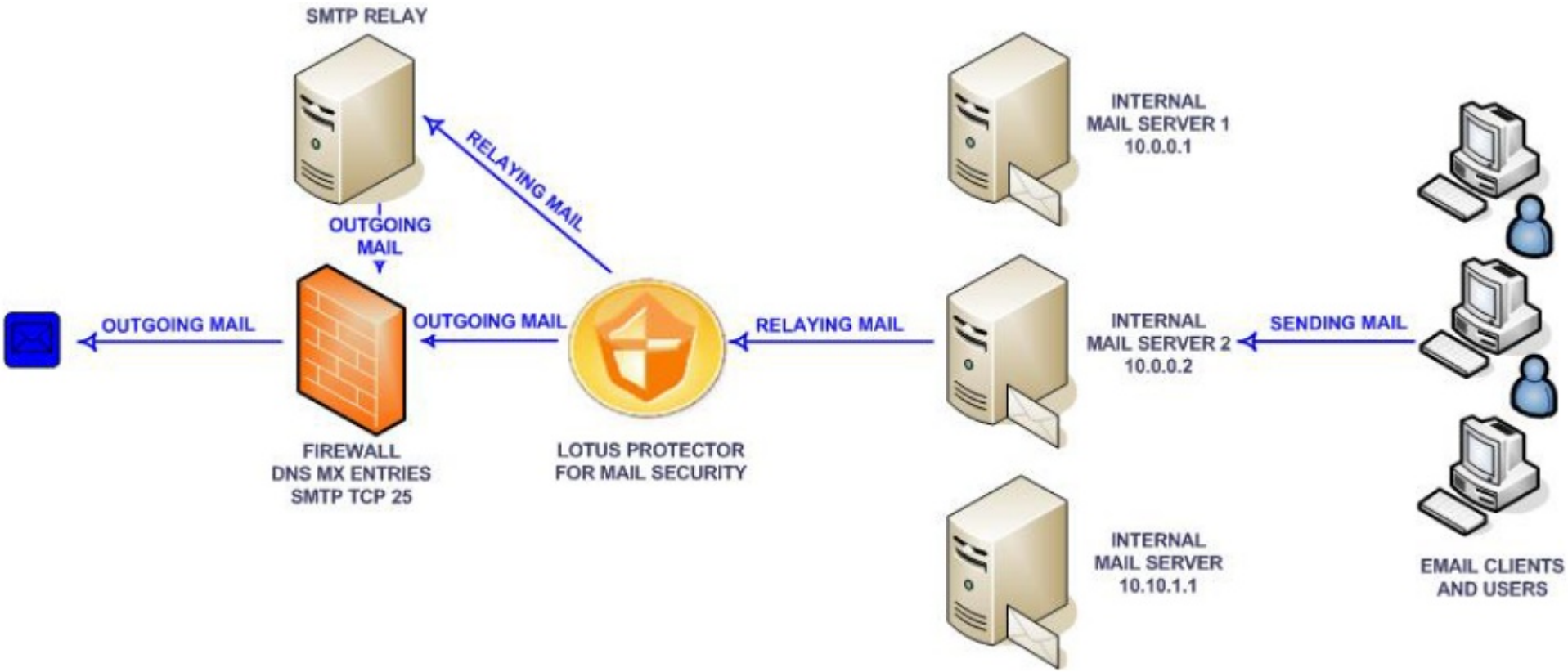
- MX-Einträge im DNS steuern, an welche Server E-Mails für eine Domäne zugestellt werden
- mehrere MX-Einträge für eine Domäne möglich
- Reihenfolge über MX Preference (~ Kosten):
  - Server mit niedrigeren Werten zuerst
  - Server mit gleichen Werten „zufällig“
- Nach der Installation müssen MX-Einträge aller Domänen auf LPMS-Server umgestellt werden

Eingehende E-Mails



Quelle: IBM Lotus Protector for Mail Security Getting Started Guide Version 2.8 (SC27-3830-00)

Ausgehende E-Mails: direkt oder via Relay



Quelle: IBM Lotus Protector for Mail Security Getting Started Guide Version 2.8 (SC27-3830-00)

LDAP

- LDAP einrichten und testen
- Softerra LDAP Browser, Apache Directory Studio oder LDAPSearch (im Notes-Client-Programmverzeichnis)
- Beispiel:
  ldapsearch -h ldap.tbahn.local -p 389 -D "cn=LDAP-Bind" -w ****** "maildomain=TBahn" cn

assono

Firewall

- ausgehend ins Internet:
  - HTTPS tcp/443
  - SMTP tcp/25
  - DNS udp/53 und optional tcp/53
- eingehend aus dem Internet:
  - SMTP tcp/25
- in Richtung internes Netzwerk
  - SMTP tcp/25 ein- und ausgehend
  - LDAP tcp/389 (oder AD)
  - NTP udp/123

assono

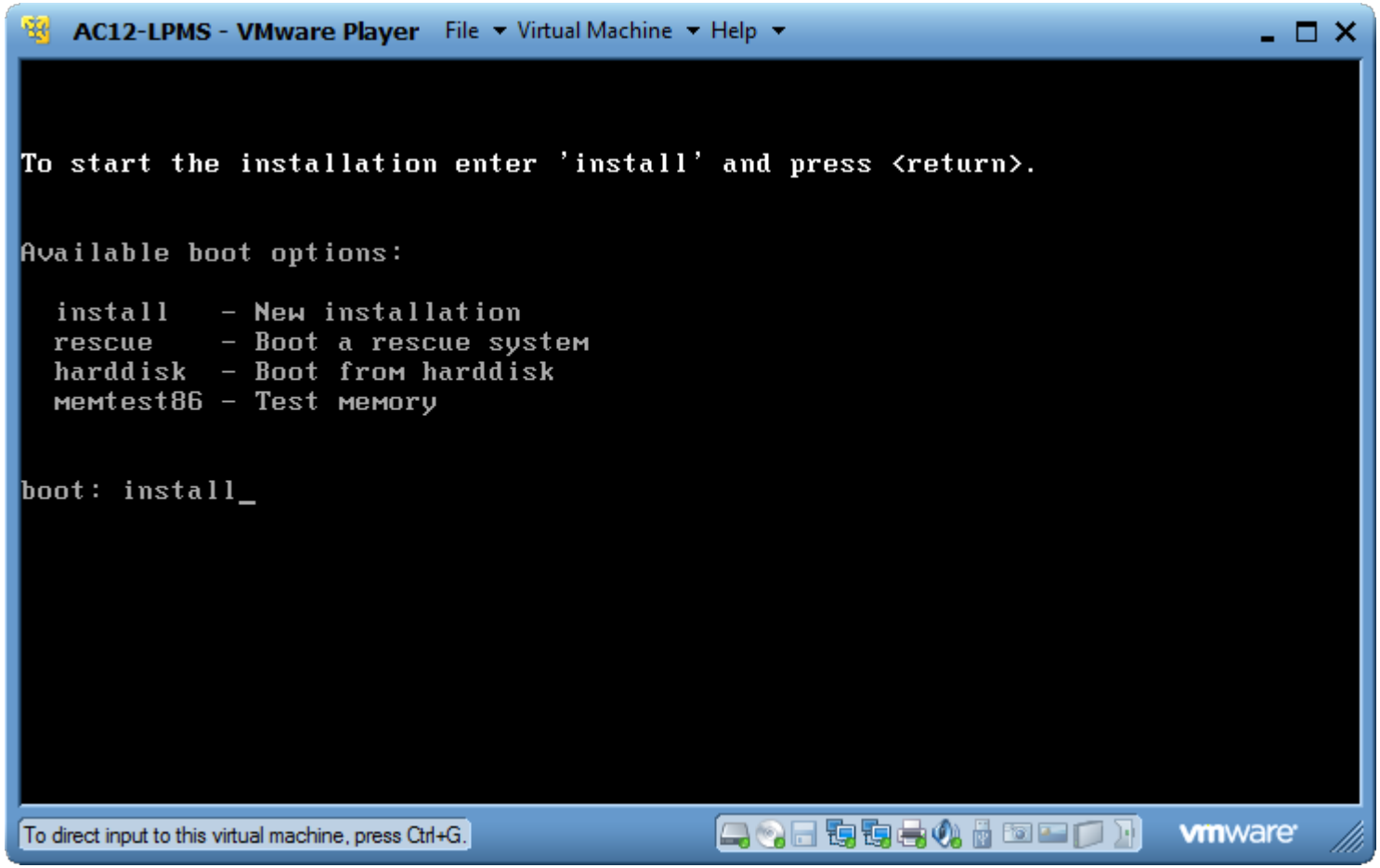
Firewall

- aus dem Management-Netzwerk:
  - HTTPS tcp/443
  - SSH tcp/22
  - SNMP udp/161
  - Datenbank-Zugriff tcp/5432
  - Cluster-Kommunikation tcp/4990
- aus dem Benutzer-Netzwerk oder HTTPS-Proxy
  - Endbenutzer-Zugriff tcp/4443

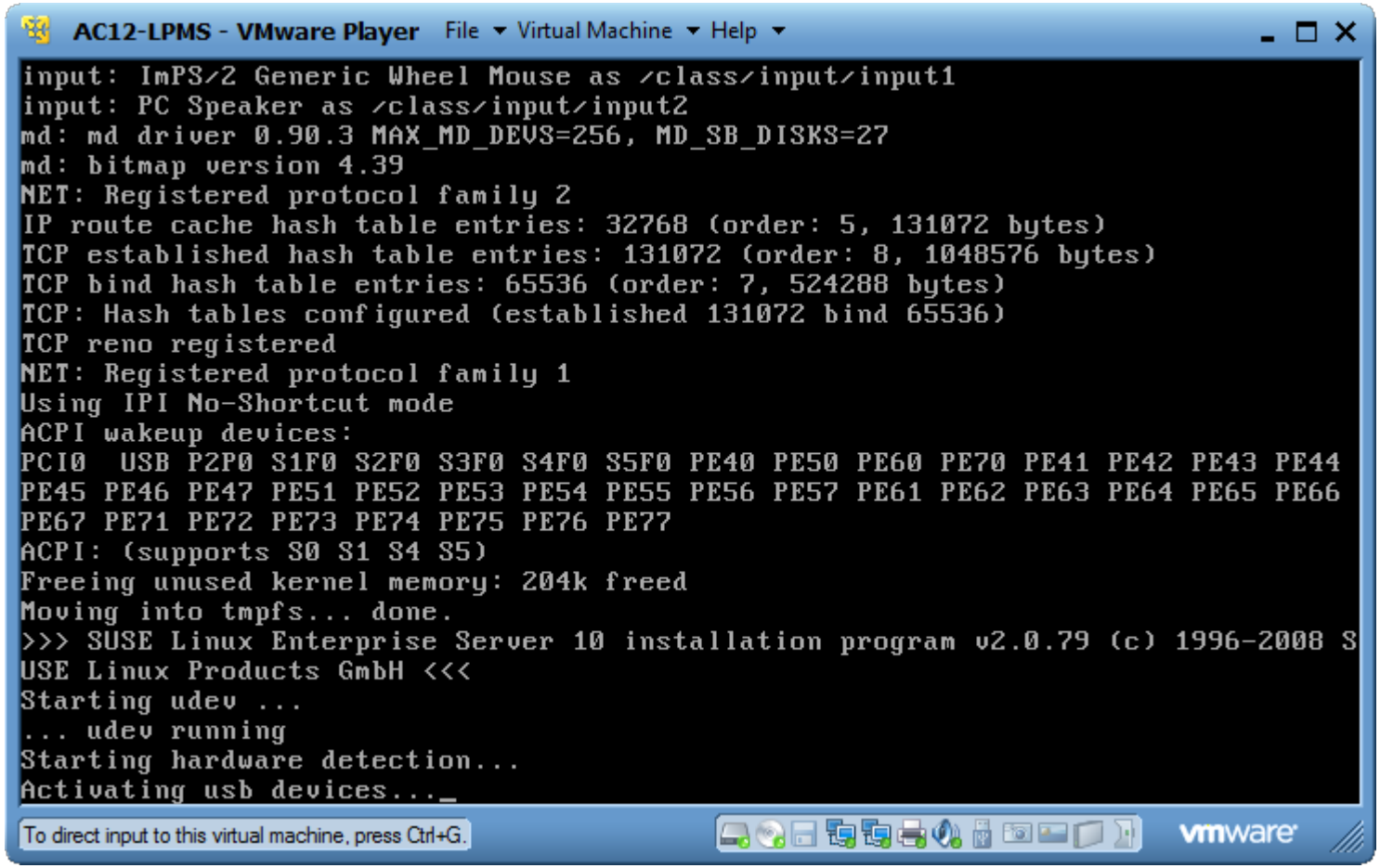
Hardware oder VMware

- LPMS läuft als Appliance auf dedizierter Hardware oder in der VMware-VM
- Anforderungen siehe Dokumentation
- Installations-ISO-Datei brennen bzw. einhängen

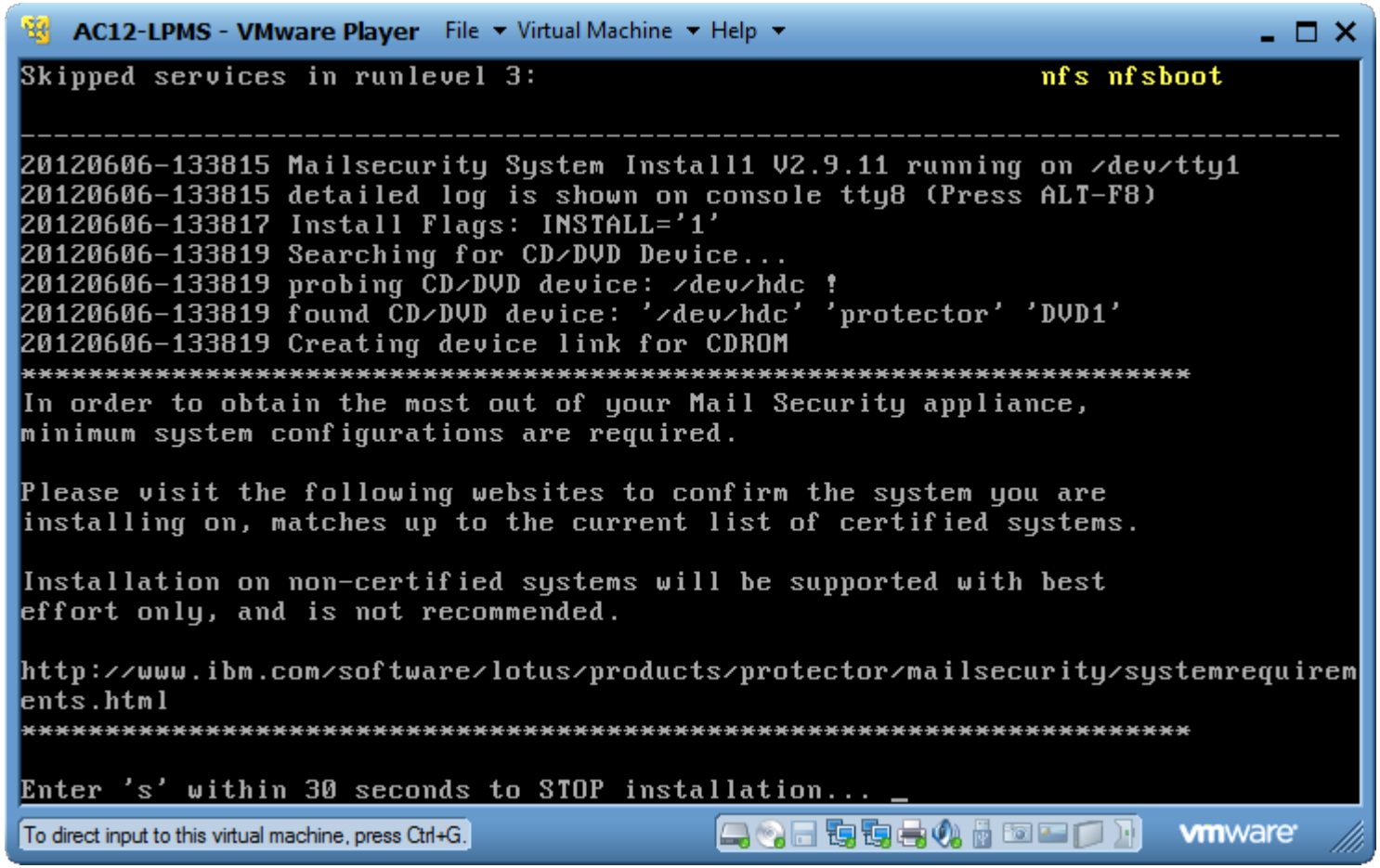
Installation



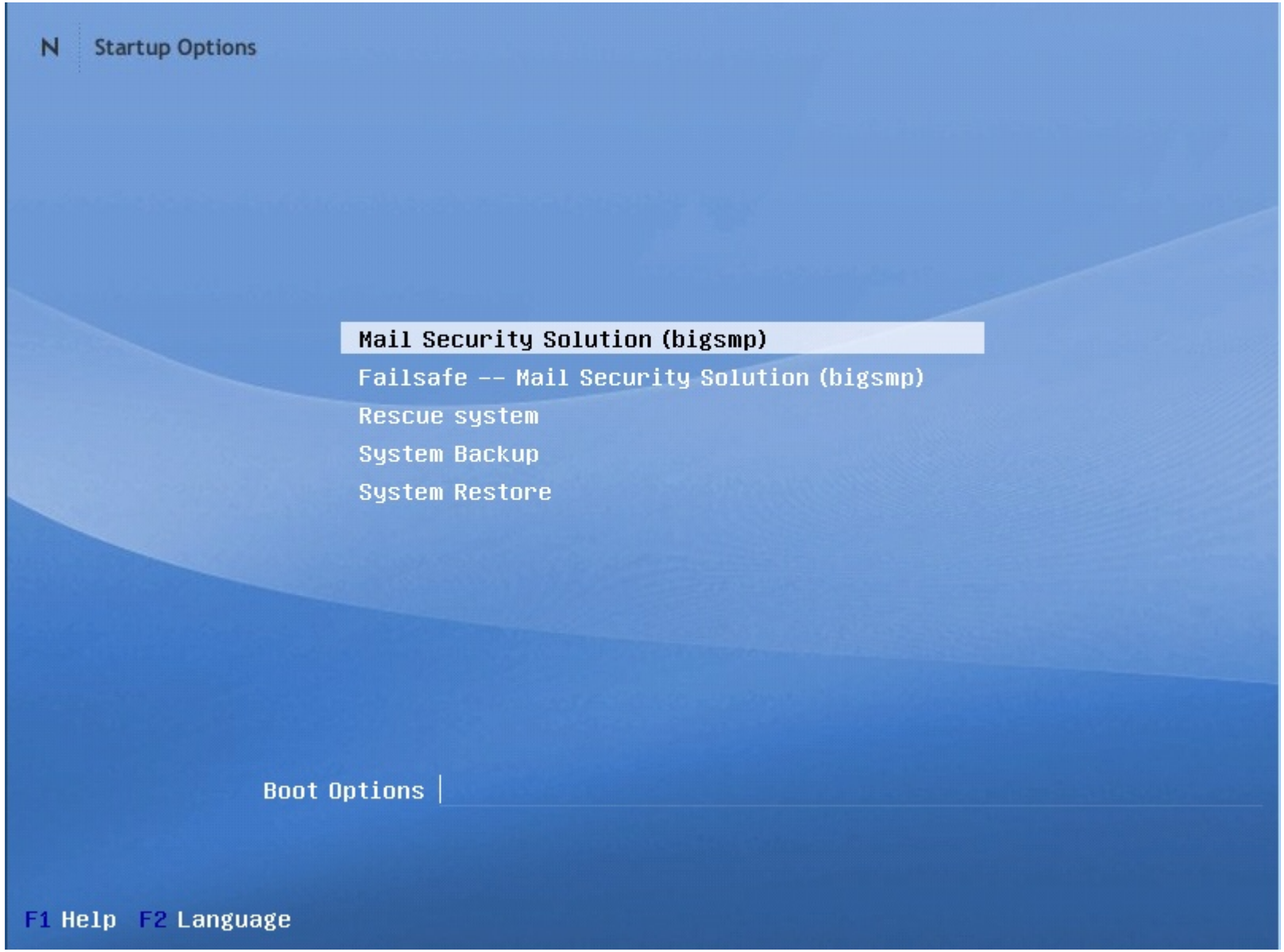
Installation



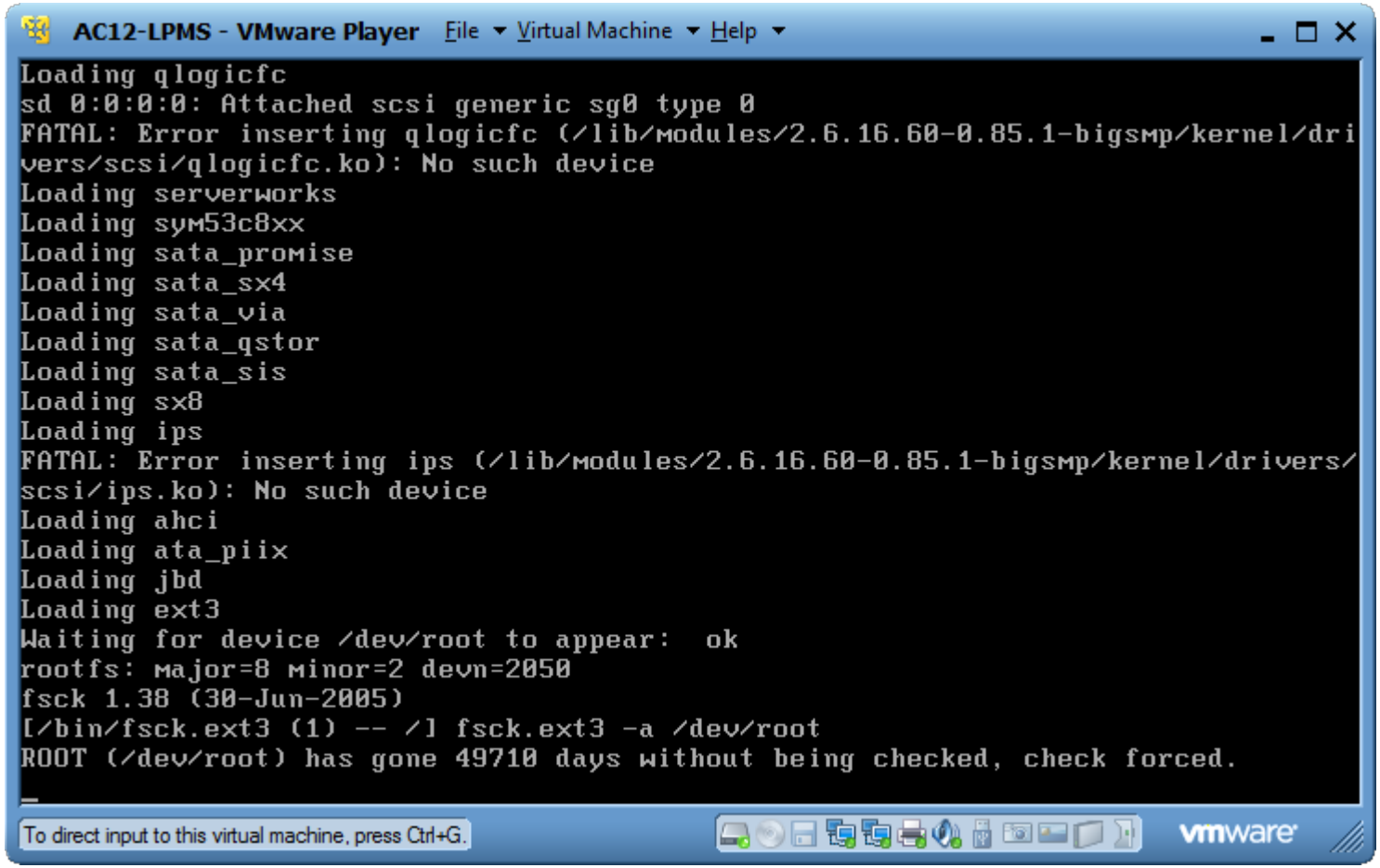
Installation



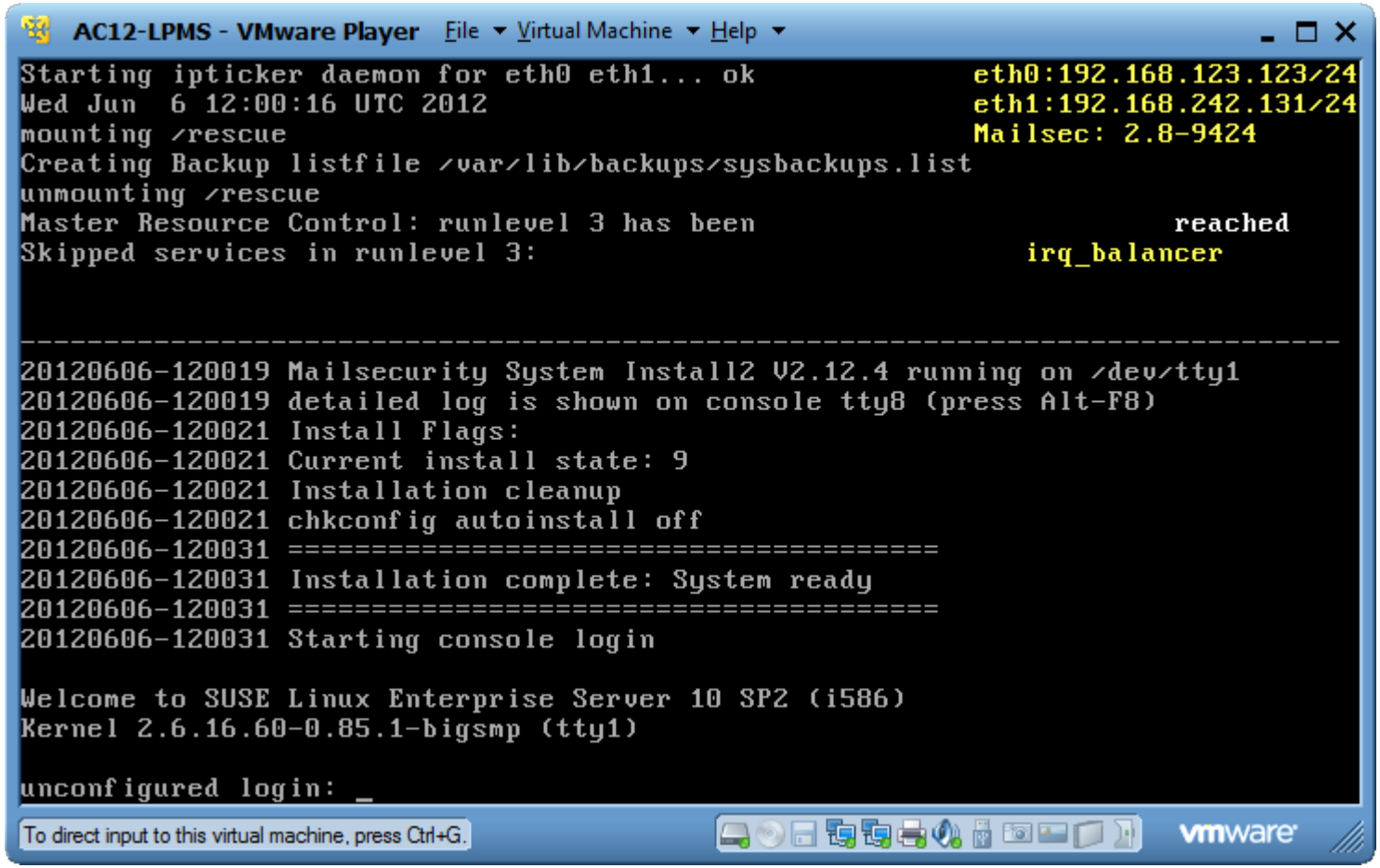
Installation



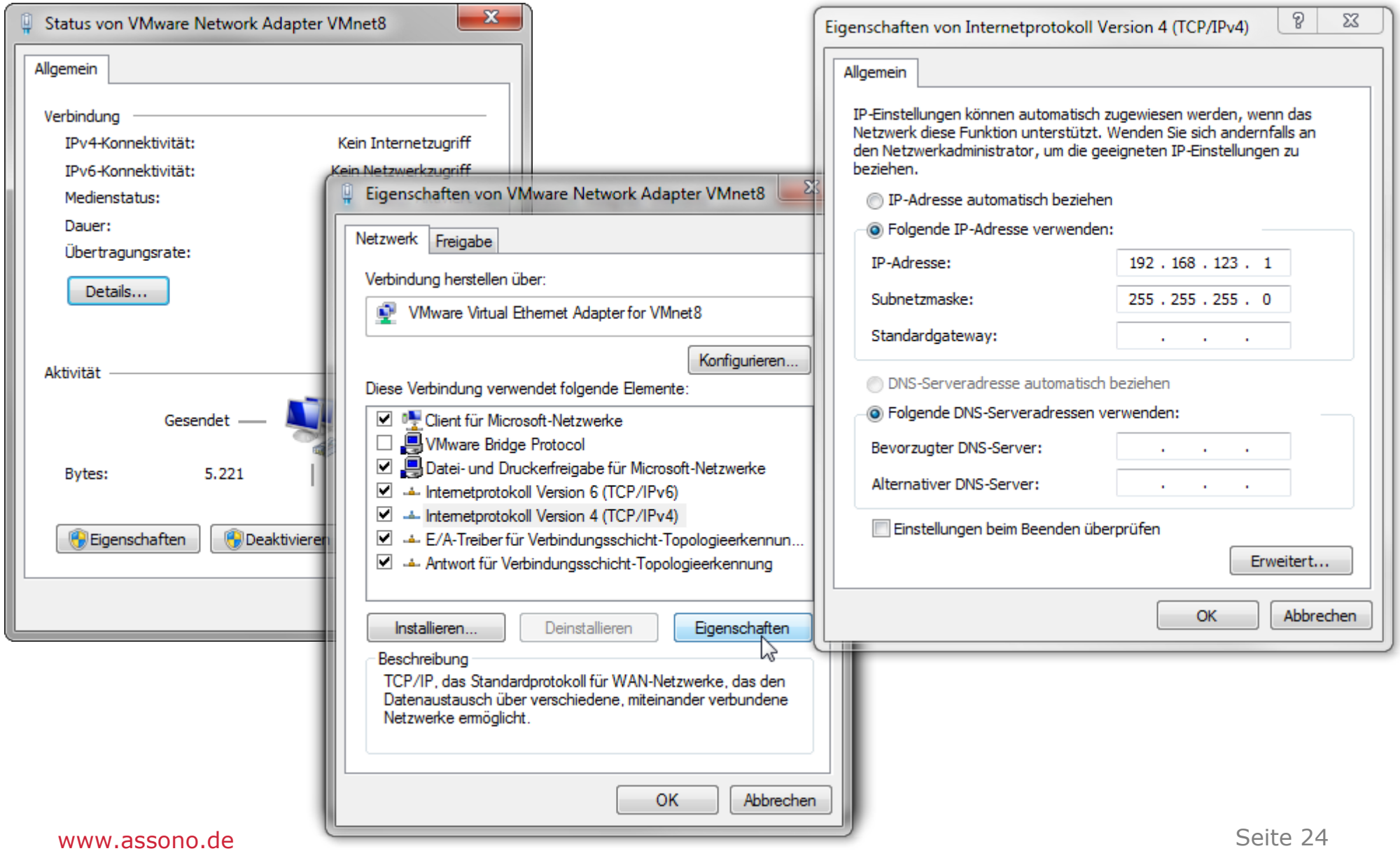
Installation



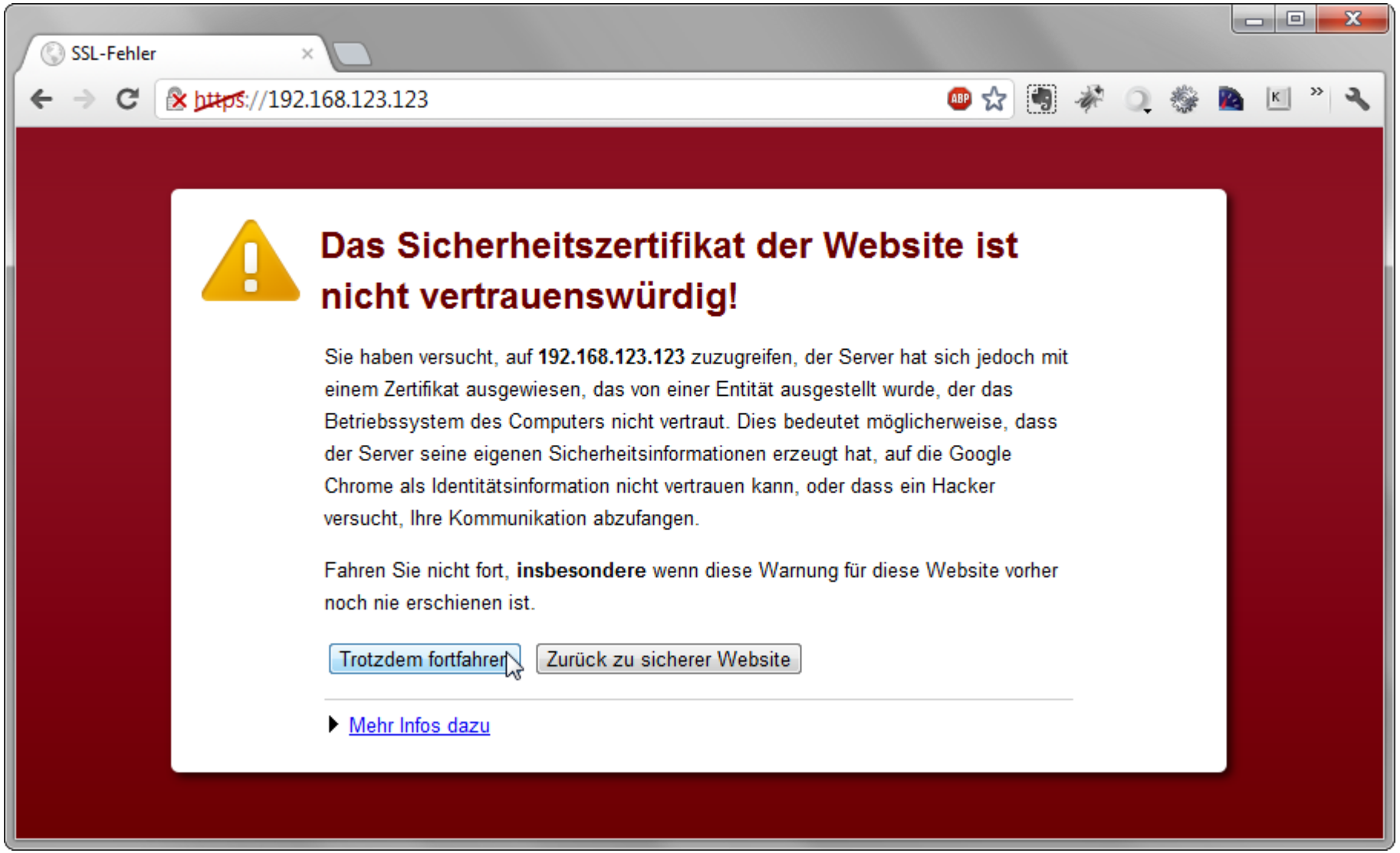
Installation



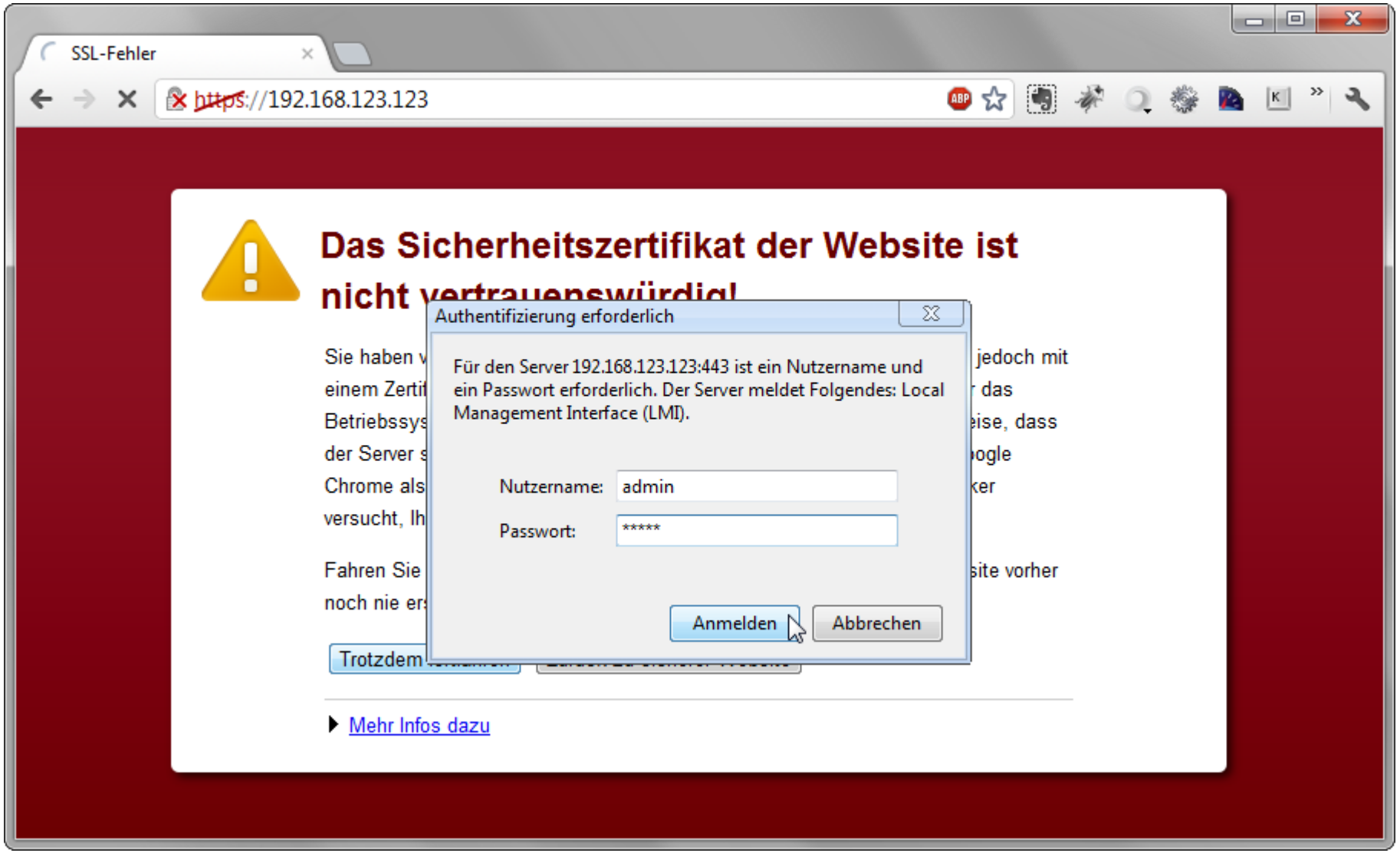
Netzwerk-Einstellungen des Clients anpassen



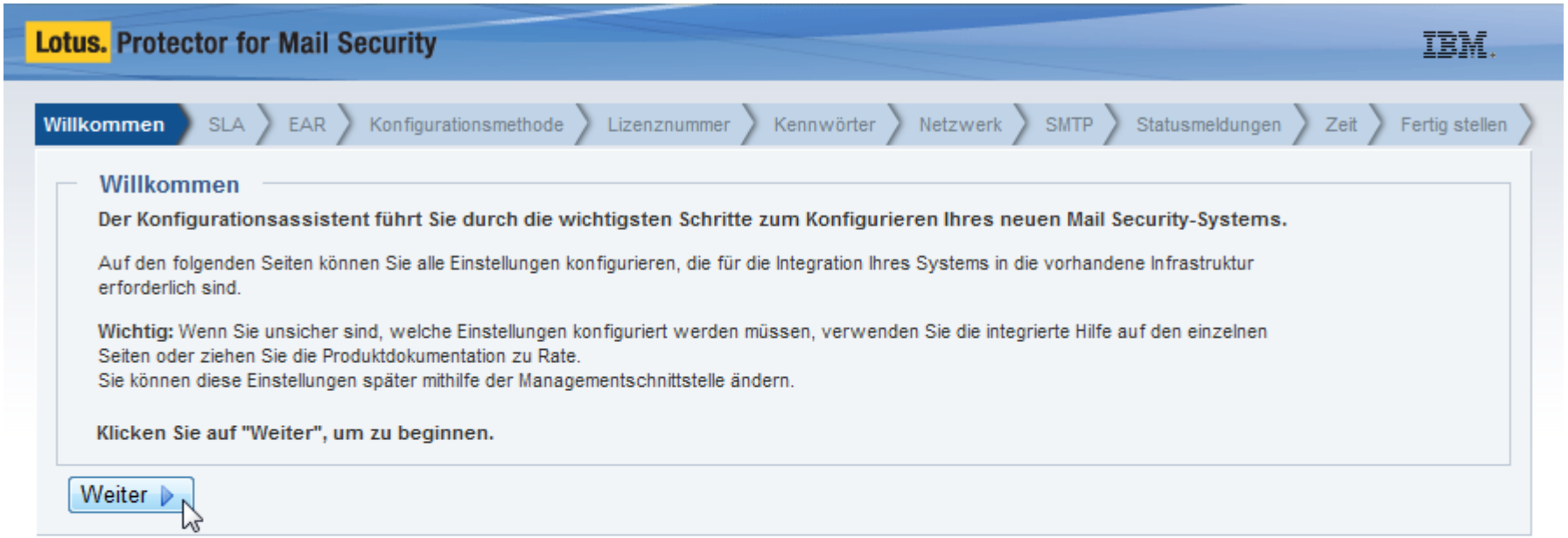
Weiter geht’s im Browser



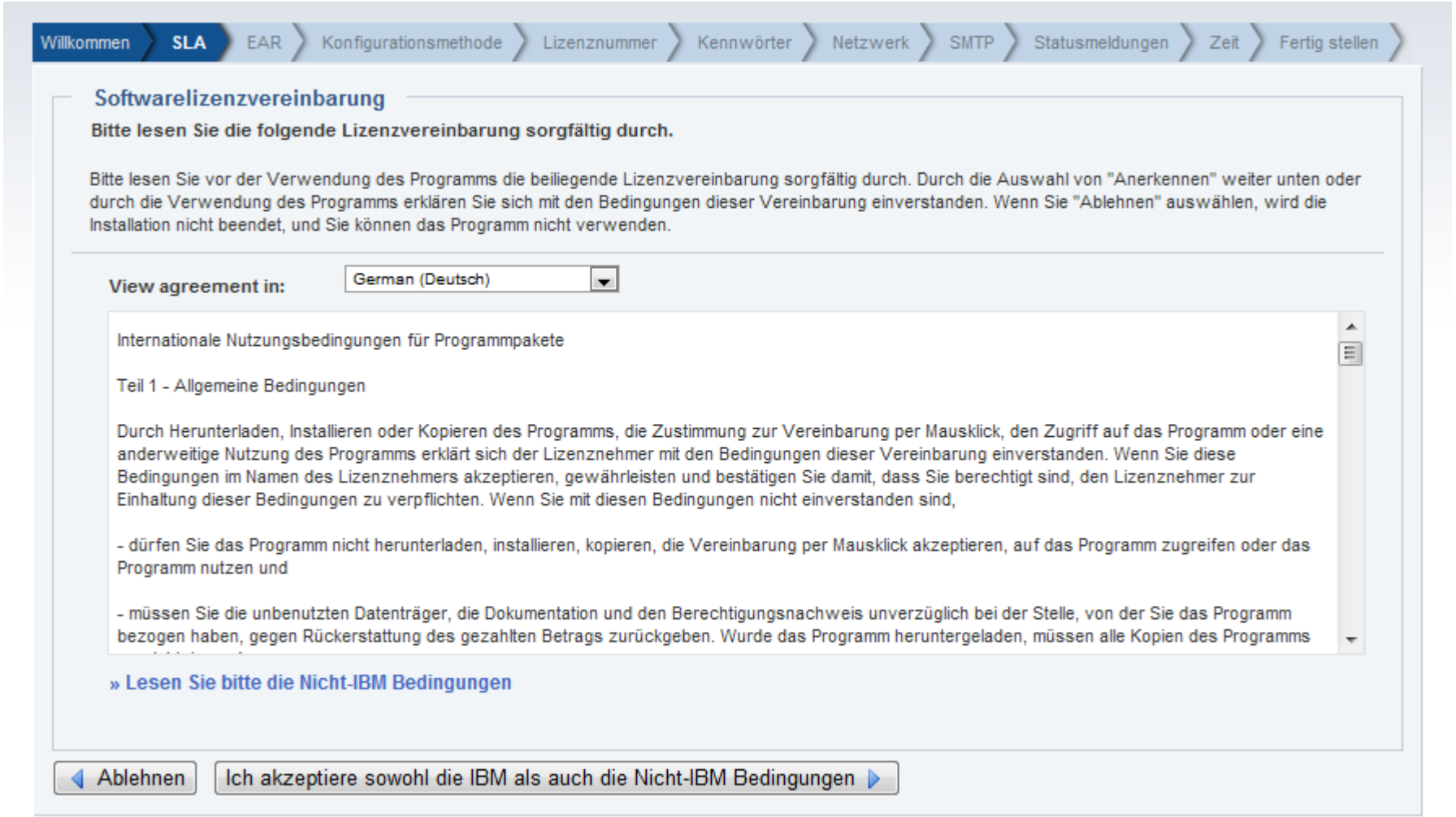
Weiter geht’s im Browser



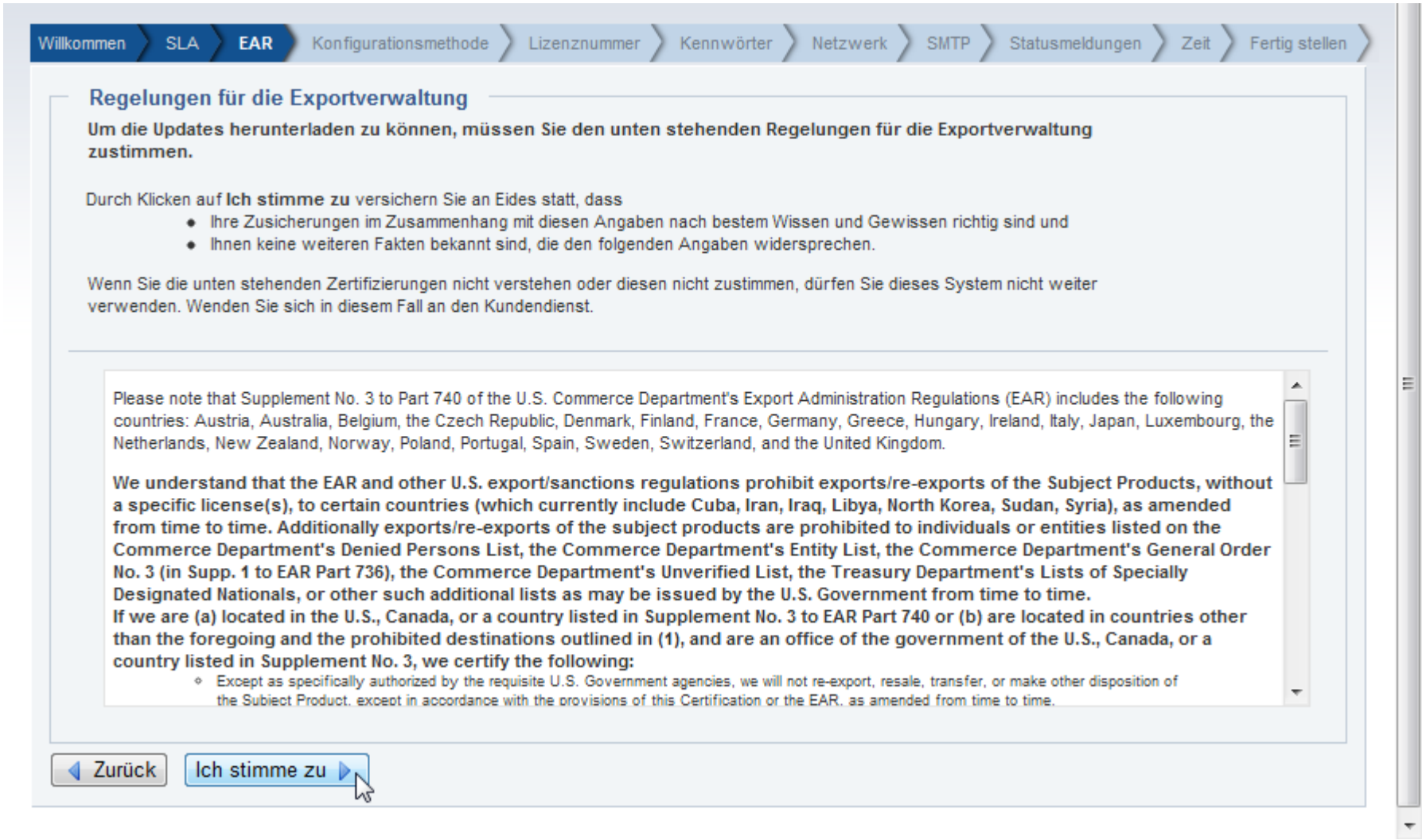
Erstkonfiguration



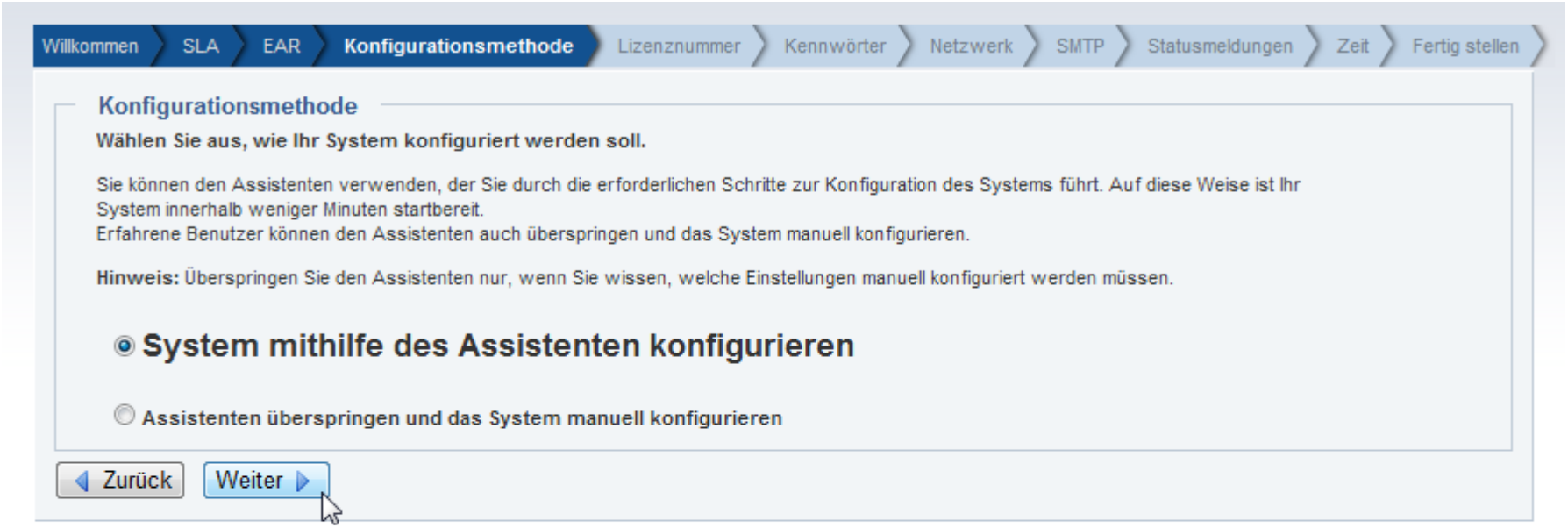
Erstkonfiguration



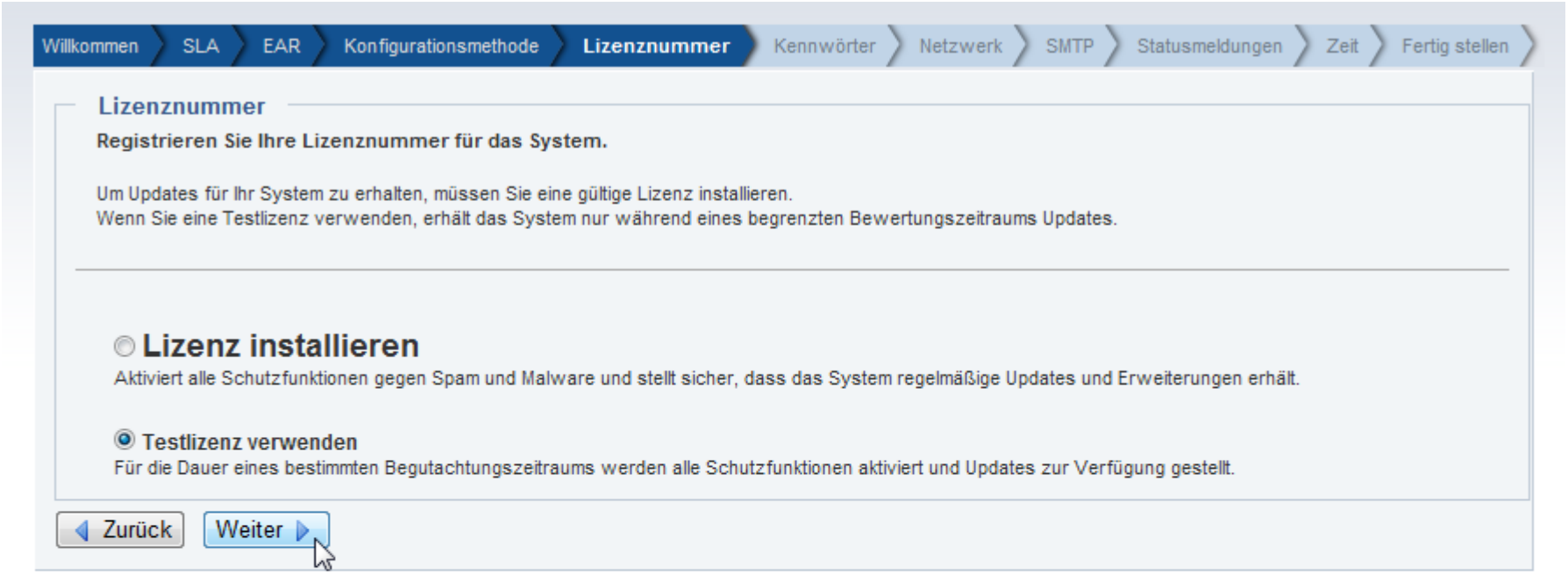
Erstkonfiguration



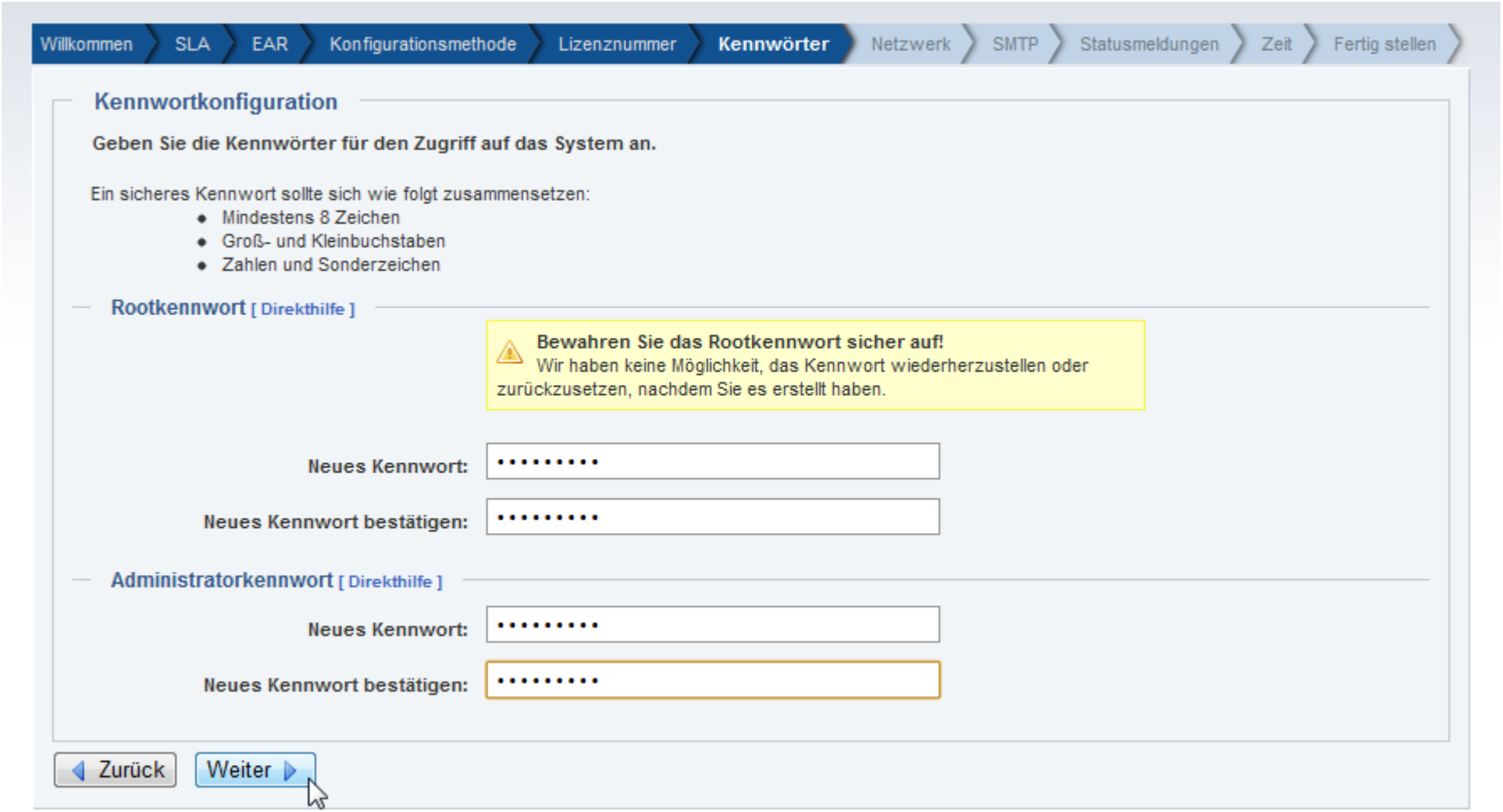
Erstkonfiguration

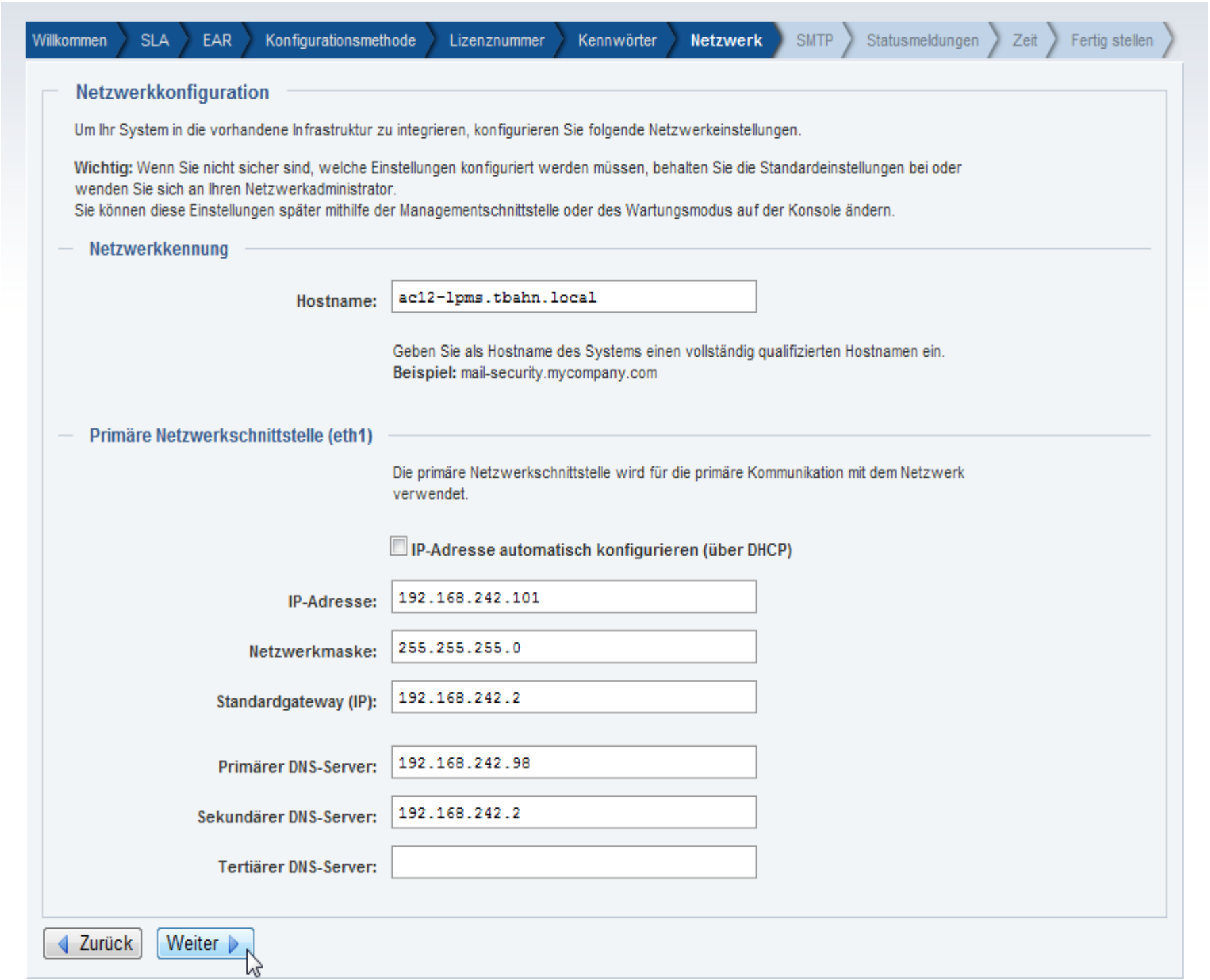


Erstkonfiguration



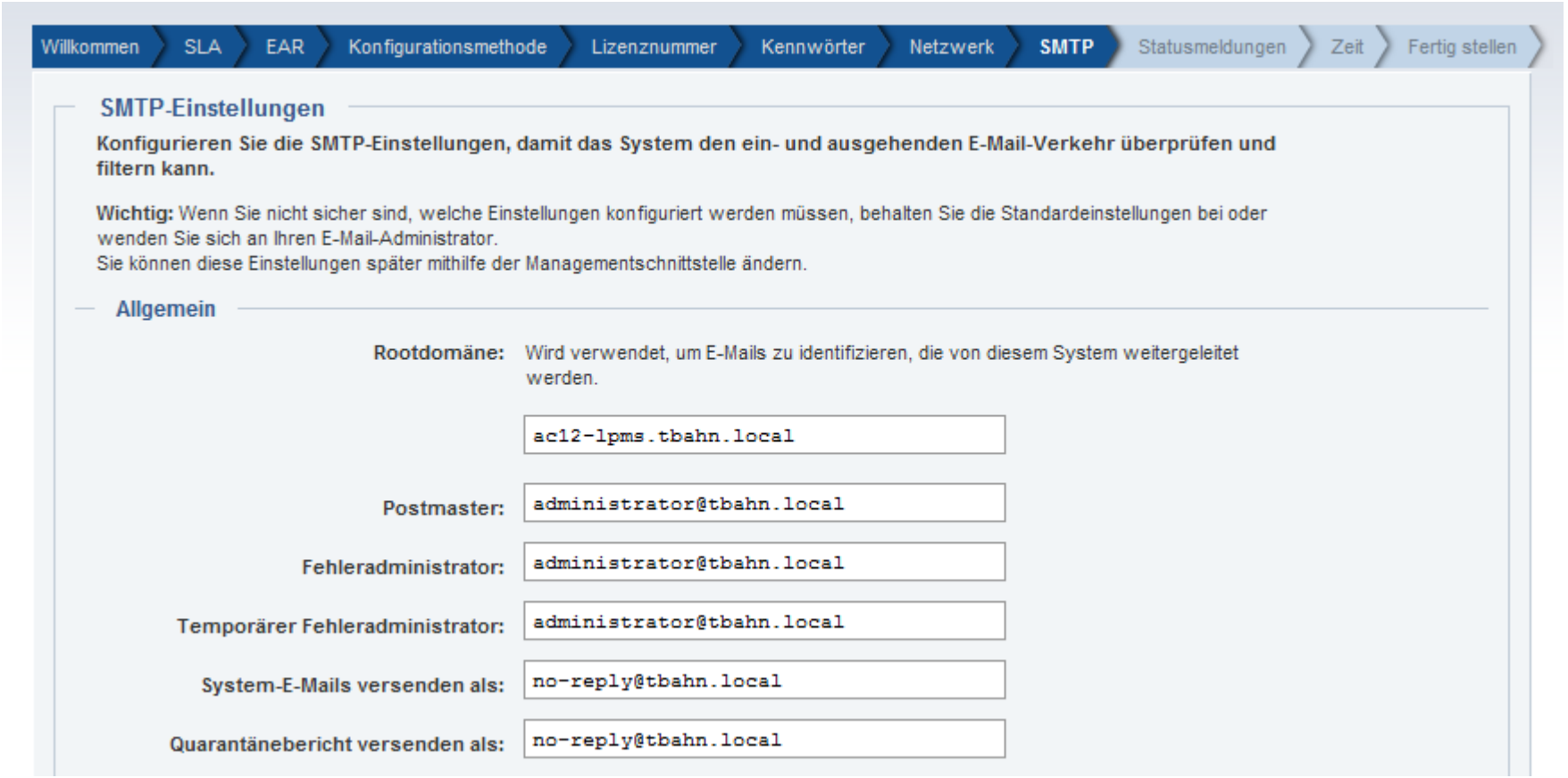
Erstkonfiguration



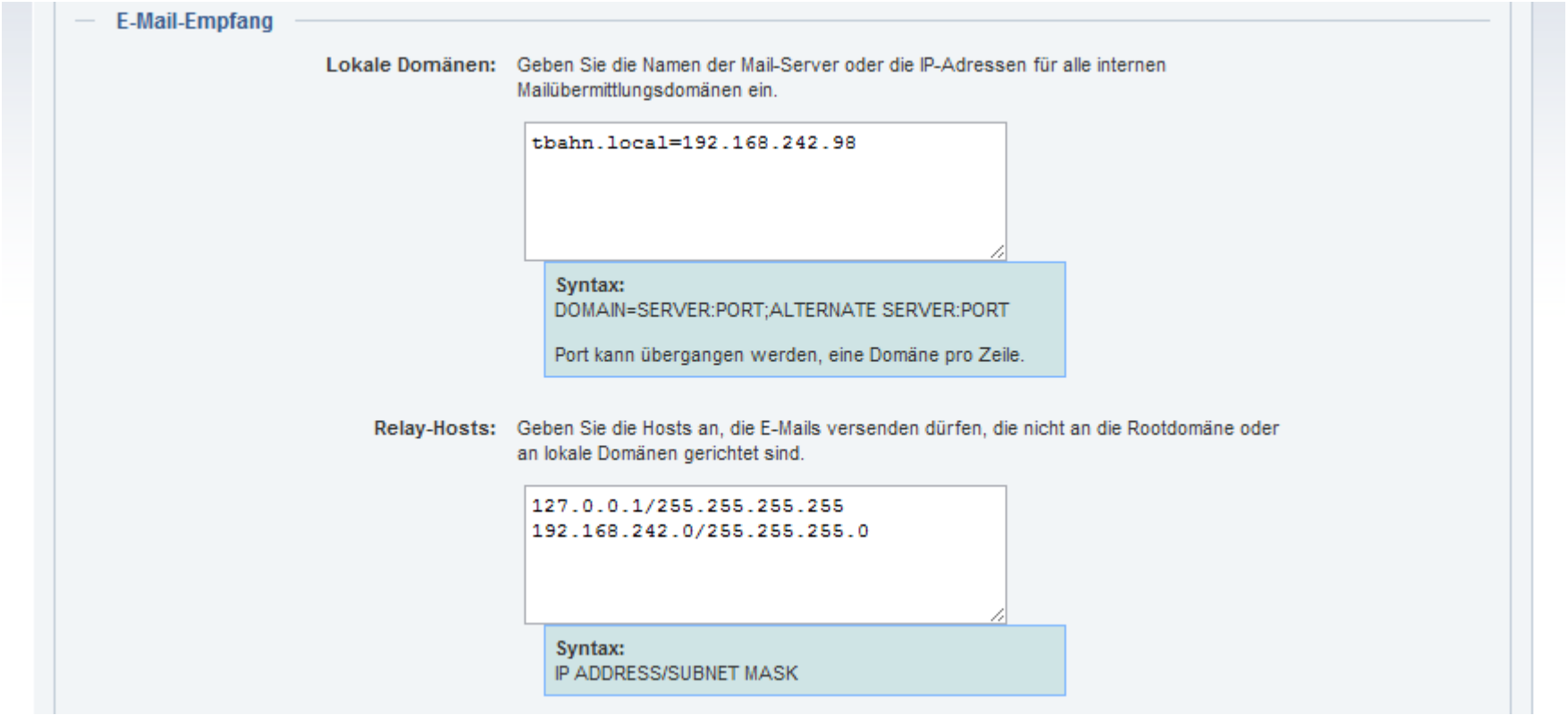

Willkommen
SLA
EAR
Konfigurationsmethode
Lizenznummer
Kennwörter
Netzwerk
SMTP
Statusmeldungen
Zeit
Fertig stellen
Netzwerkkonfiguration
Um Ihr System in die vorhandene Infrastruktur zu integrieren, konfigurieren Sie folgende Netzwerkeinstellungen.
Wichtig: Wenn Sie nicht sicher sind, welche Einstellungen konfiguriert werden müssen, behalten Sie die Standardeinstellungen bei oder wenden Sie sich an Ihren Netzwerkadministrator.
Sie können diese Einstellungen später mithilfe der Managementschnittstelle oder des Wartungsmodus auf der Konsole ändern.
Netzwerkkennung
Hostname:
ac12-lpms.tbahn.local
Geben Sie als Hostname des Systems einen vollständig qualifizierten Hostnamen ein.
Beispiel: mail-security.mycompany.com
Primäre Netzwerkschnittstelle (eth1)
Die primäre Netzwerkschnittstelle wird für die primäre Kommunikation mit dem Netzwerk verwendet.
IP-Adresse automatisch konfigurieren (über DHCP)
IP-Adresse:
192.168.242.101
Netzwerkmaske:
255.255.255.0
Standardgateway (IP):
192.168.242.2
Primärer DNS-Server:
192.168.242.98
Sekundärer DNS-Server:
192.168.242.2
Tertiärer DNS-Server:
Zurück
Weiter

Erstkonfiguration

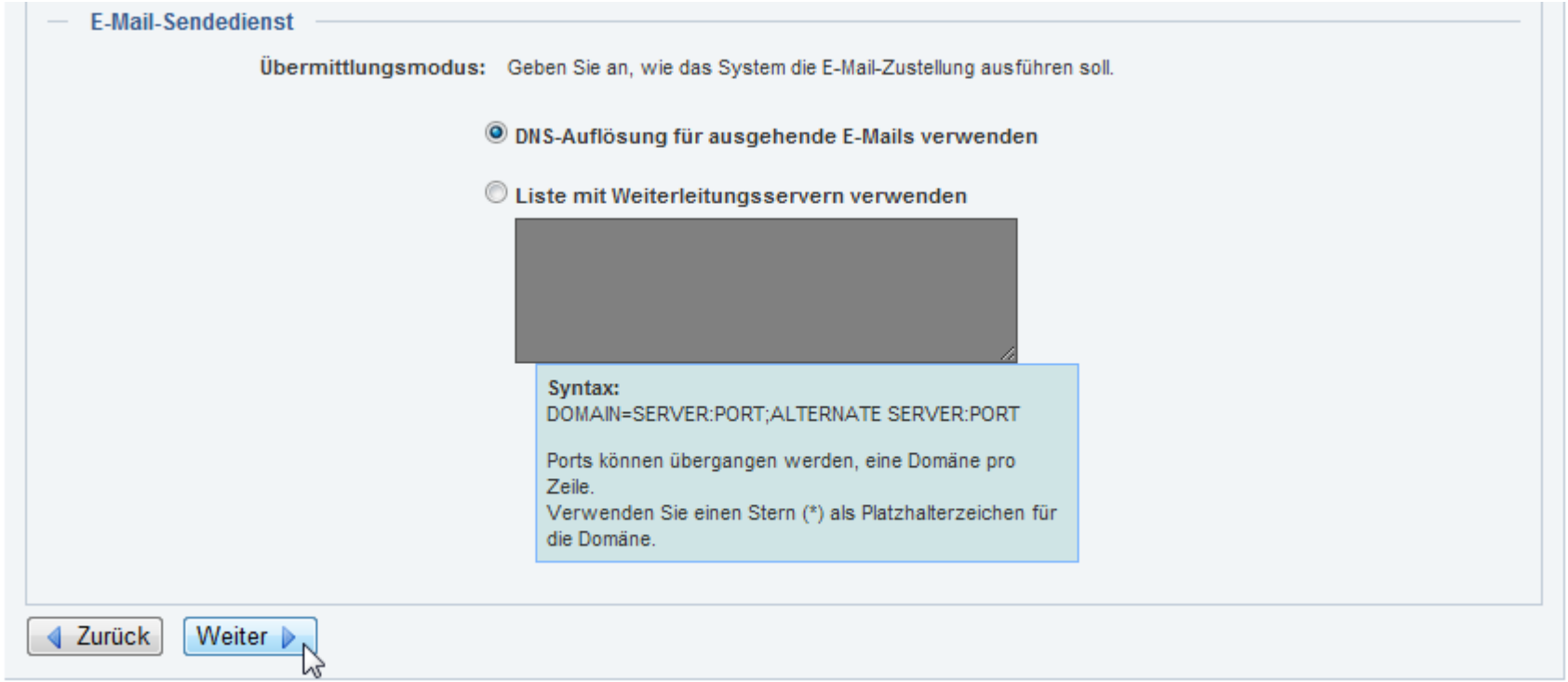
Erstkonfiguration



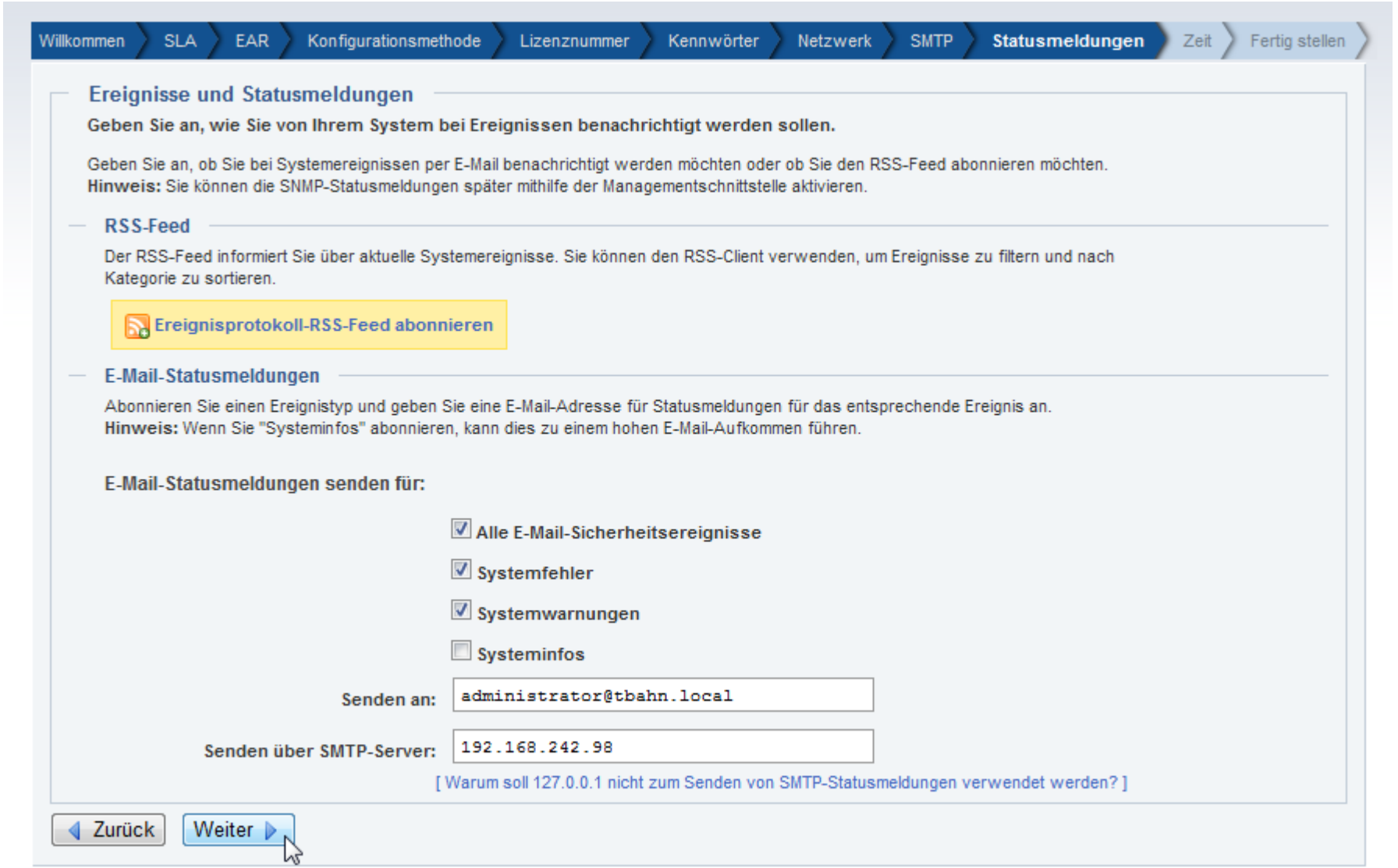
Erstkonfiguration



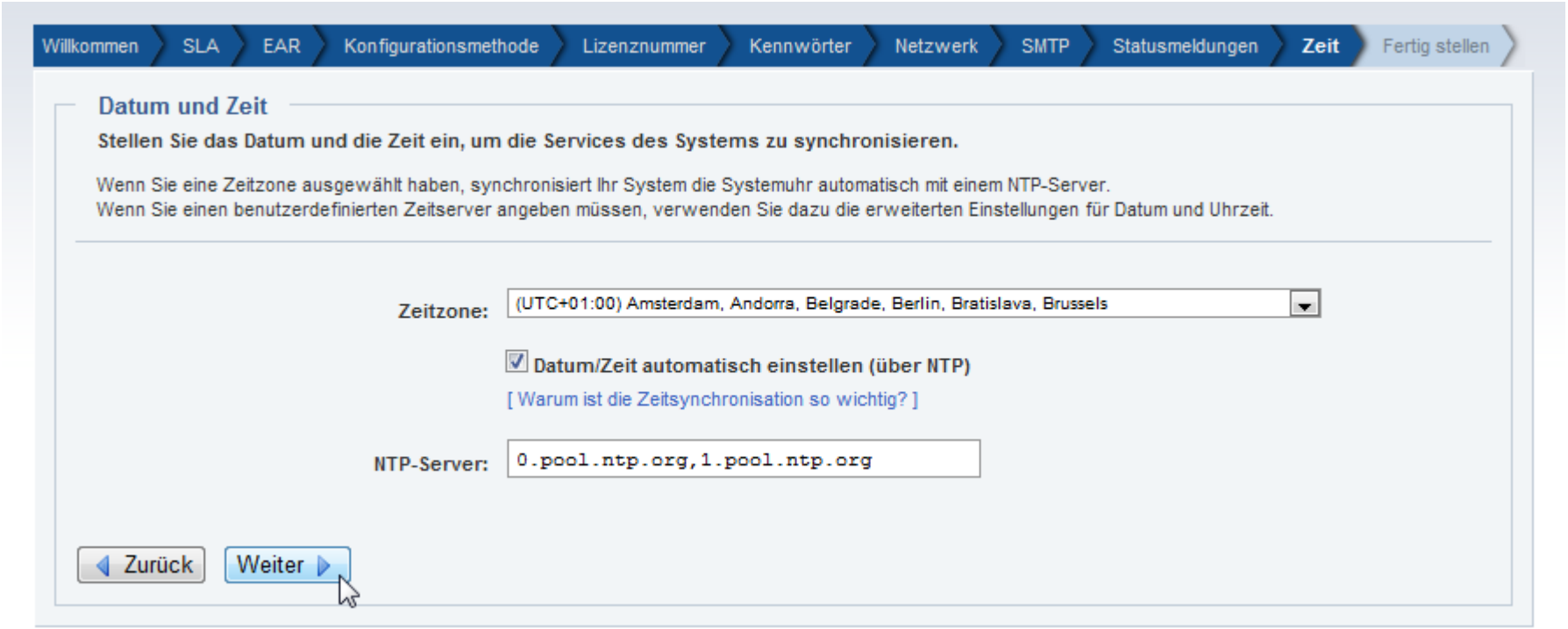
Erstkonfiguration



Erstkonfiguration

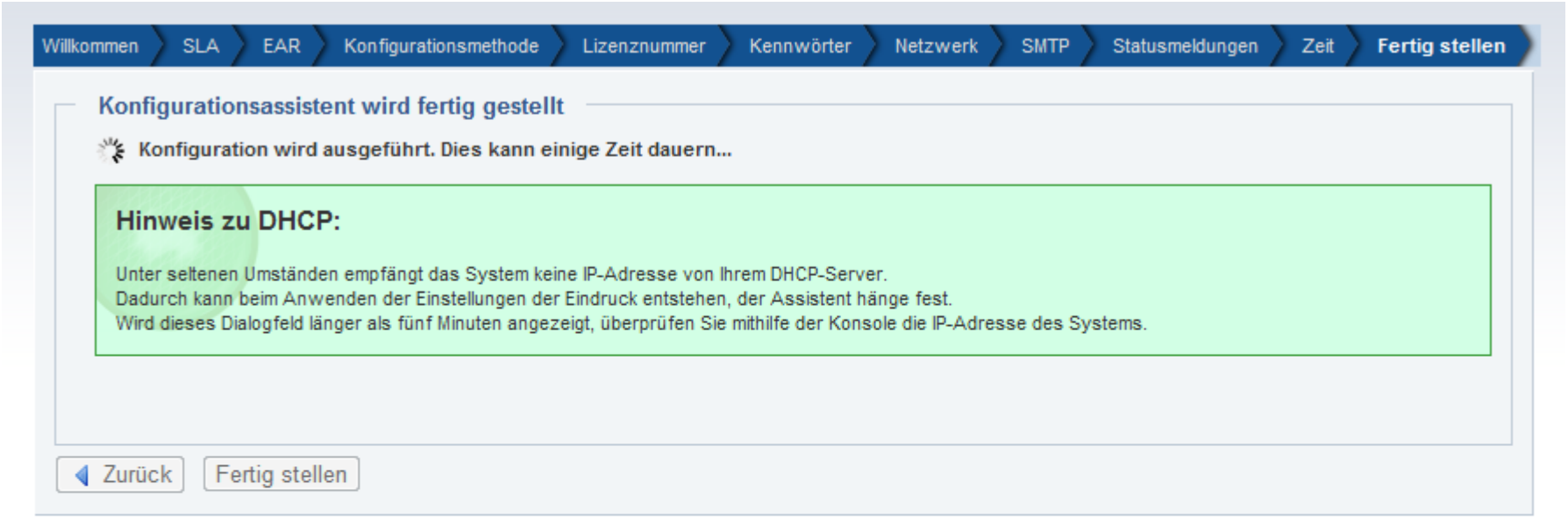


Erstkonfiguration

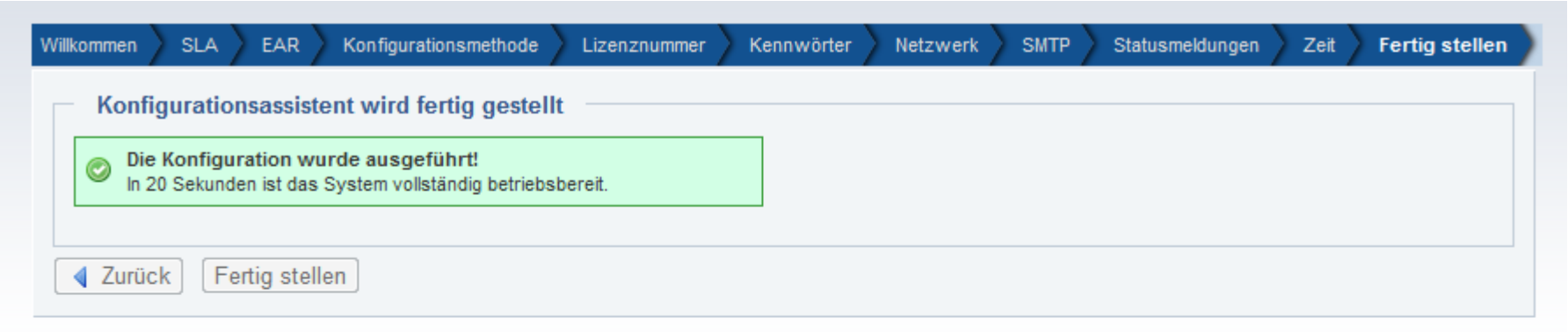


Erstkonfiguration

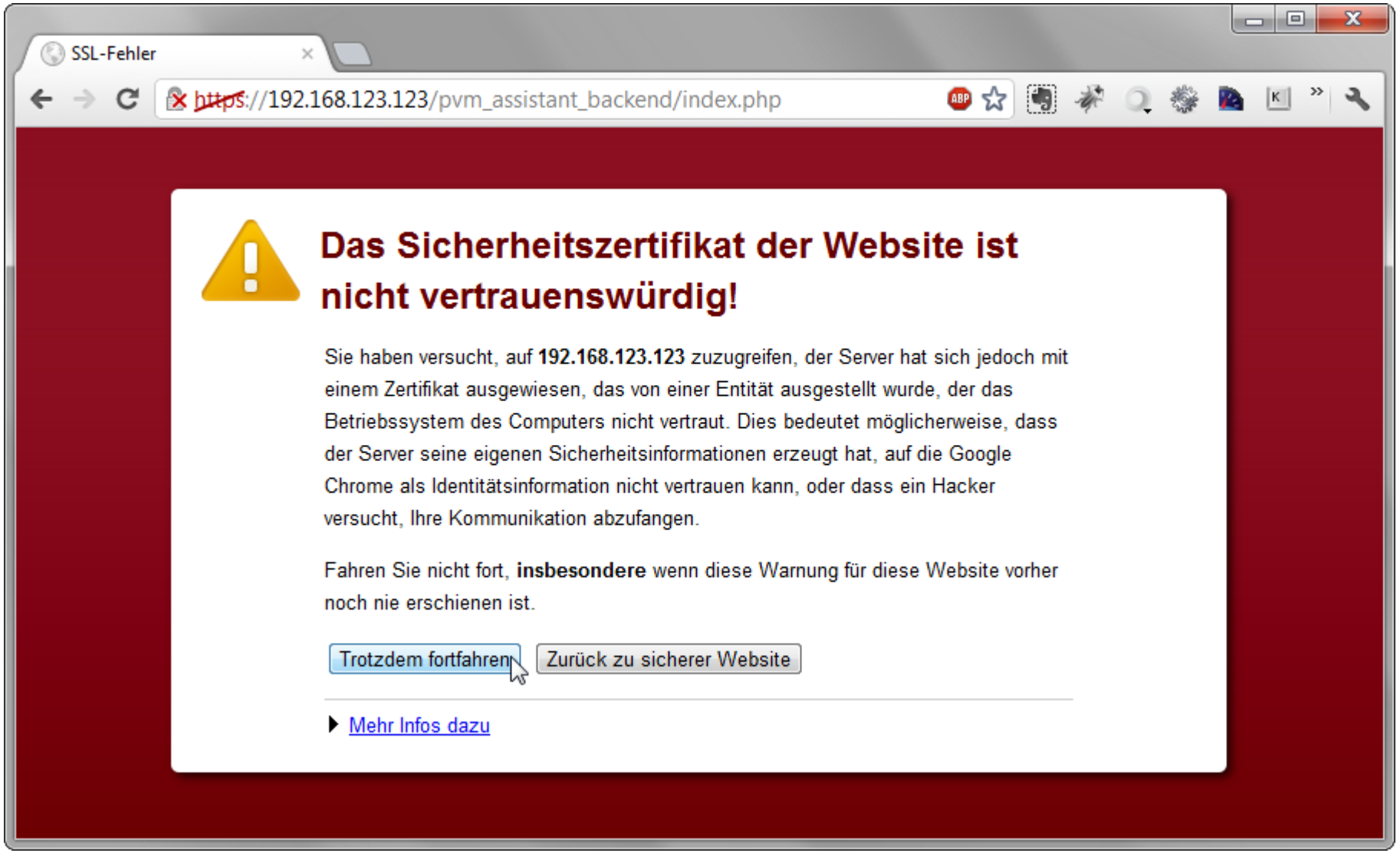
Erstkonfiguration



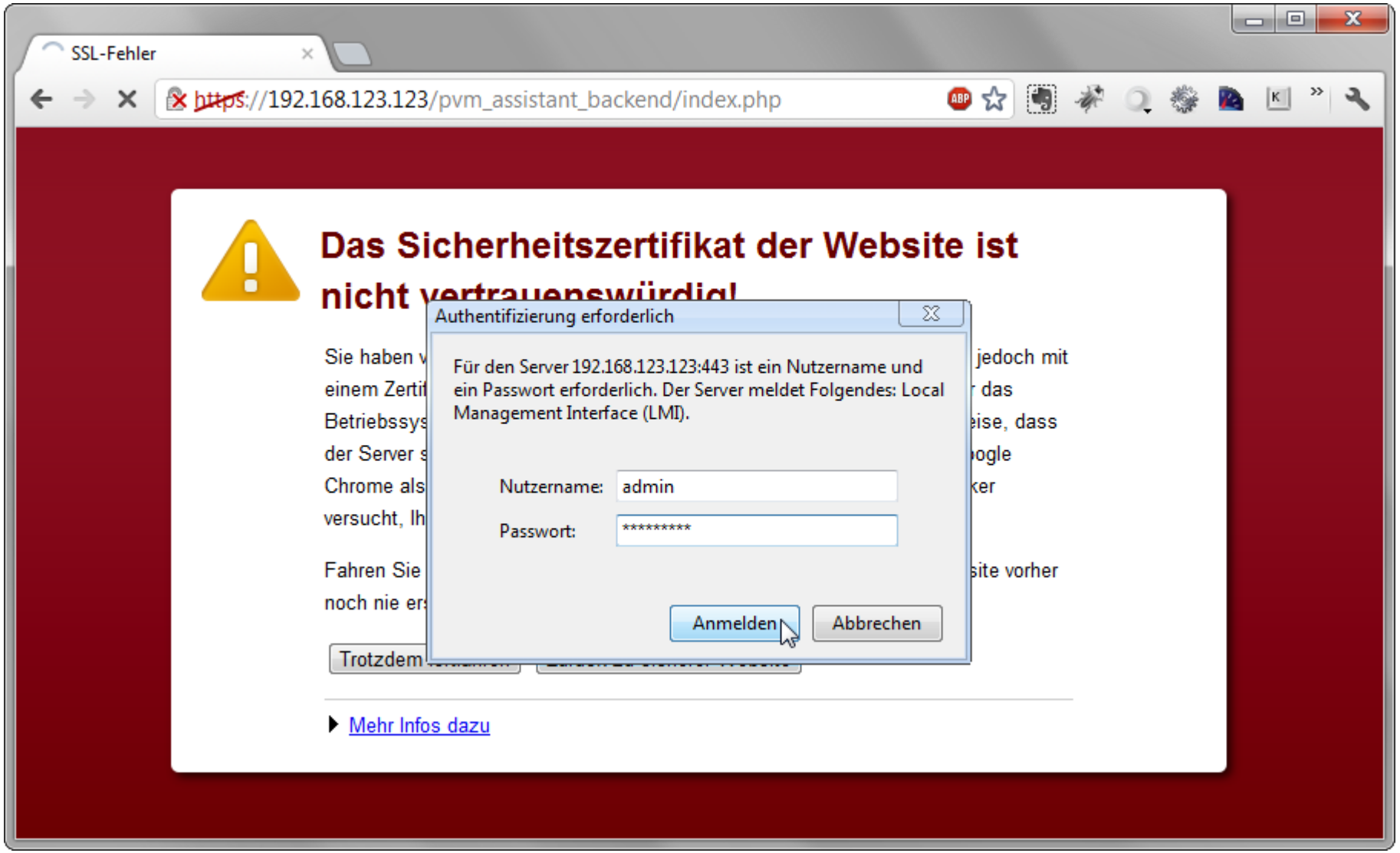
Erstkonfiguration



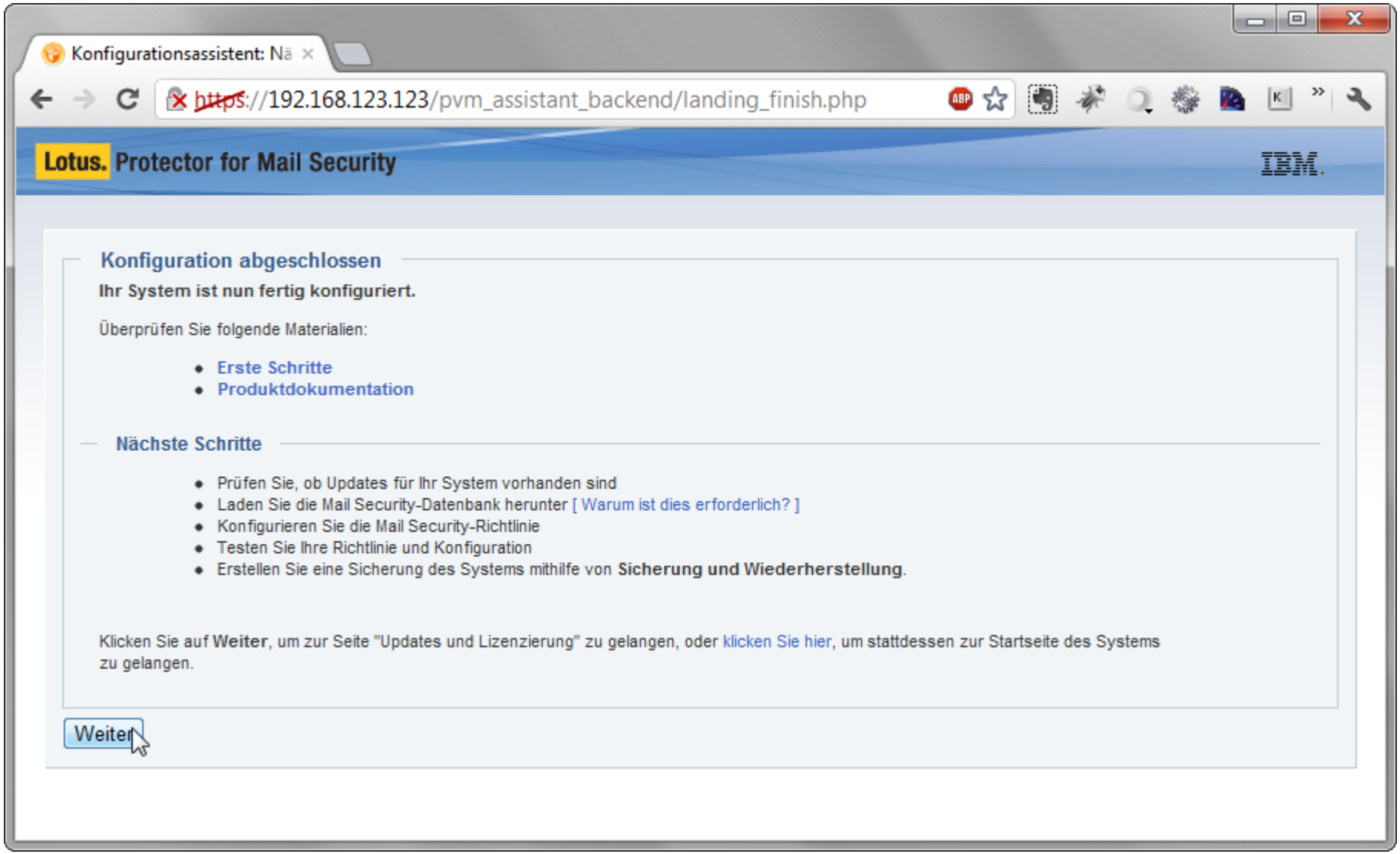
Noch einmal im Browser



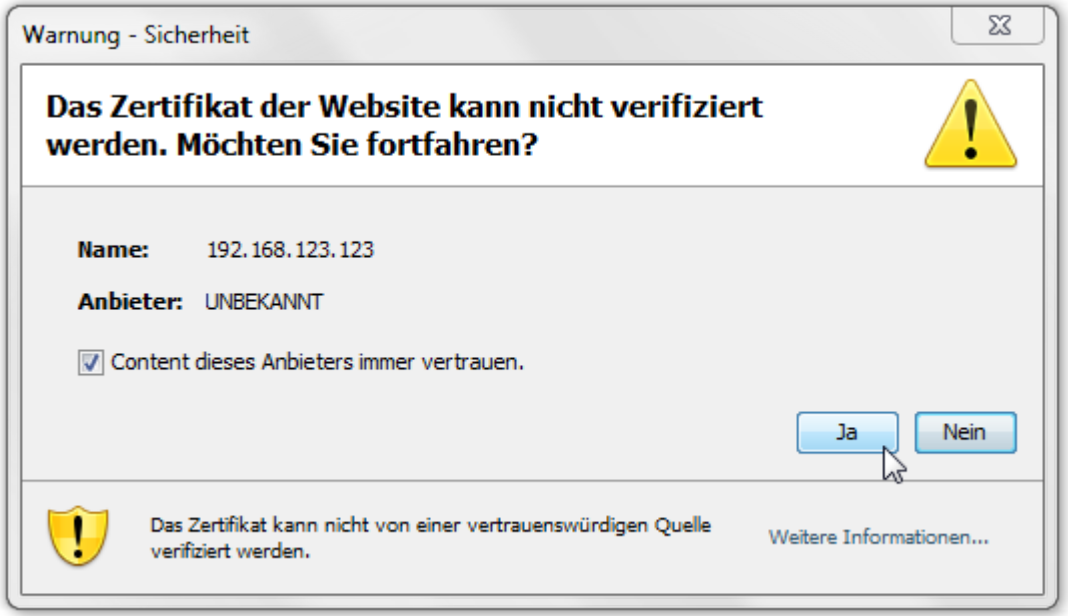
Noch einmal im Browser



Abschluss der Erstkonfiguration

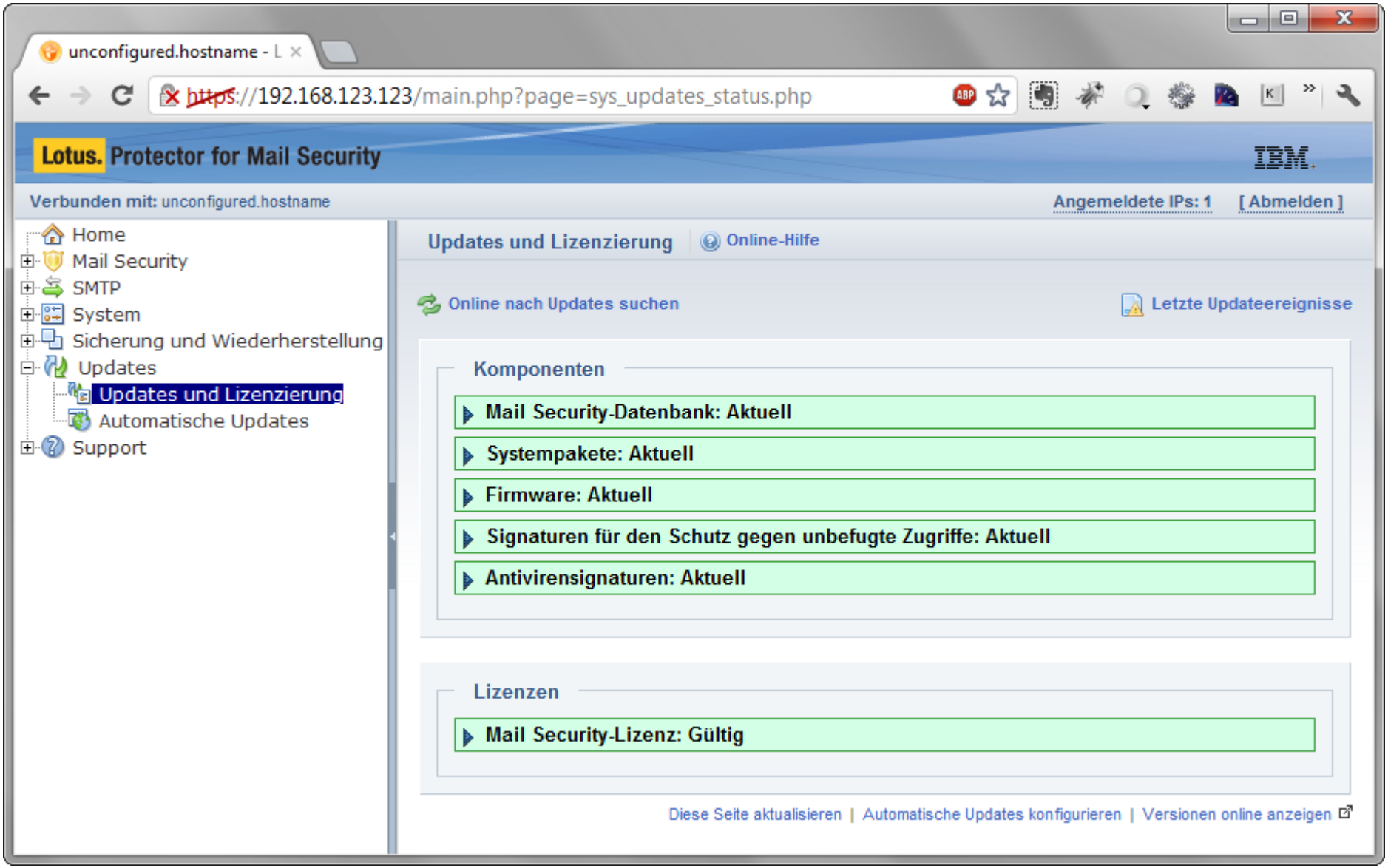


Benutzeroberfläche verwendet Java

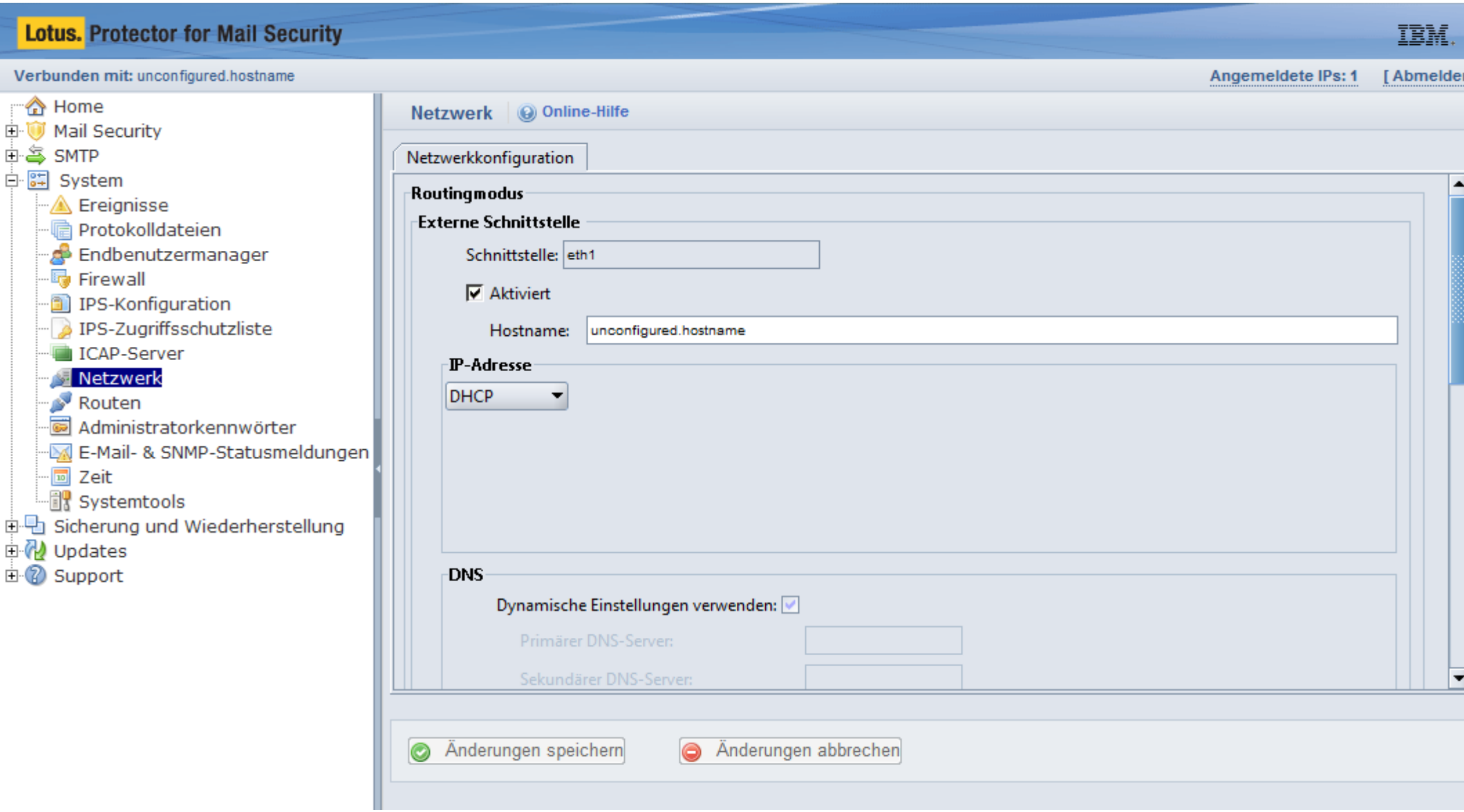


Benutzeroberfläche verwendet Java

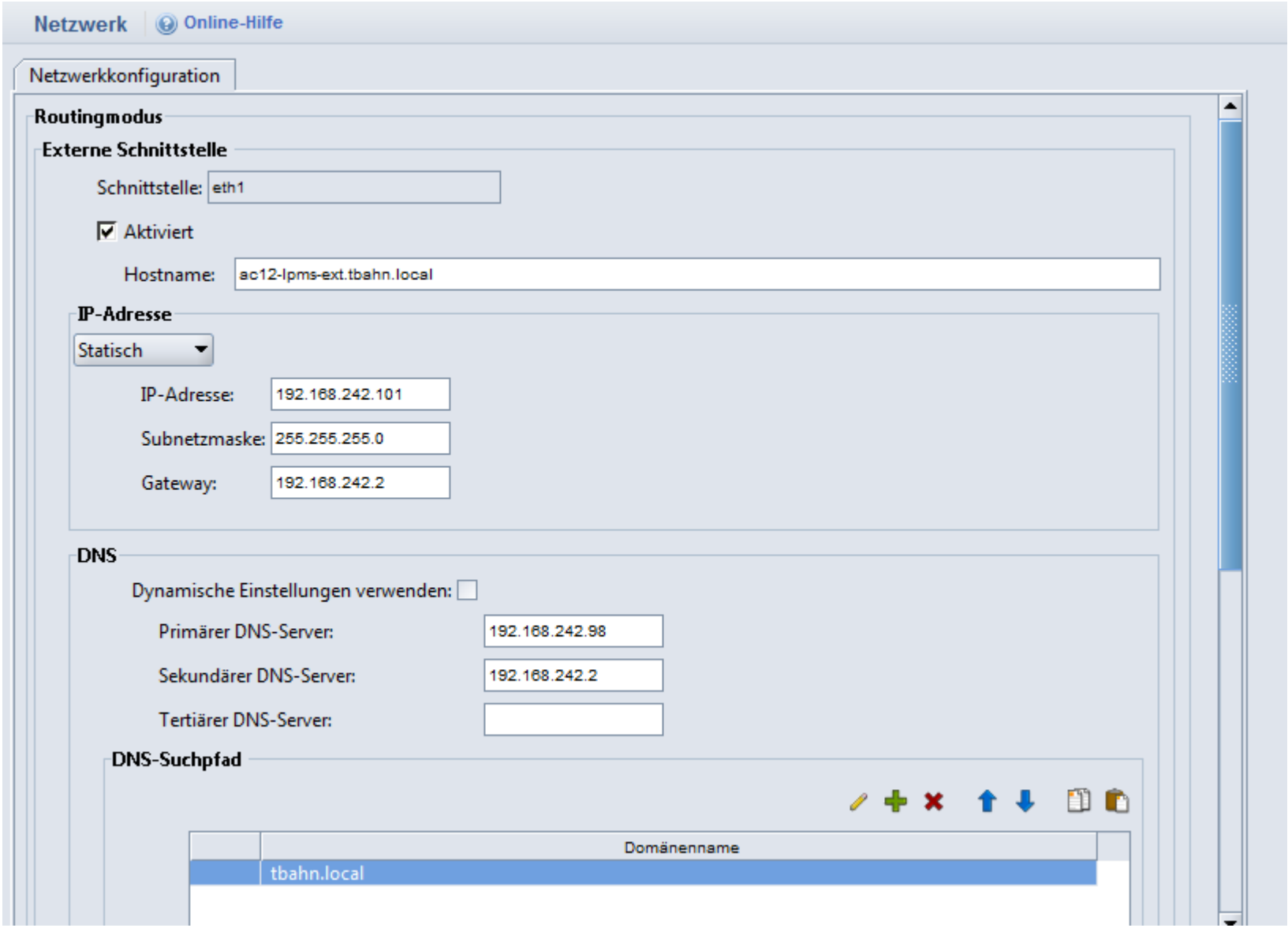
Alles im grünen Bereich…



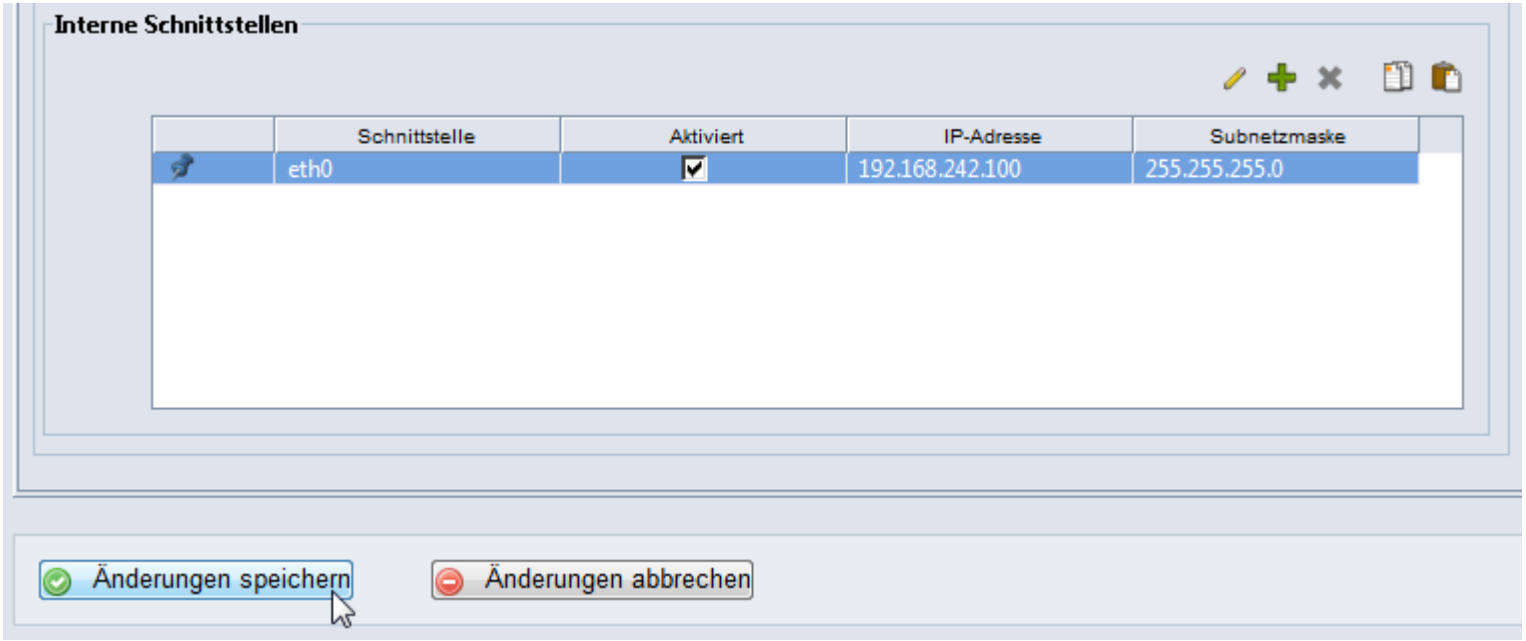
Netzwerkkonfiguration



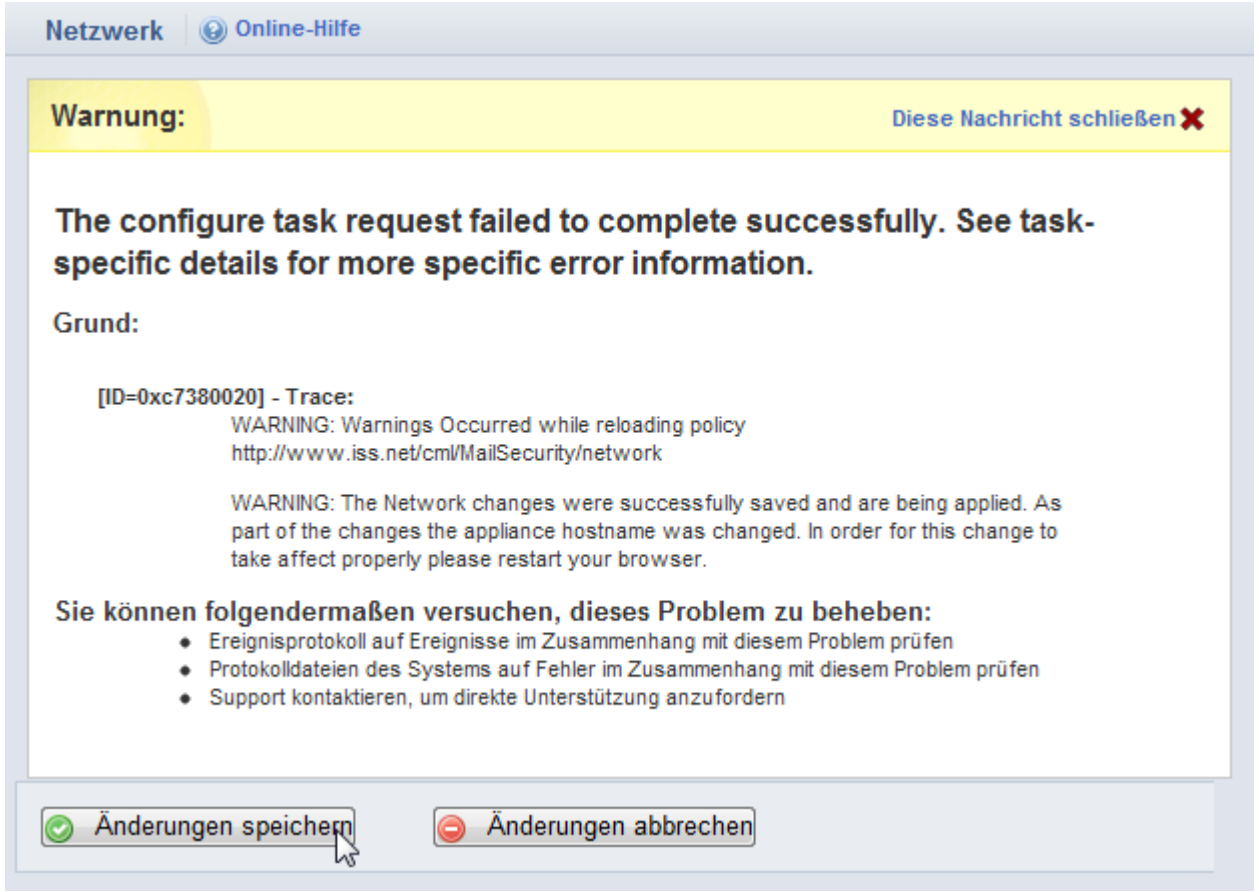
Netzwerkkonfiguration



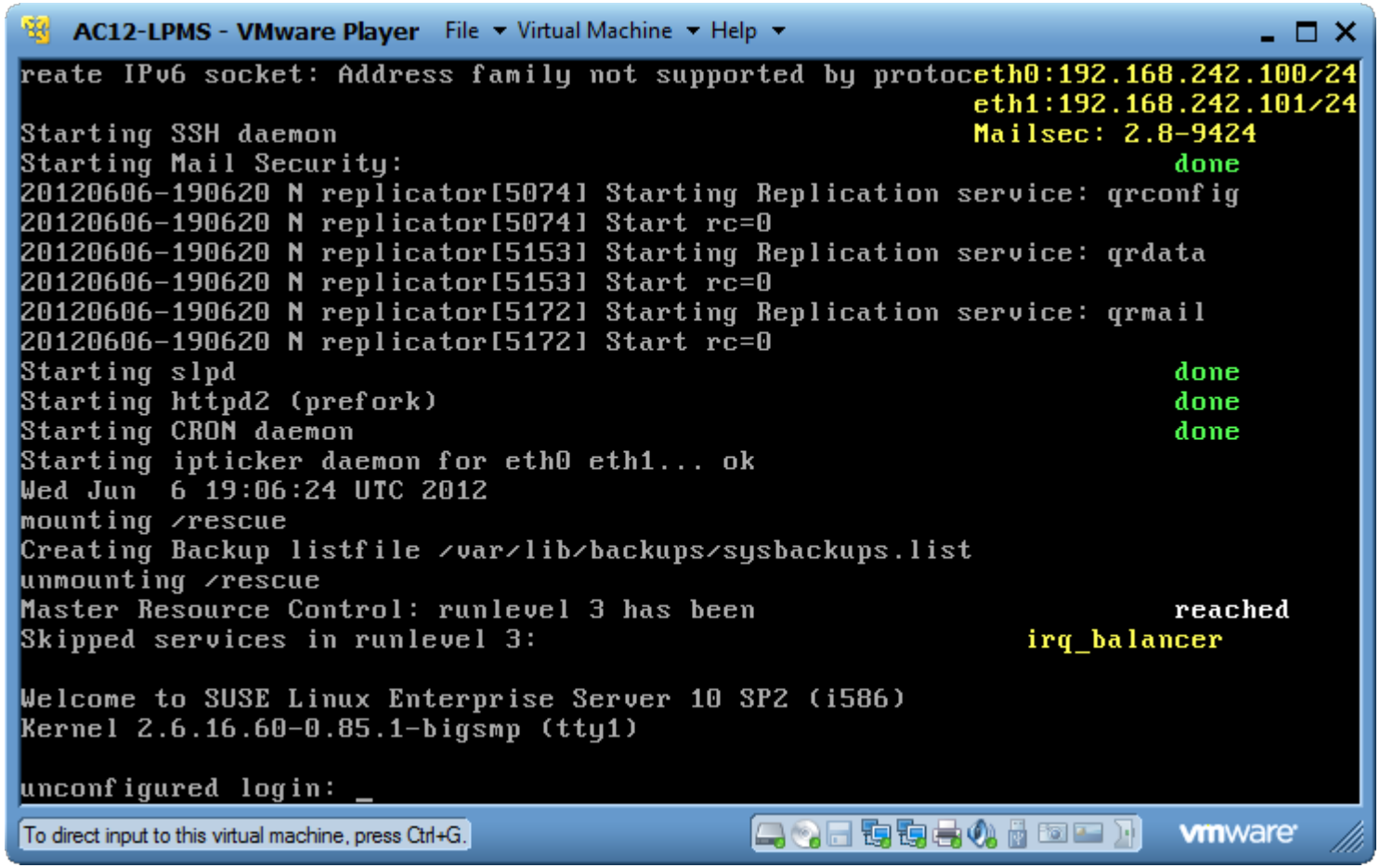
Netzwerkkonfiguration



Netzwerkkonfiguration



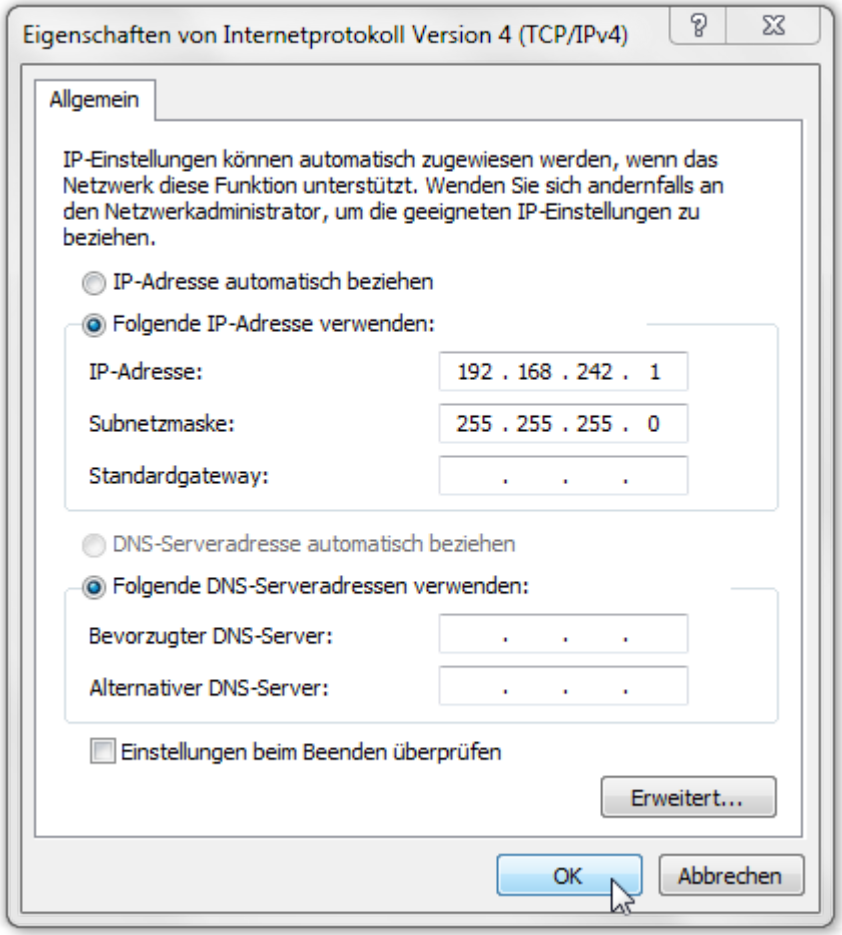
Netzwerkkonfiguration



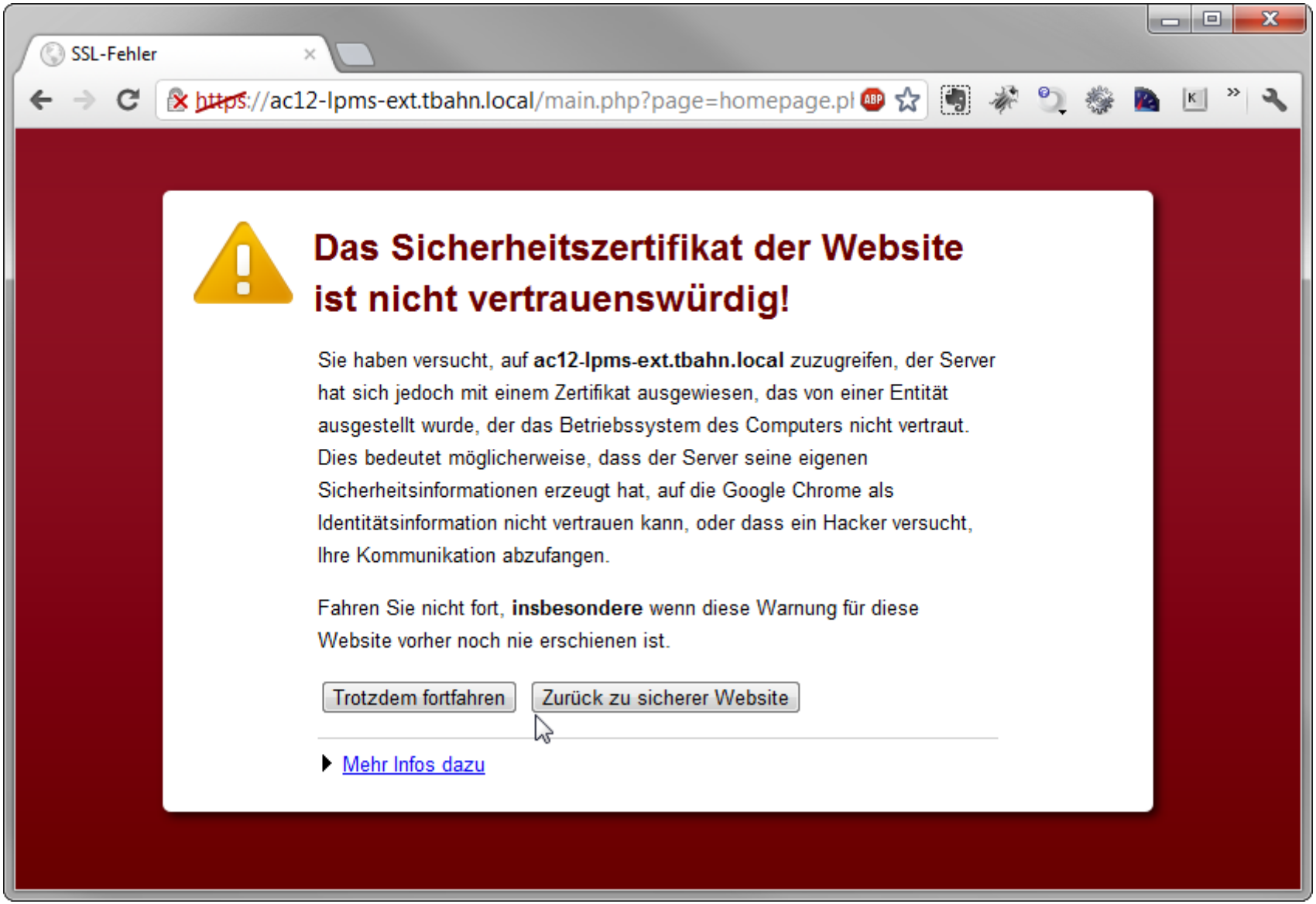
Änderungen über Konsole oder SSH

- Nur-Lesen unproblematisch
- Änderungen bewirken Garantieverlust, außer wenn
  - autorisiert vom IBM Support
  - durchgeführt von IBM Partner, Reseller oder internen Mitarbeiter
  - dokumentiert in Textdatei /root/lib/customization
- Bei Problemen kann IBM fordern, die Änderungen rückgängig zu machen

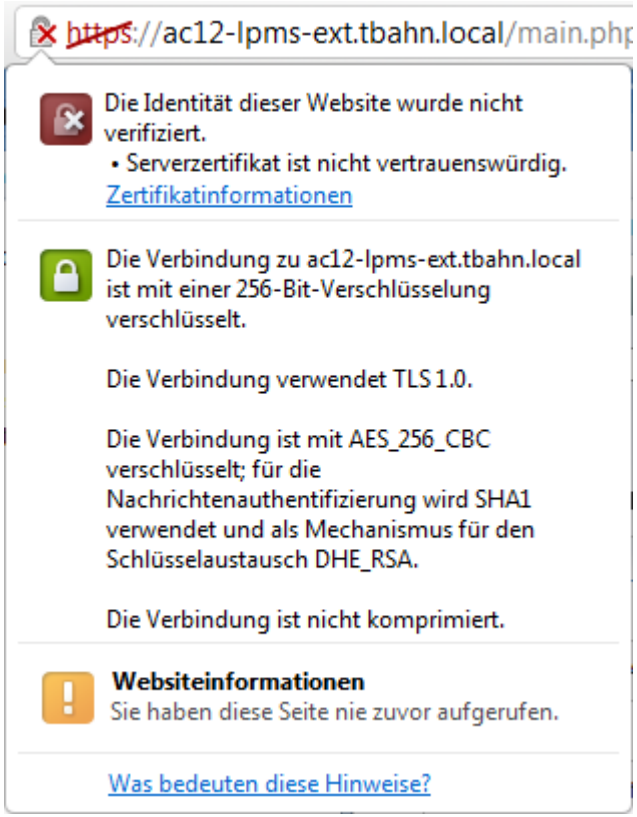
Netzwerk-Einstellungen des Clients wiederherstellen



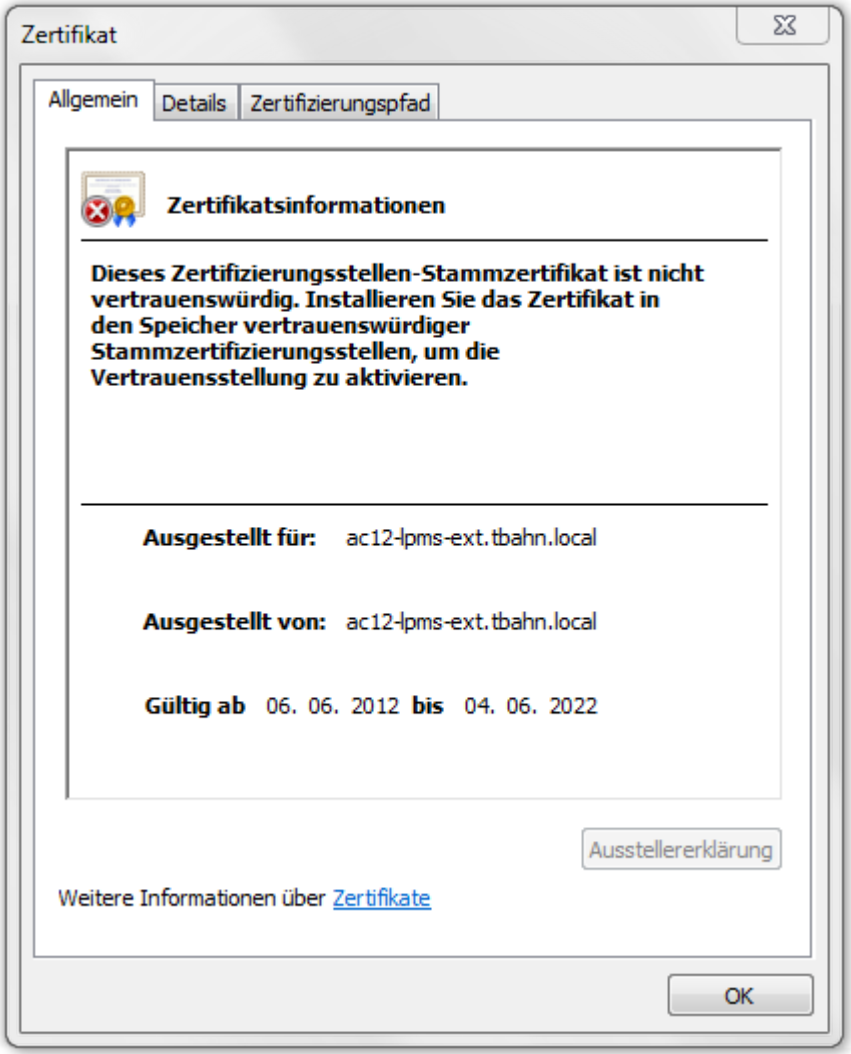
Warnung wegen des SSL-Zertifikats



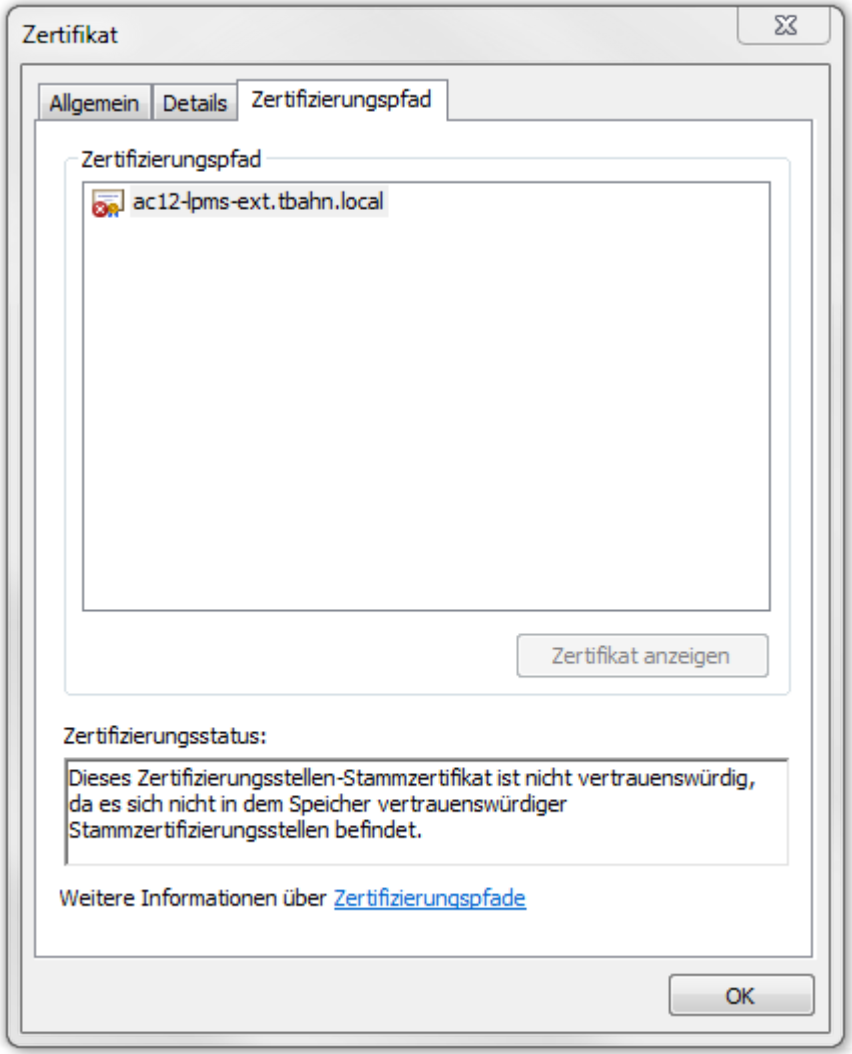
Warnung wegen des SSL-Zertifikats



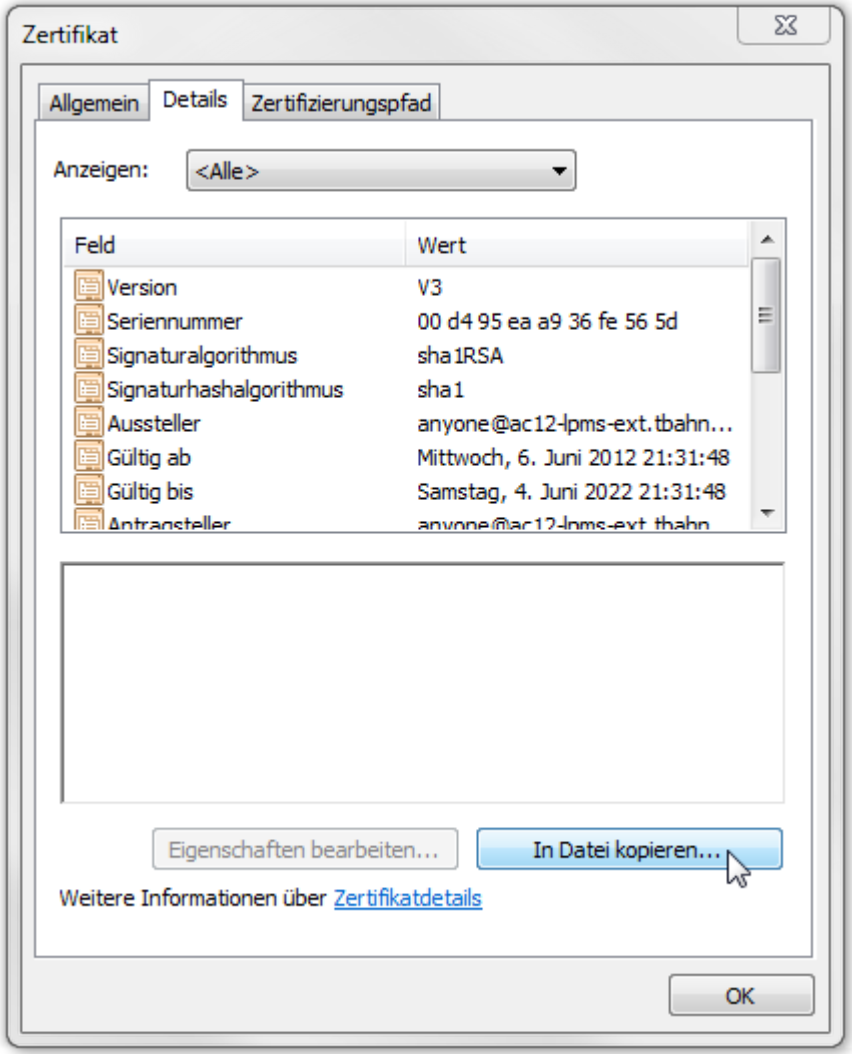
Warnung wegen des SSL-Zertifikats



Warnung wegen des SSL-Zertifikats

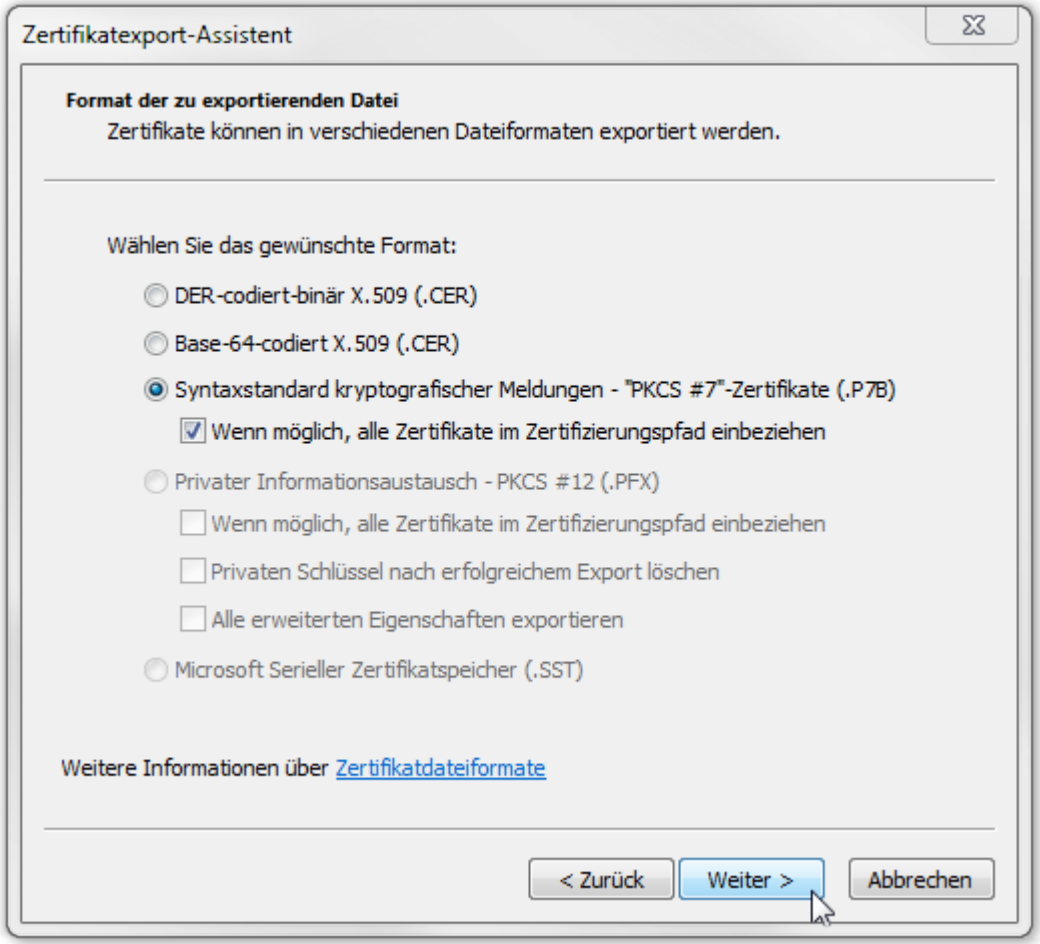


Warnung wegen des SSL-Zertifikats

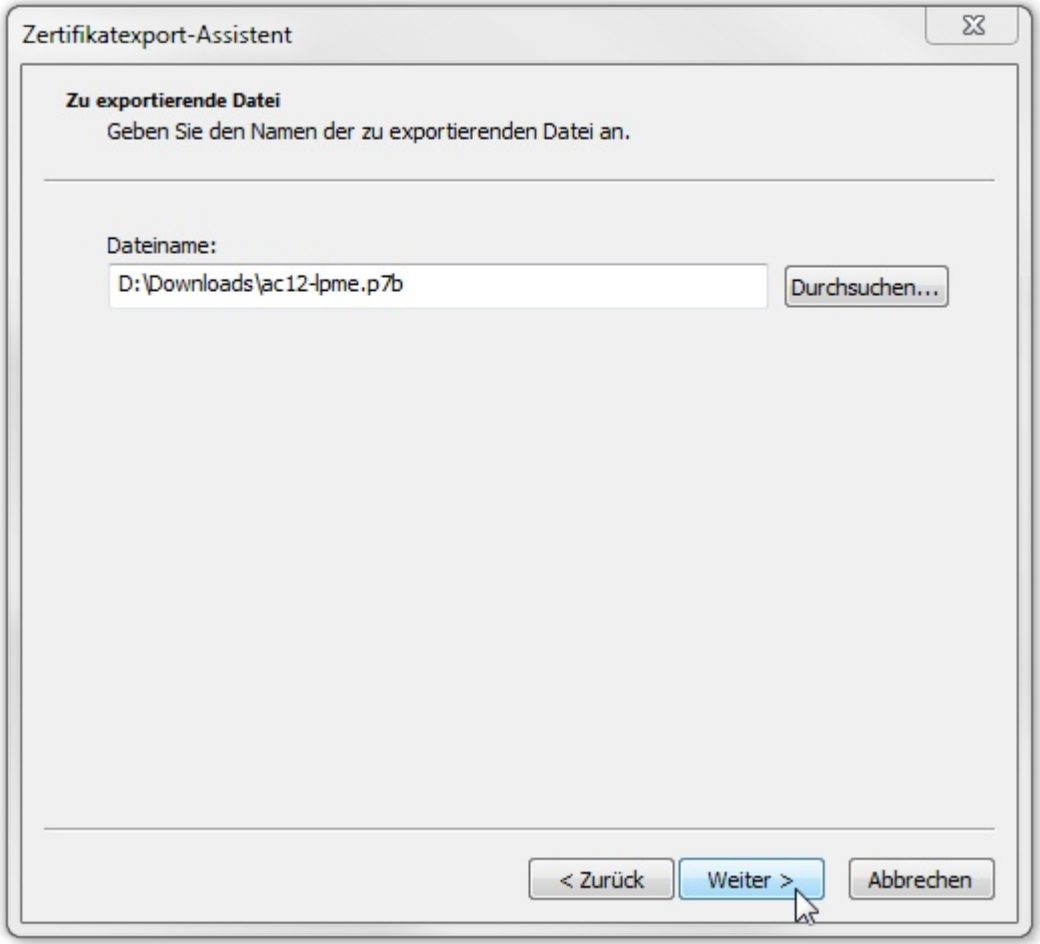


Warnung wegen des SSL-Zertifikats

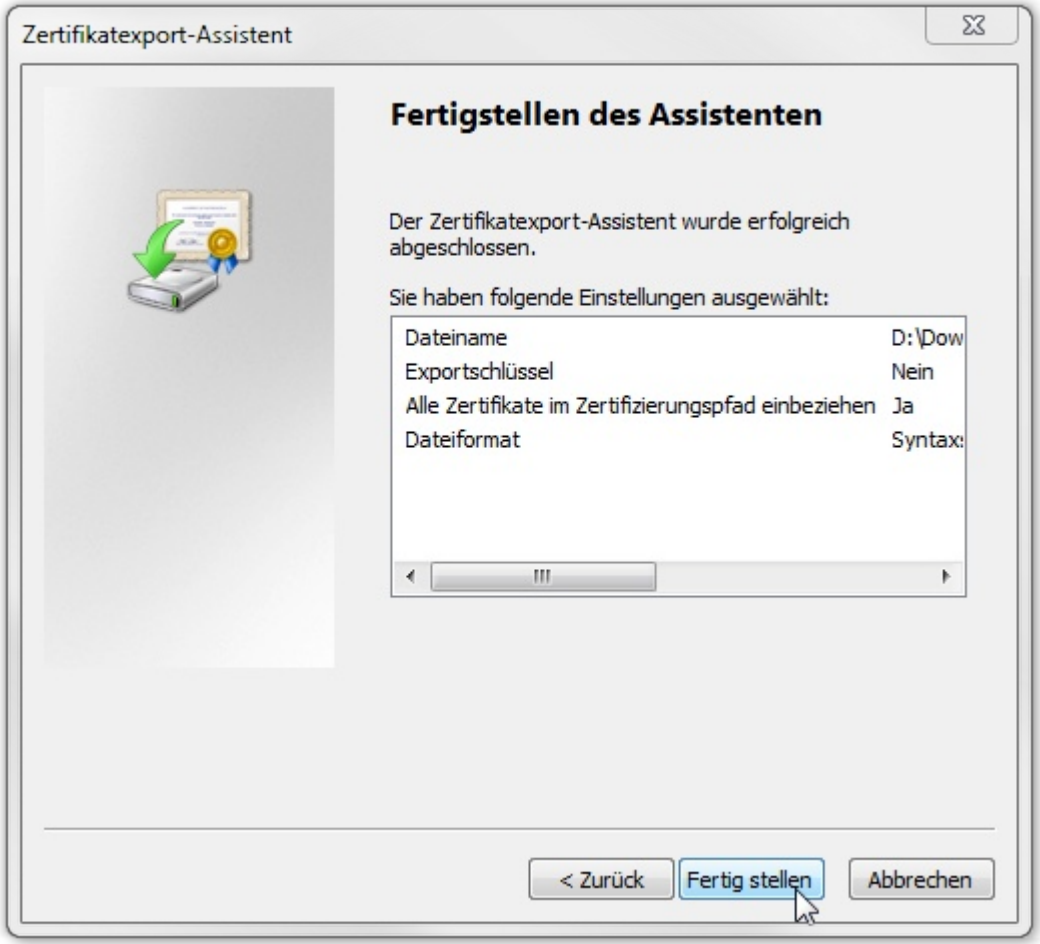
Warnung wegen des SSL-Zertifikats



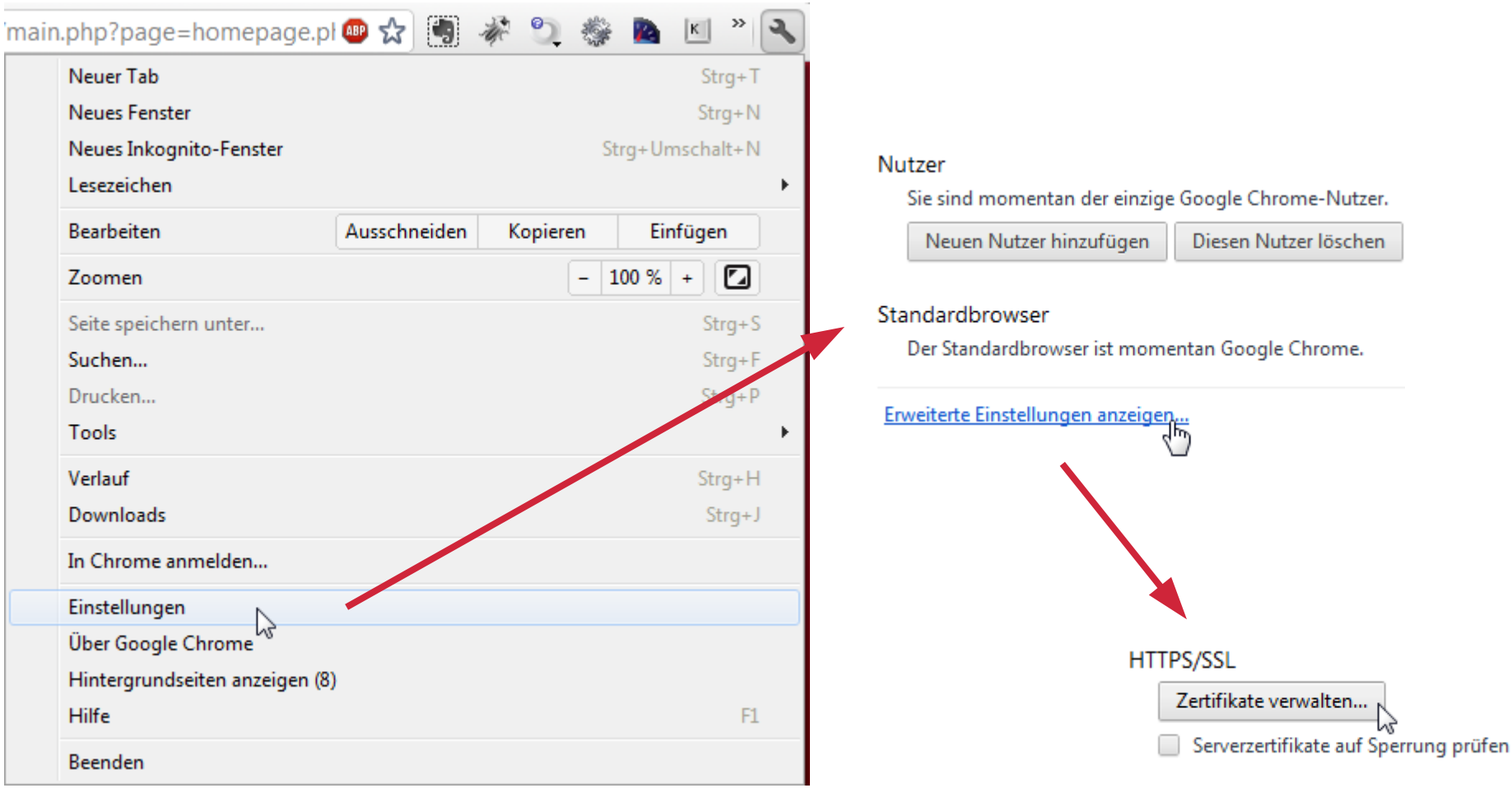
Warnung wegen des SSL-Zertifikats



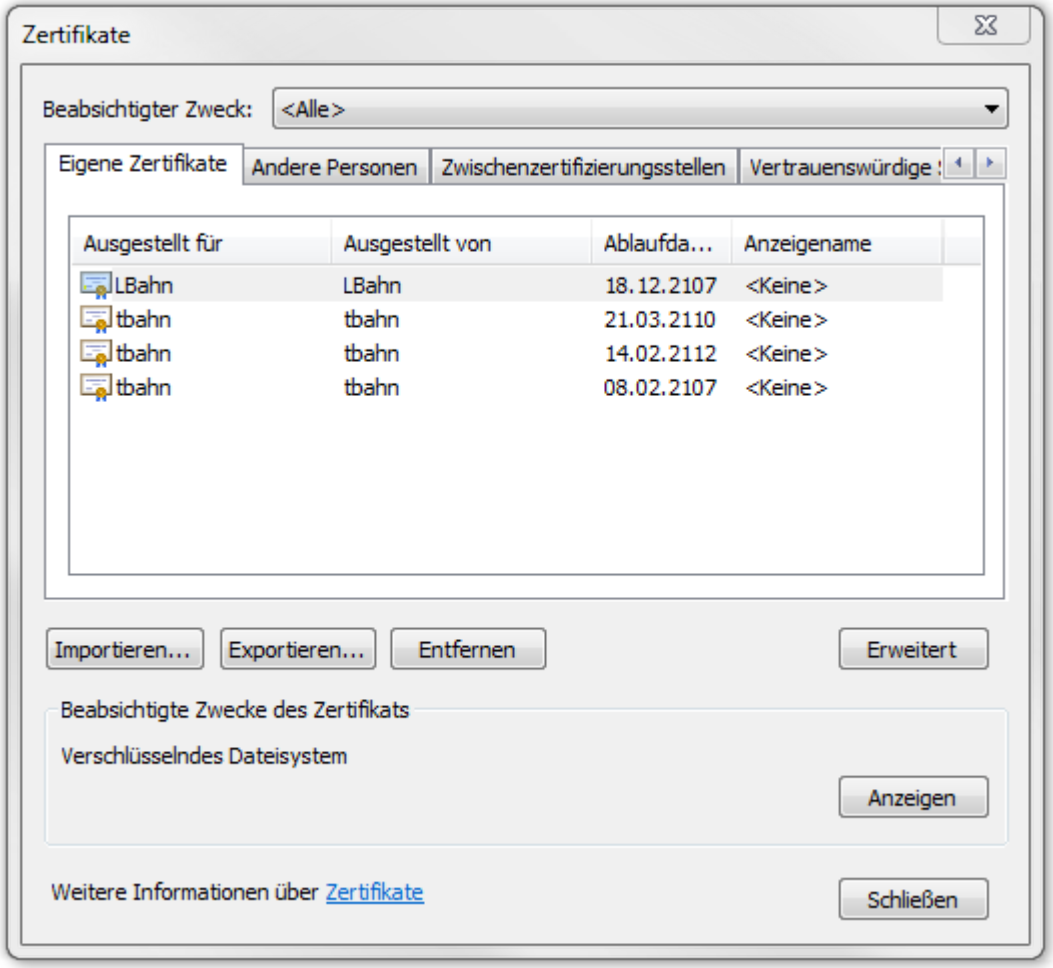
Warnung wegen des SSL-Zertifikats



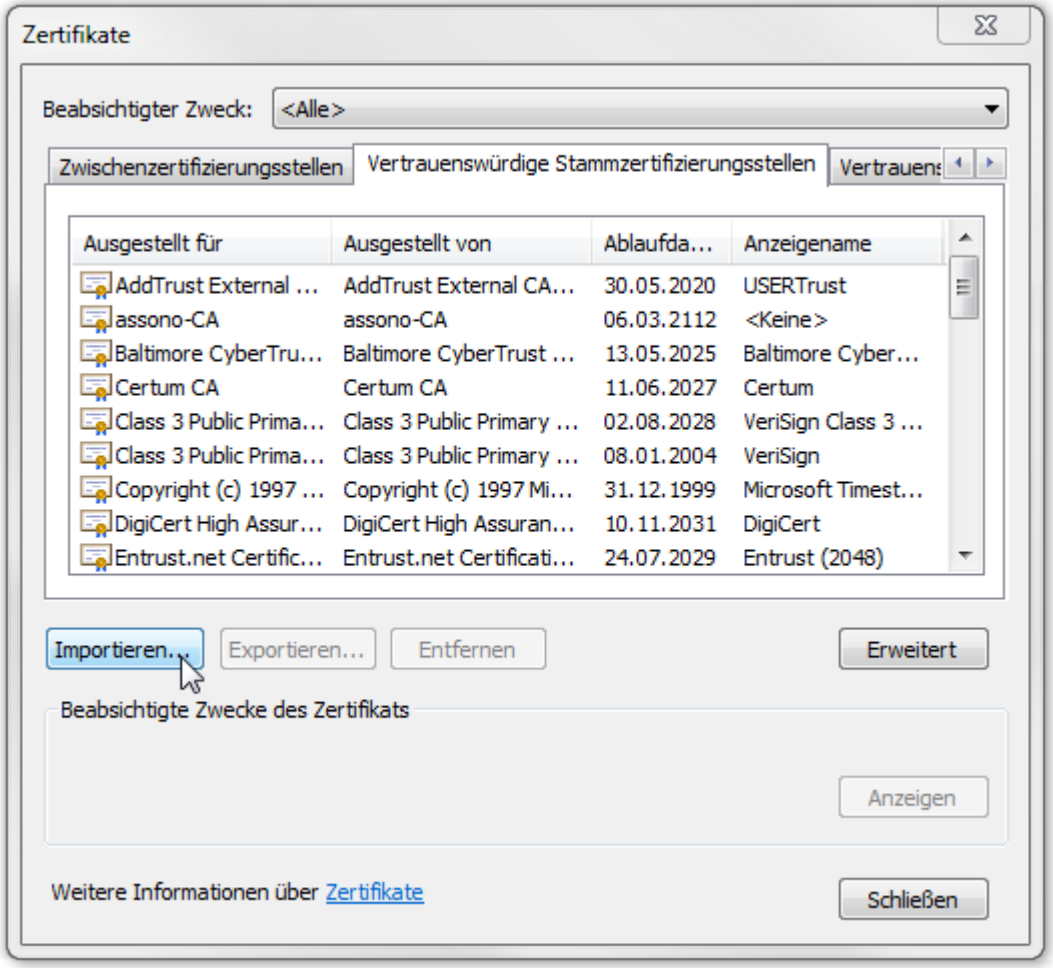
Warnung wegen des SSL-Zertifikats



Warnung wegen des SSL-Zertifikats

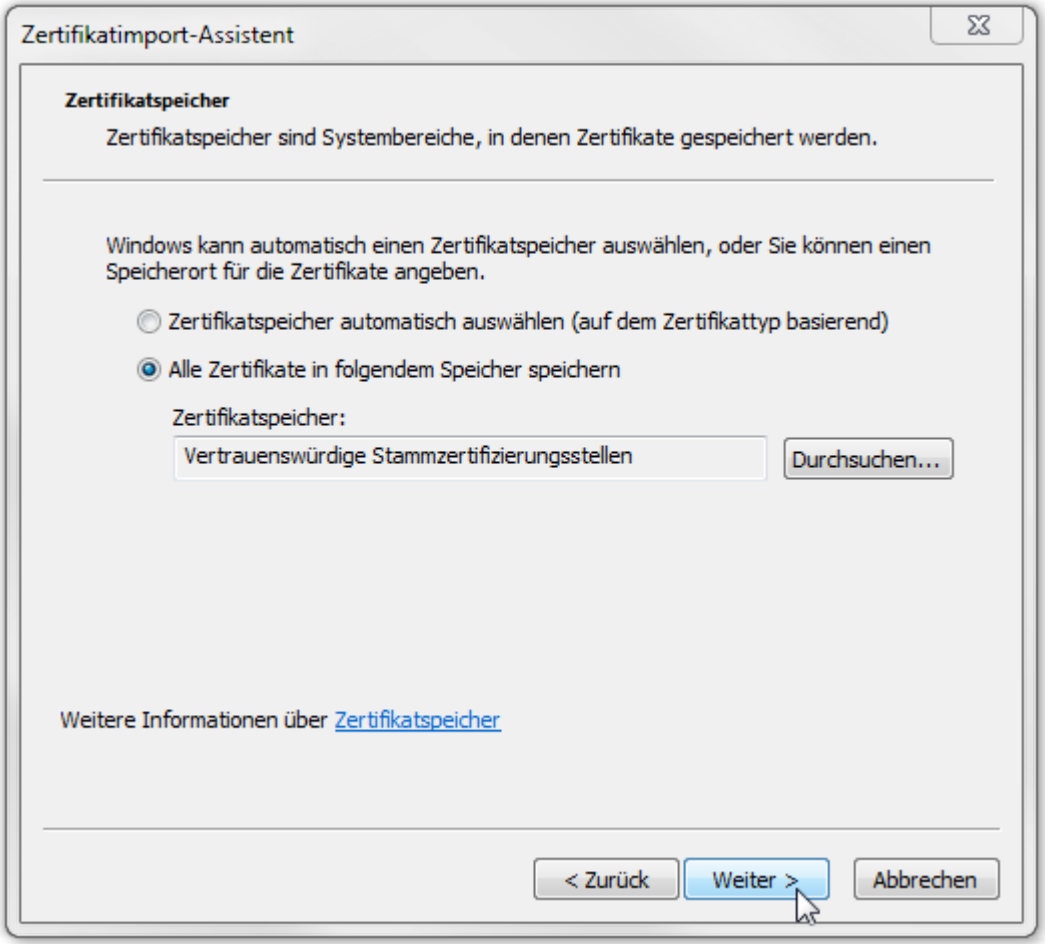


Warnung wegen des SSL-Zertifikats

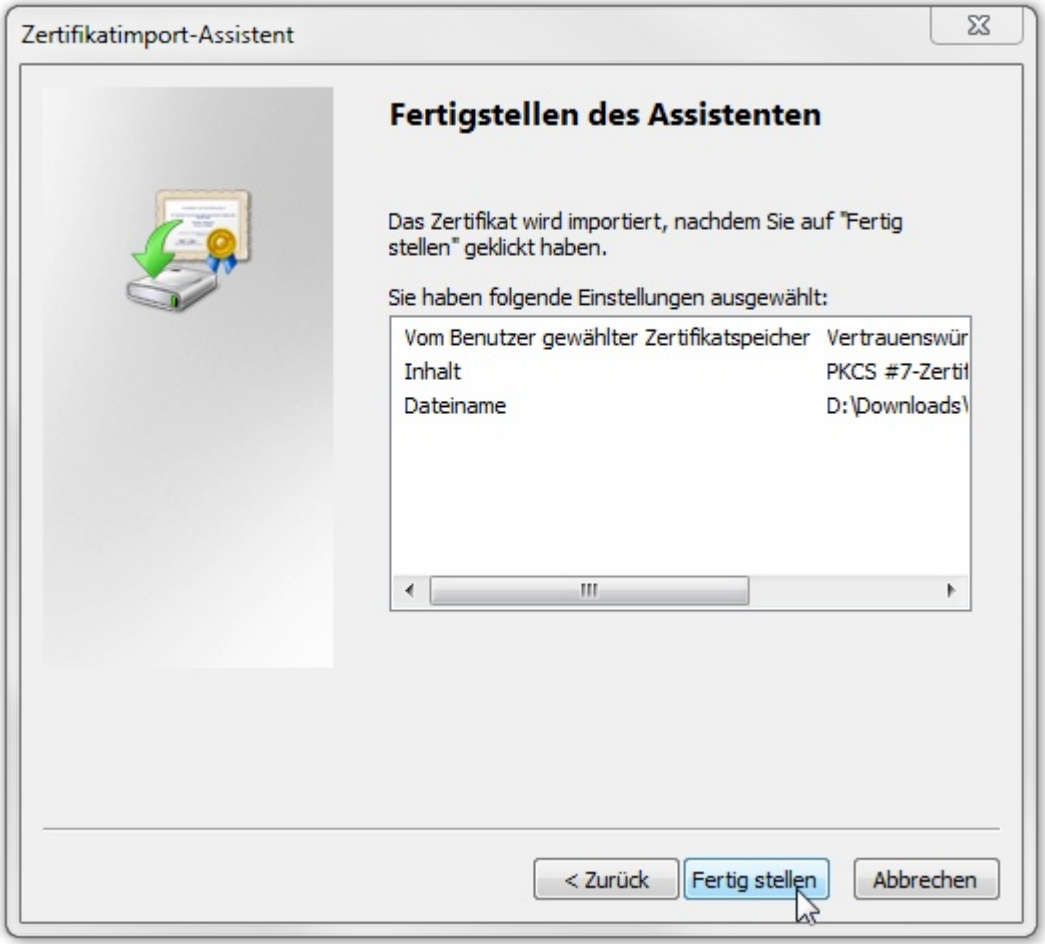


Warnung wegen des SSL-Zertifikats

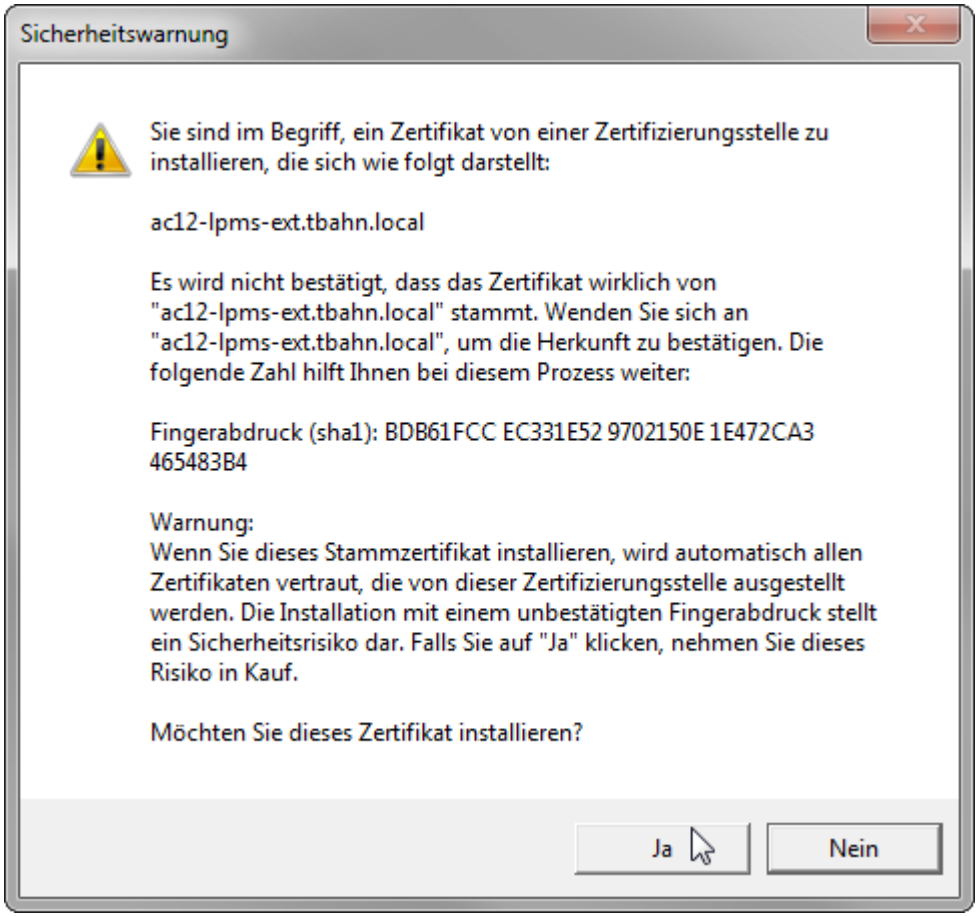
Warnung wegen des SSL-Zertifikats



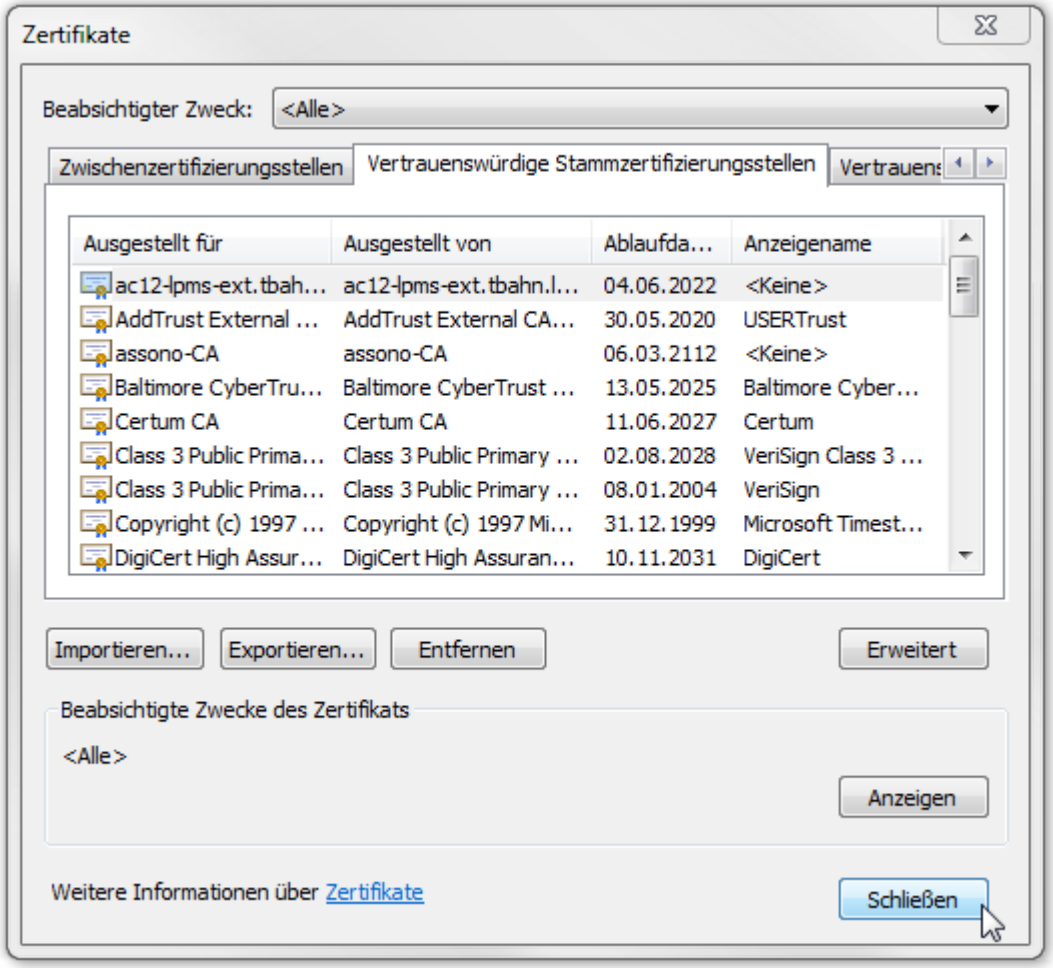
Warnung wegen des SSL-Zertifikats



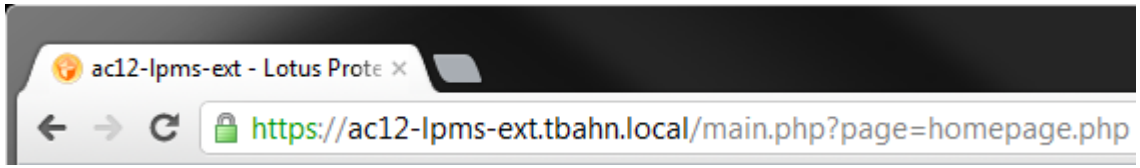
Warnung wegen des SSL-Zertifikats



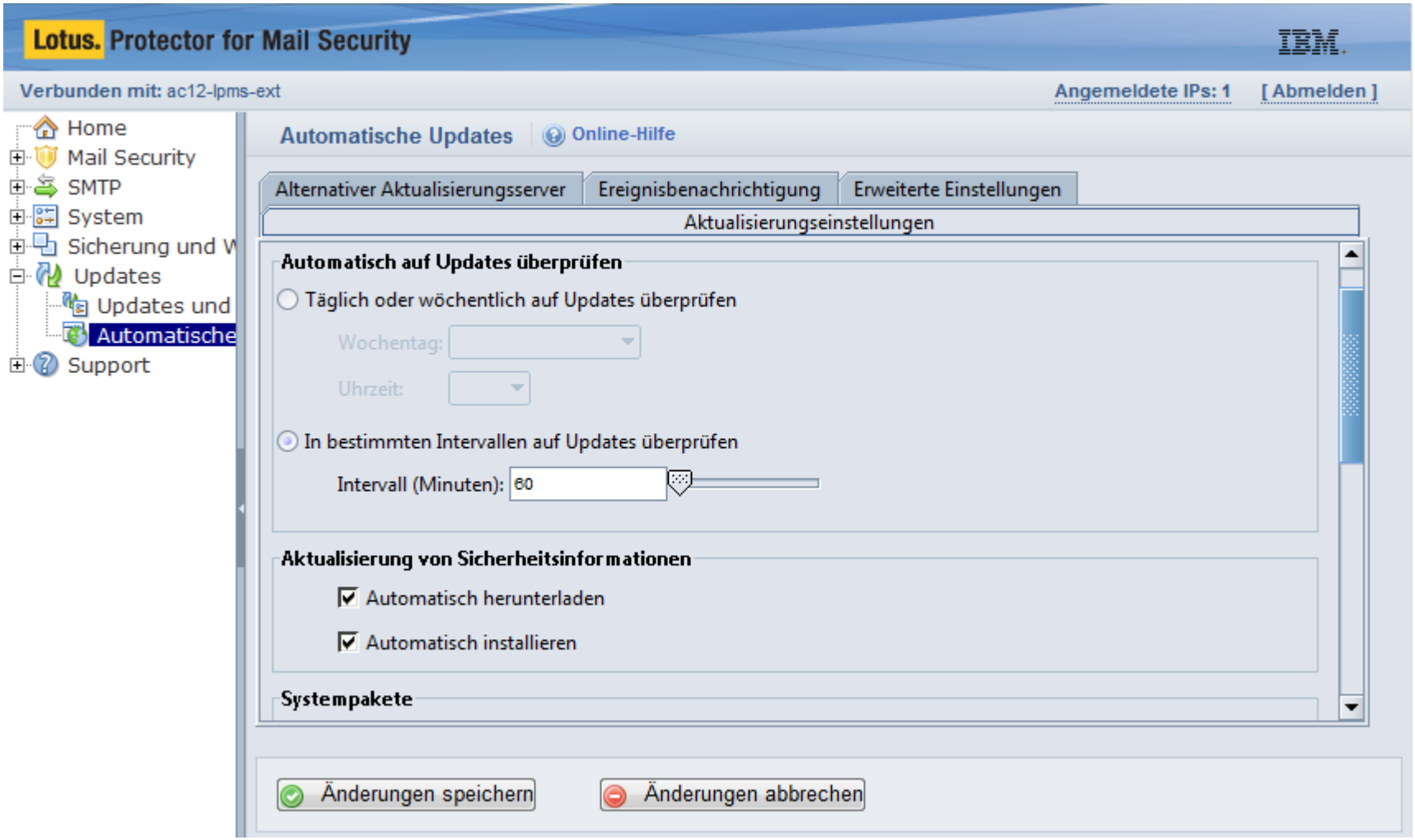
Warnung wegen des SSL-Zertifikats



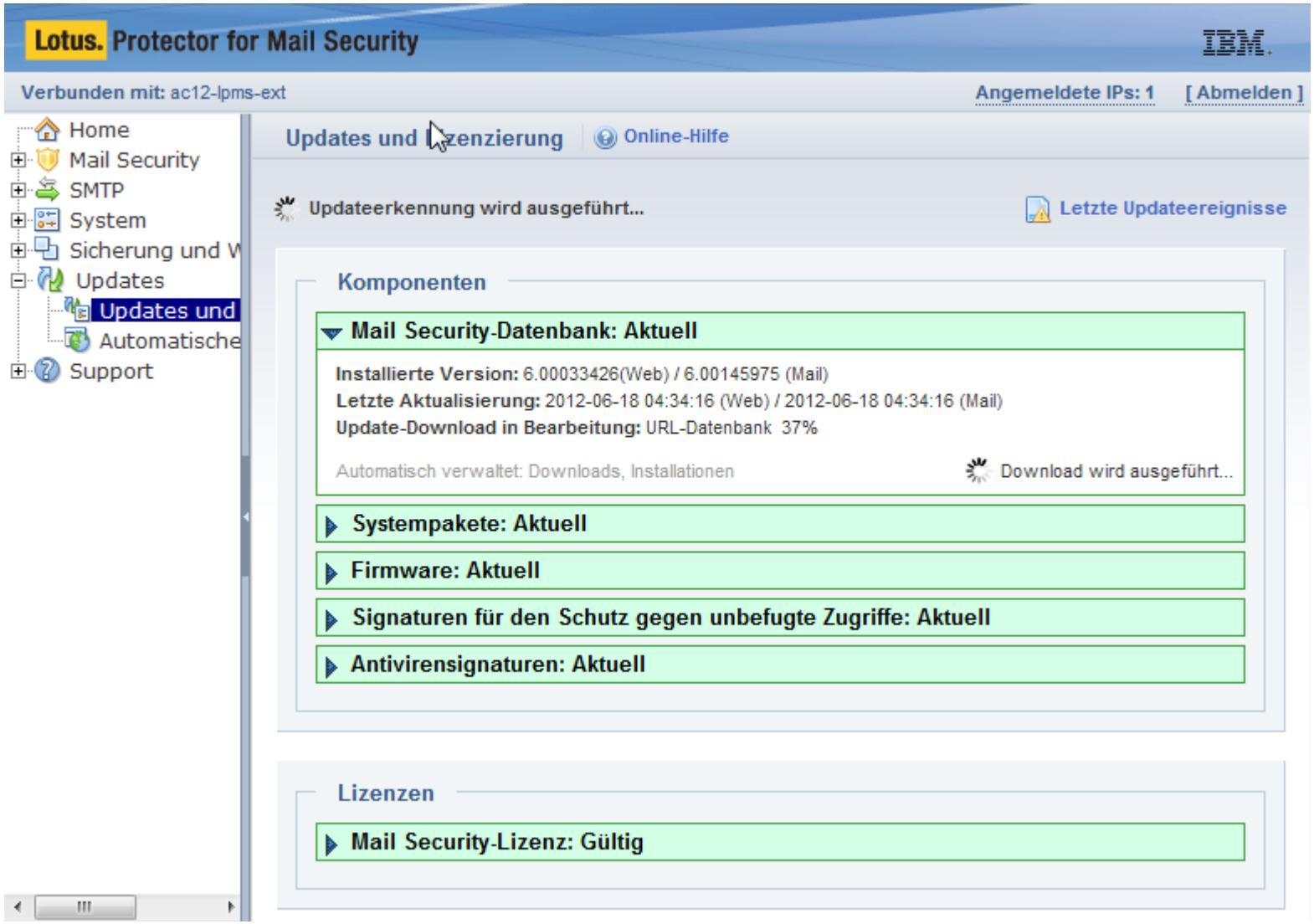
Warnung wegen des SSL-Zertifikats



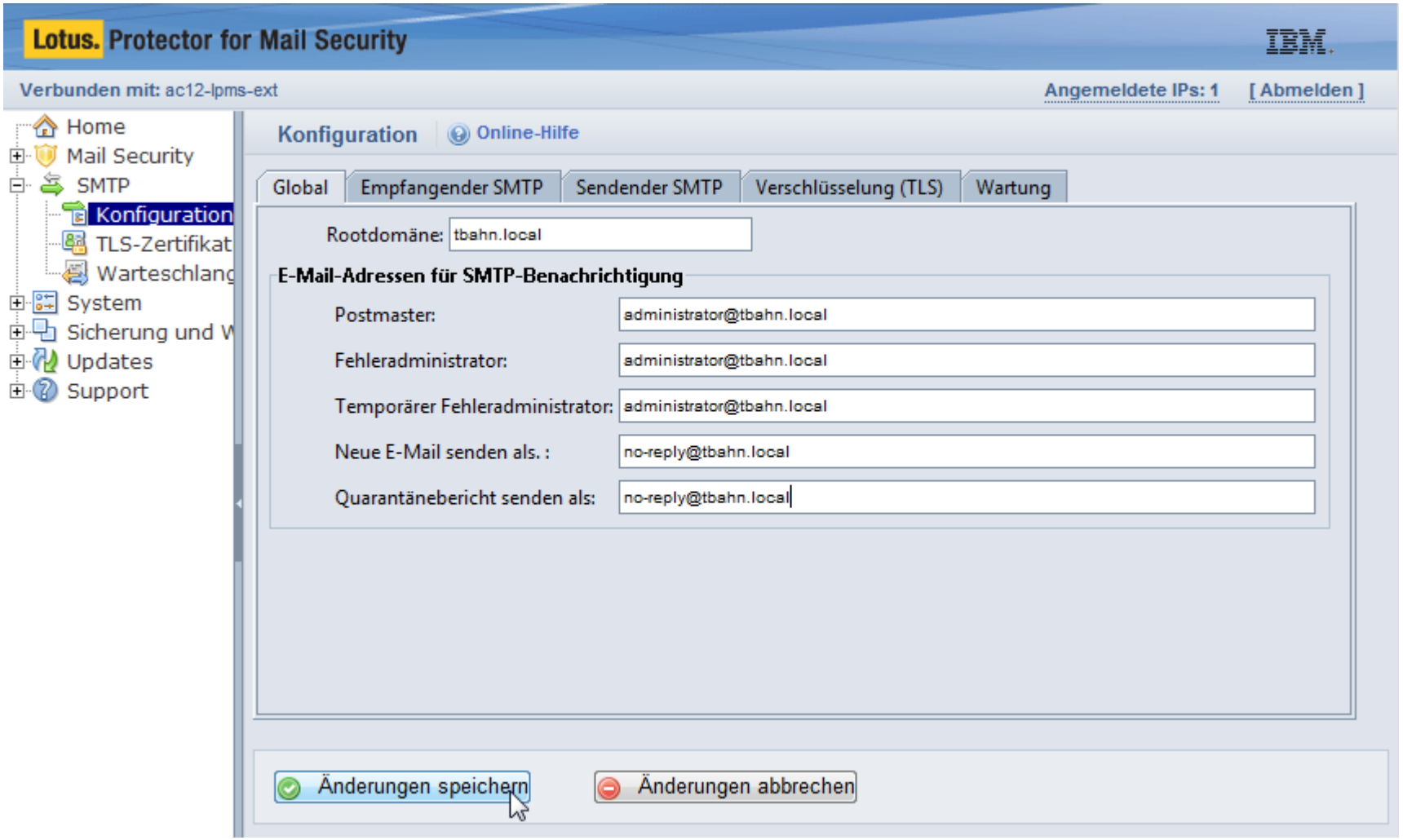
Automatische Aktualisierungen konfigurieren



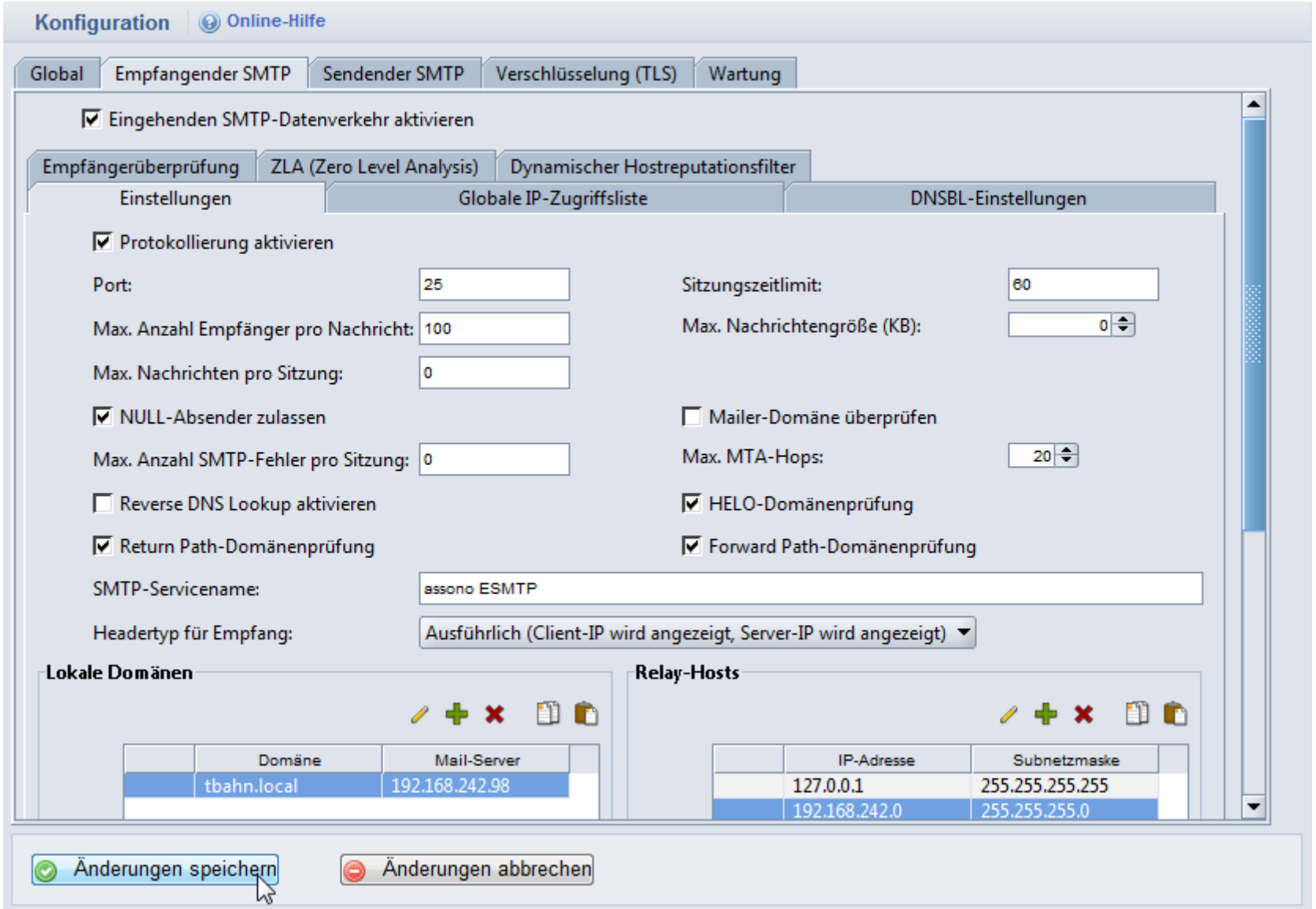
Aktualisierungsstatus und Mail Security-Datenbank



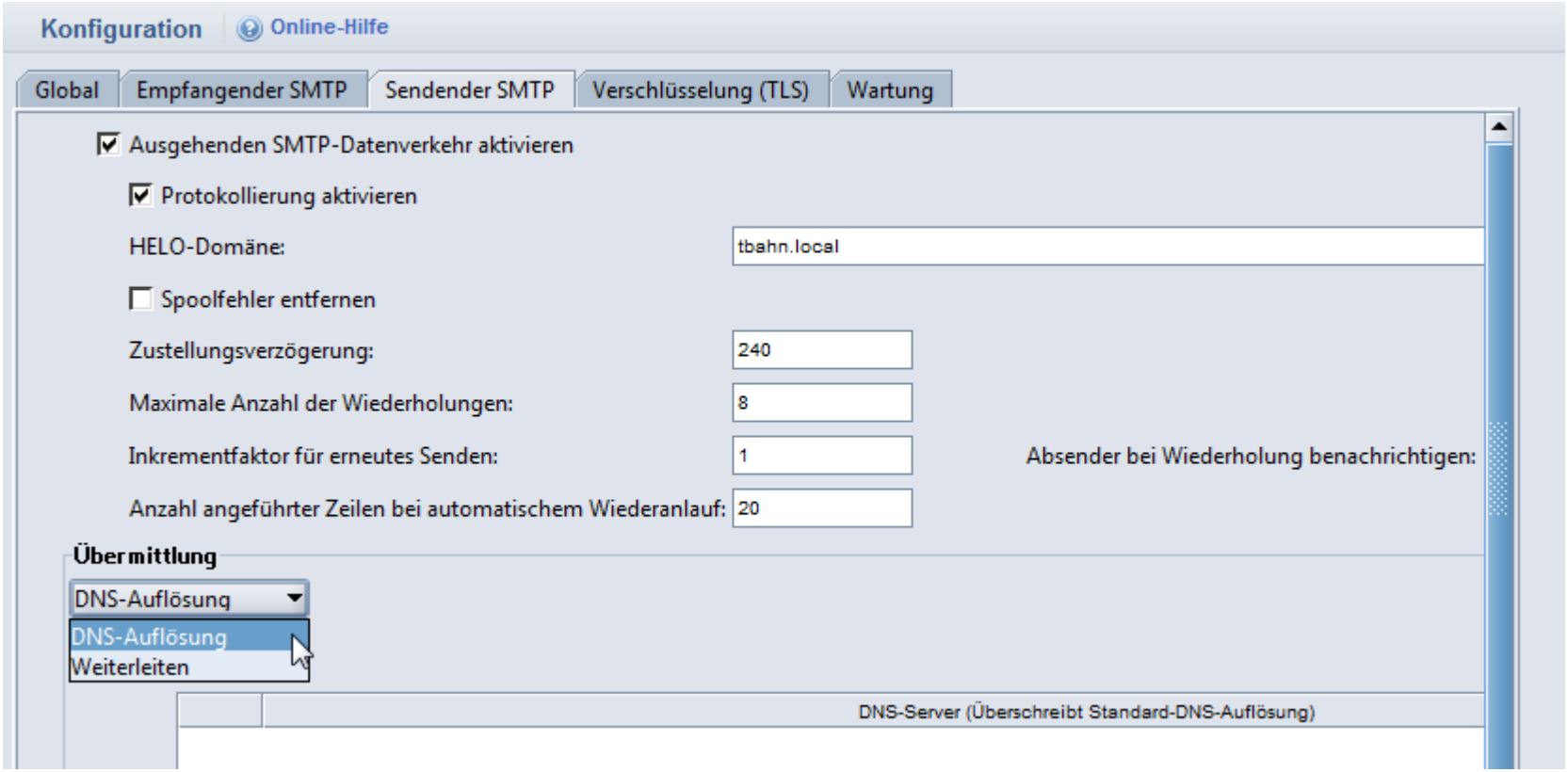
SMTP-Konfiguration



SMTP-Konfiguration

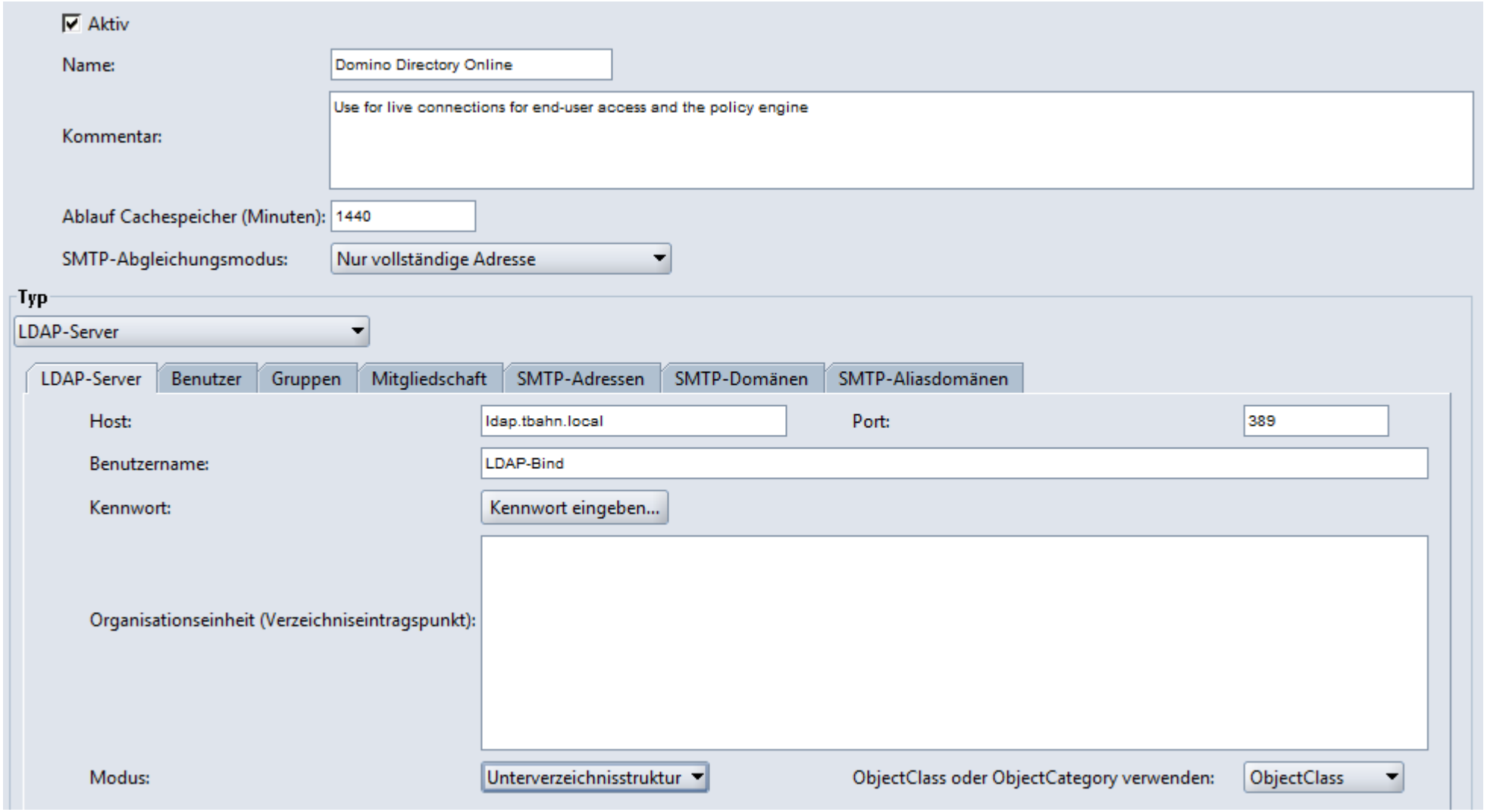


SMTP-Konfiguration

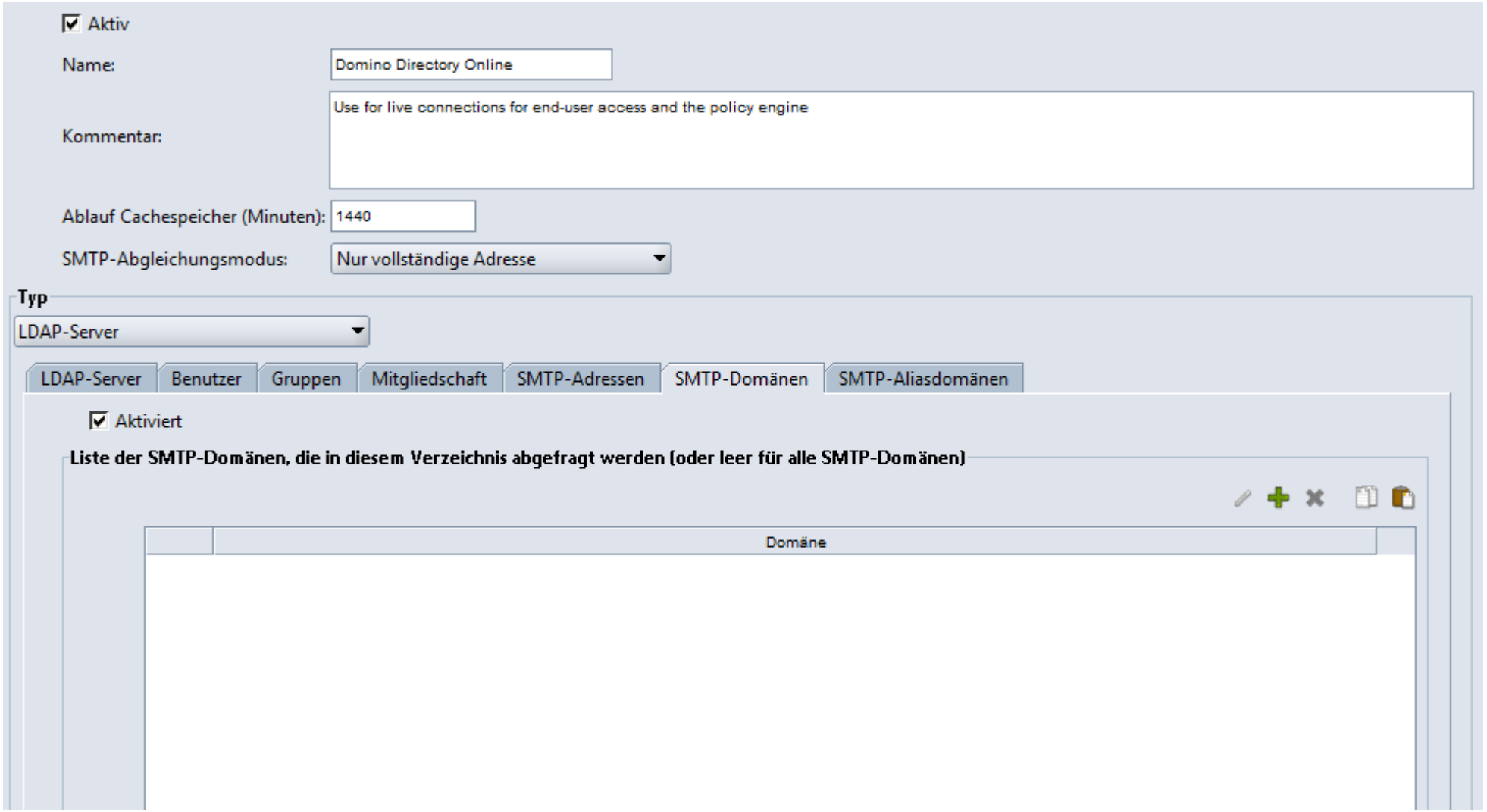


Domino-LDAP einstellen

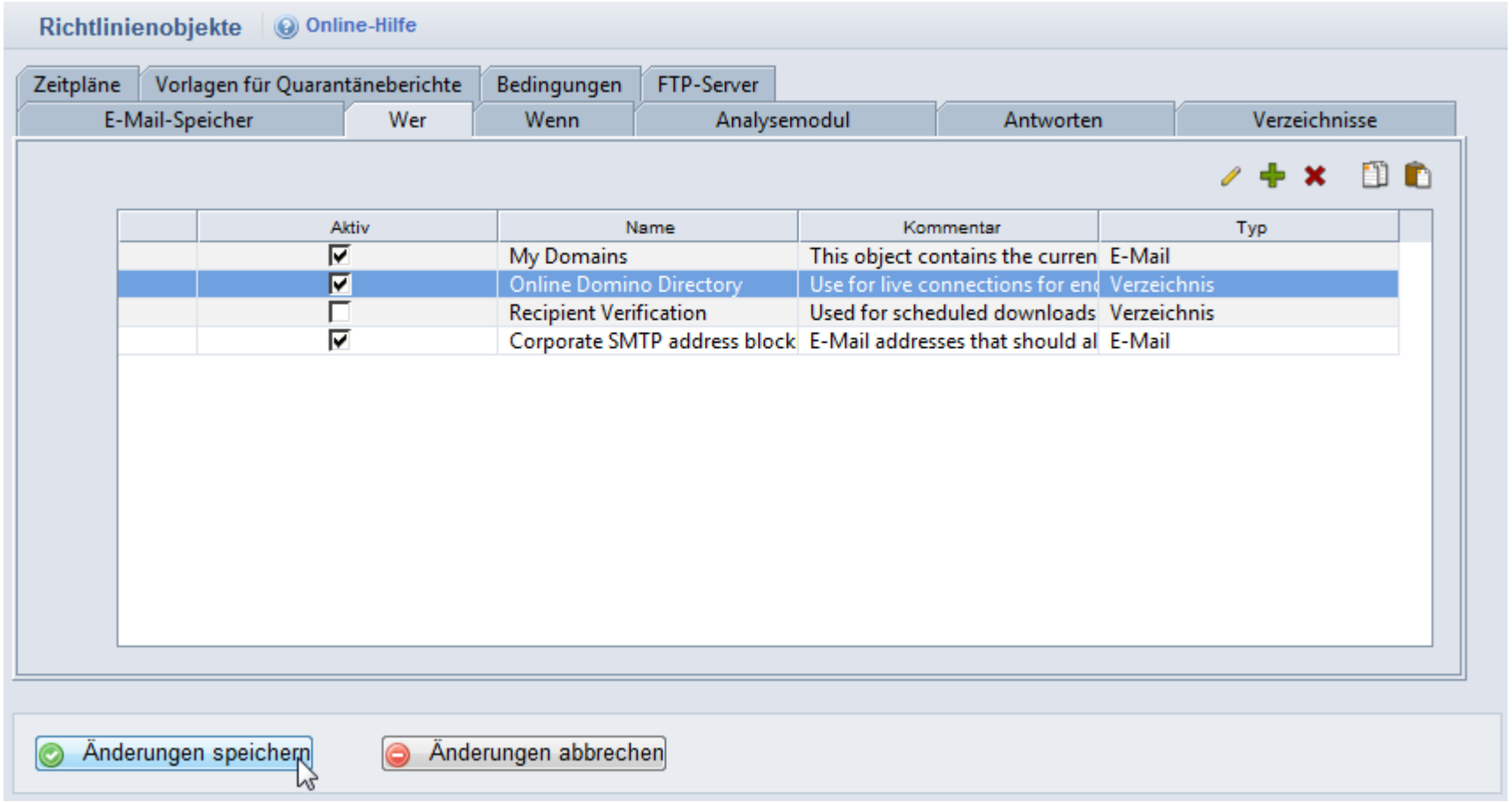
Domino-LDAP einstellen



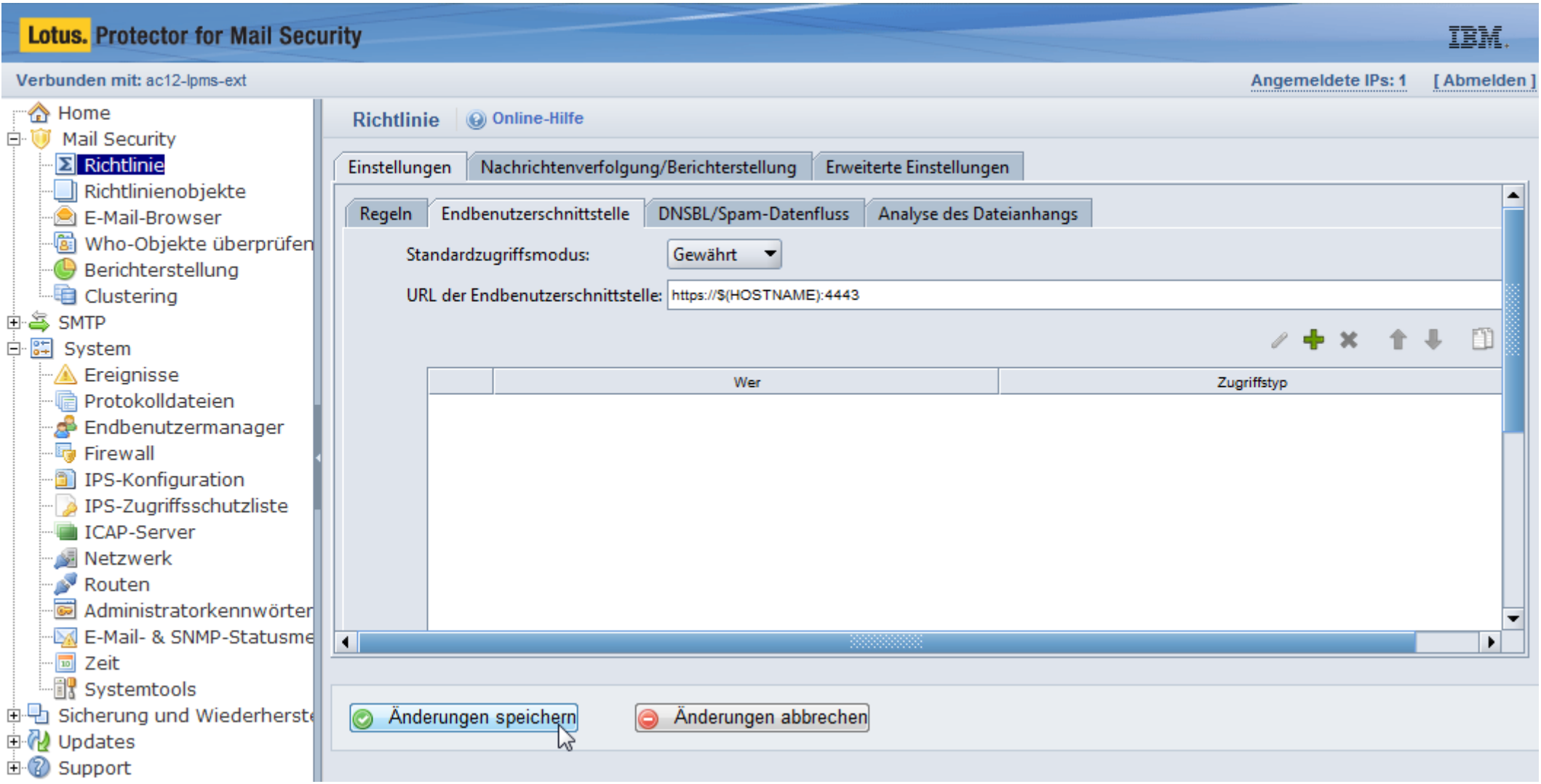
Domino-LDAP einstellen



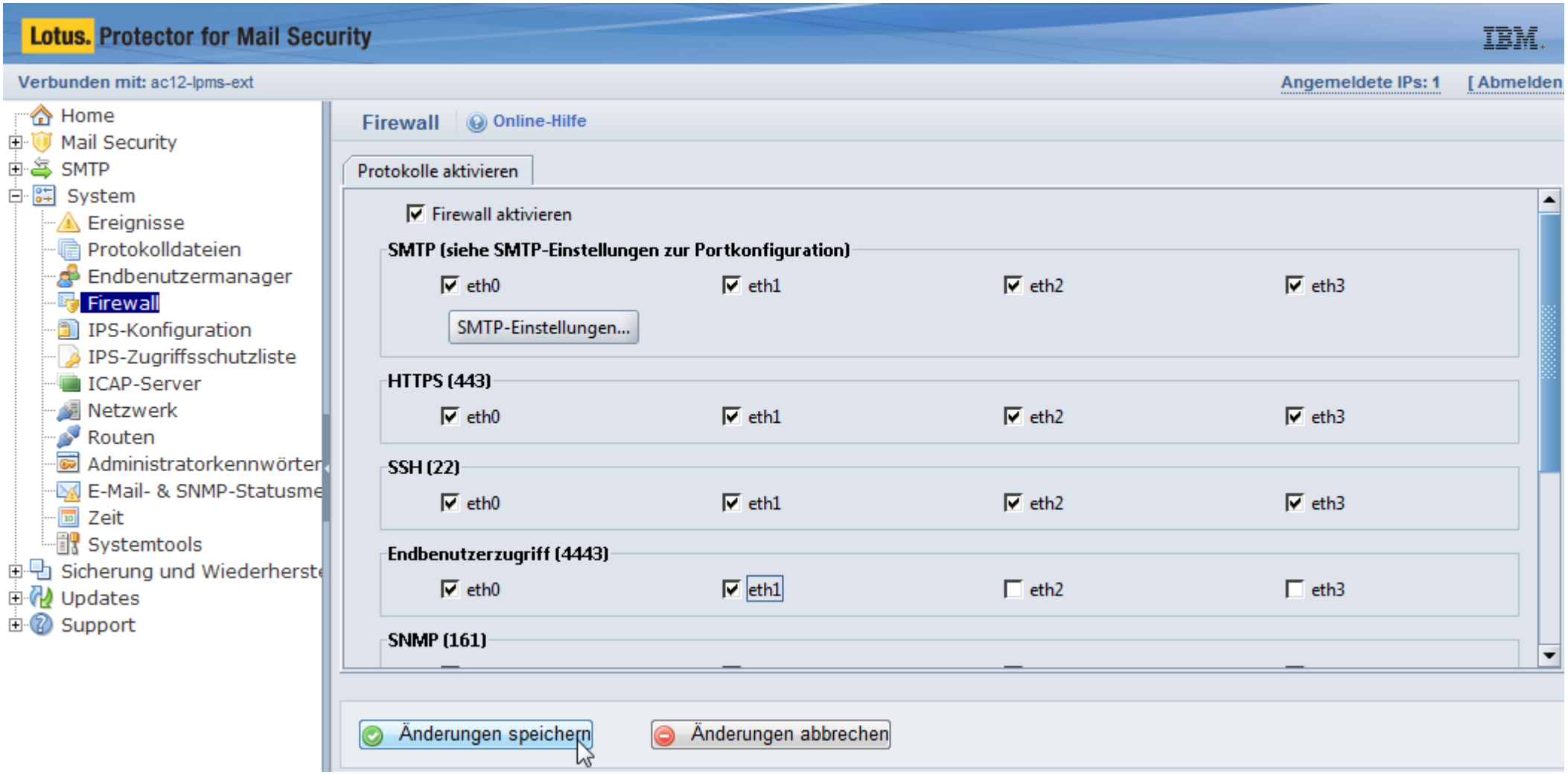
Domino-LDAP einstellen



Endbenutzer-Schnittstelle



Endbenutzer-Schnittstelle



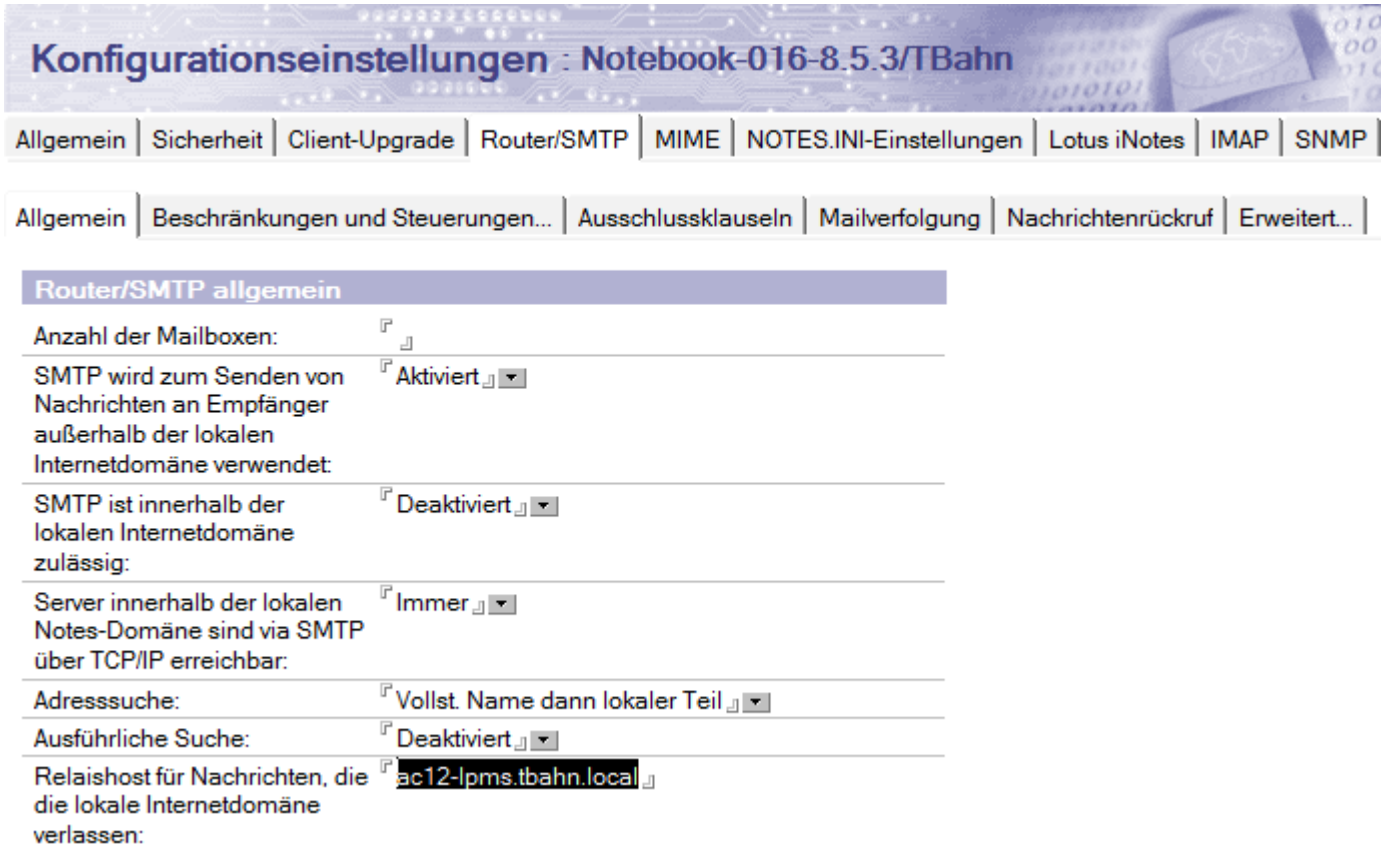
Endbenutzer-Schnittstelle

Endbenutzer-Schnittstelle

Endbenutzer-Schnittstelle

Endbenutzer-Schnittstelle

Konfiguration des Domino-Servers



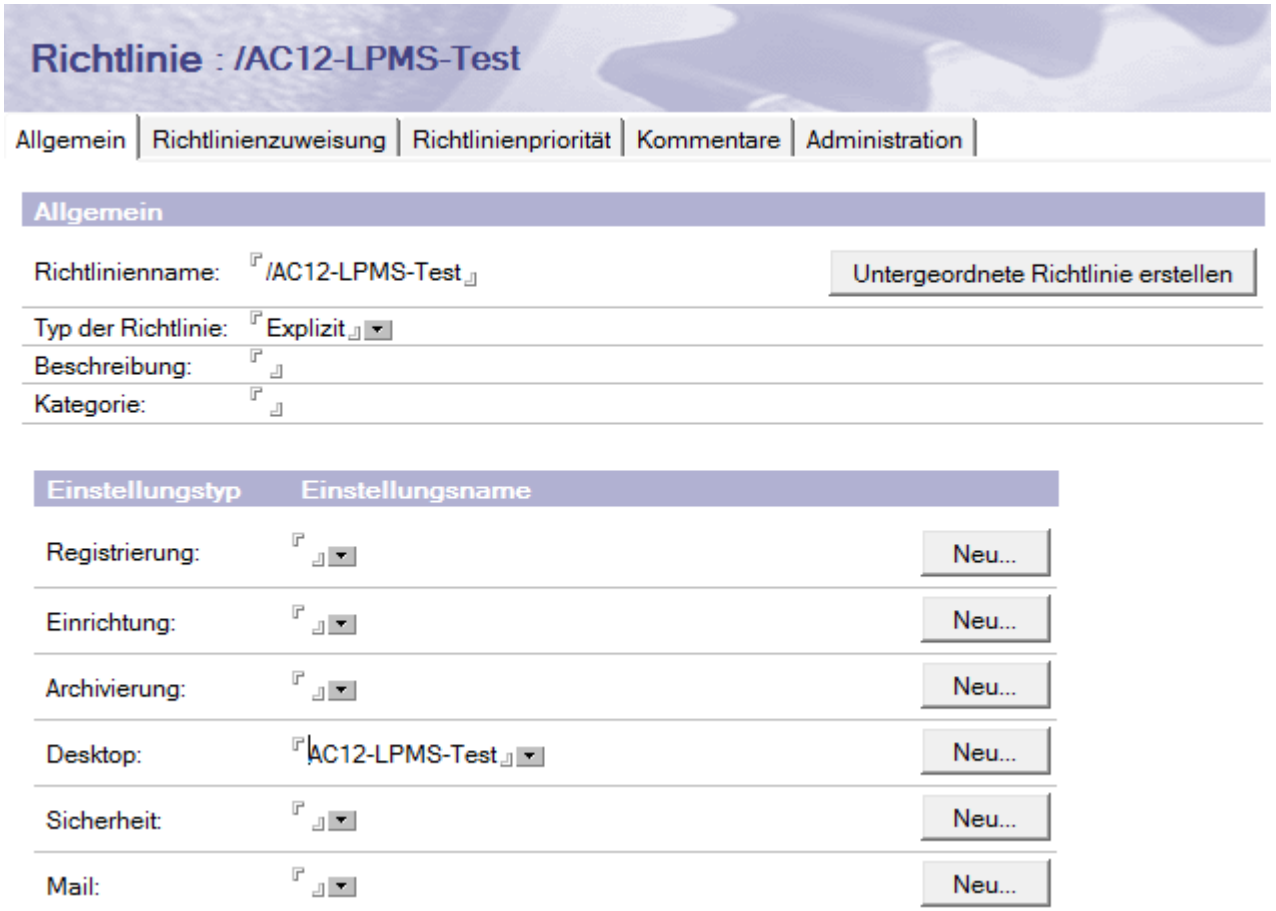
Konfiguration des Notes-Clients (via Richtlinie)

Allgemein

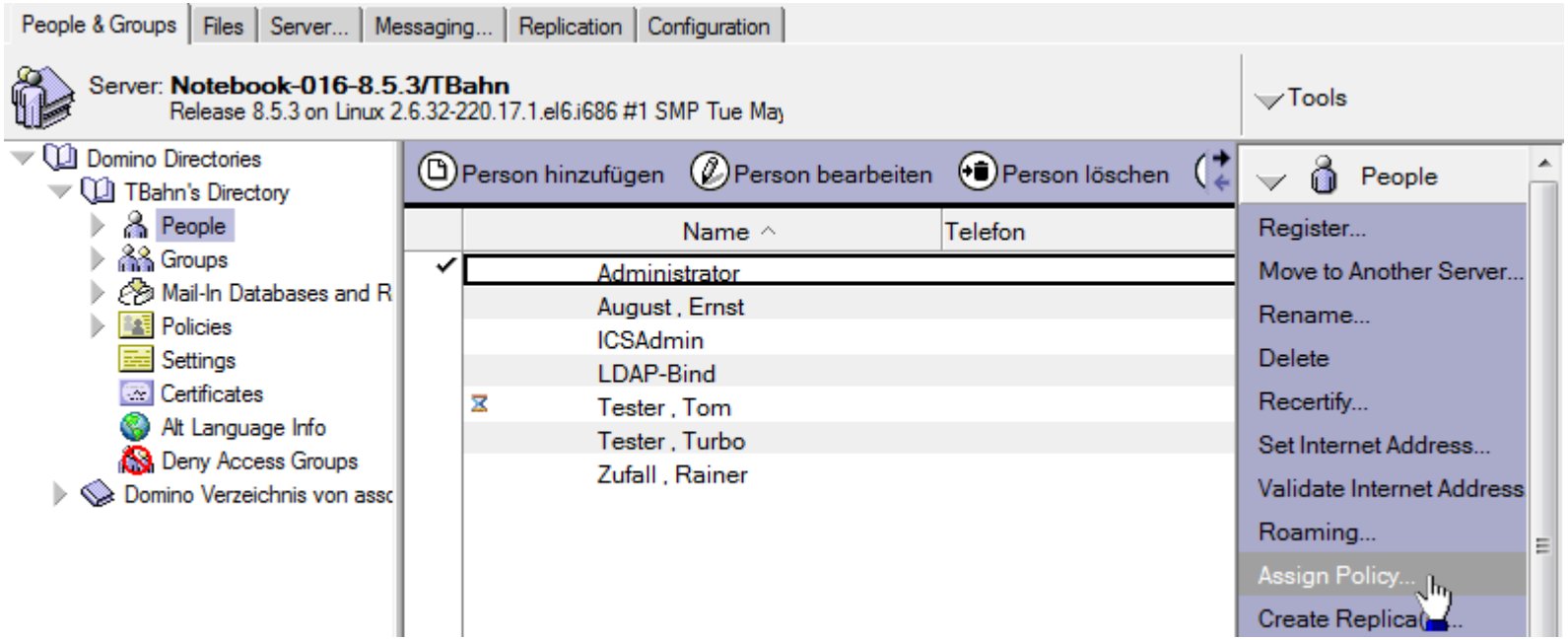
Name:	AC12-LPMS-Test
Beschreibung:	

Optionen für Lotus Protector		Wie diese Einstellung angewendet wird:	Übernehmen von übergeordneter Richtlinie:	Zwingend in untergeordneten Richtlinien:
Geben Sie die URL für den Zugriff auf Protector-Server an:	ac12-lpms-ext.tbahn.local:4443	☐ Wert nicht festlegen	☐ Übernehmen	☐ Zwingend

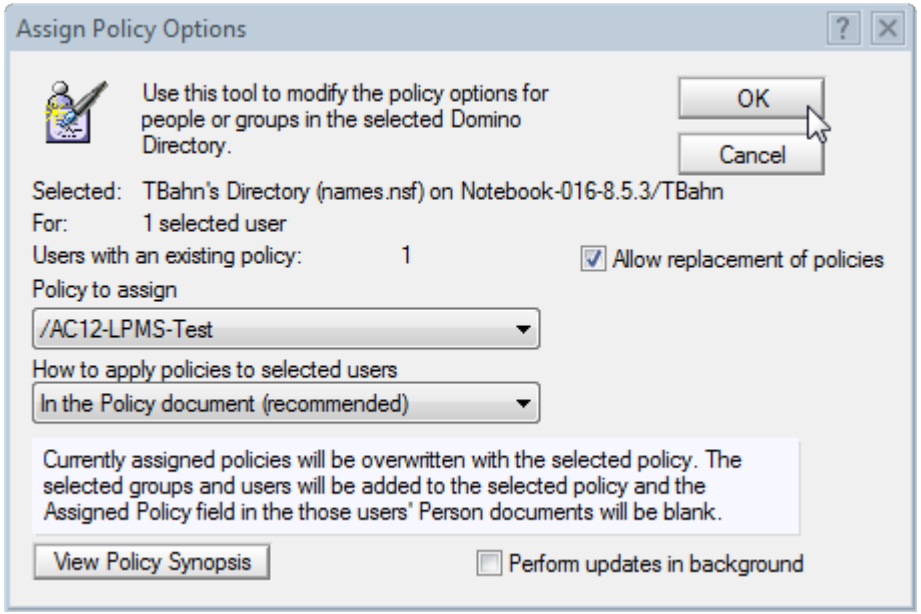
Konfiguration des Notes-Clients (via Richtlinie)

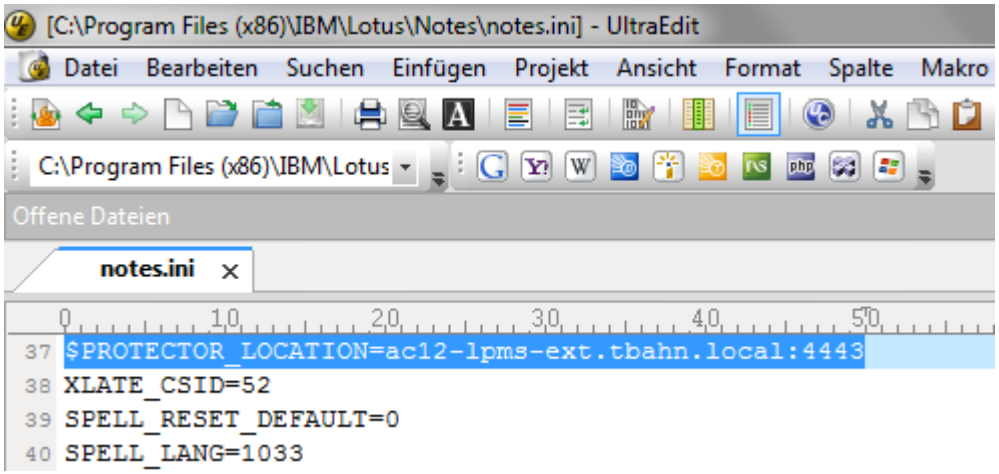


Konfiguration des Notes-Clients (via Richtlinie)



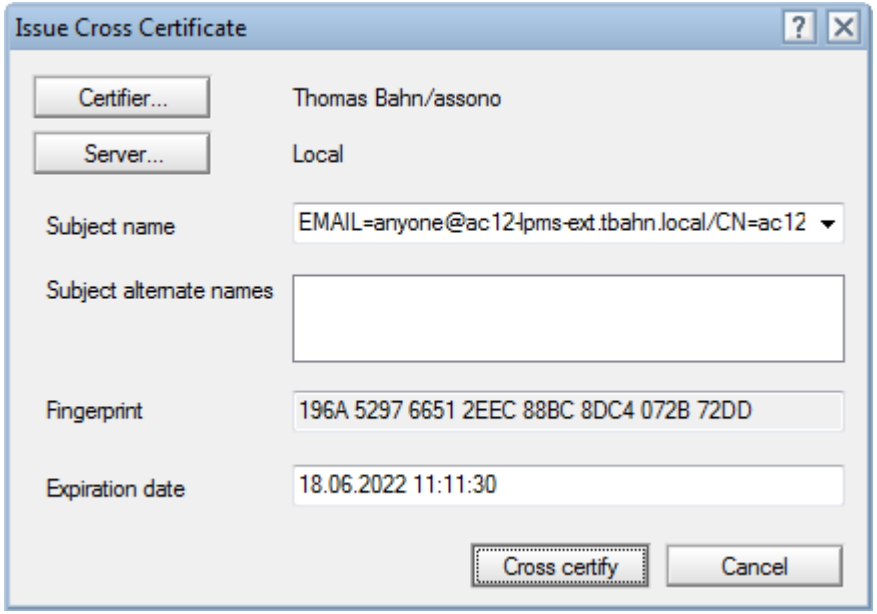
Konfiguration des Notes-Clients (via Richtlinie)

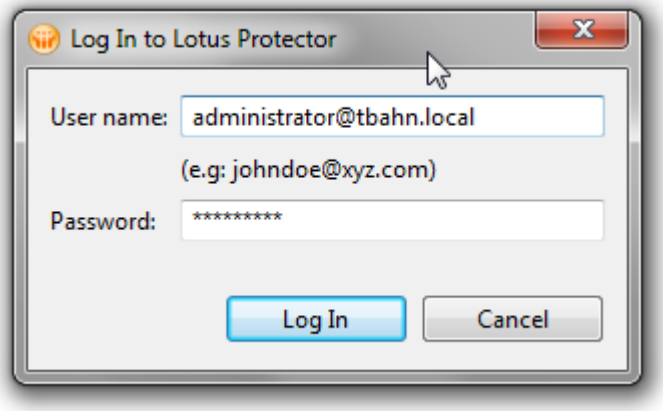




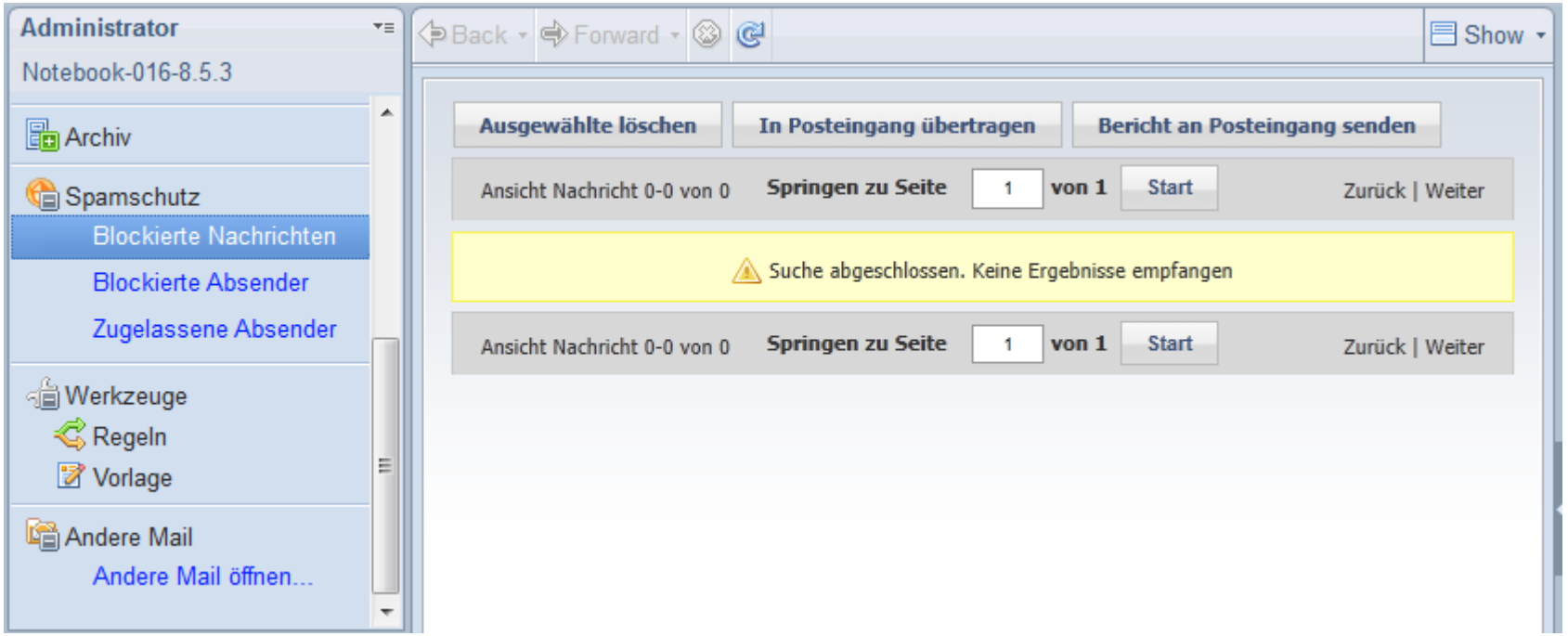
LPMS aus Benutzersicht im Notes-Client

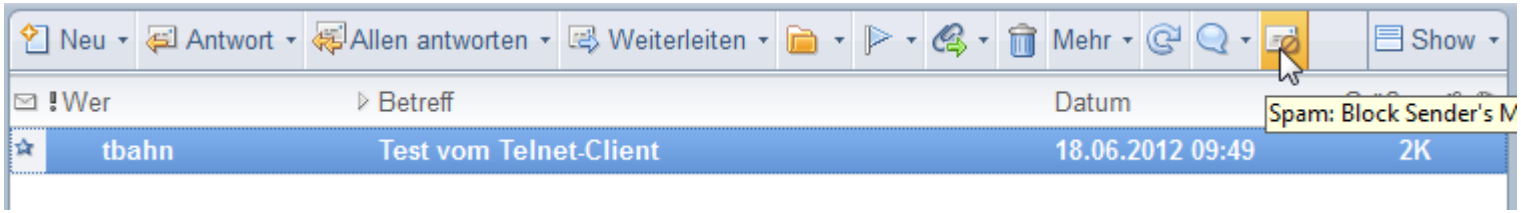
LPMS aus Benutzersicht im Notes-Client





LPMS aus Benutzersicht im Notes-Client



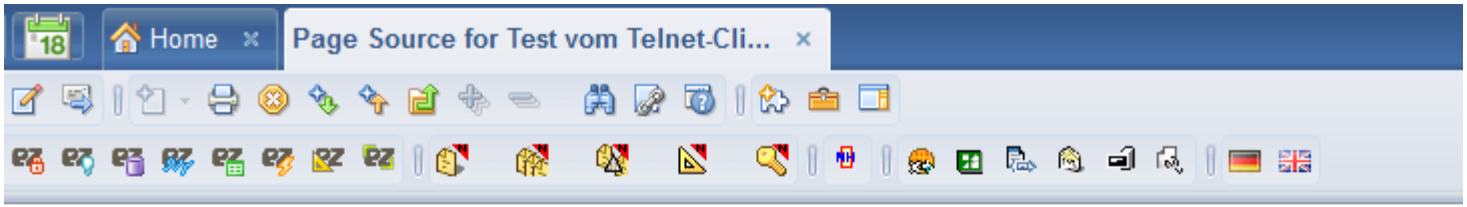


Testen mit Telnet

```
220 assono ESMTP service ready; Mon, 18 Jun 2012 07:42:00 -0000
helo ich
250 tbahn.local
mail from: <tbahn@gmx.de>
250 OK
rcpt to: <administrator@tbahn.local>
250 OK
data
354 Start mail input; end with <CRLF>.<CRLF>
subject: Test vom Telnet-Client

Testing...

.
250 OK <12061807-4094-0000-0000-000000090001>
```

```
220 assono ESMTP service ready; Mon, 18 Jun 2012 07:46:18 -0000
helo ichh
250 tbahn.local
mail from: <administrator@tbahn.local>
250 OK
rcpt to: <tbahn@assono.de>
250 OK
data
354 Start mail input; end with <CRLF>.<CRLF>
subject: Test vom Telnet-Client 2

Testing...
.
250 OK <12061807-4094-0000-0000-000000090002>
```

Testergebnis




```
Received: from tbahn.local ([192.168.242.100])
          by notebook-016-98.tbahn.local
          with ESMTP id 2012061809431888-1 ;
          Mon, 18 Jun 2012 09:43:18 +0200
Received: from /spool/local
             by tbahn.local with assono ESMTP
             for <administrator@tbahn.local> from <tbahn@gmx.de>;
             Mon, 18 Jun 2012 07:43:16 -0000
Received: from ich ([192.168.242.1])
             by tbahn.local ([192.168.242.100]) with assono ESMTP;
             Mon, 18 Jun 2012 07:42:31 -0000
subject: Test vom Telnet-Client
x-cbid: 12061807-4094-0000-0000-000000090001
X-IBM-ISS-SpamDetectors: Score=0; BY=0; FL=0; FP=0; FZ=0; HX=0; KW=0; PH=0;
 SC=0; ST=0; TS=0; UL=0; ISC=
X-IBM-ISS-DetailInfo:  BY=3.00000281; HX=3.00000190; KW=3.00000007;
 PH=3.00000001; SC=3.00000002; SDB=6.00149055; UDB=6.00033909; UTC=2012-06-18
 07:43:16
X-MIMETrack: Itemize by SMTP Server on Notebook-016-8.5.3/TBahn at 18.06.2012 09:43:19,
             Serialize by Notes Client on Thomas Bahn/assono(Build V854_03202012|March
 20, 2012) at 18.06.2012 11:23:08,
             Serialize complete at 18.06.2012 11:23:08
X-TNEFEvaluated: 1
From: tbahn@gmx.de
Date: Mon, 18 Jun 2012 09:43:19 +0200
Message-ID: <OF50872FFF.52BF1836-ONC1257A21.002A6AF4@LocalDomain>

Testing...
```

assono

Lotus Protector for Mail Encryption

Theorie

Lotus Protector for Mail Encryption (LPME)

Lotus® Protector for Mail Encryption

- E-Mail-Verschlüsselung
- unterstützt 2 Standardverfahren
  - PGP
  - S/MIME
- automatische Schlüsselverwaltung
- verschlüsselt regel-basiert (Policies auf dem Server) und/oder benutzergesteuert (via Notes-Add-In)

Lotus Protector for Mail Encryption (LPME)

- Focus auf einfache Benutzbarkeit
  - regelbasiert: ohne Benutzerinteraktion
  - benutzergesteuert: genauso wie Verschlüsselung innerhalb von Lotus Notes und Domino
- bei neuen, noch unbekannten Empfängern
  - nicht zustellbar zurück
  - unverschlüsselter Versand
  - Web-Oberfläche
  - PDFs
  - Smart Trailer

assono

Einsatzszenarien

- Server:
  - Platzierung als Gateway (Das willst du!)
  - interne Platzierung
- interne Platzierung
  - für E-Mail-Clients (POP, IMAP) und Outlook (MAPI)
  - LPME-Server zwischen Client und Mail-Server
- Client (Add-On)
  - extra Lizenzierung (und Kosten)
  - Client kommuniziert mit LPME-Server direkt
  - Client ver-/entschlüsselt und signiert selbst

assono

Lotus Protector for Mail Encryption

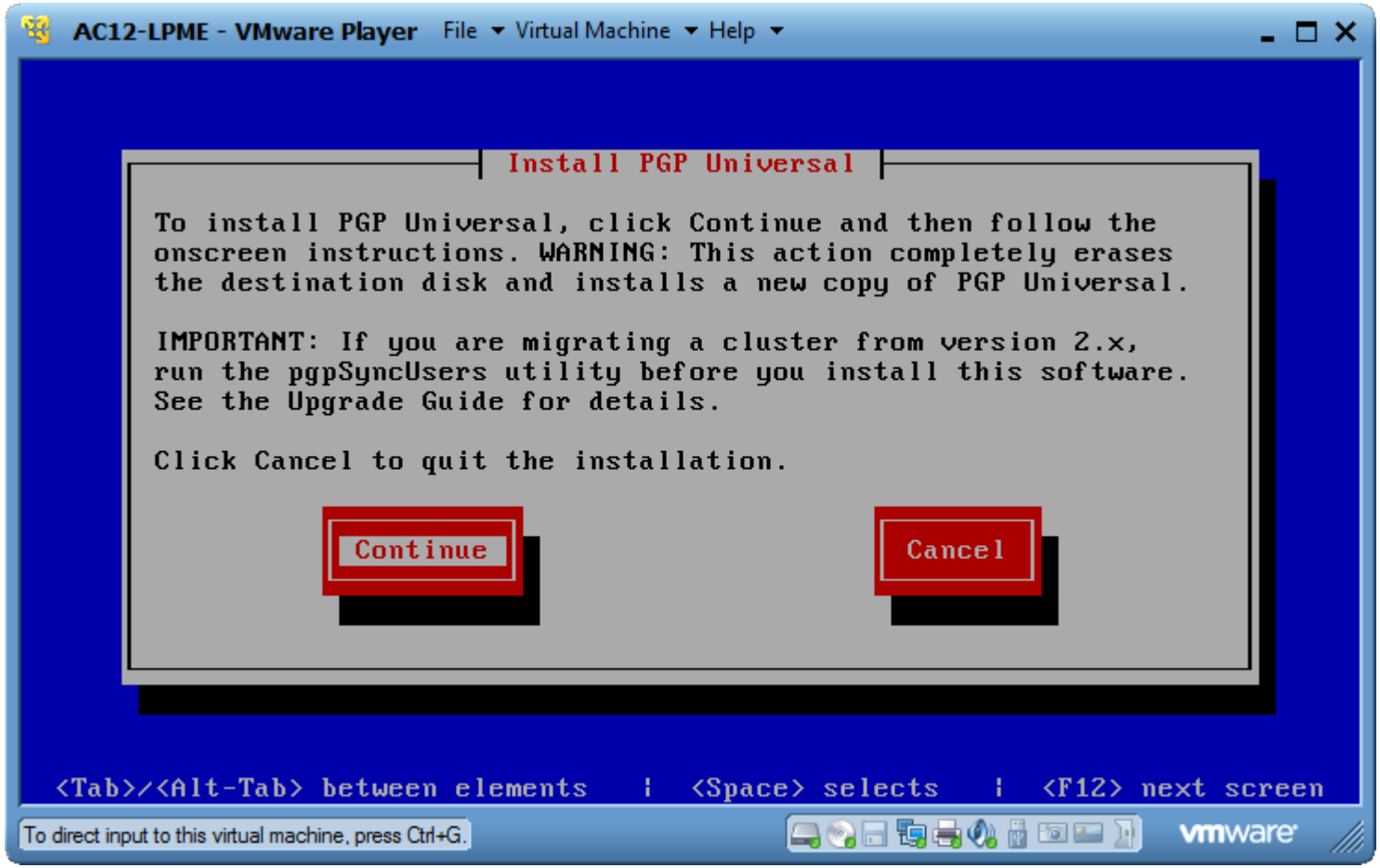
Praxis

MX-Einträge (DNS)

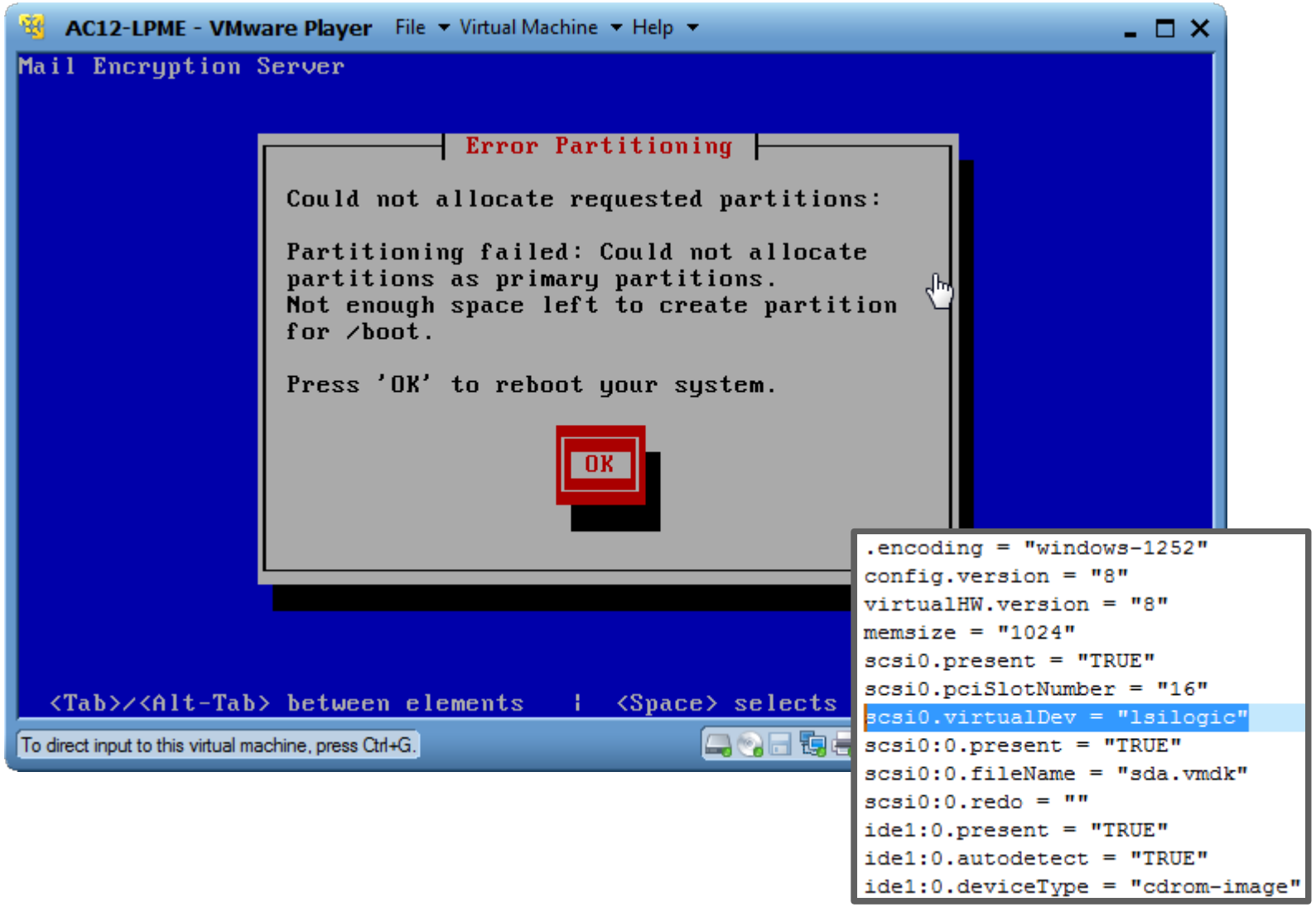
- MX-Einträge im DNS steuern, an welche Server E-Mails für eine Domäne zugestellt werden
- mehrere MX-Einträge für eine Domäne möglich
- Reihenfolge über MX Preference (~ Kosten):
  - Server mit niedrigeren Werten zuerst
  - Server mit gleichen Werten „zufällig“
- Nach der Installation müssen MX-Einträge aller Domänen auf LPME-Server umgestellt werden

Installation

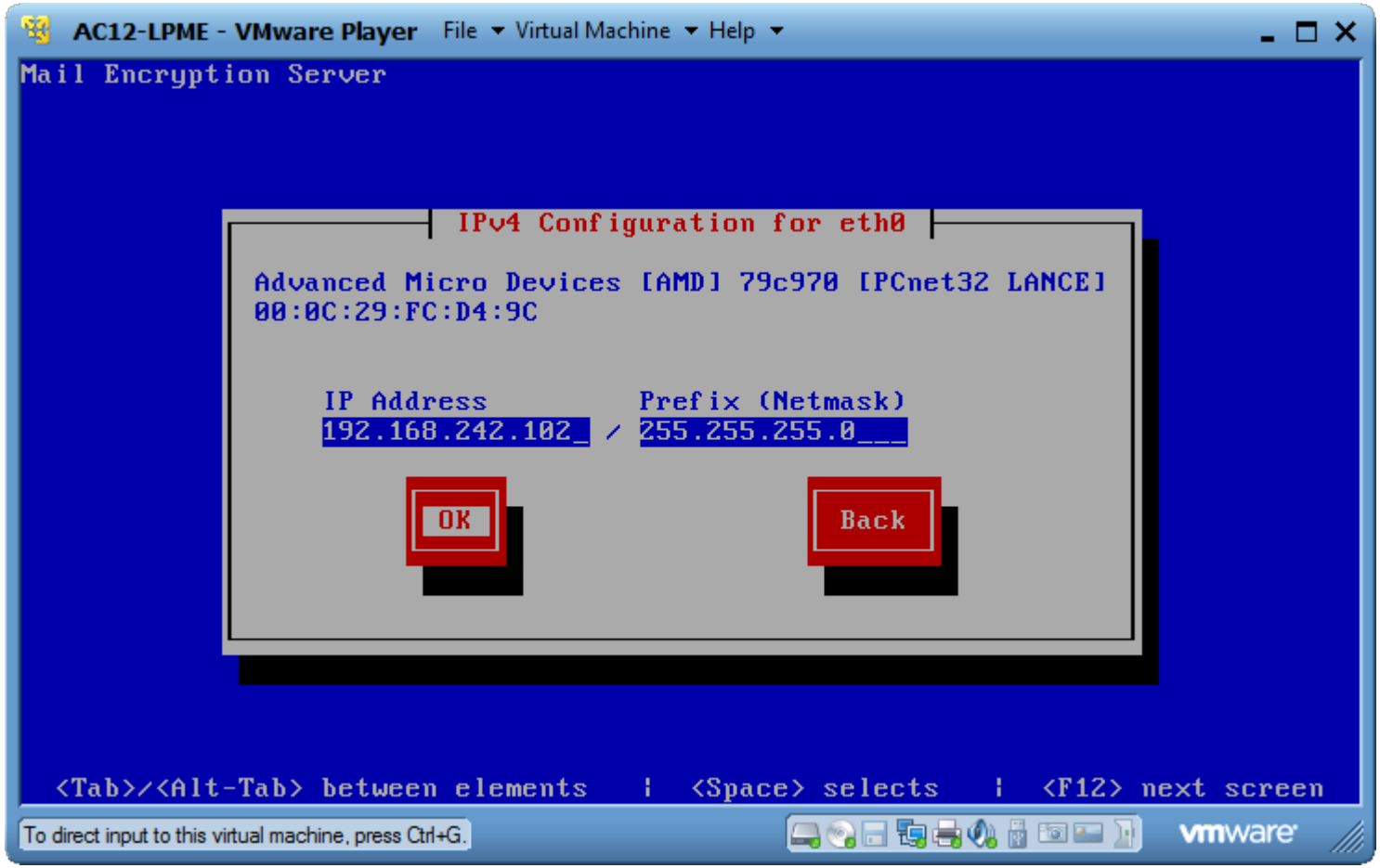
Installation



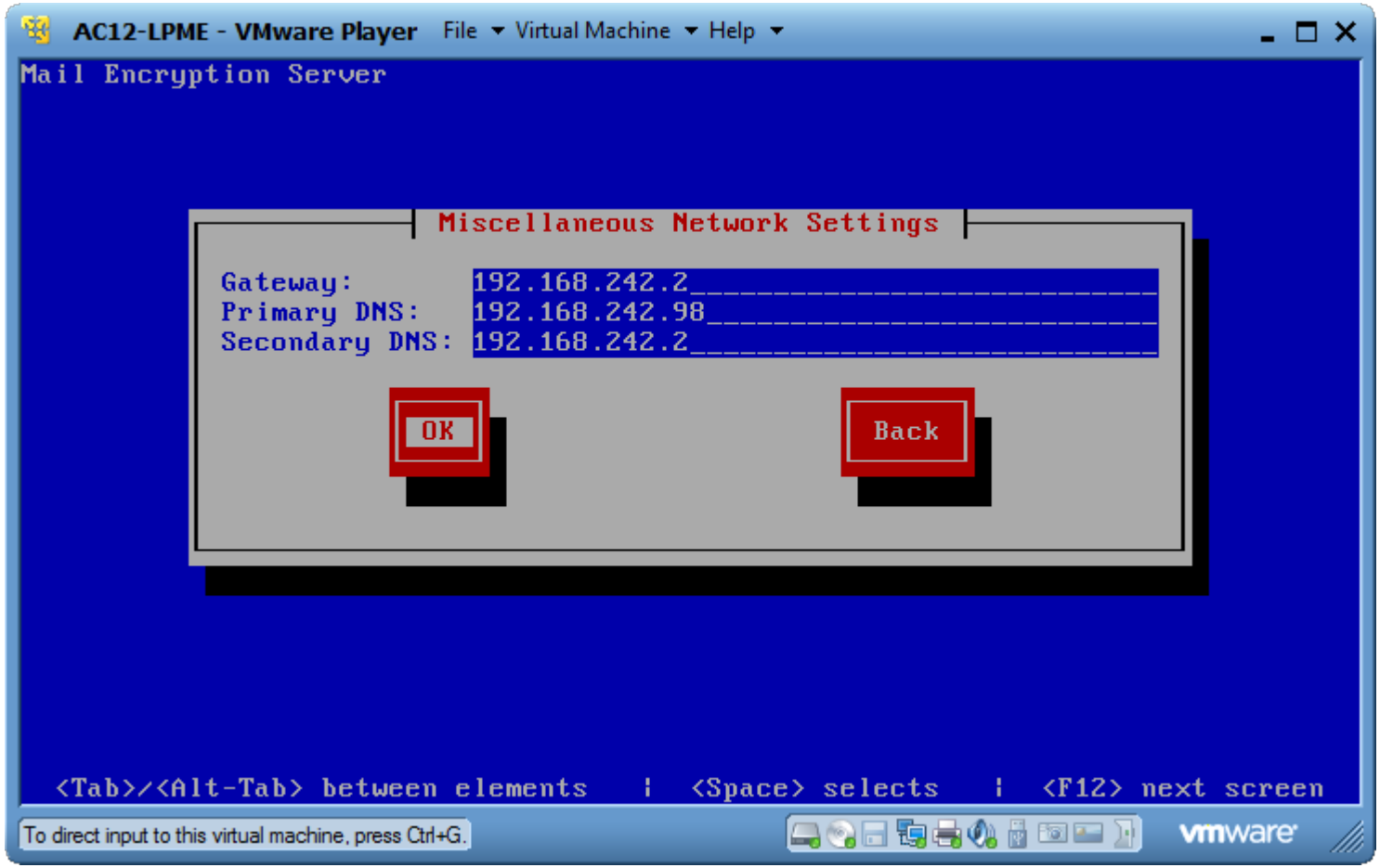
Installation



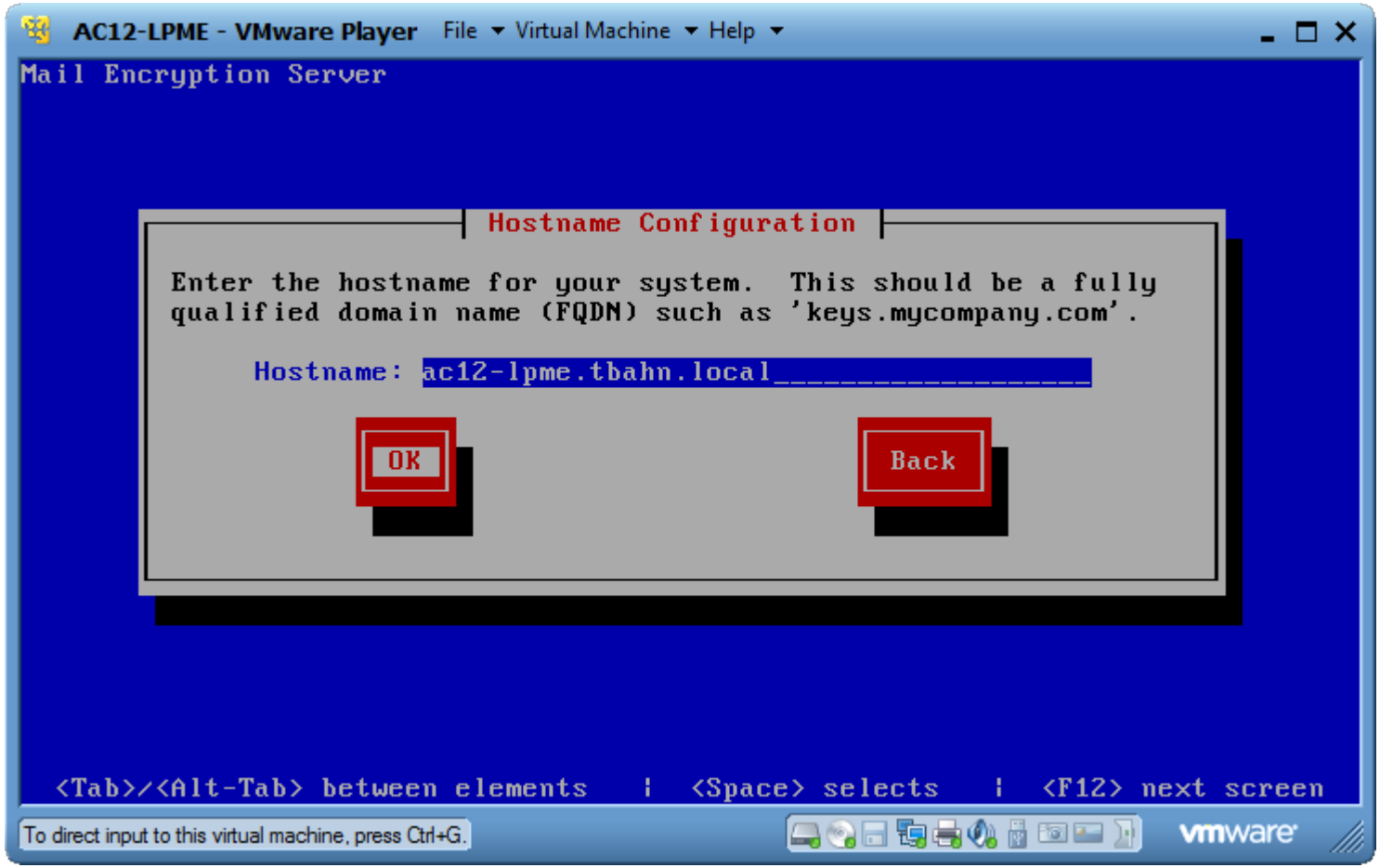
Installation



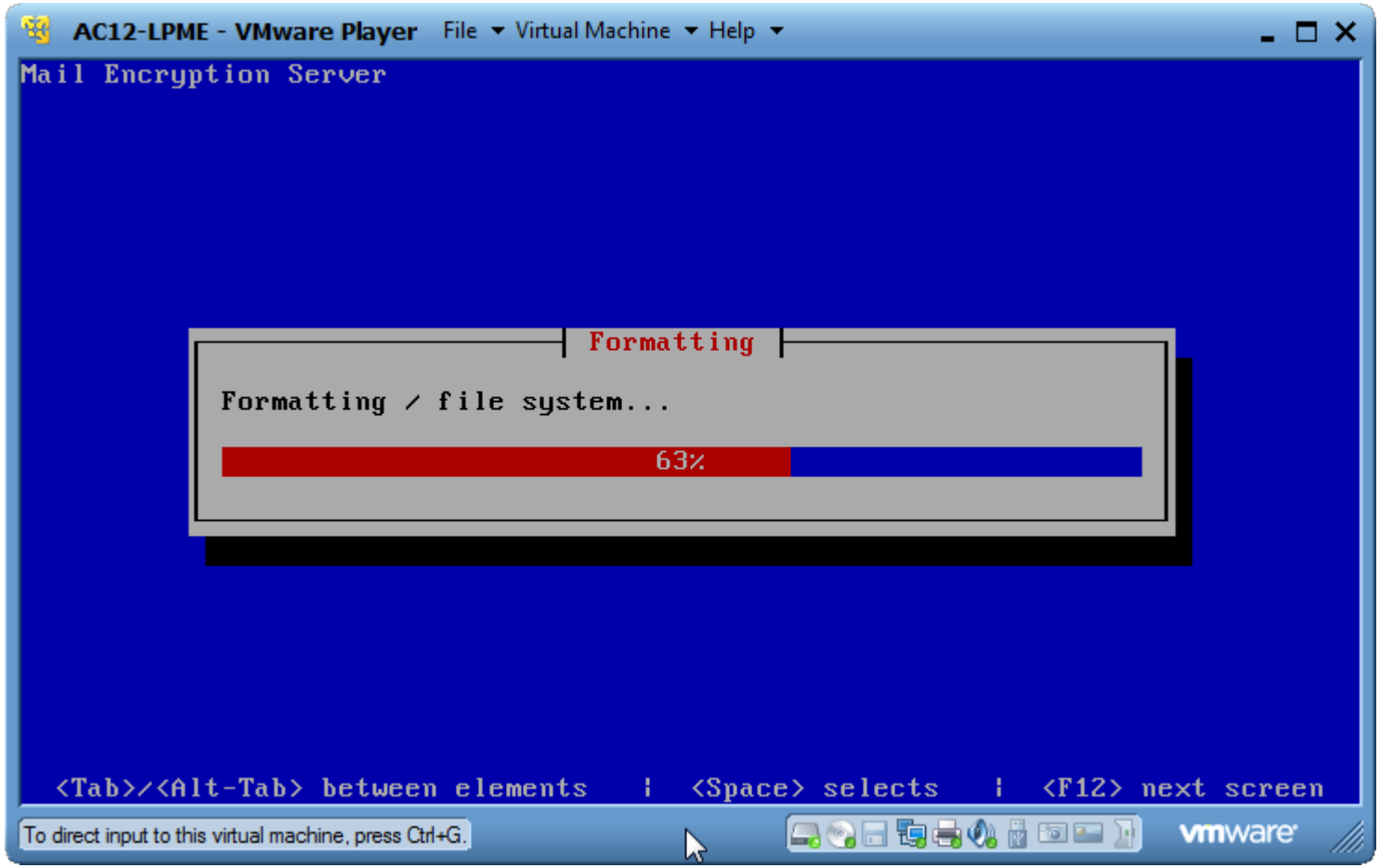
Installation



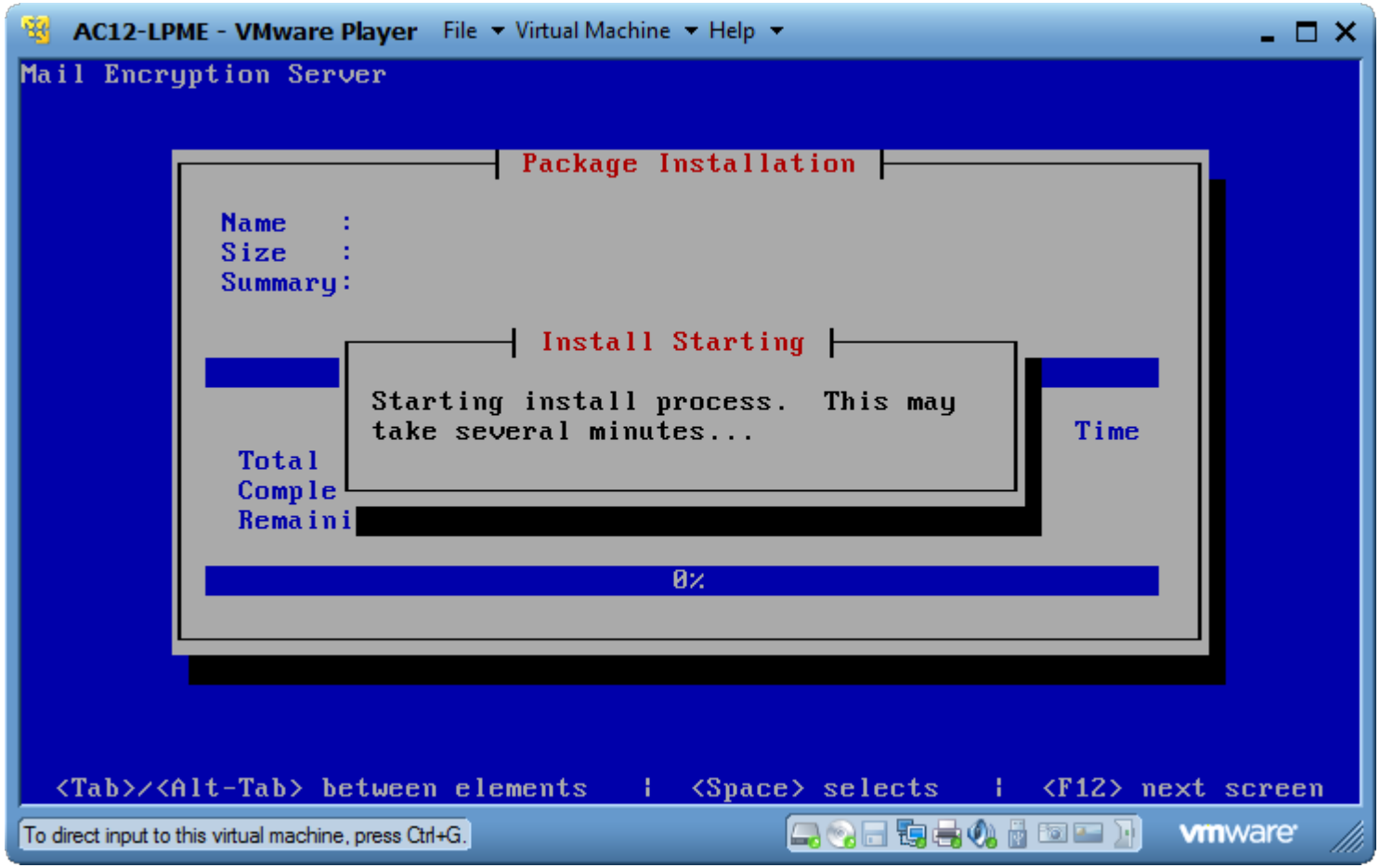
Installation



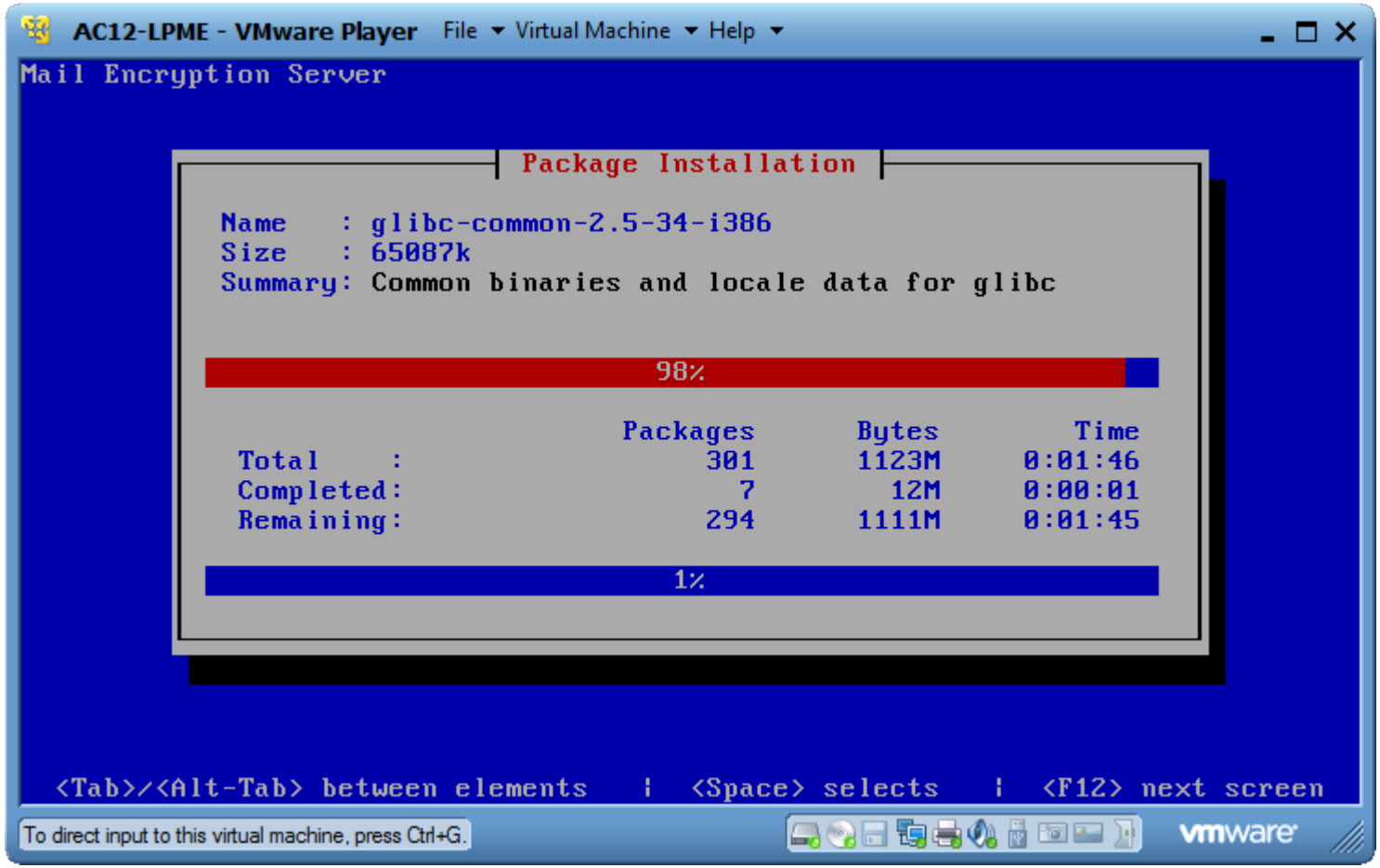
Installation



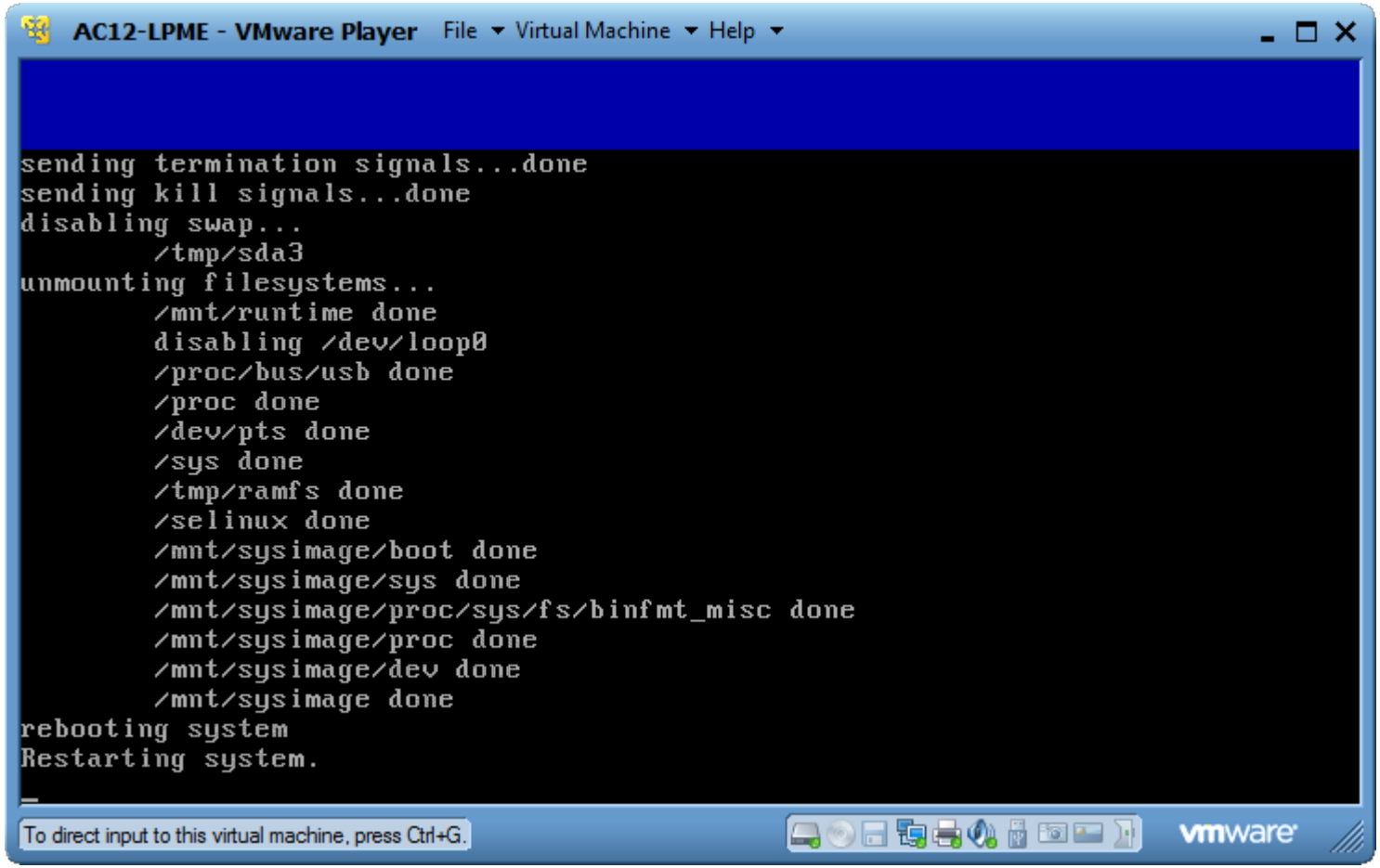
Installation



Installation

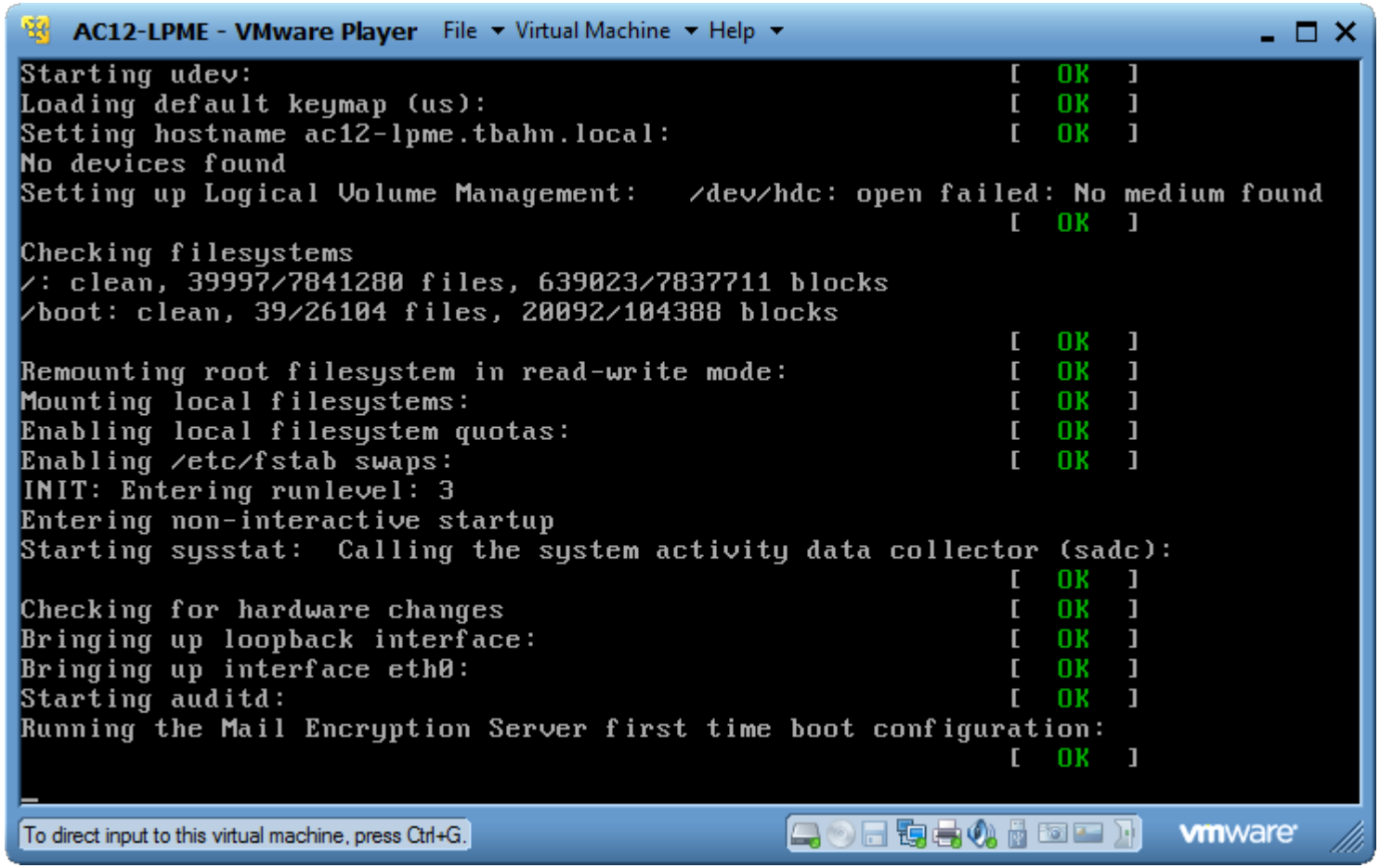


Installation

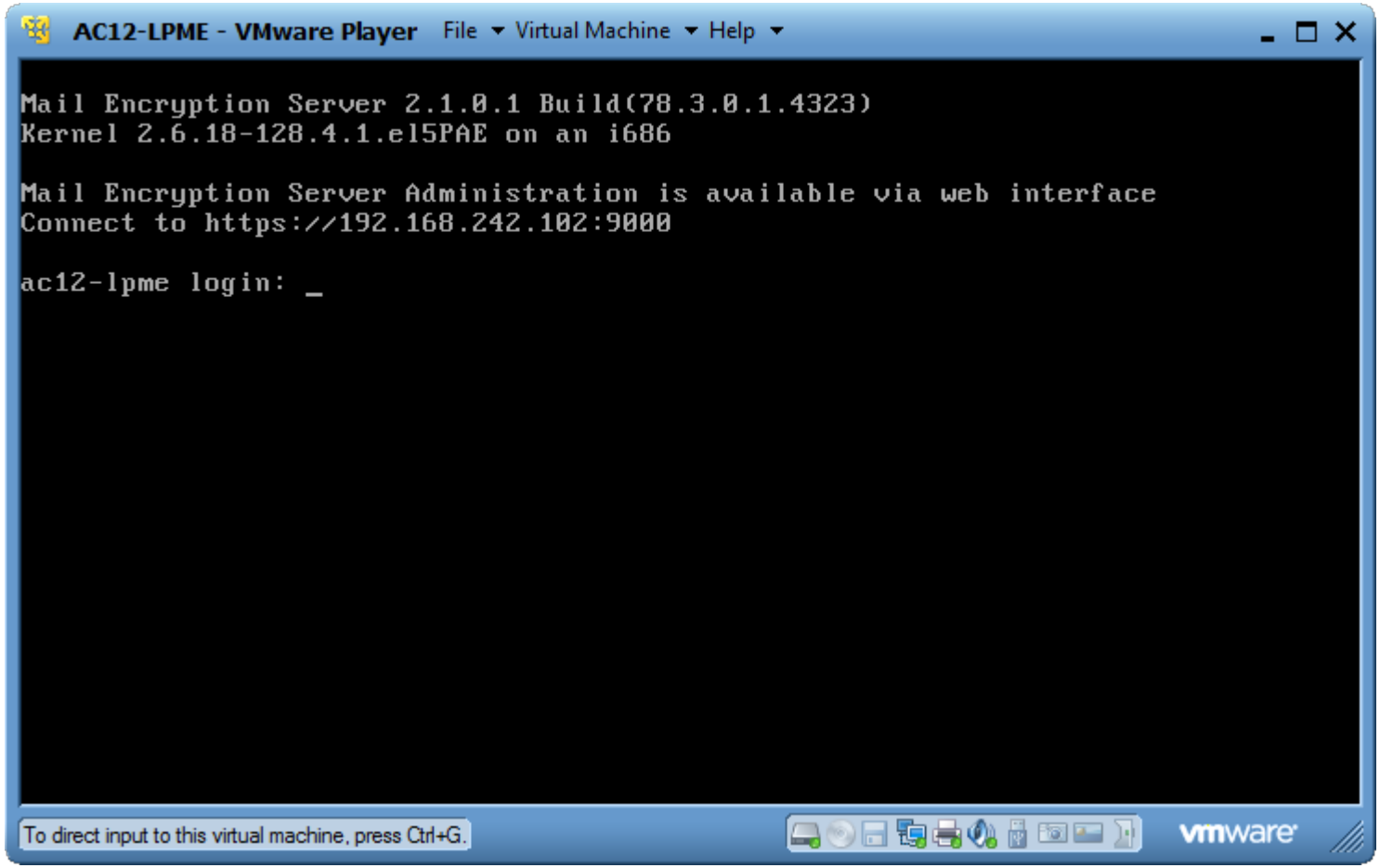


Installation

Installation

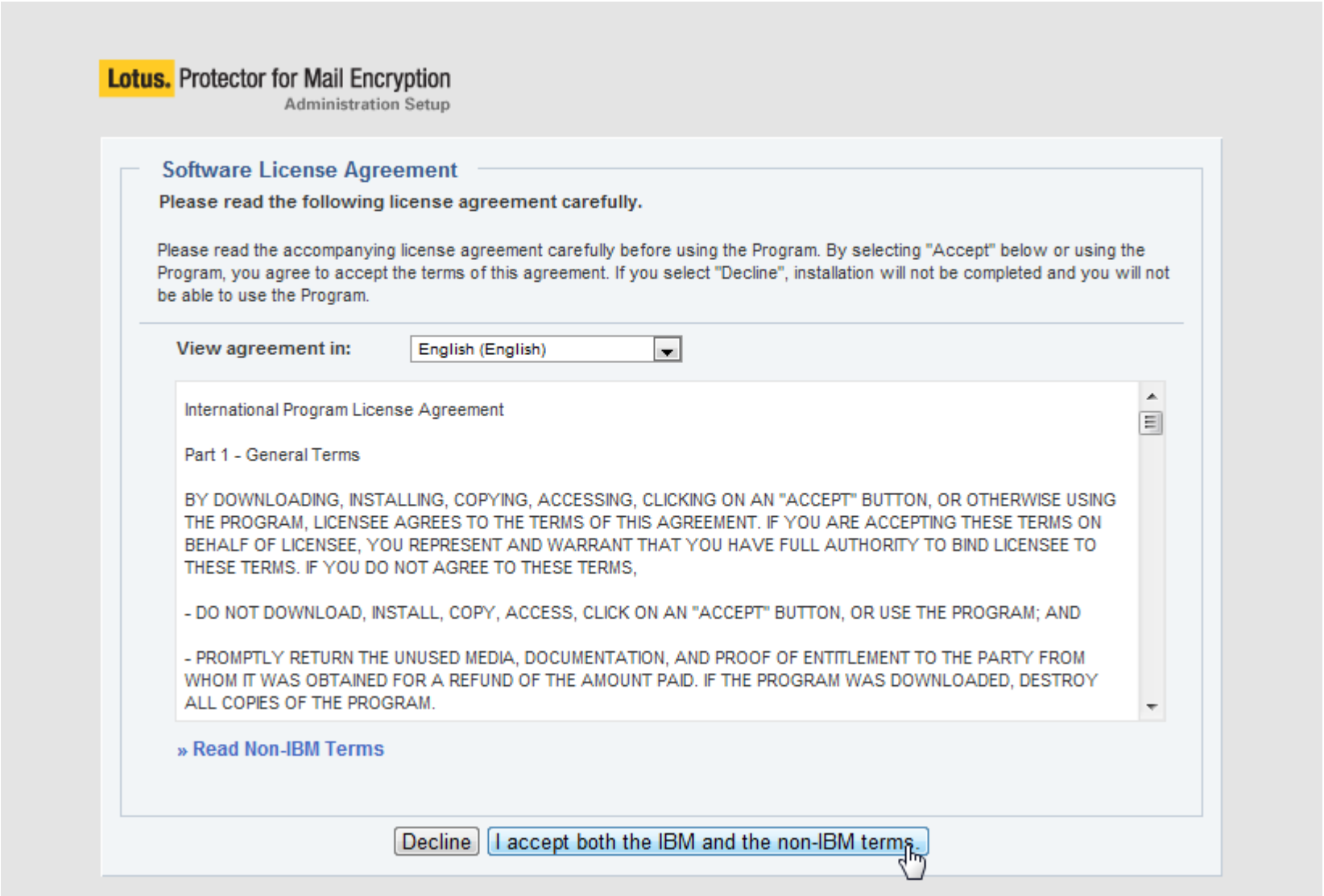


Installation

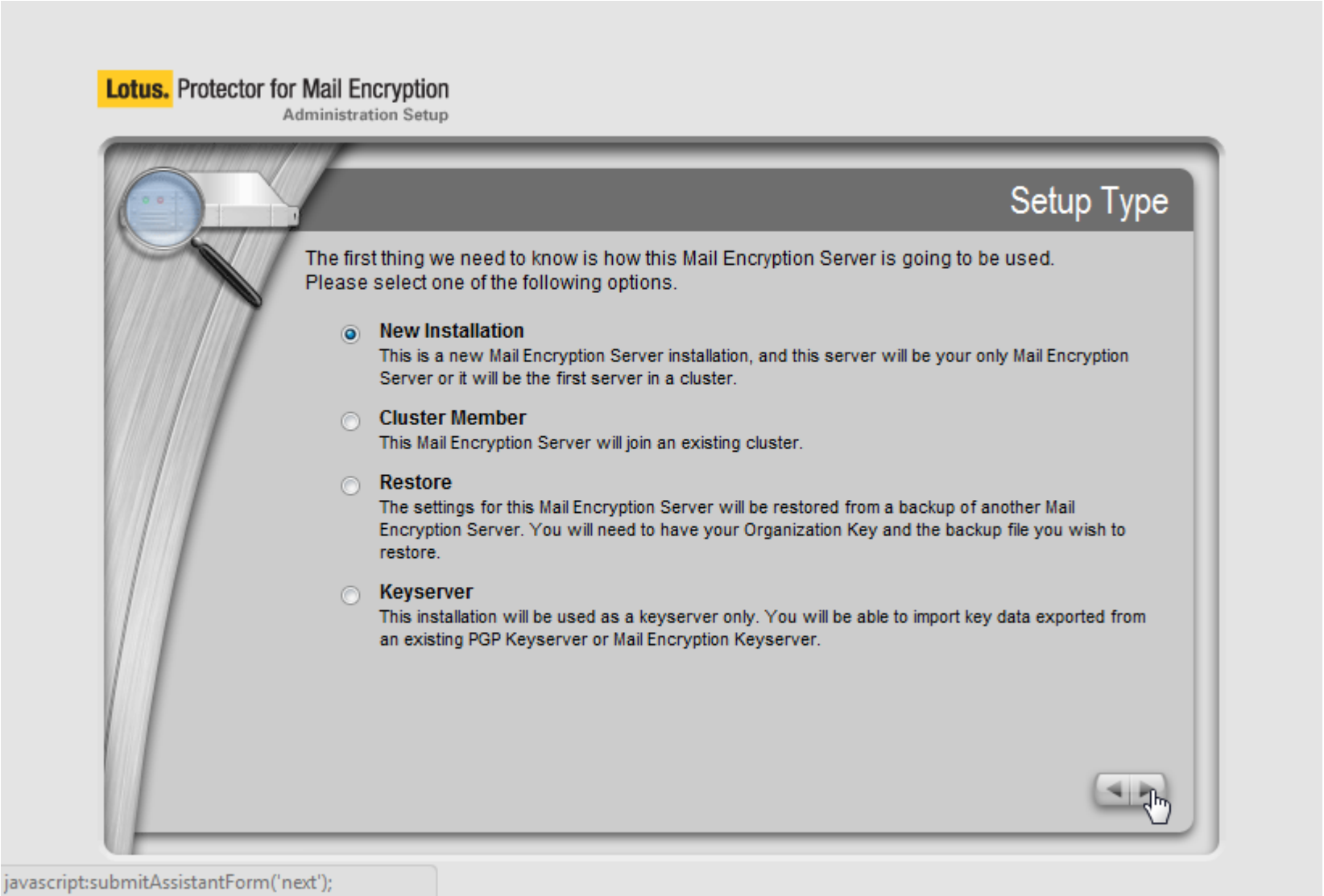


Erstkonfiguration

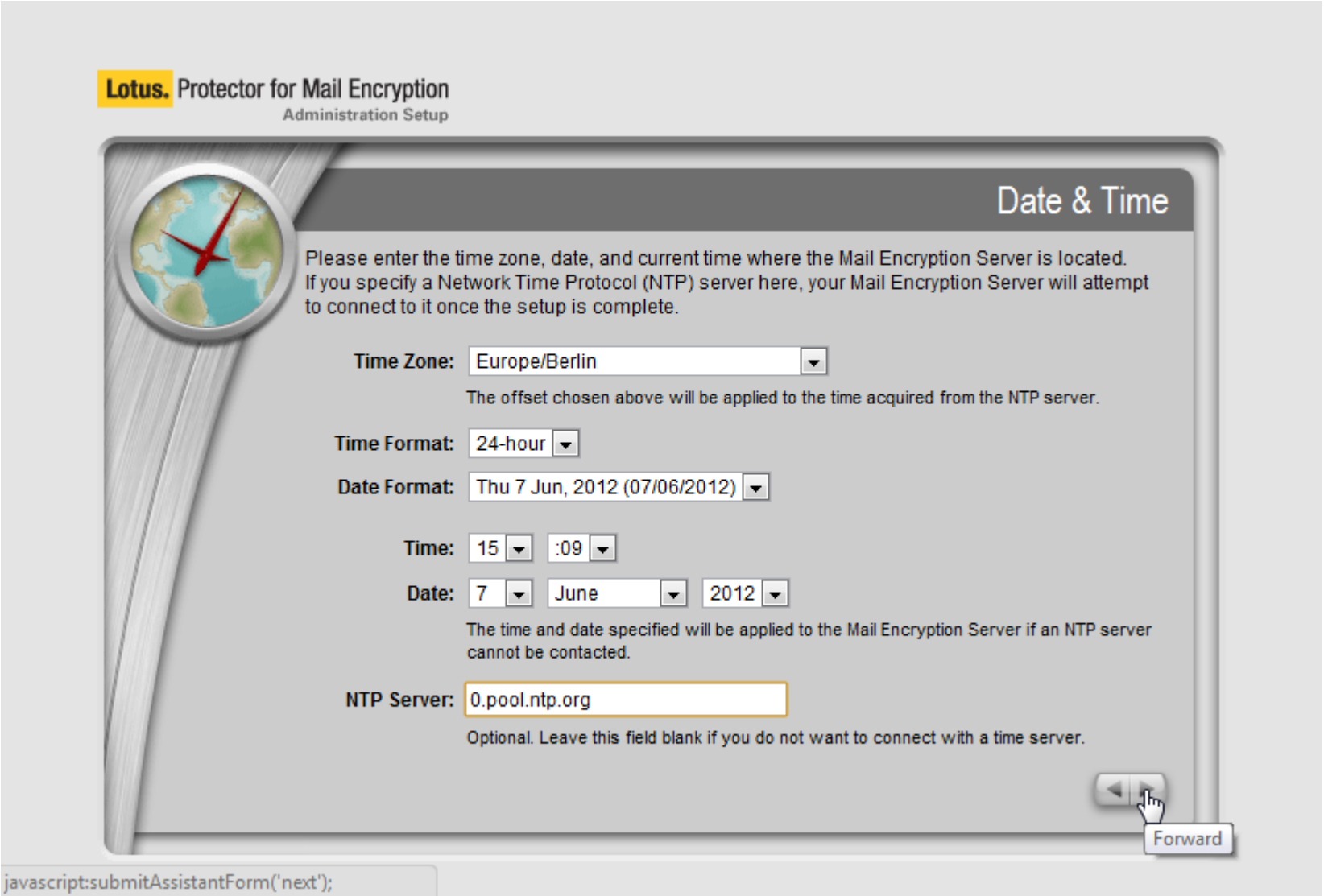
Erstkonfiguration



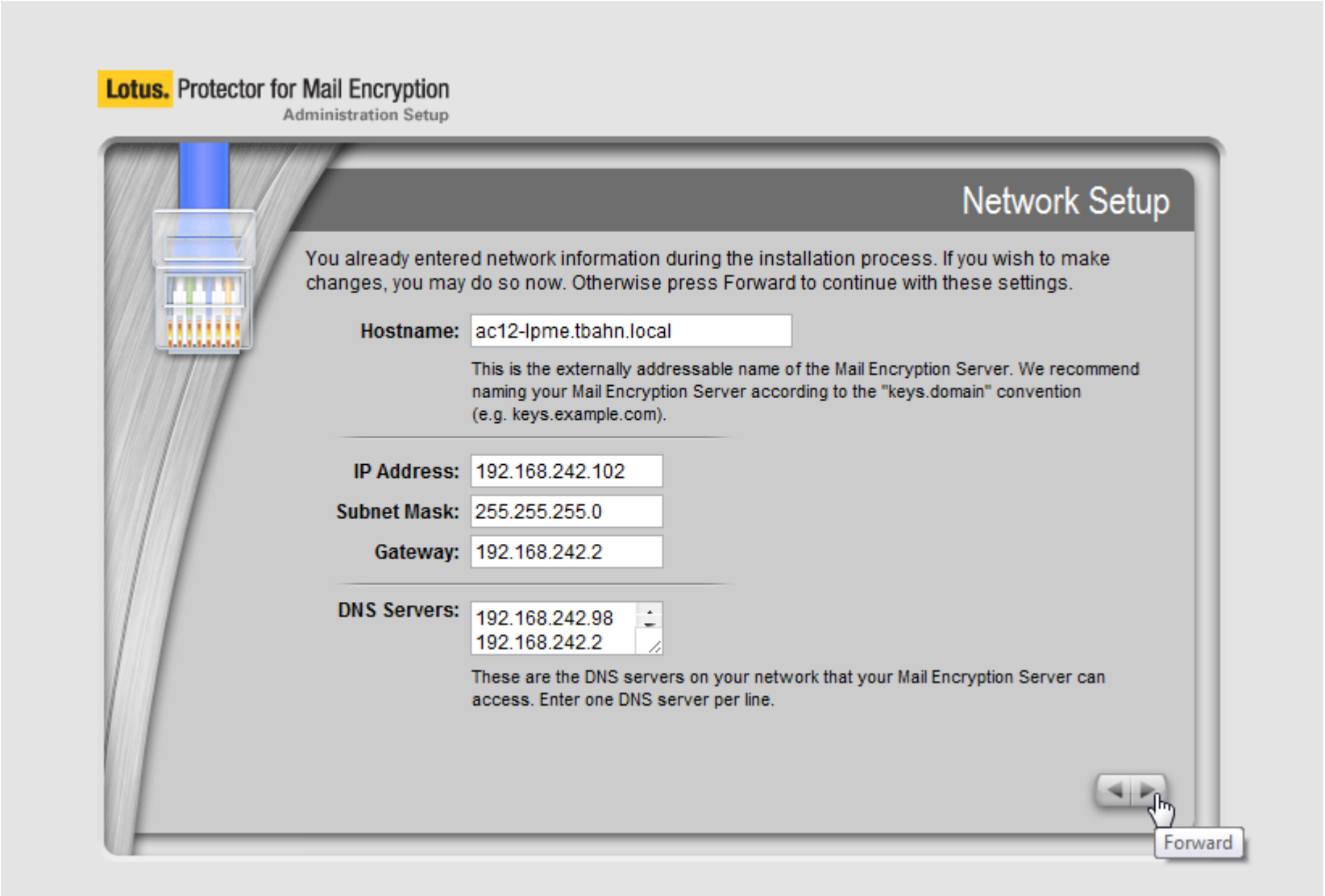
Erstkonfiguration



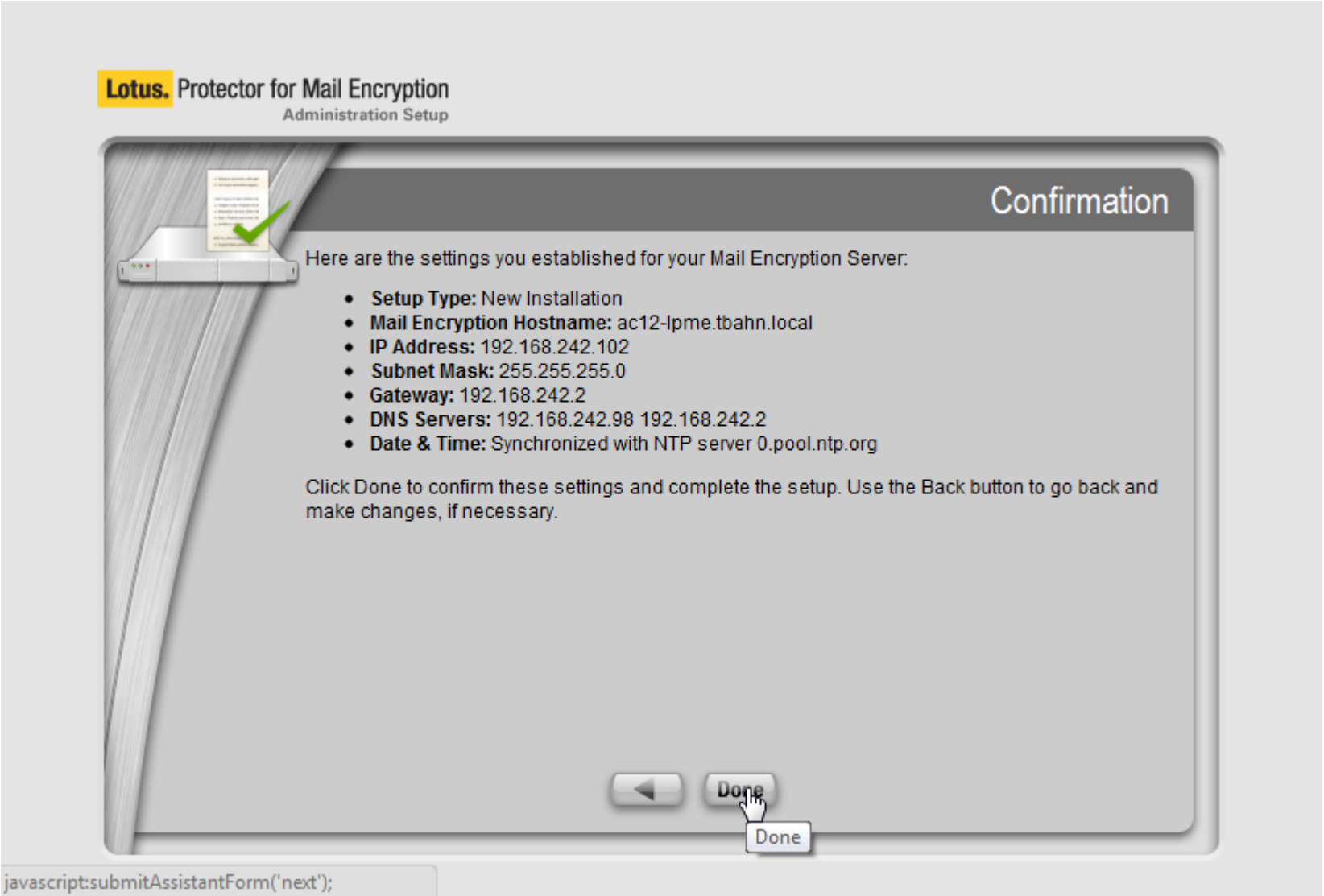
Erstkonfiguration



Erstkonfiguration

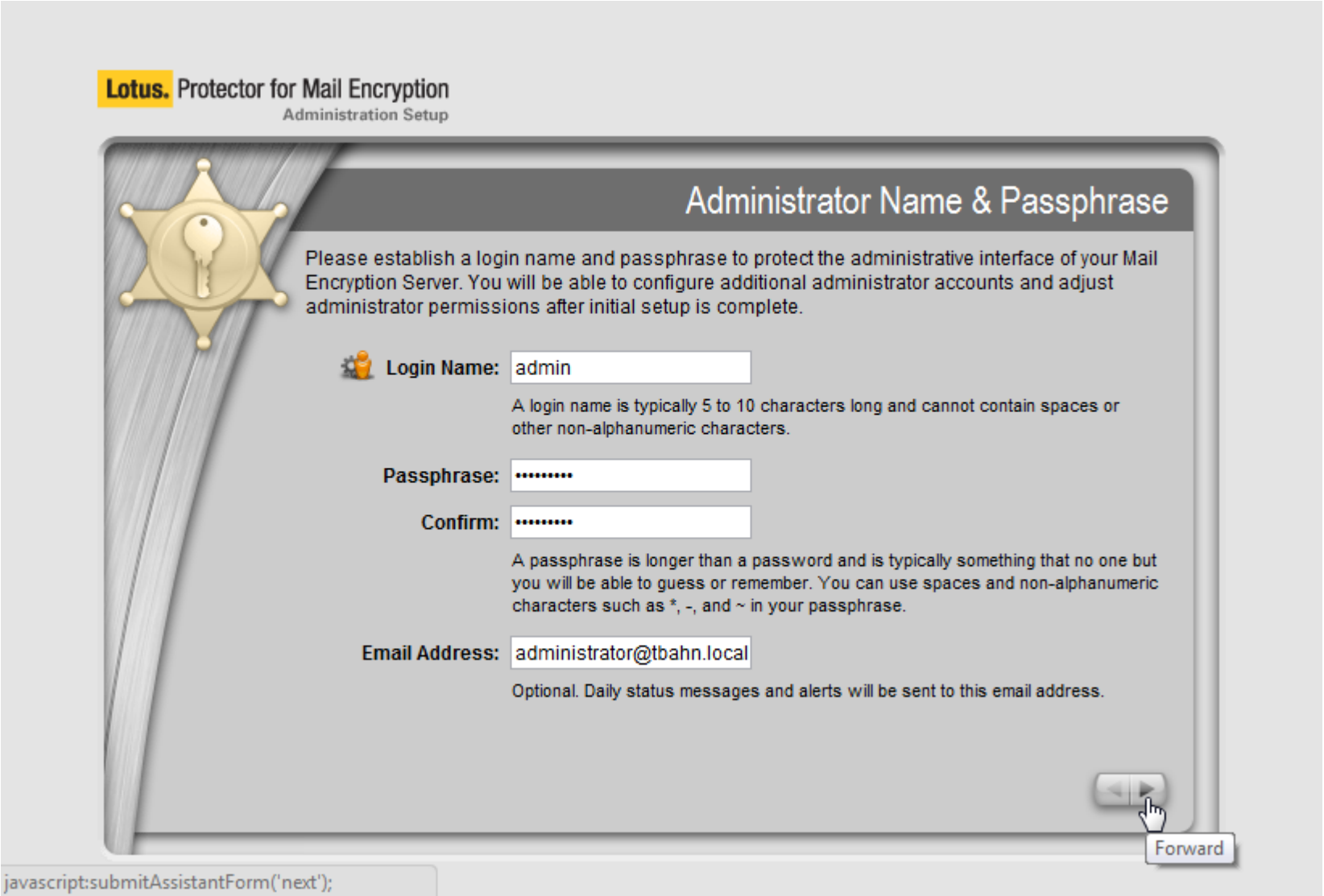


Erstkonfiguration

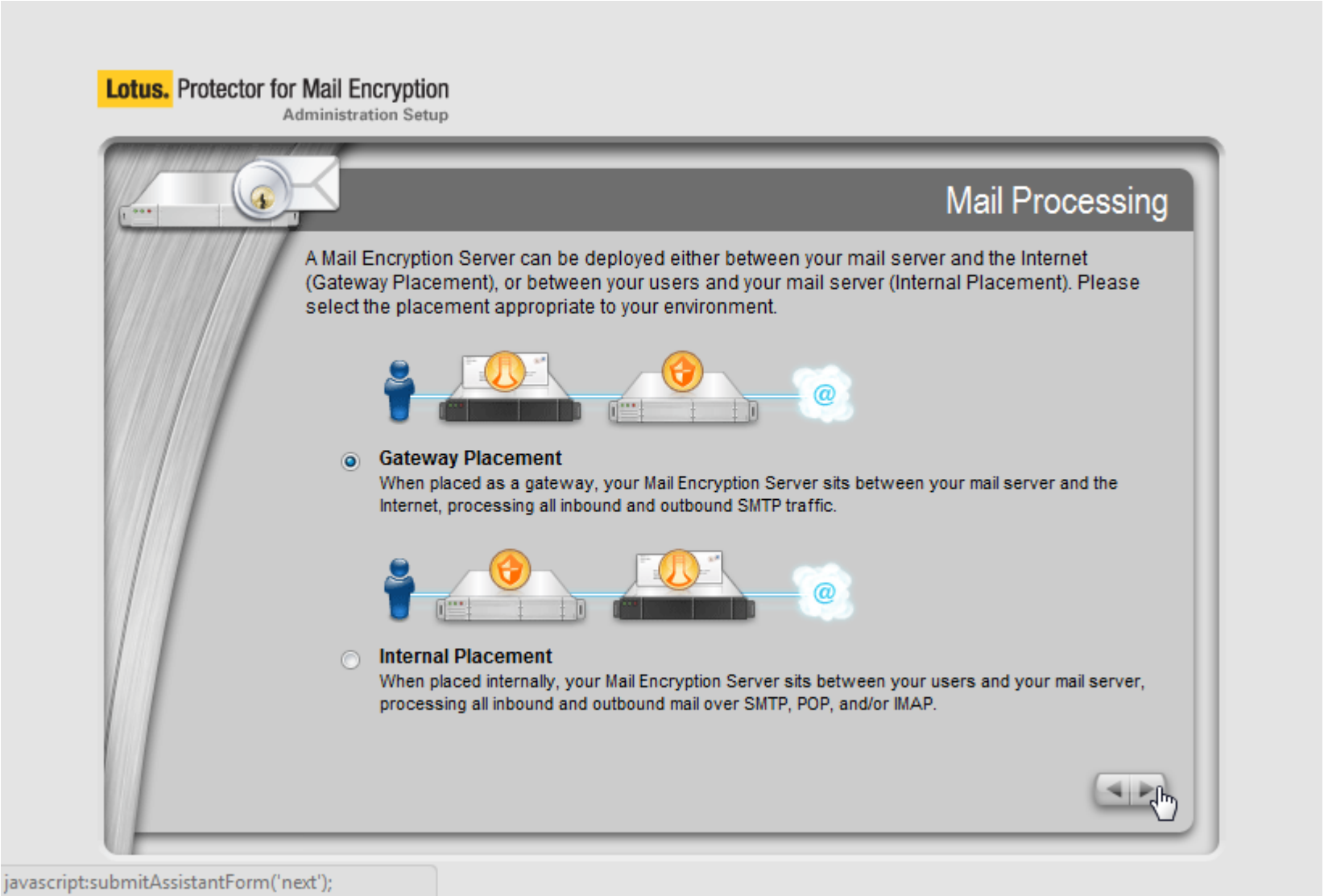


Erstkonfiguration

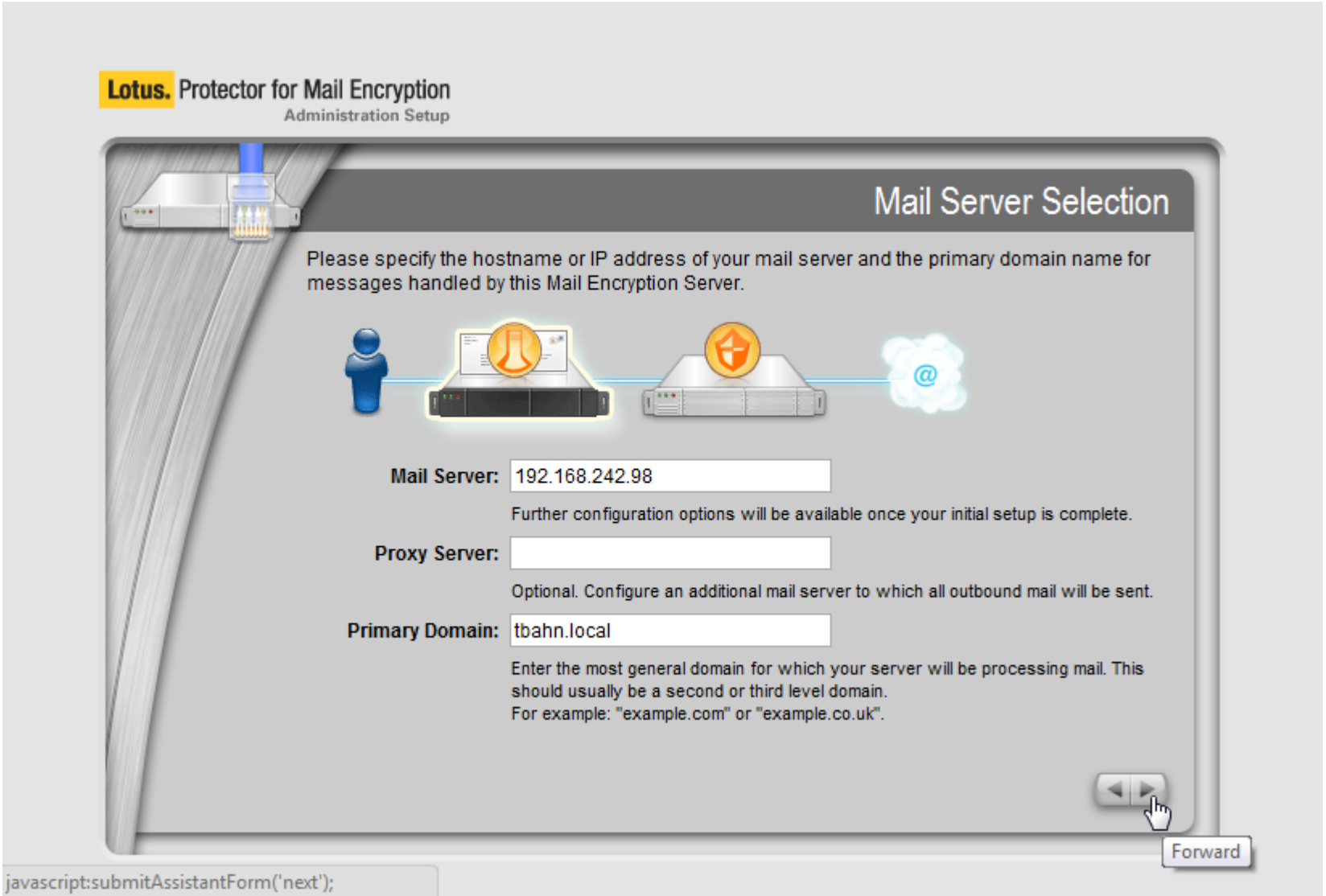
Erstkonfiguration



Erstkonfiguration

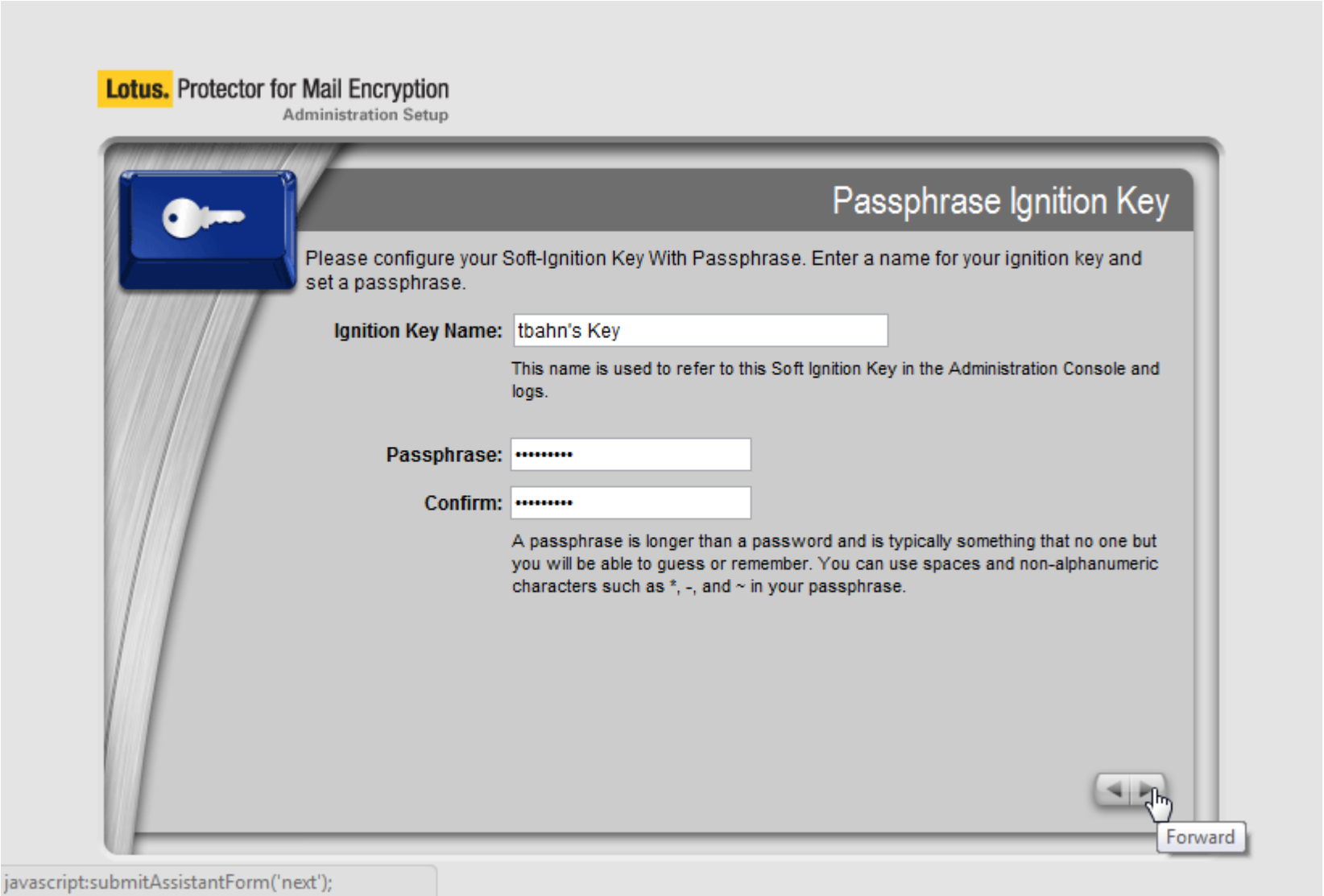


Erstkonfiguration

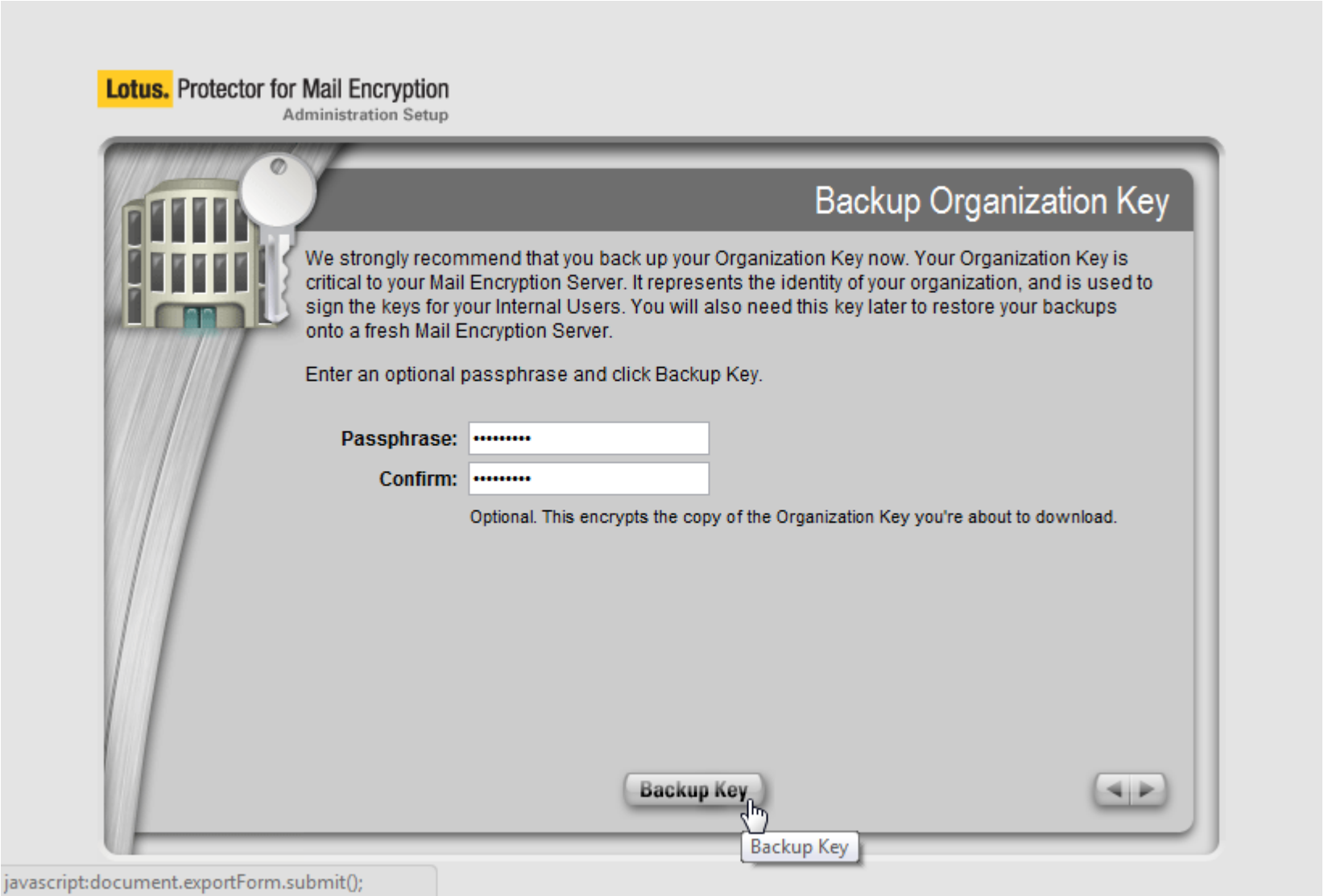


Erstkonfiguration

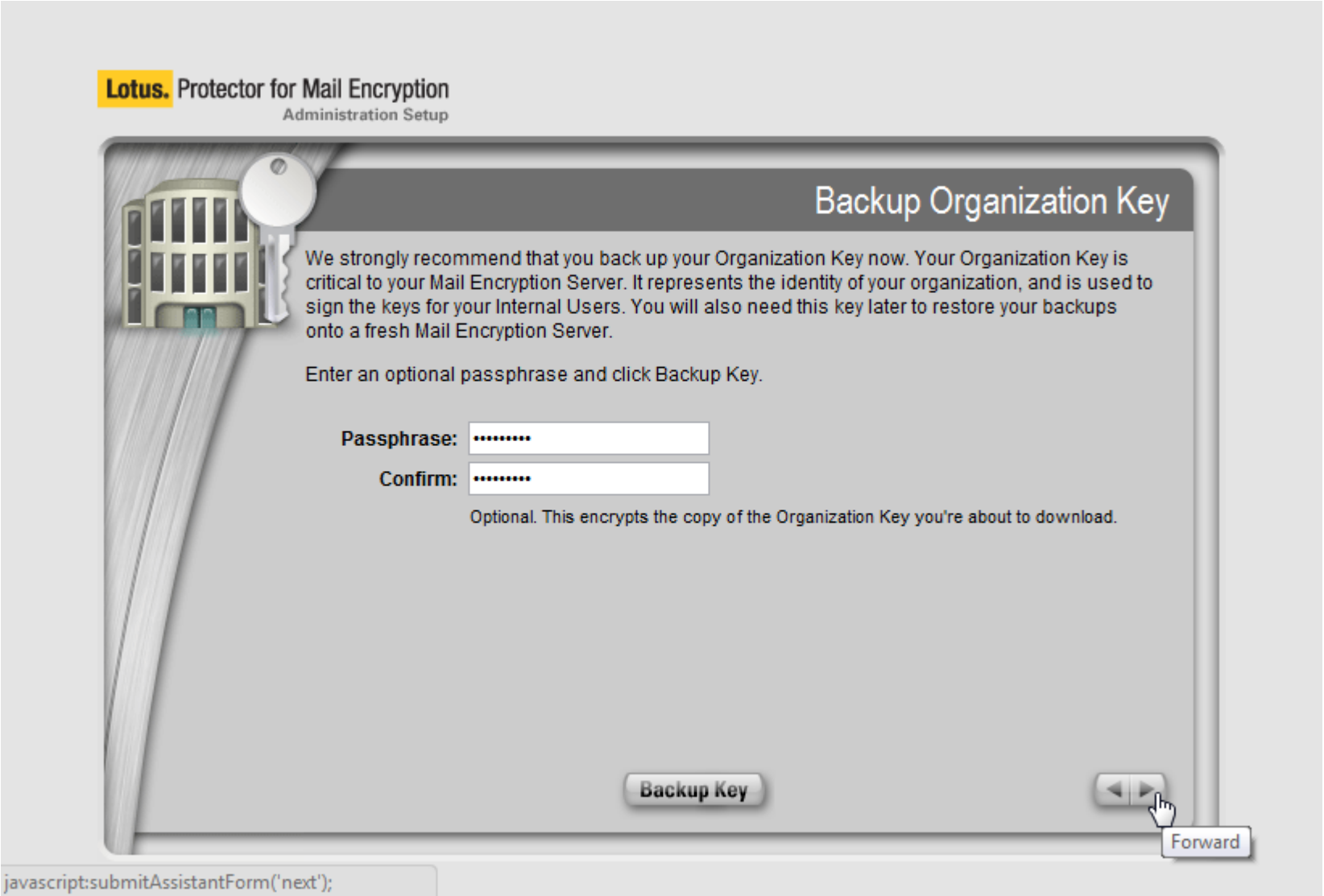
Erstkonfiguration



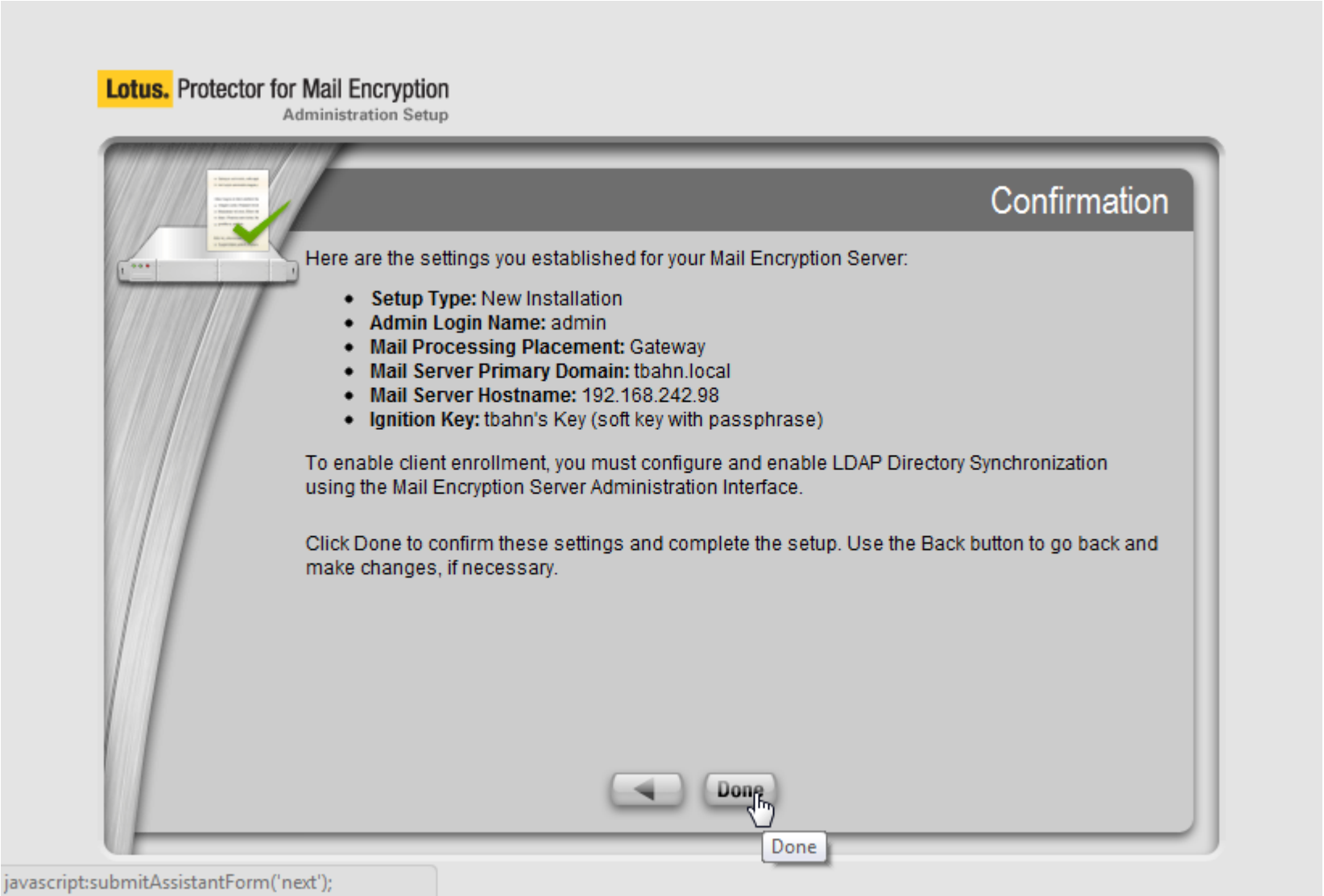
Erstkonfiguration



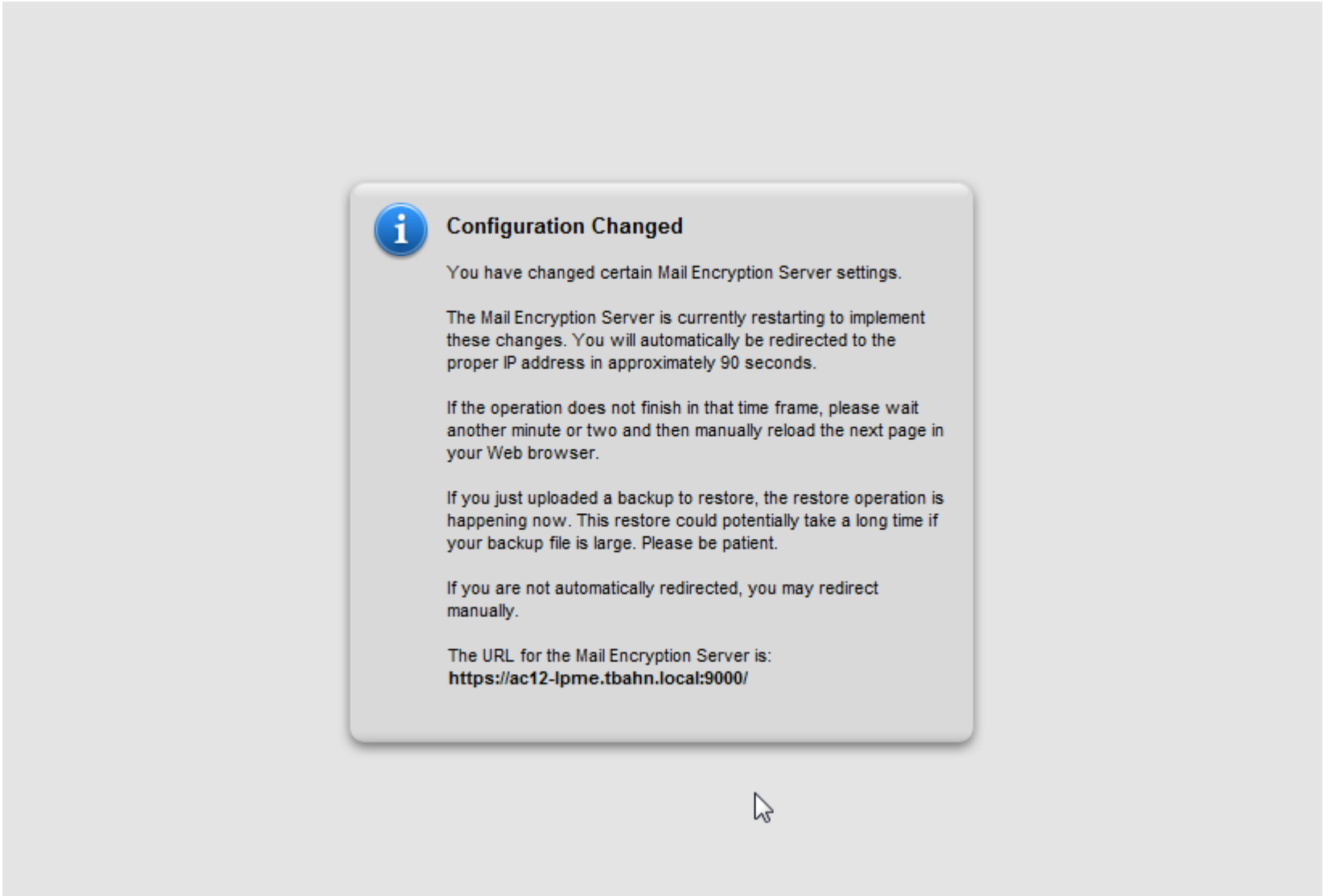
Erstkonfiguration



Erstkonfiguration



Erstkonfiguration



Erster Start (Neuanmeldung im Browser)

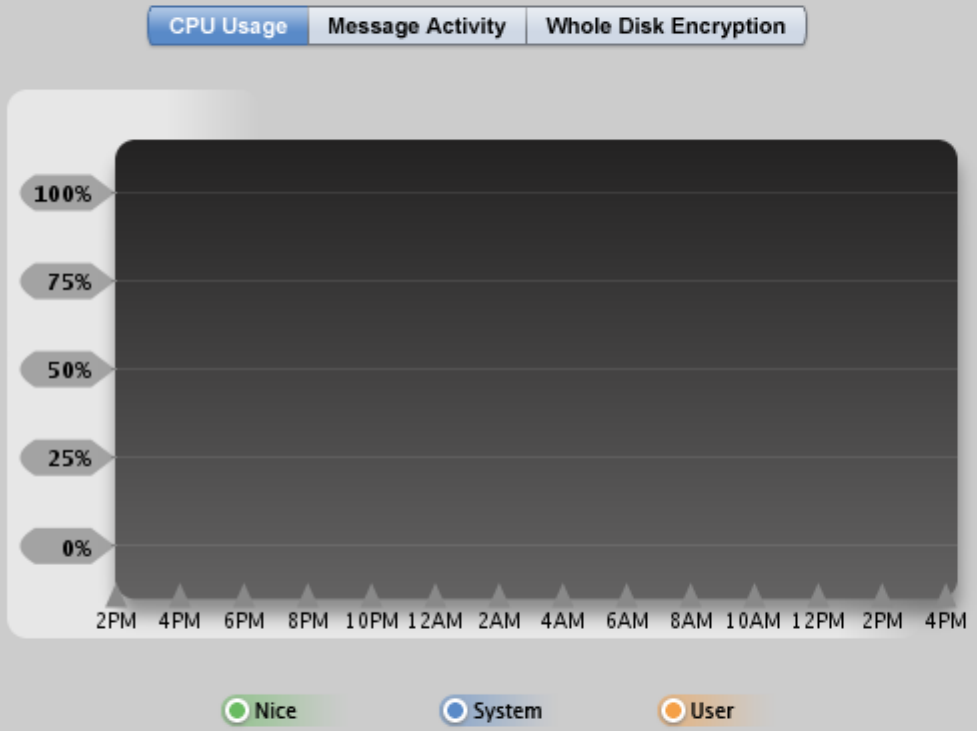
System Overview

Refresh

ac12-lpme.tbahn.local

Thu 7 Jun, 2012 at 15:18

System Graphs



Services

Web Messenger https://ac12-lpme.tbahn.l... 0 users		Running
Keyserver ldap://ac12-lpme.tbahn.lo... 1 key		Running
SNMP		Stopped
Verified Directory http://ac12-lpme.tbahn.lo... 0 users		Stopped
Mail Proxies		Running
Certificate Revocation		Running
Universal Services Protocol		Running

Statistics

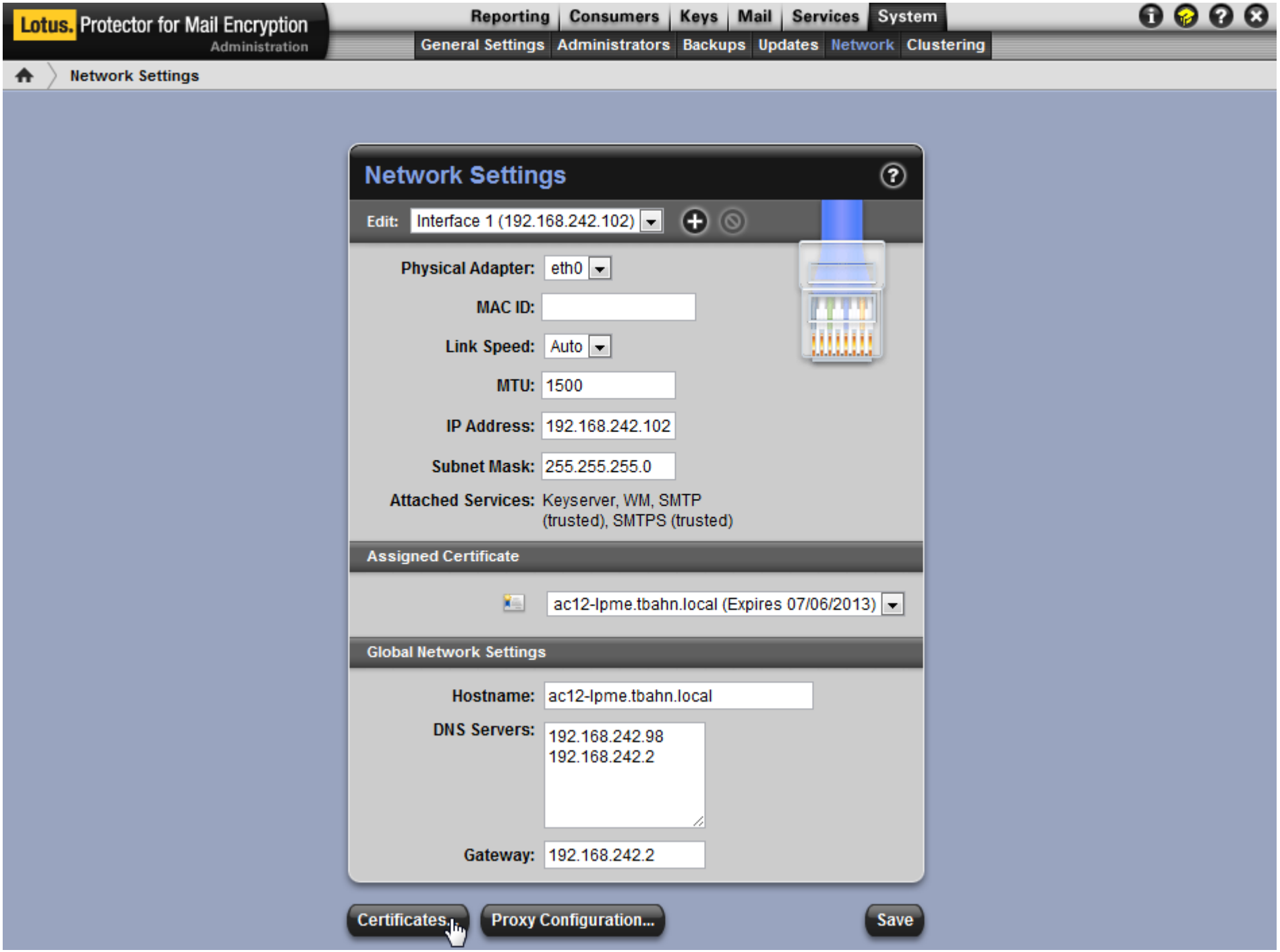
Server Version	2.1.0.1 Build (78.3.0.1.4323)
System Uptime	0d, 00h, 14m
Total Messages Processed	0

Mail Queue

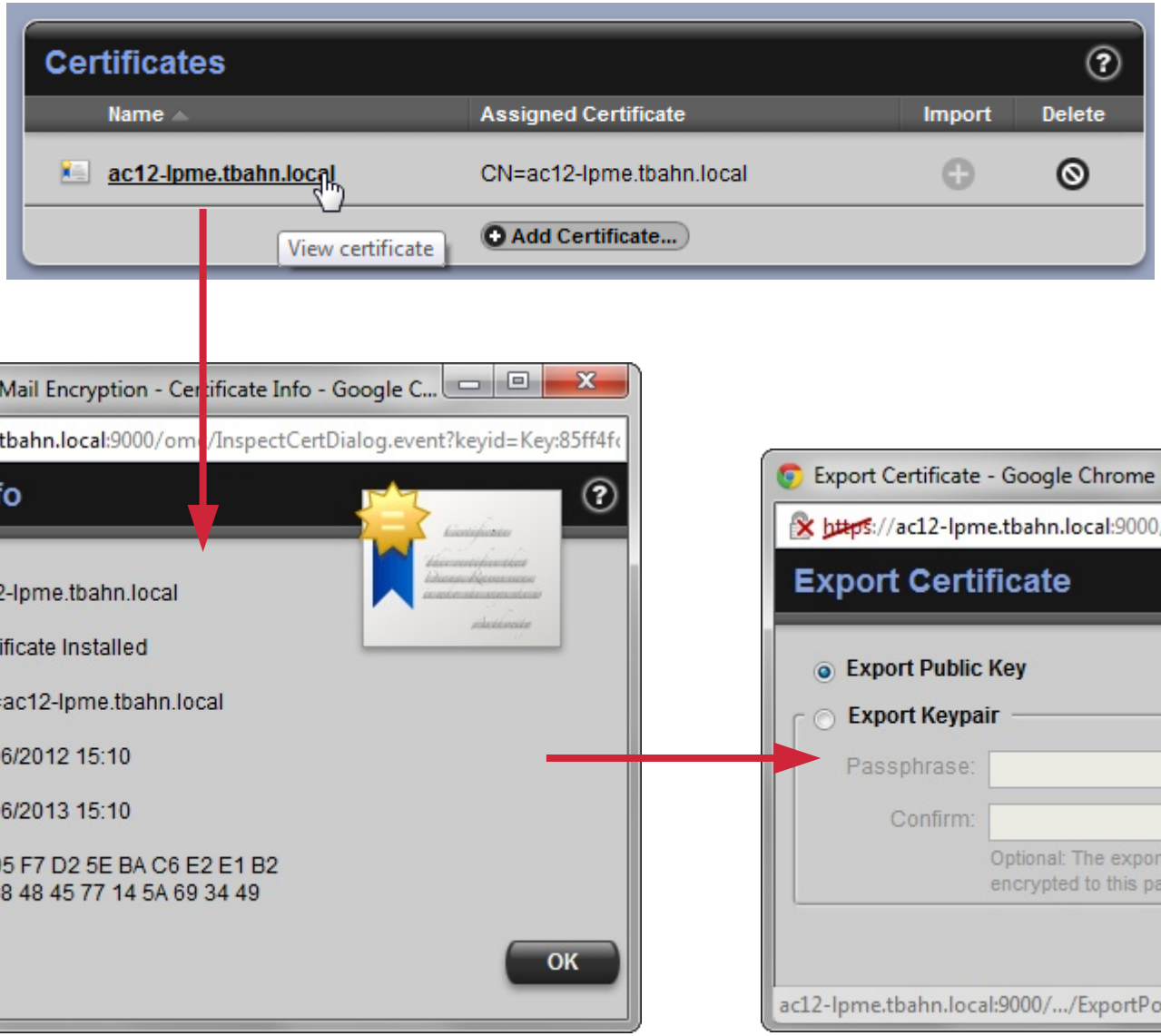
Messages	0
Size	0 KB

Estimated Policy Group Membership

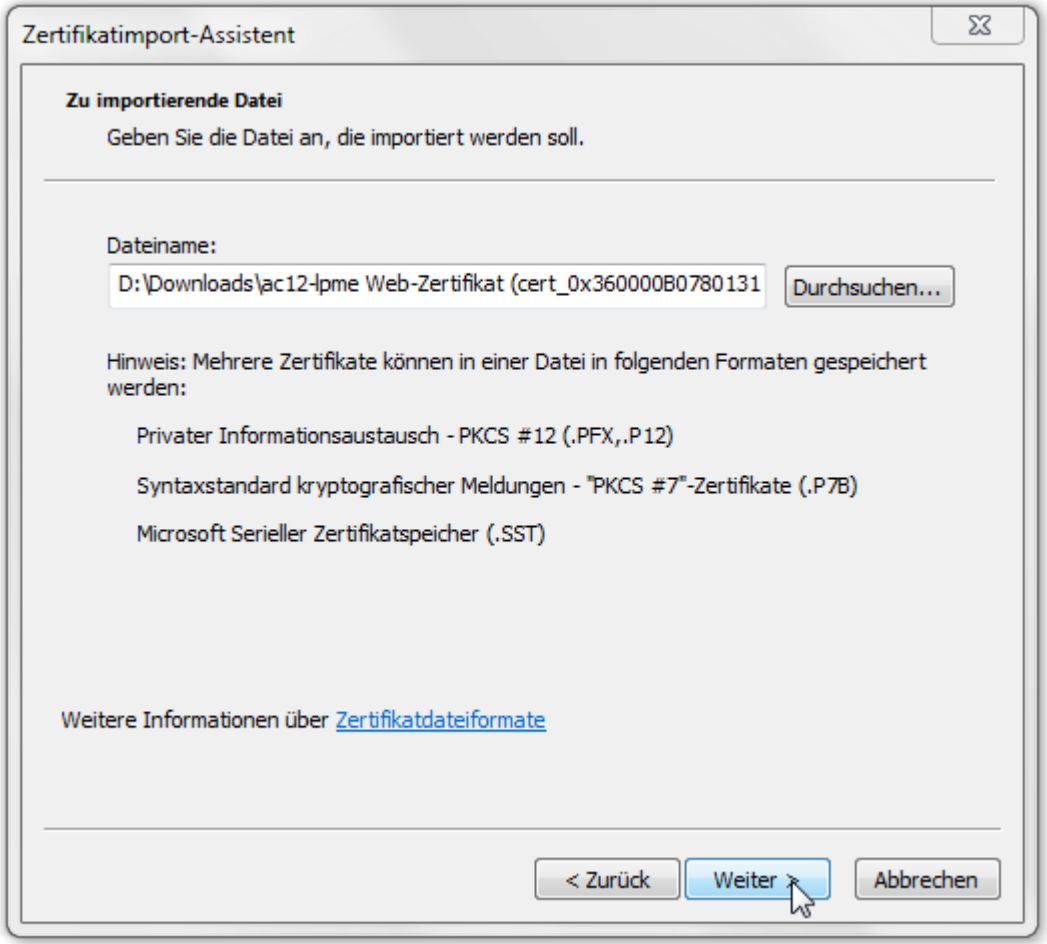
Everyone	0


Lotus. Protector for Mail Encryption
Administration
Reporting
Consumers
Keys
Mail
Services
System
General Settings
Administrators
Backups
Updates
Network
Clustering
Network Settings
Network Settings
Edit:
Interface 1 (192.168.242.102)
Physical Adapter:
eth0
MAC ID:
Link Speed:
Auto
MTU:
1500
IP Address:
192.168.242.102
Subnet Mask:
255.255.255.0
Attached Services:
Keyserver, WM, SMTP (trusted), SMTPS (trusted)
Assigned Certificate
ac12-lpme.tbahn.local (Expires 07/06/2013)
Global Network Settings
Hostname:
ac12-lpme.tbahn.local
DNS Servers:
192.168.242.98
192.168.242.2
Gateway:
192.168.242.2
Certificates...
Proxy Configuration...
Save

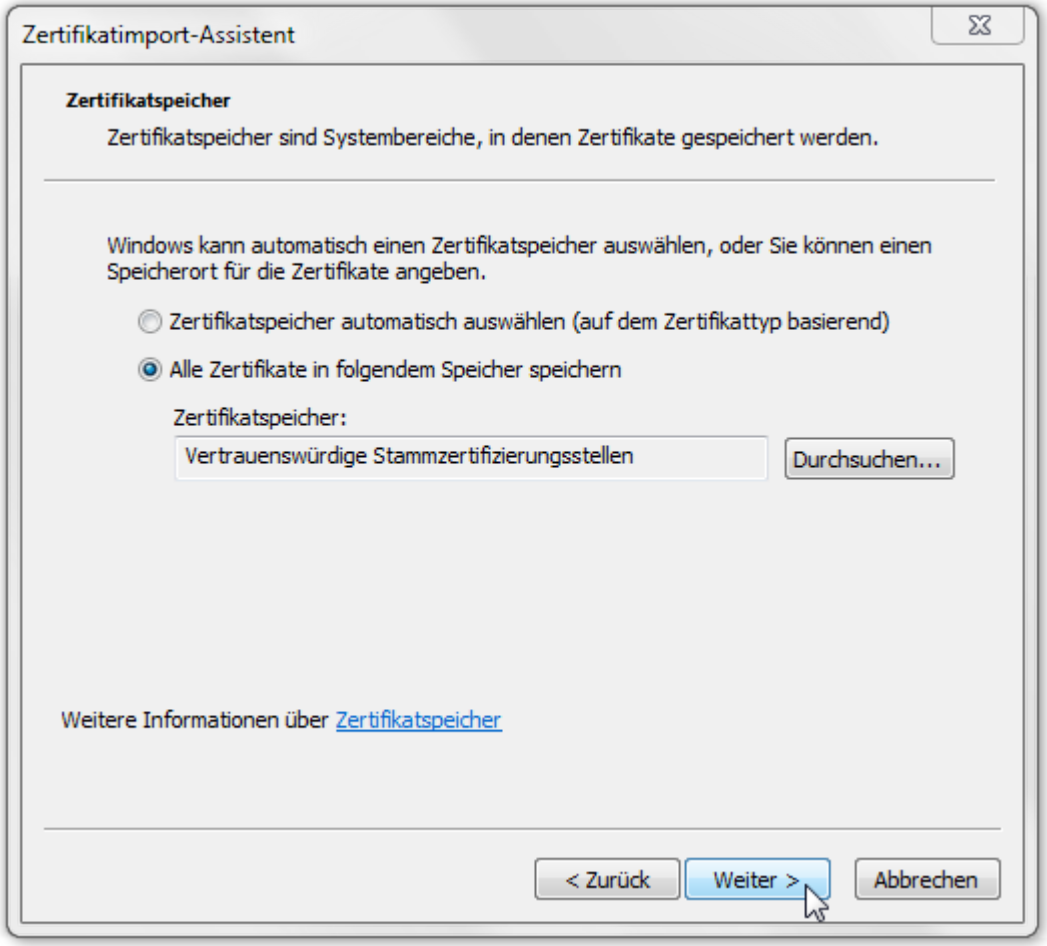
Warnung wegen des SSL-Zertifikats



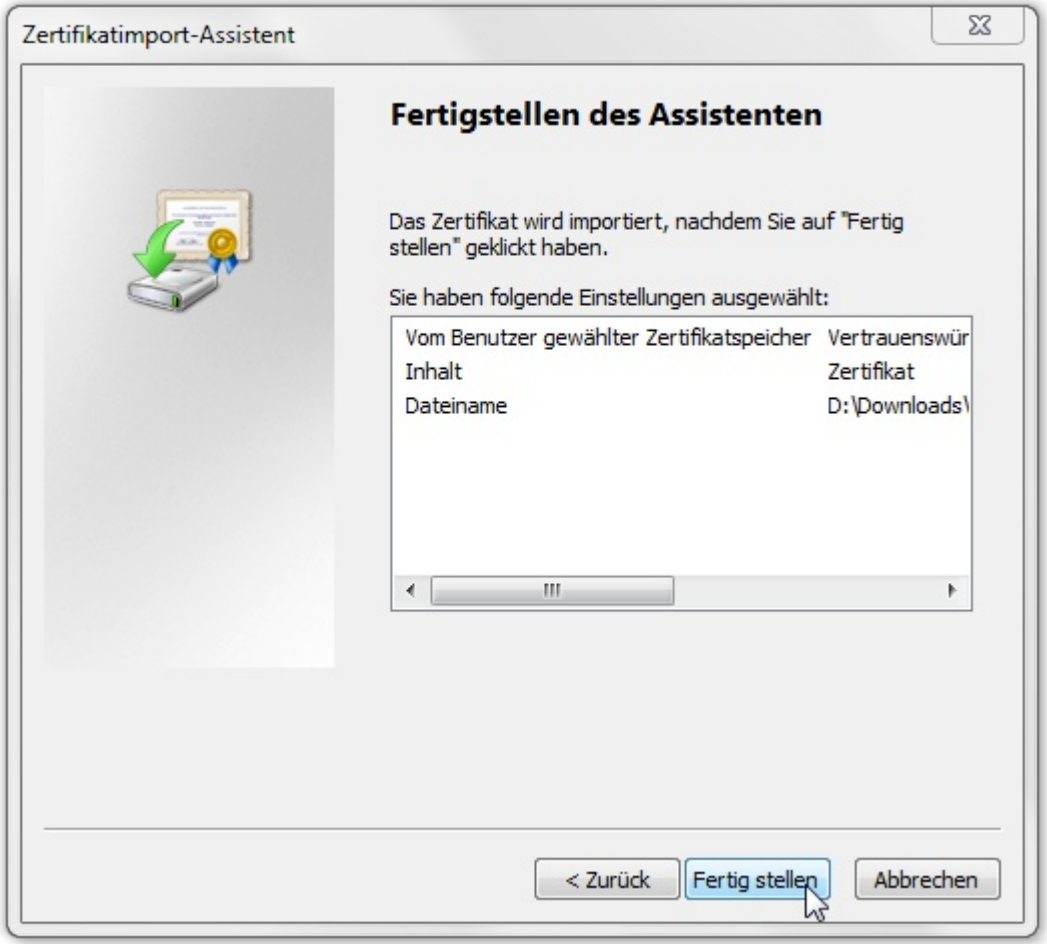
Warnung wegen des SSL-Zertifikats



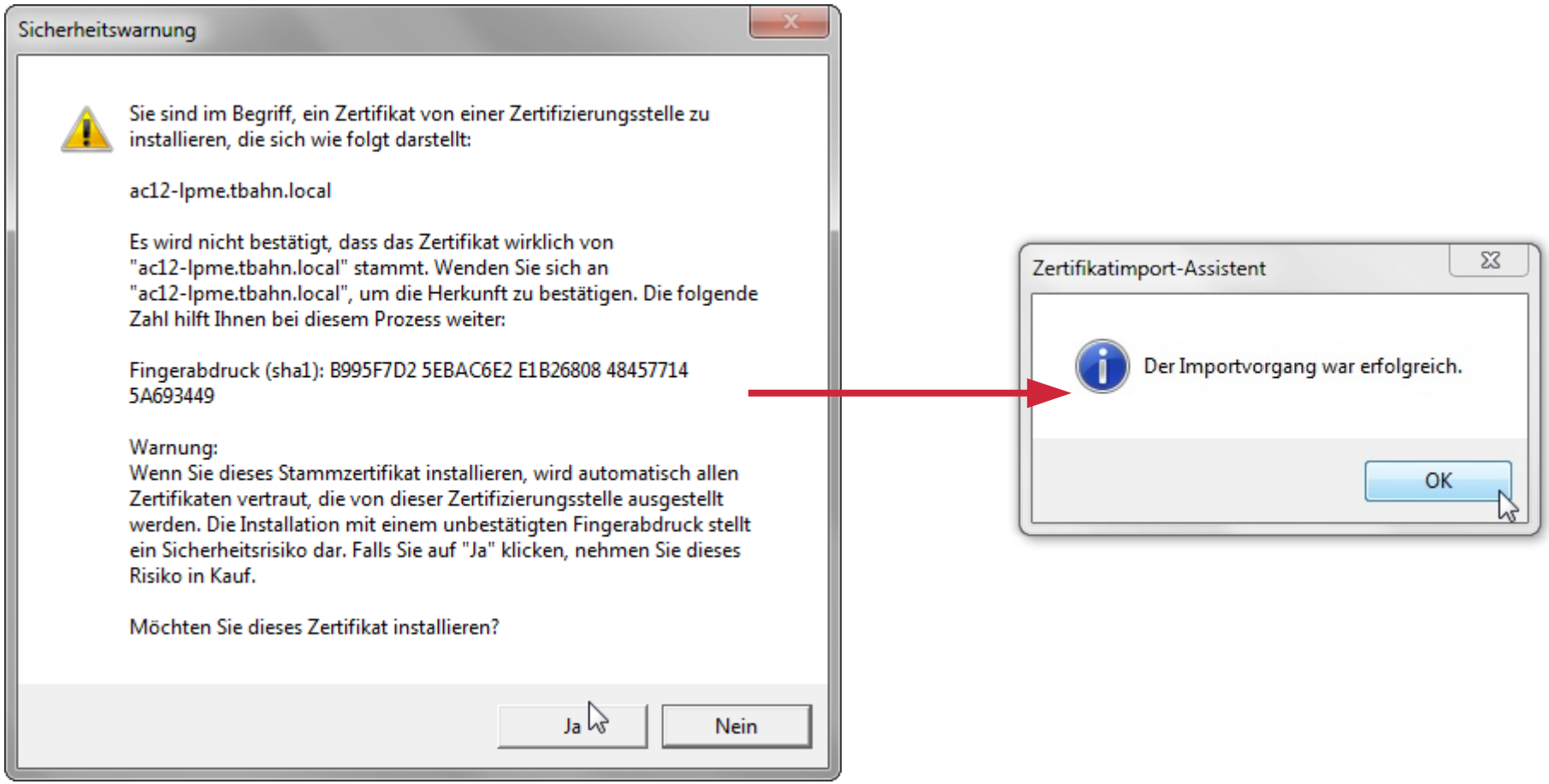
Warnung wegen des SSL-Zertifikats



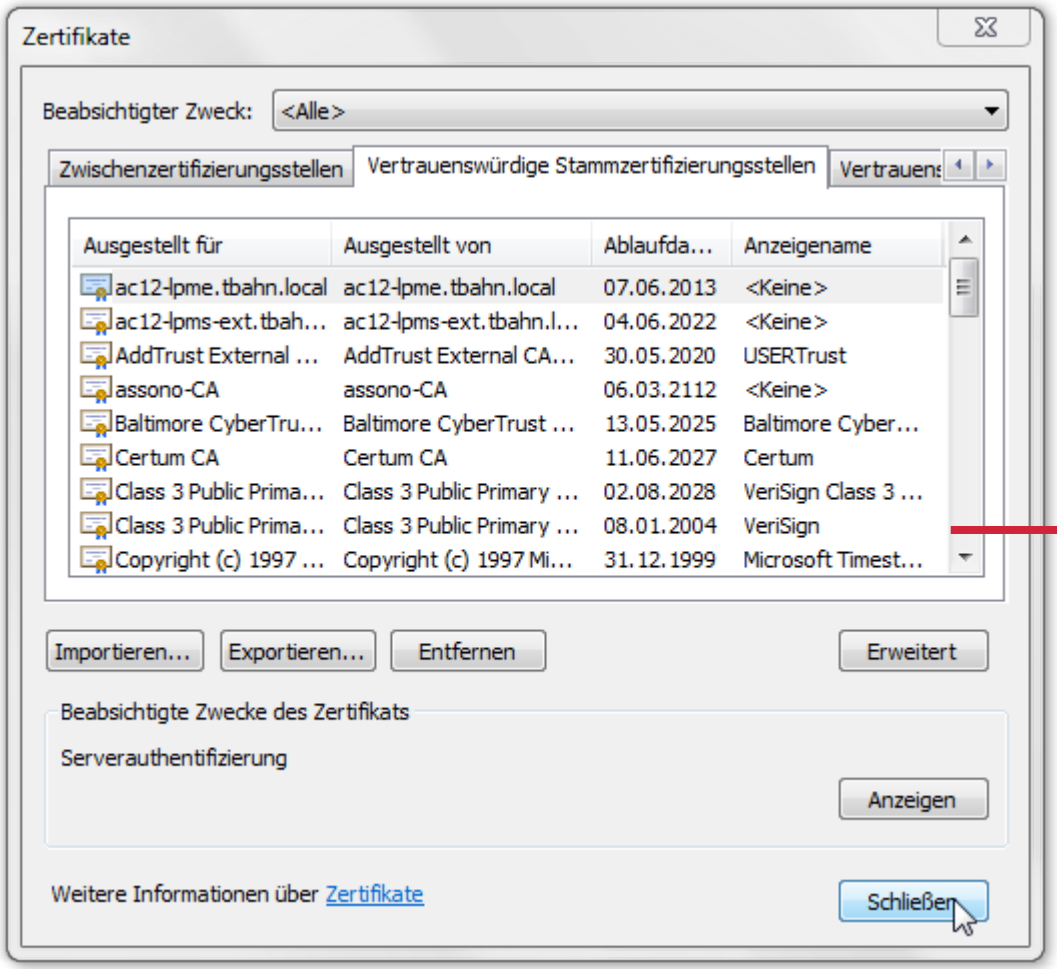
Warnung wegen des SSL-Zertifikats

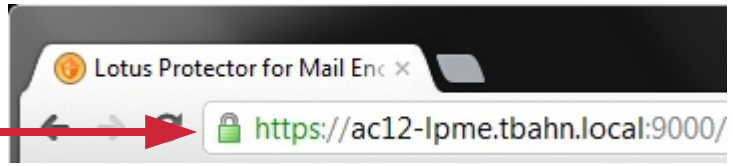


Warnung wegen des SSL-Zertifikats

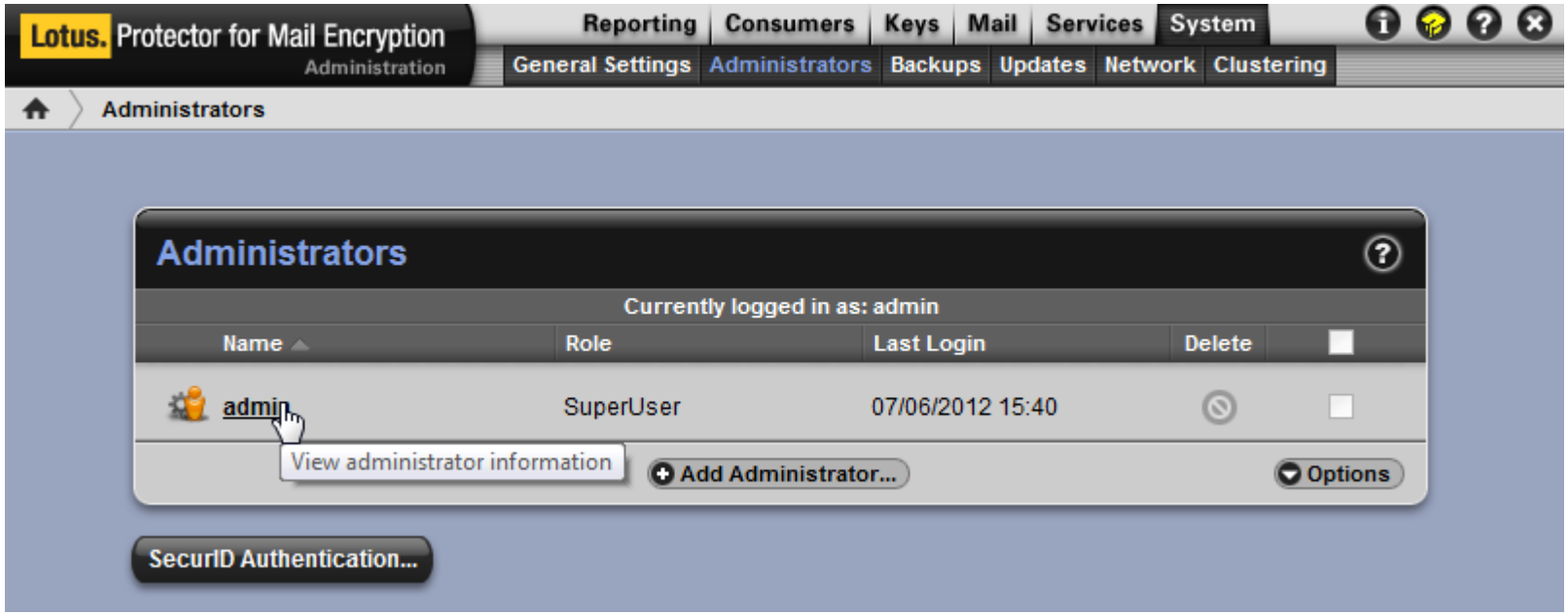


Warnung wegen des SSL-Zertifikats

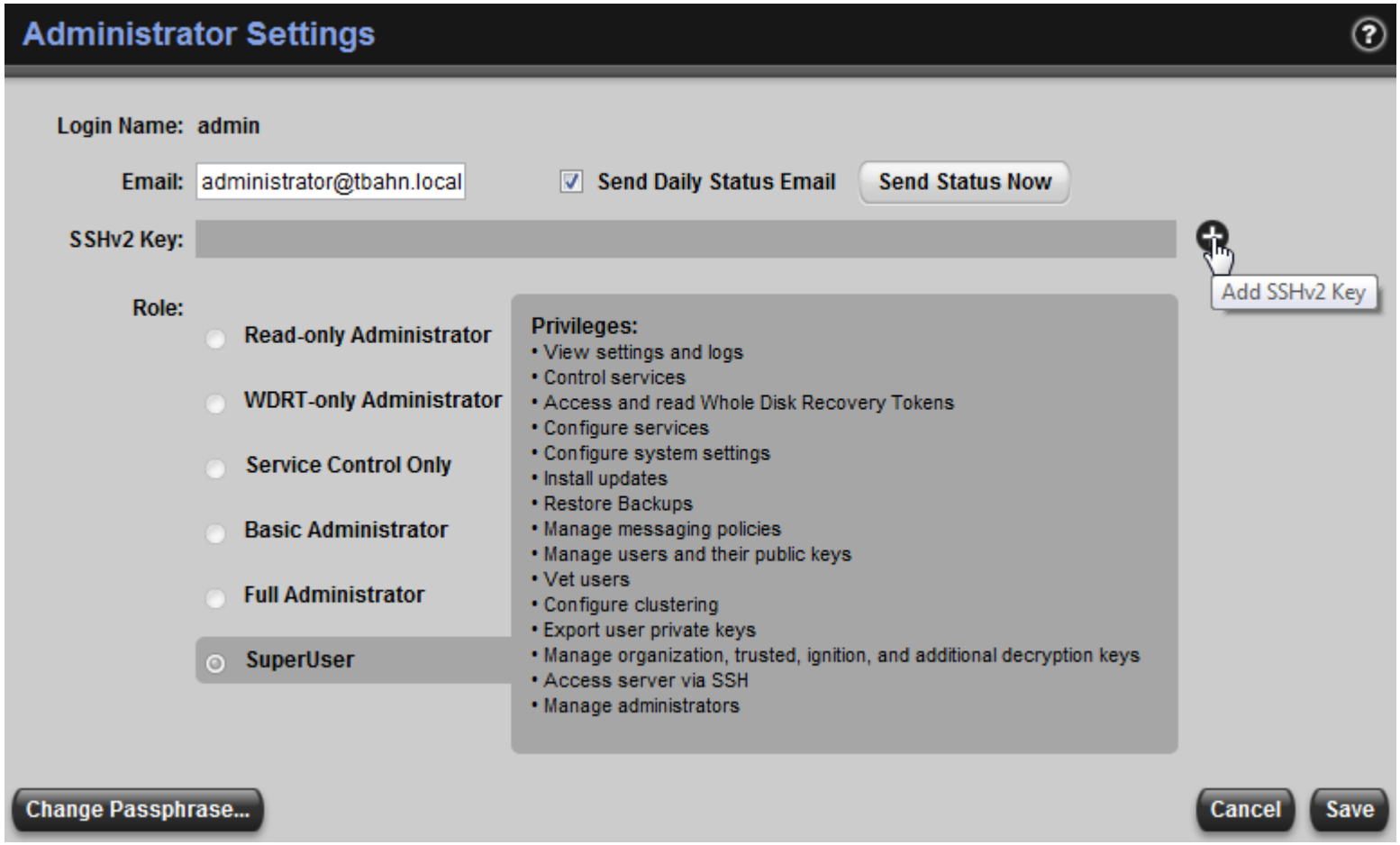




SSH-Zugriff (Public Key)



SSH-Zugriff (Public Key)

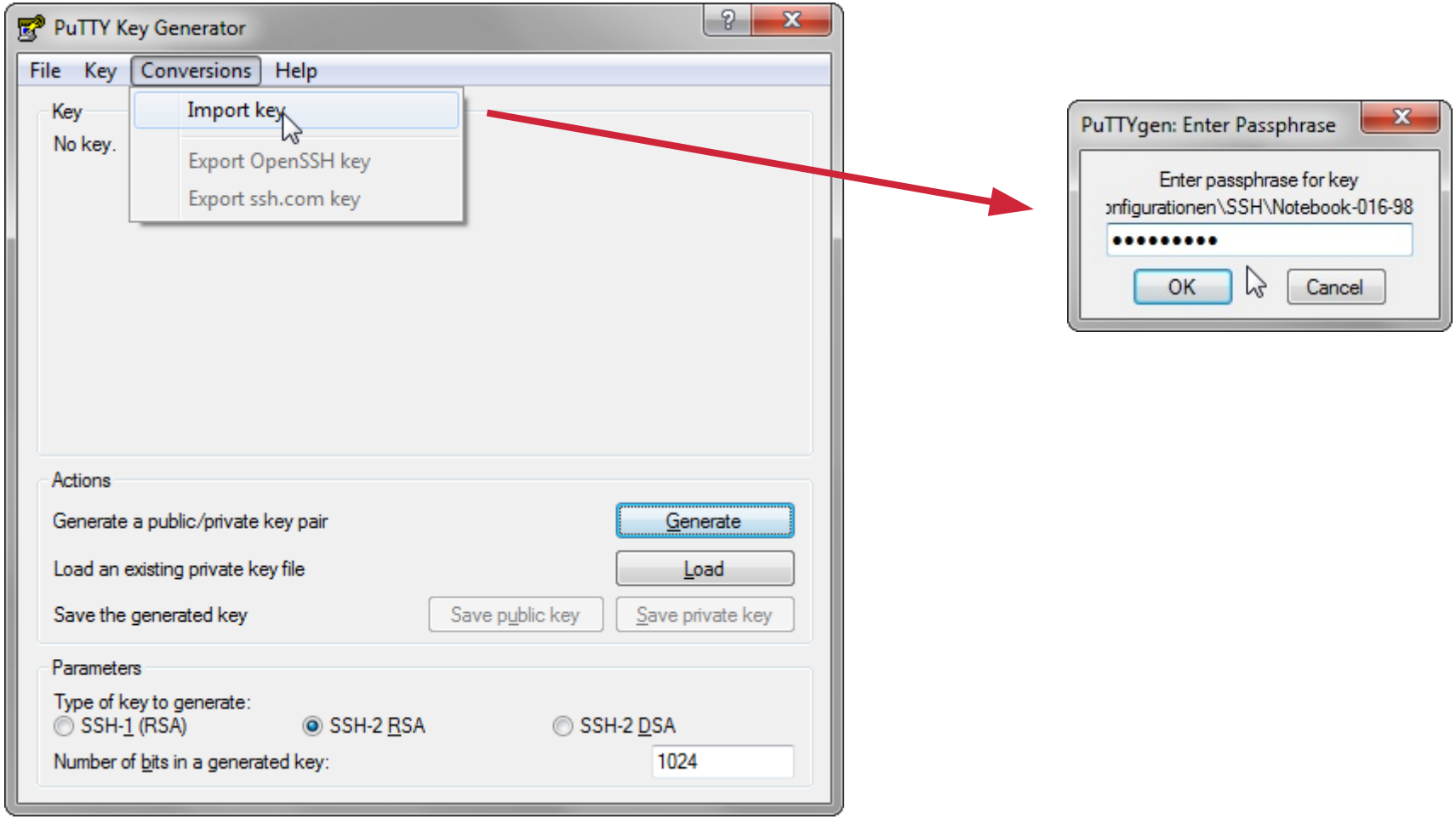


assono

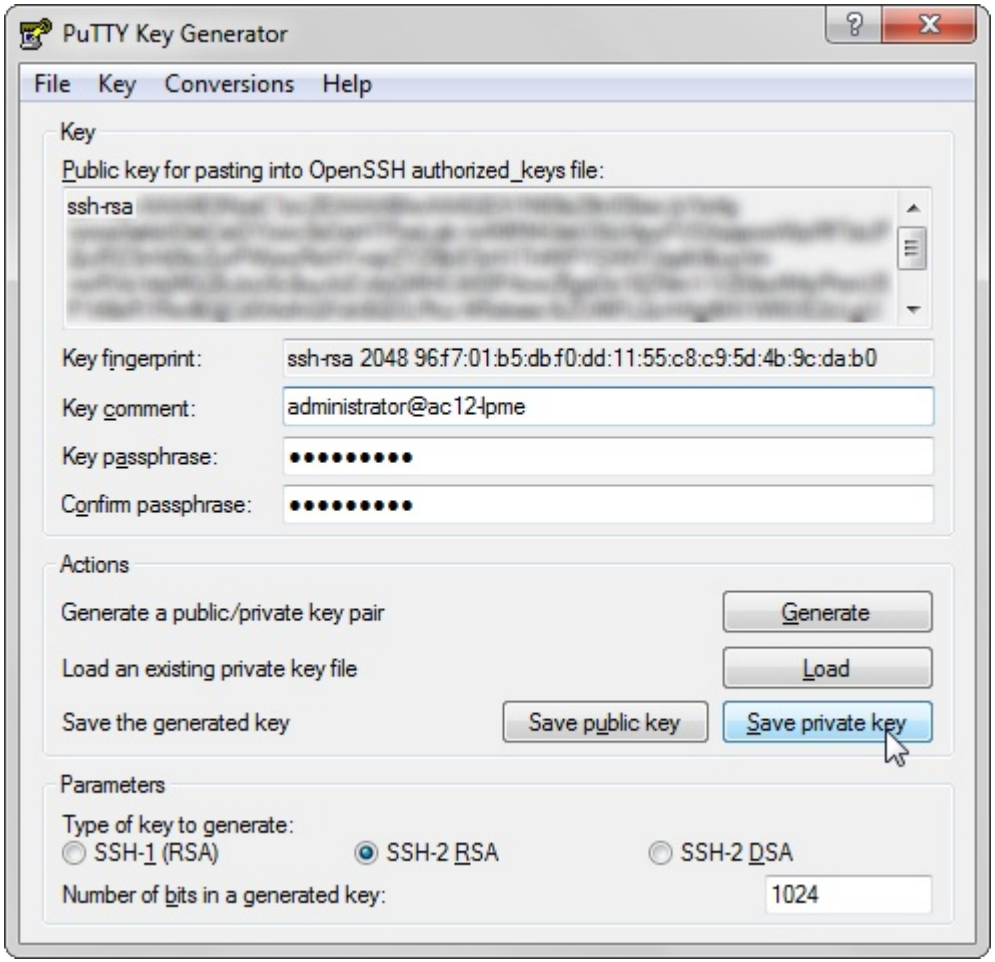
SSH-Zugriff (Public Key)

```
[administrator@notebook-016-98 ~]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/administrator/.ssh/id_rsa):
Created directory '/home/administrator/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/administrator/.ssh/id_rsa.
Your public key has been saved in /home/administrator/.ssh/id_rsa.pub.
The key fingerprint is:
0f:d3:28:5d:6b:77:60:6d:50:a9:6e:b7:7e:8b:d5:25 administrator@notebook-016-98.tb
ahn.local
The key's randomart image is:
+--[ RSA 2048]----+
|             .... |
|              o.  |
|           . o.o  |
|        . + o.o   |
|       . S +.. E .|
|        . = .o...o|
|           .. . o.|
|               + .|
|              o.o.|
+-----------------+
```

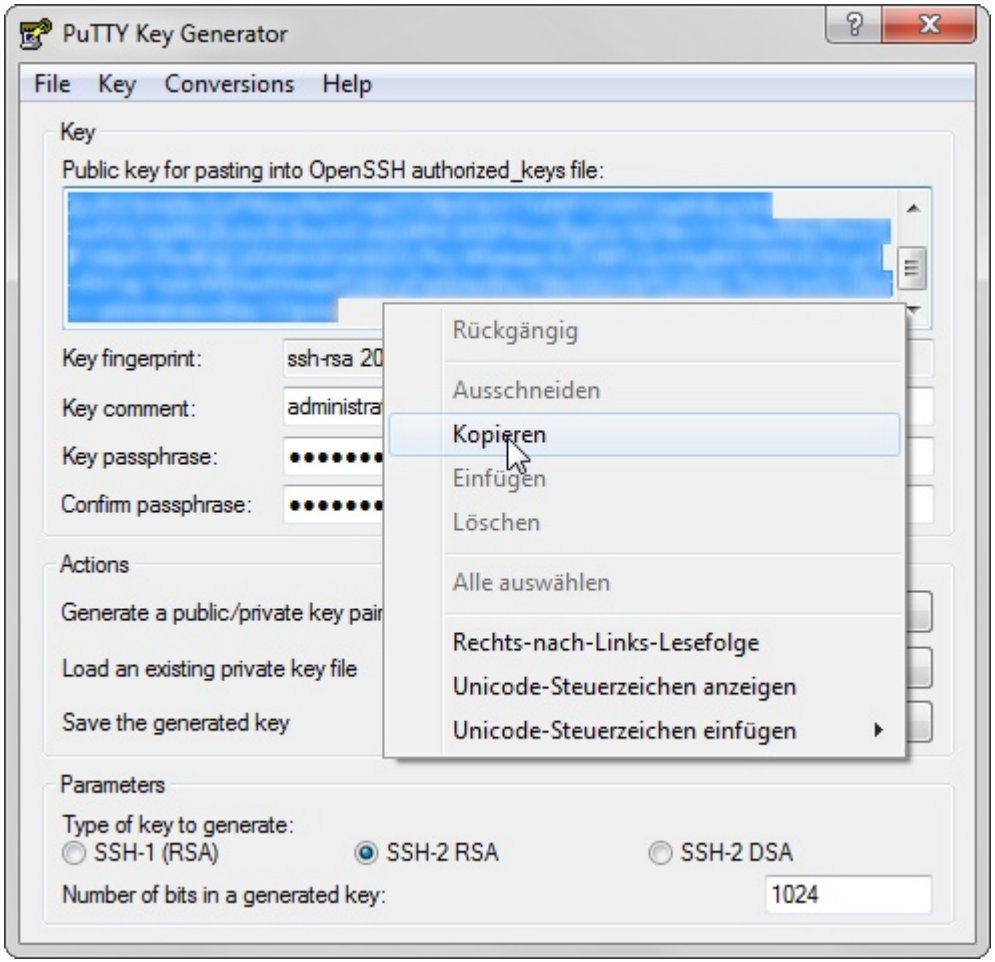
SSH-Zugriff (Public Key)



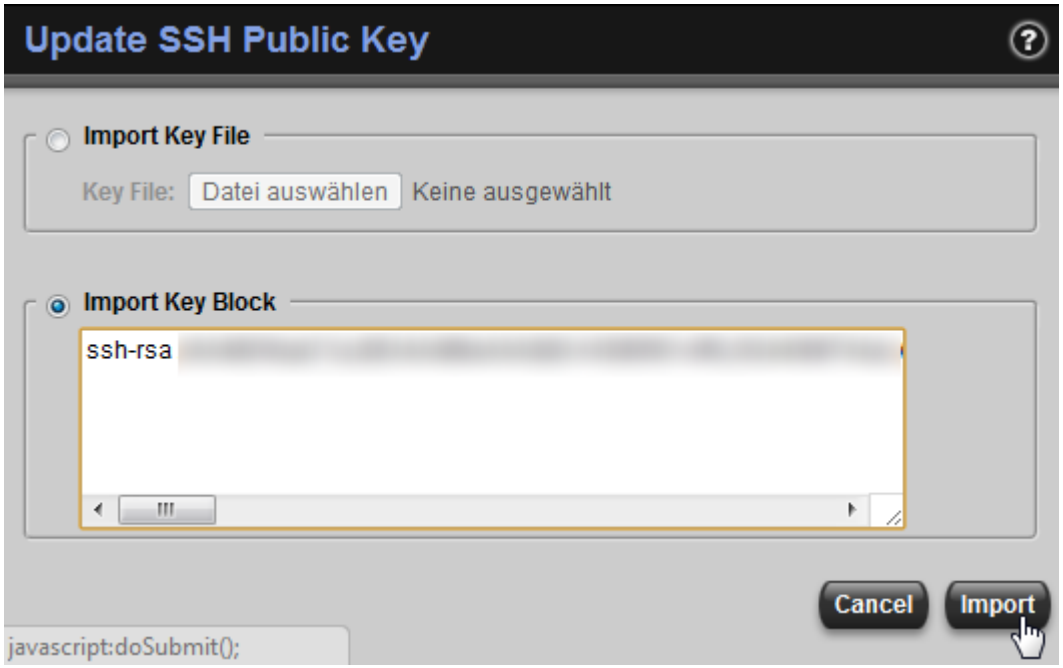
SSH-Zugriff (Public Key)



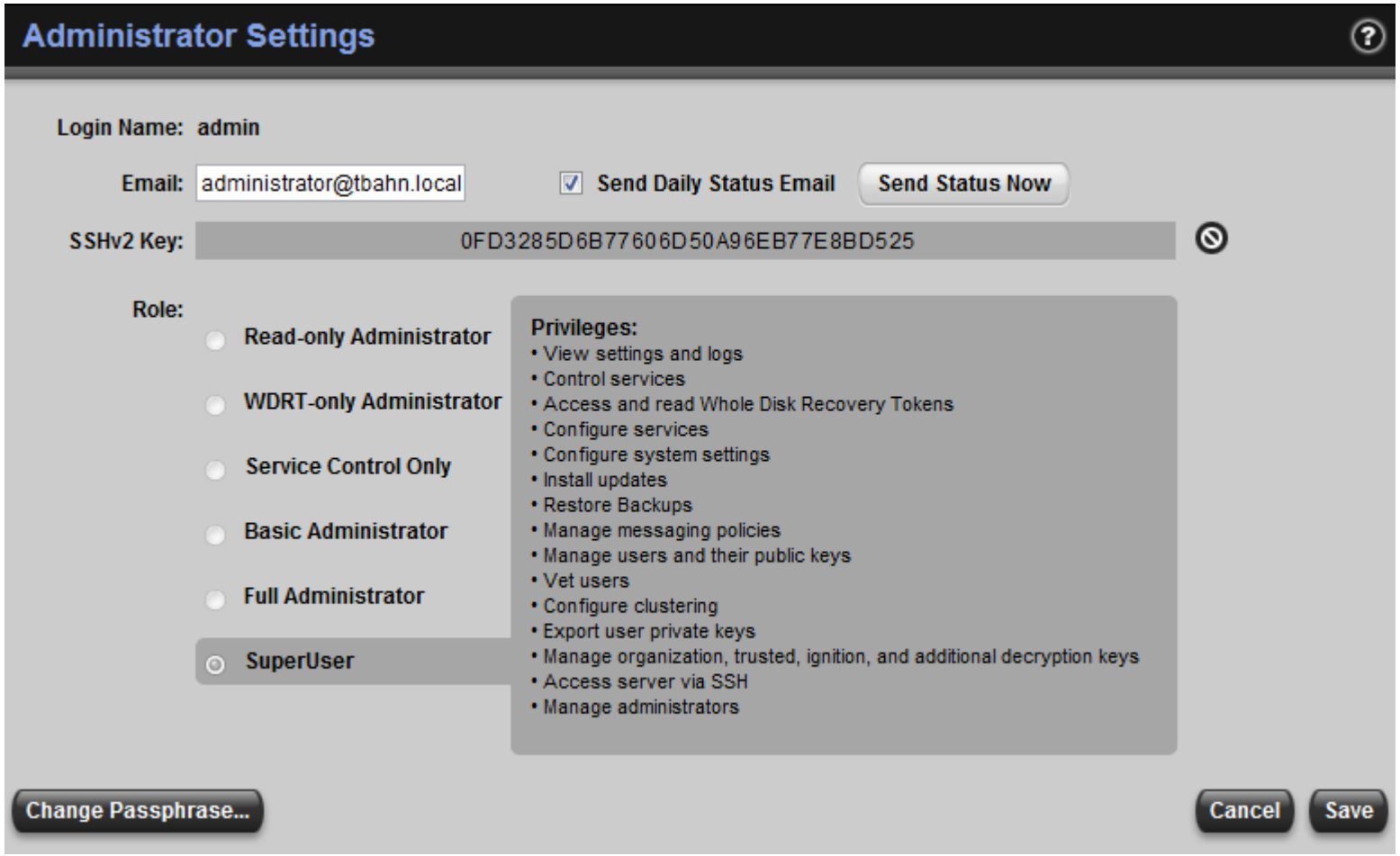
SSH-Zugriff (Public Key)



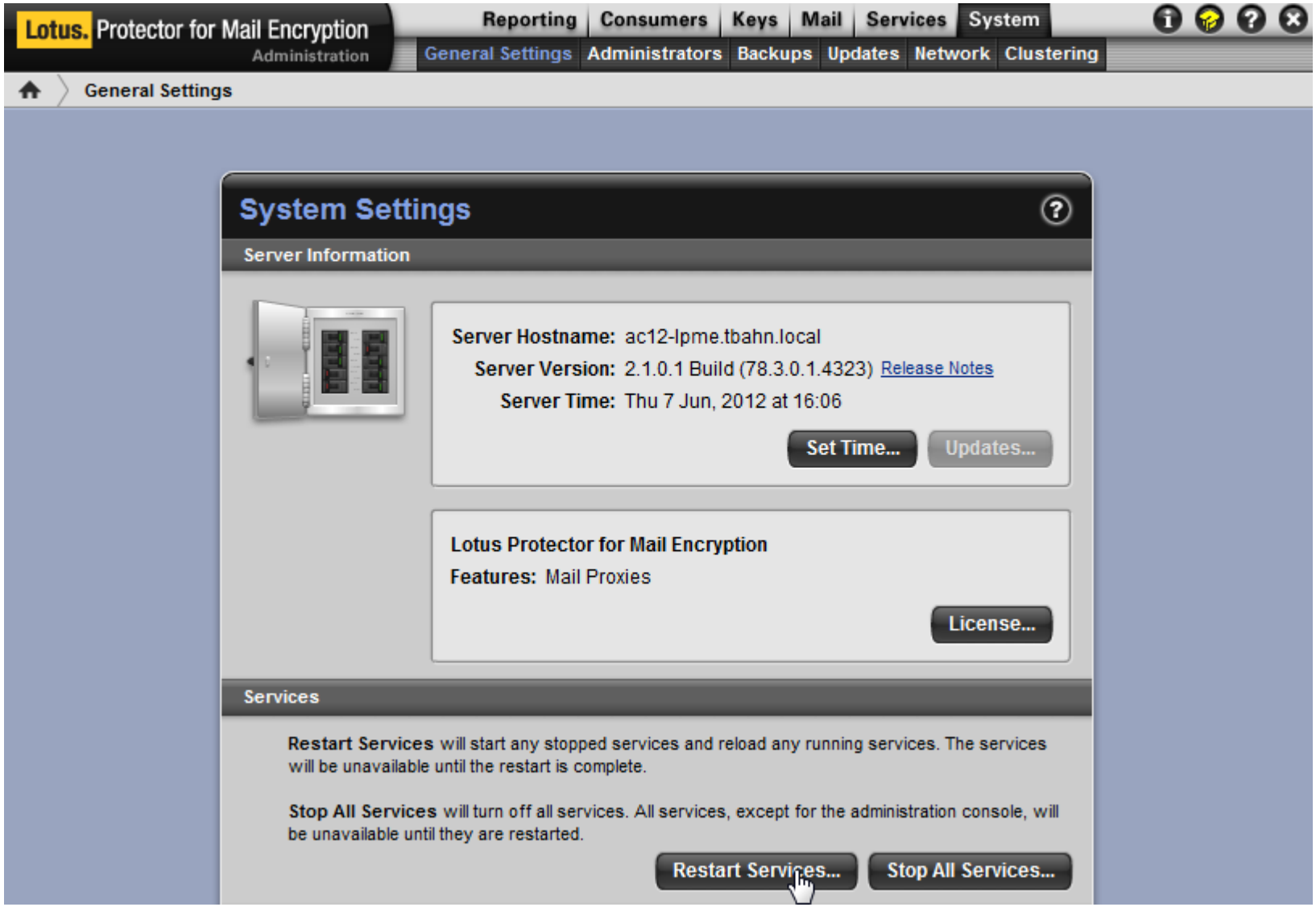
SSH-Zugriff (Public Key)



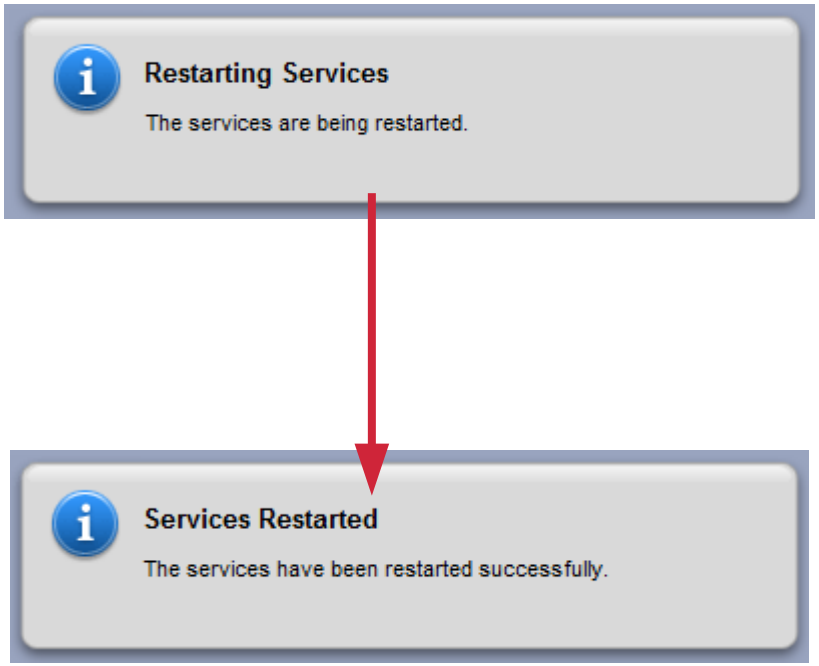
SSH-Zugriff (Public Key)



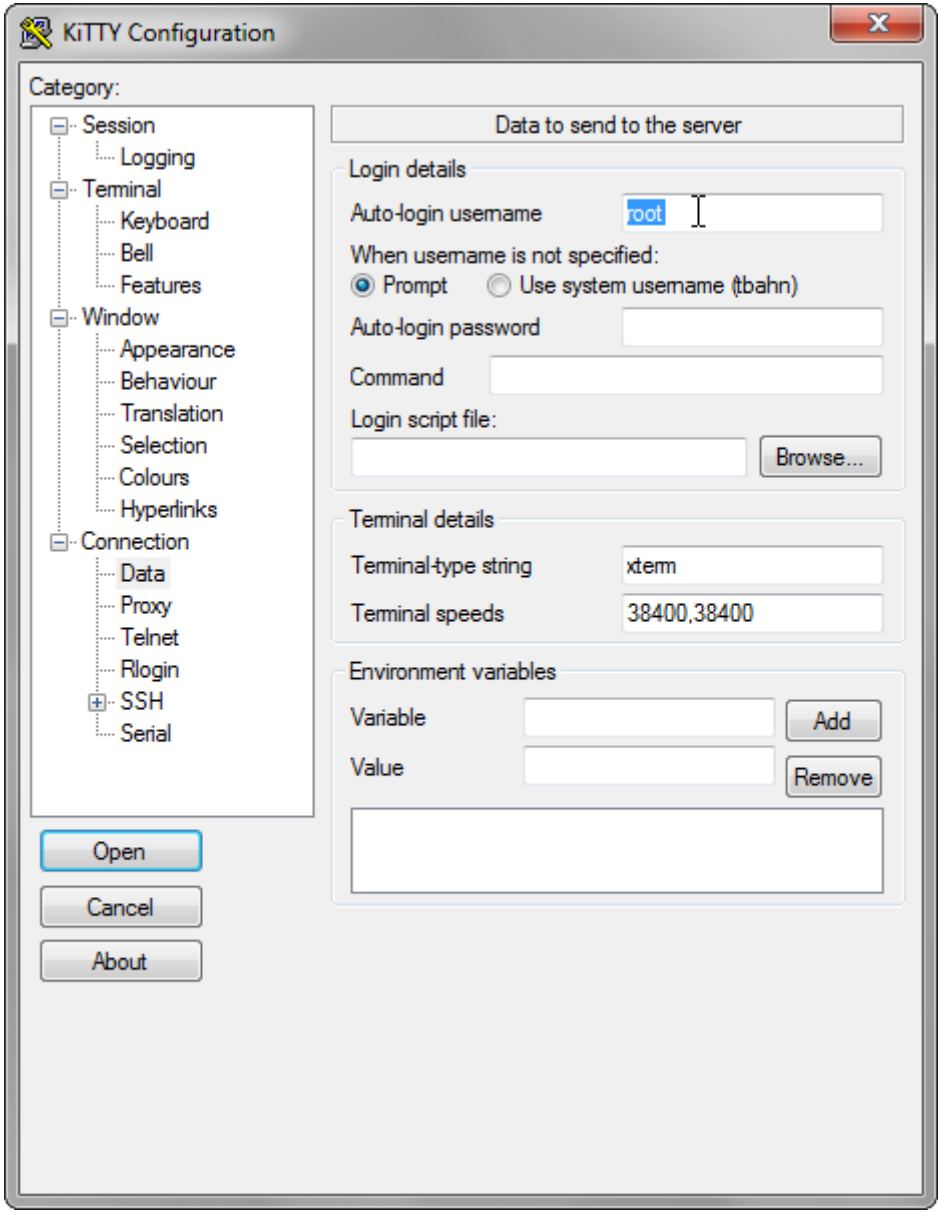
SSH-Zugriff (Public Key)



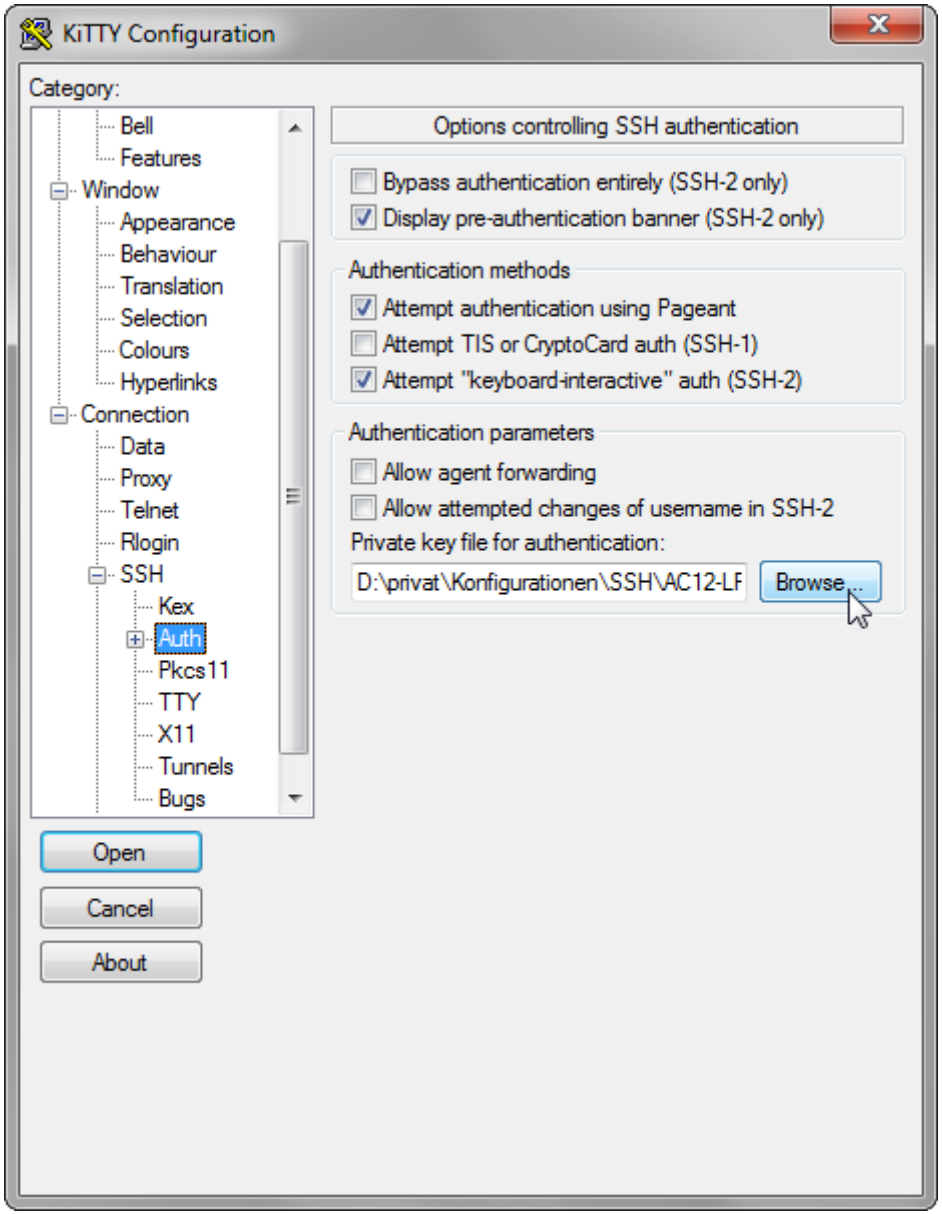
SSH-Zugriff (Public Key)



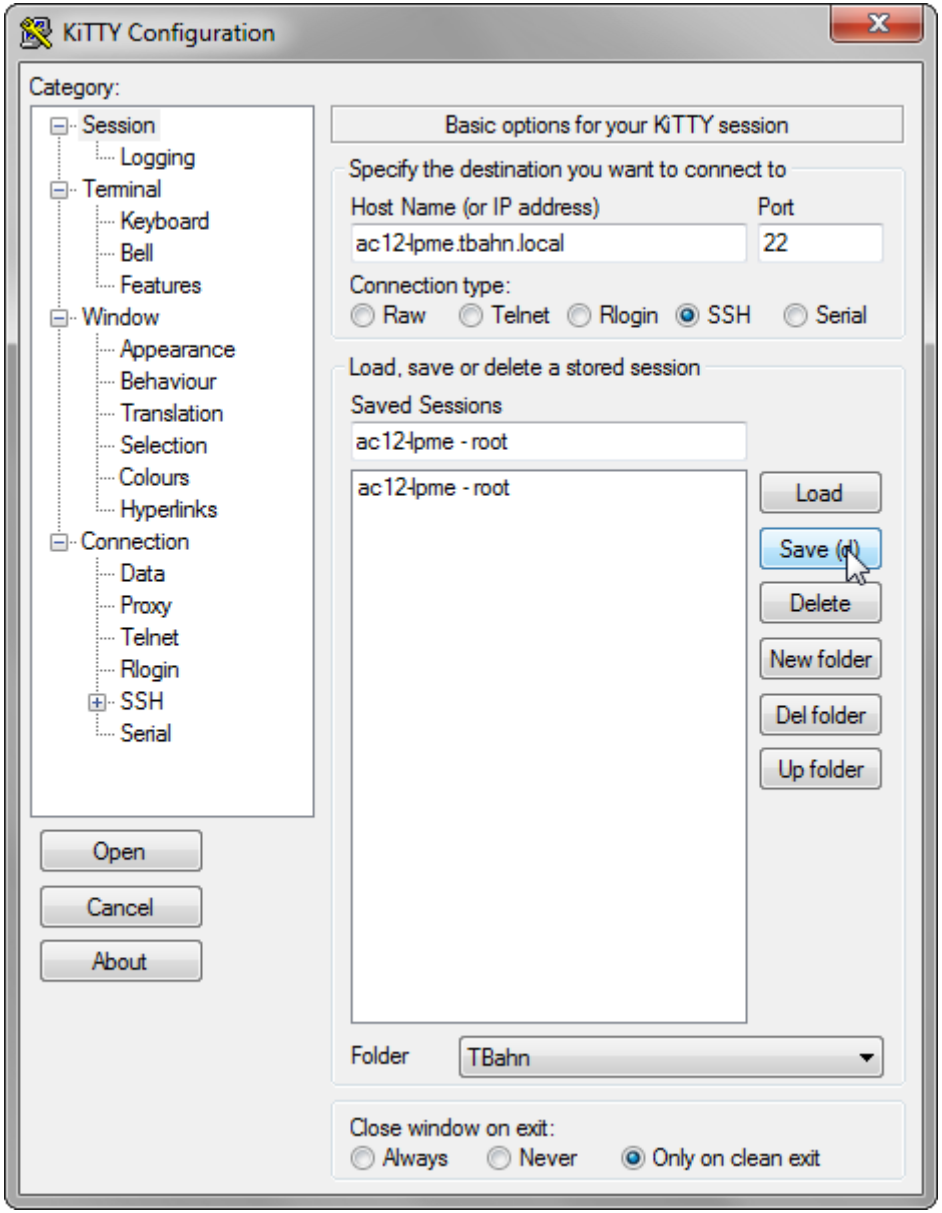
SSH-Zugriff (Public Key)



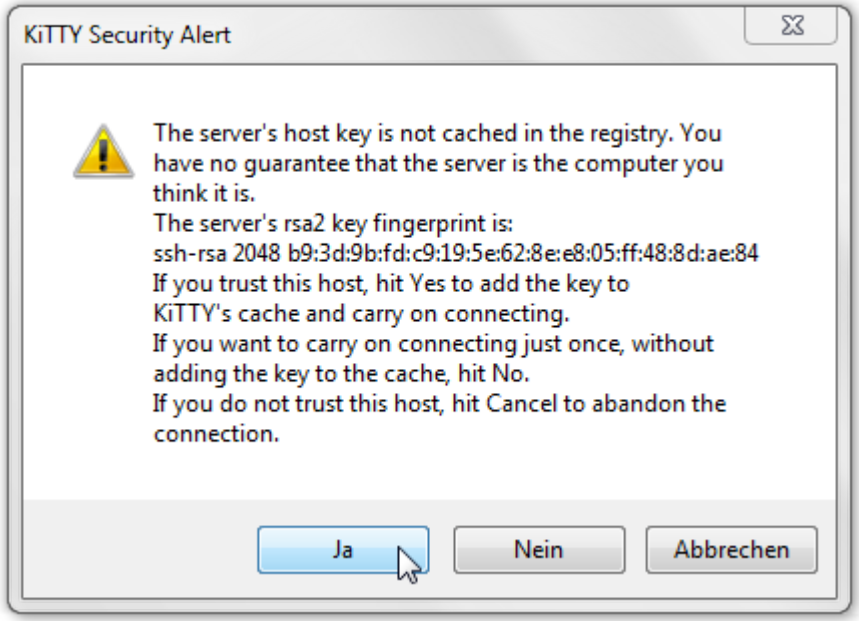
SSH-Zugriff (Public Key)



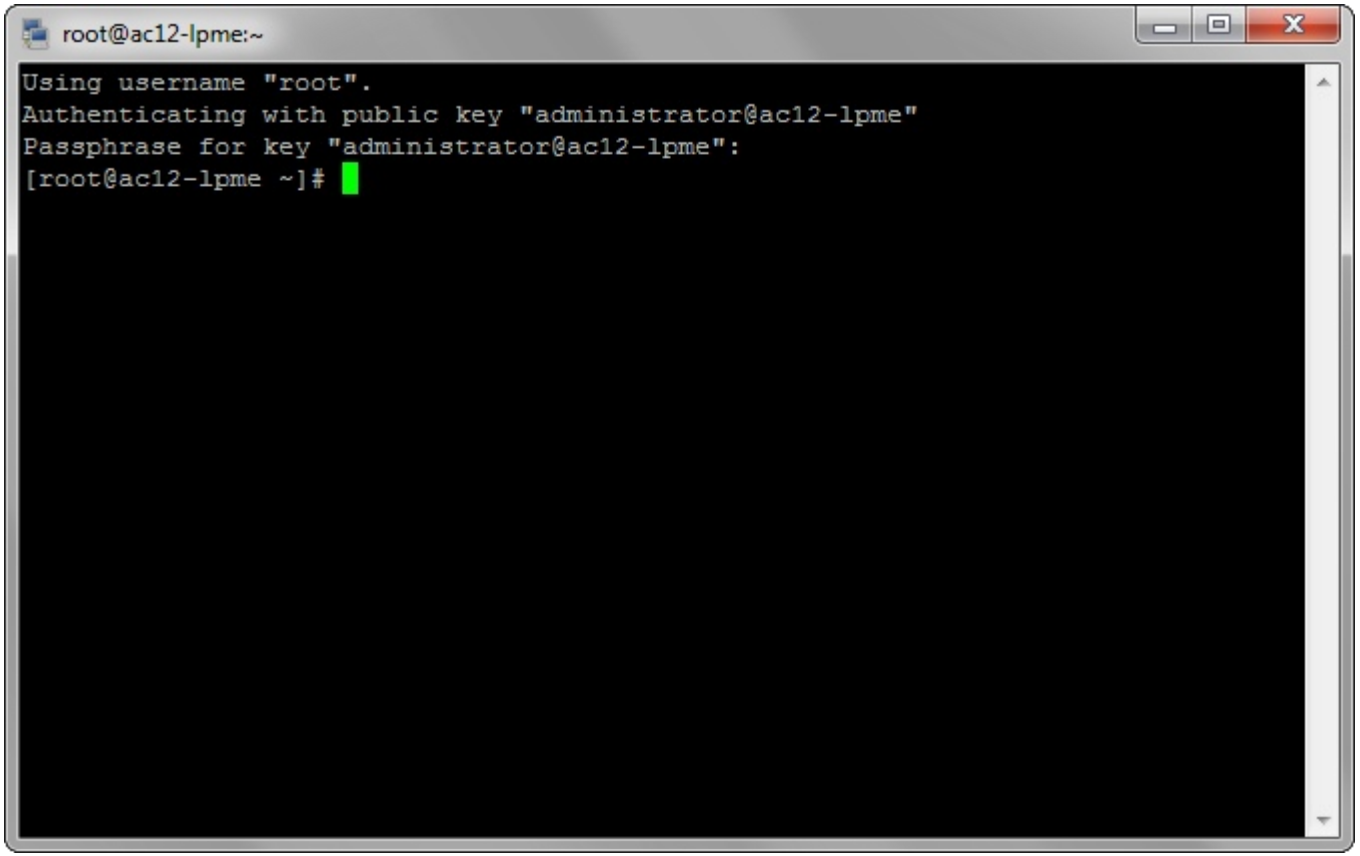
SSH-Zugriff (Public Key)



SSH-Zugriff (Public Key)



SSH-Zugriff (Public Key)



assono

SSH-Zugriff (Public Key)

```
[root@ac12-lpme ~]# chkconfig --list
anacron         0:off   1:off   2:on    3:on    4:on    5:on    6:off
atd             0:off   1:off   2:off   3:on    4:on    5:on    6:off
auditd          0:off   1:off   2:on    3:on    4:on    5:on    6:off
crond           0:off   1:off   2:on    3:on    4:on    5:on    6:off
dc_client       0:off   1:off   2:off   3:off   4:off   5:off   6:off
dc_server       0:off   1:off   2:off   3:off   4:off   5:off   6:off
gpm             0:off   1:off   2:on    3:on    4:on    5:on    6:off
haldaemon       0:off   1:off   2:off   3:on    4:on    5:on    6:off
httpd           0:off   1:off   2:on    3:on    4:on    5:on    6:off
iptables        0:off   1:off   2:on    3:on    4:on    5:on    6:off
jexec           0:on    1:on    2:on    3:on    4:on    5:on    6:on
kudzu           0:off   1:off   2:off   3:on    4:on    5:on    6:off
ldap            0:off   1:off   2:on    3:on    4:on    5:on    6:off
lm_sensors      0:off   1:off   2:on    3:on    4:on    5:on    6:off
lvm2-monitor    0:off   1:on    2:on    3:on    4:on    5:on    6:off
mcstrans        0:off   1:off   2:on    3:on    4:on    5:on    6:off
messagebus      0:off   1:off   2:off   3:on    4:on    5:on    6:off
multipathd      0:off   1:off   2:off   3:off   4:off   5:off   6:off
netconsole      0:off   1:off   2:off   3:off   4:off   5:off   6:off
netfs           0:off   1:off   2:off   3:on    4:on    5:on    6:off
netplugd        0:off   1:off   2:off   3:off   4:off   5:off   6:off
network         0:off   1:off   2:on    3:on    4:on    5:on    6:off
nscd            0:off   1:off   2:on    3:on    4:on    5:on    6:off
ntpd            0:off   1:off   2:on    3:on    4:on    5:on    6:off
ntpdate         0:off   1:off   2:on    3:on    4:on    5:on    6:off
pcscd           0:off   1:off   2:on    3:on    4:on    5:on    6:off
pgpconfigure    0:off   1:off   2:on    3:on    4:on    5:on    6:off
pgpdatalayer    0:off   1:off   2:on    3:on    4:on    5:on    6:off
pgpdbinit       0:off   1:off   2:on    3:on    4:on    5:on    6:off
pgpfixsystem    0:off   1:off   2:on    3:on    4:on    5:on    6:off
pgpgroupd       0:off   1:off   2:on    3:on    4:on    5:on    6:off
pgprep          0:off   1:off   2:on    3:on    4:on    5:on    6:off
pgpsdkrmi       0:off   1:off   2:on    3:on    4:on    5:on    6:off
pgptcpwrapper   0:off   1:off   2:on    3:on    4:on    5:on    6:off
pgptokend       0:off   1:off   2:on    3:on    4:on    5:on    6:off
pgpuniversal    0:off   1:off   2:on    3:on    4:on    5:on    6:off
postfix         0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

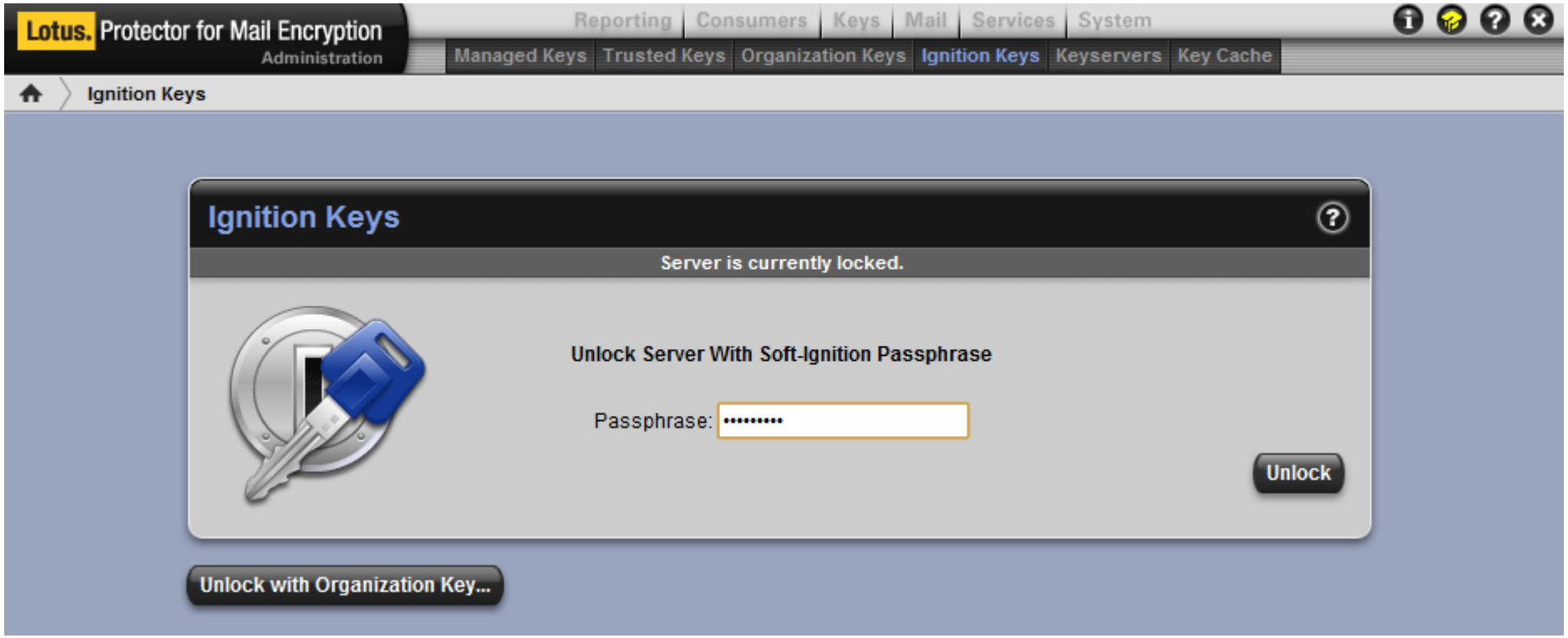
SSH-Zugriff (Public Key)

```
login as: root
Using keyboard-interactive authentication.
Password:
Last login: Thu Jun  7 15:24:29 2012 from 192.168.242.1
ac12-lpms-ext:~ # cd .ssh
ac12-lpms-ext:~/.ssh # ls -l
total 8
-rw------- 1 root root 1192 Jun  6 13:31 id_dsa
-rw-r--r-- 1 root root 1119 Jun  6 13:31 id_dsa.pub
ac12-lpms-ext:~/.ssh # cat id_dsa.pub >> authorized_keys
ac12-lpms-ext:~/.ssh # /etc/init.d/sshd restart
Shutting down SSH daemon                                   done
Starting SSH daemon                                        done
```

```
RSAAuthentication yes
PubkeyAuthentication yes
PermitEmptyPasswords no
PasswordAuthentication no
PermitRootLogin yes
```

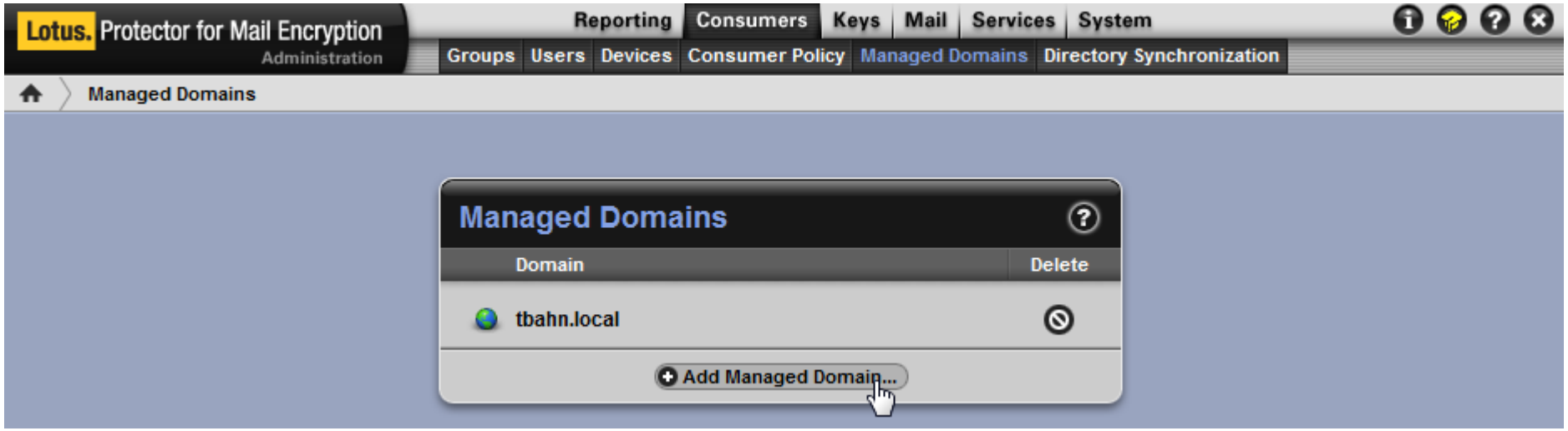
```
Using username "root".
Authenticating with public key "root@ac12-lpms"
Passphrase for key "root@ac12-lpms":
Last login: Thu Jun  7 15:25:29 2012 from 192.168.242.1
ac12-lpms-ext:~ # vi /etc/ssh/sshd_config
ac12-lpms-ext:~ # /etc/init.d/sshd restart
Shutting down SSH daemon                                   done
Starting SSH daemon                                        done
```

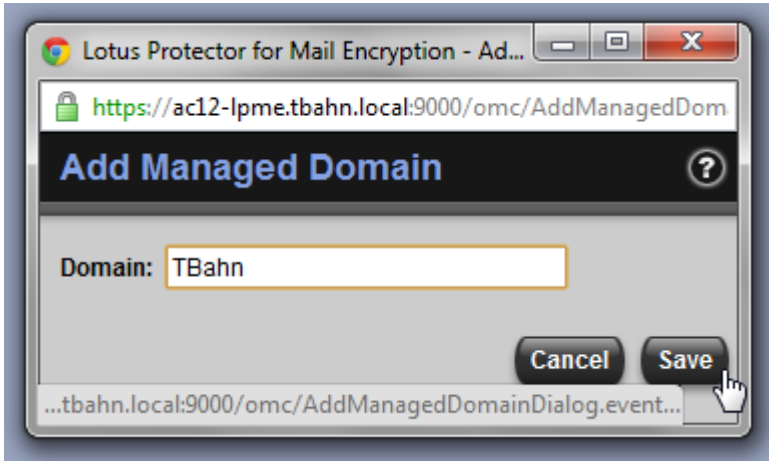
Nach jedem Neustart...



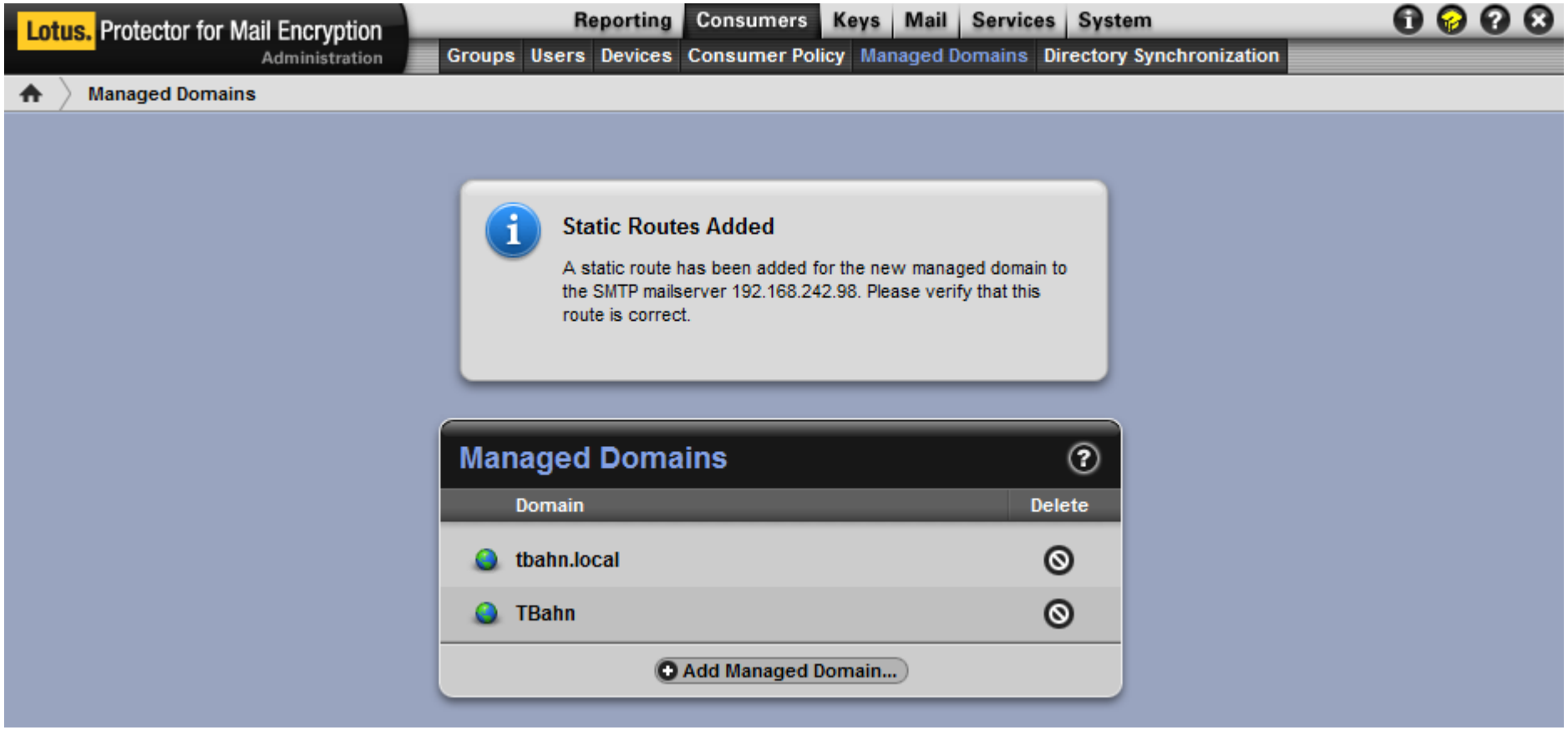
Nach jedem Neustart...

Domino-Domäne hinzufügen

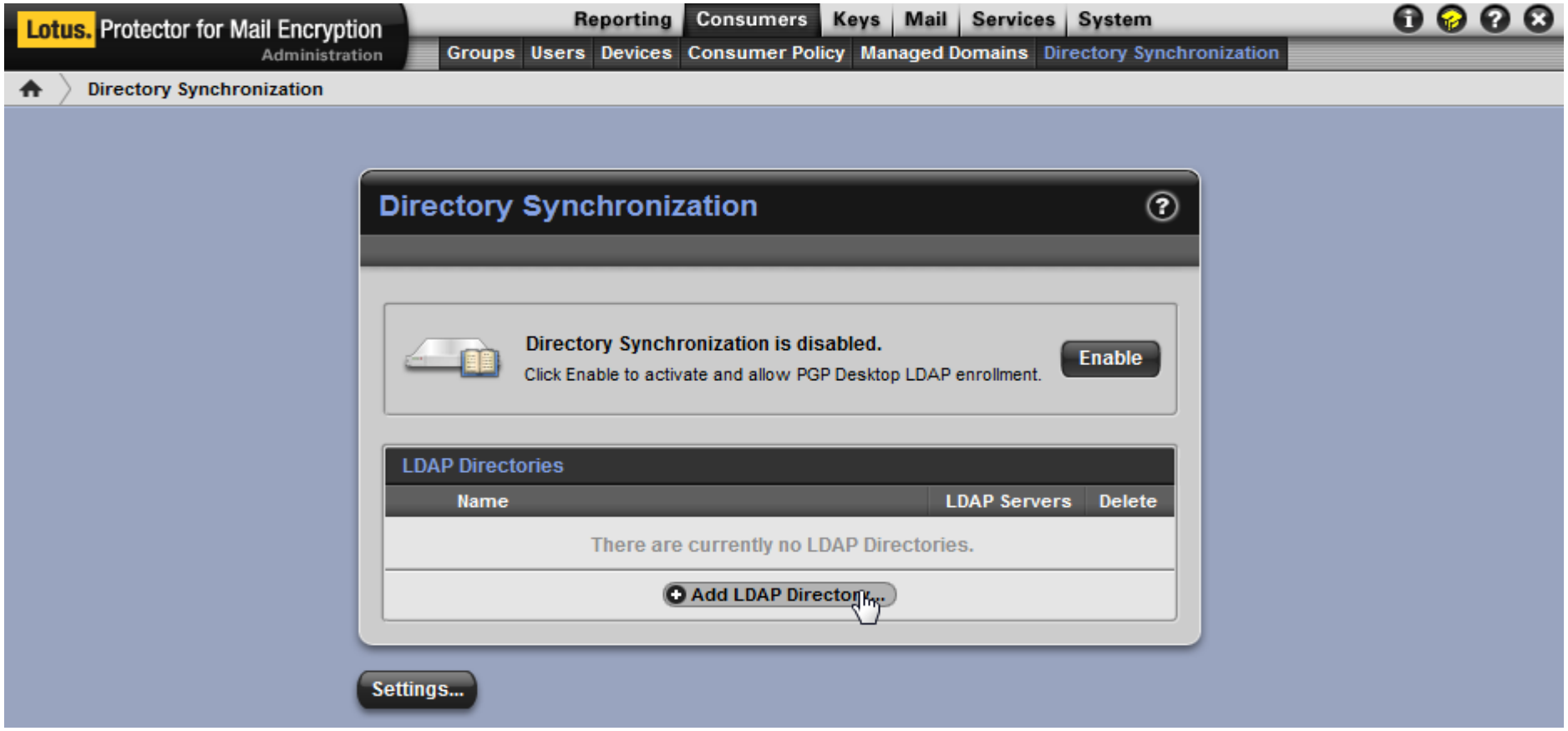




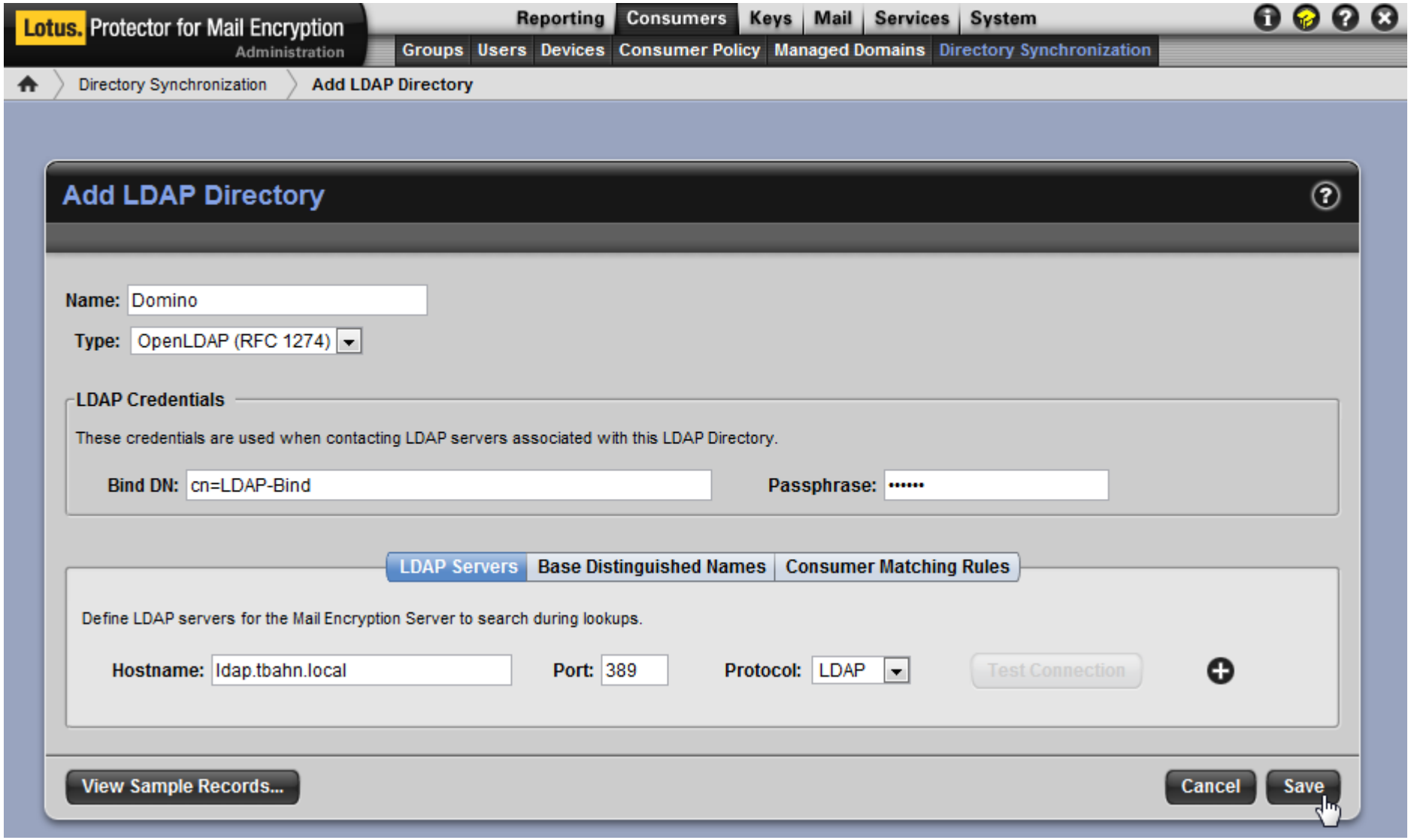
Domino-Domäne hinzufügen



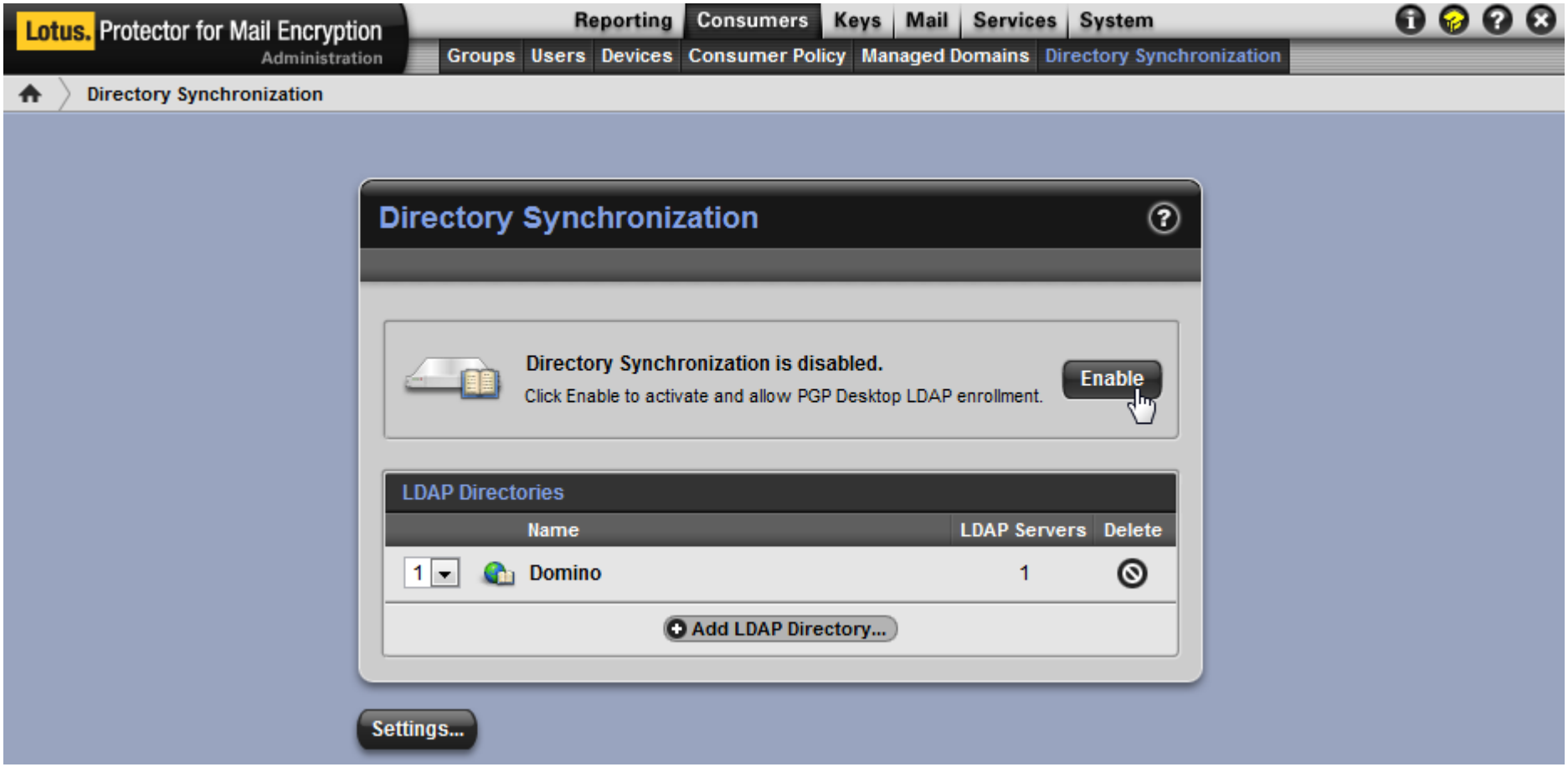
Domino-Benutzer (LDAP) hinzufügen



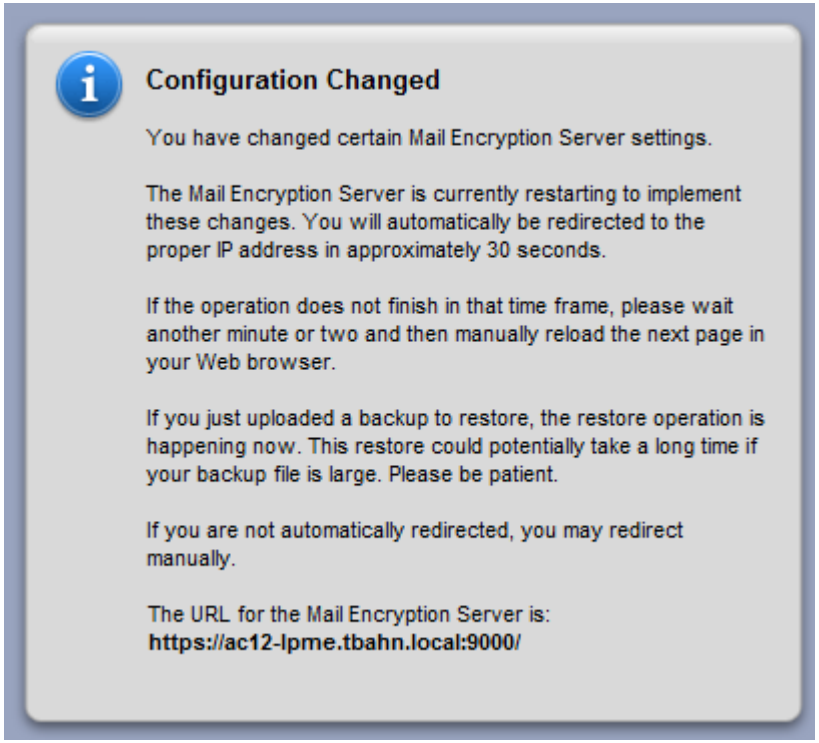
Domino-Benutzer (LDAP) hinzufügen



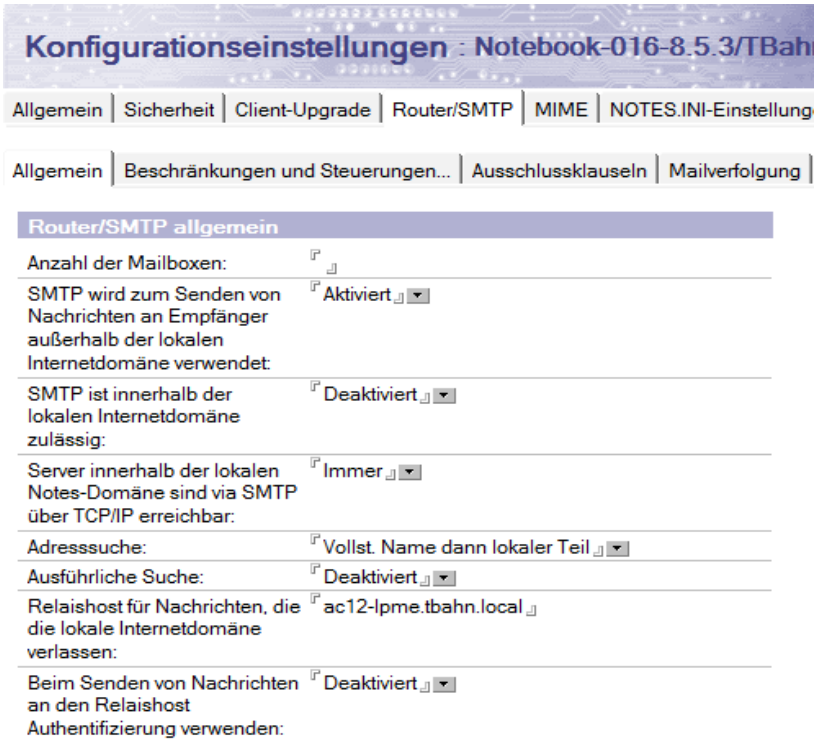
Domino-Benutzer (LDAP) hinzufügen



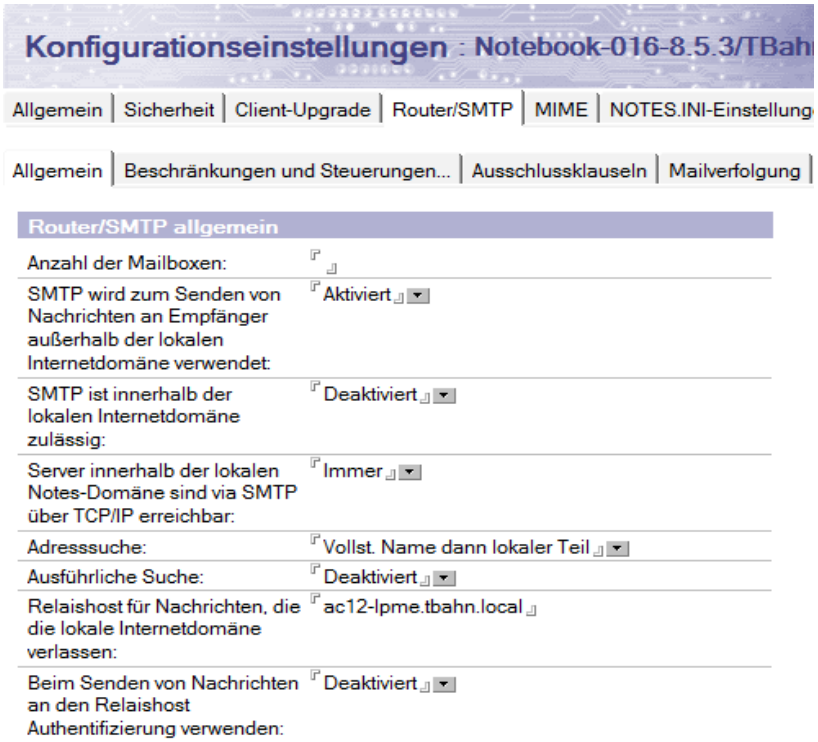
Domino-Benutzer (LDAP) hinzufügen



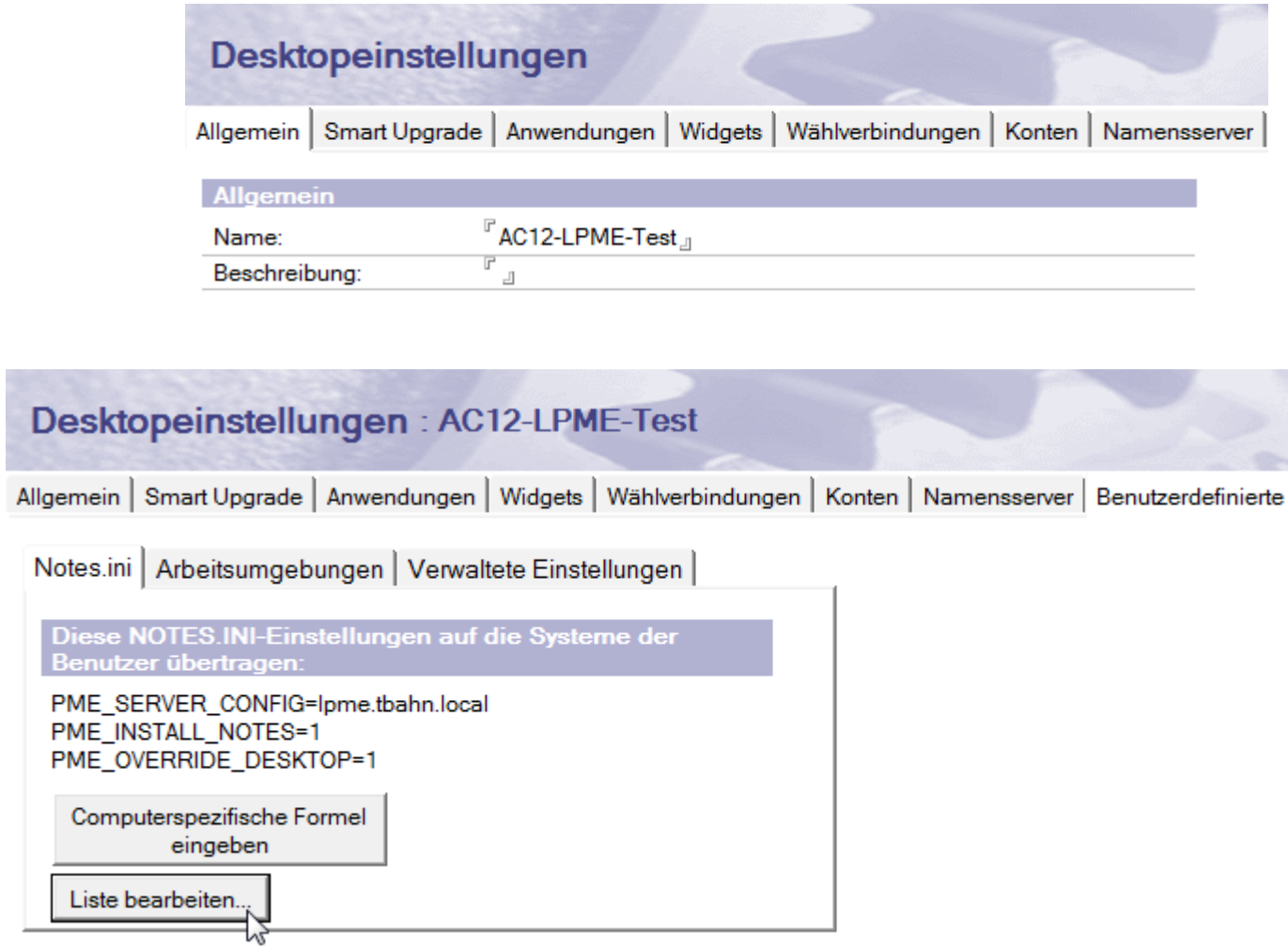
Konfiguration des Domino-Servers



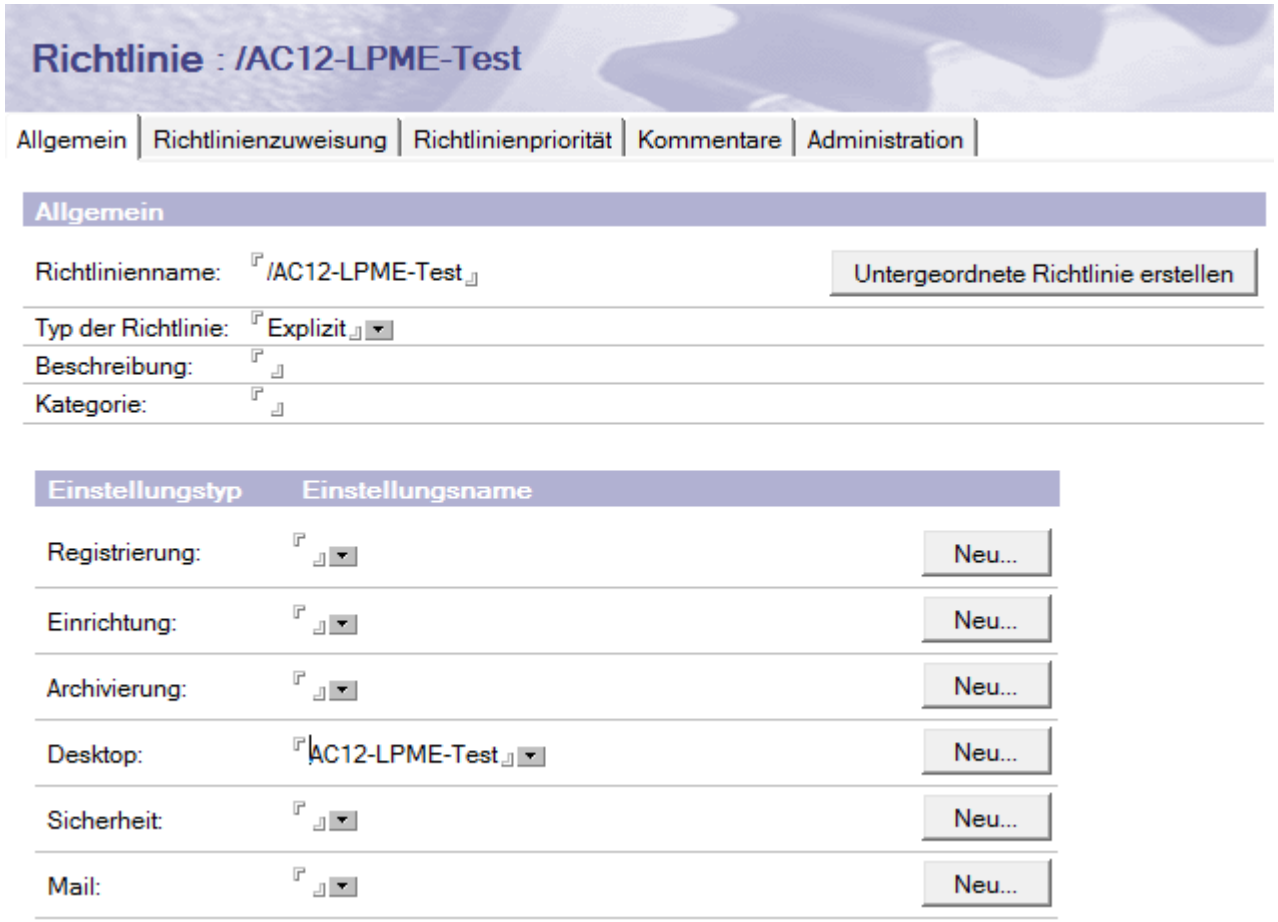
Konfiguration des Domino-Servers



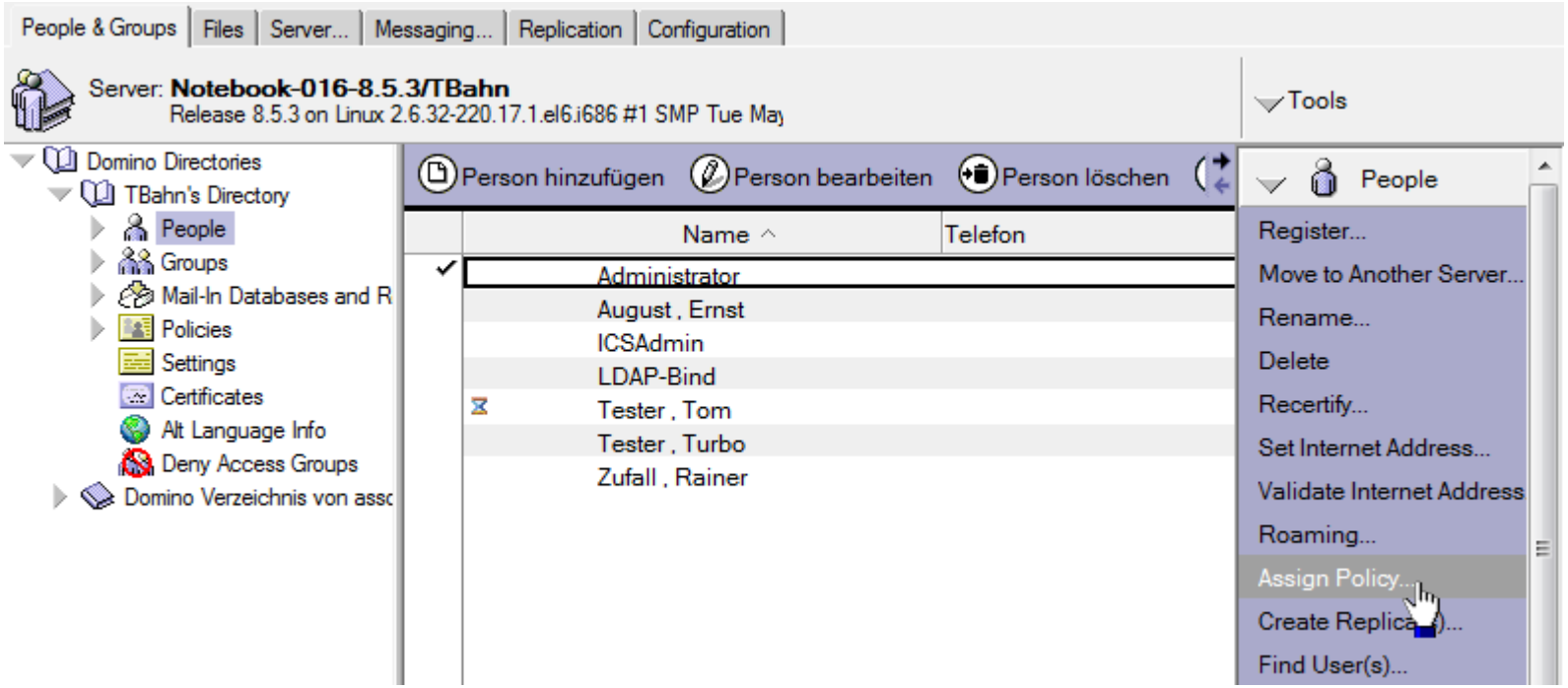
Konfiguration des Notes-Clients (via Richtlinie)



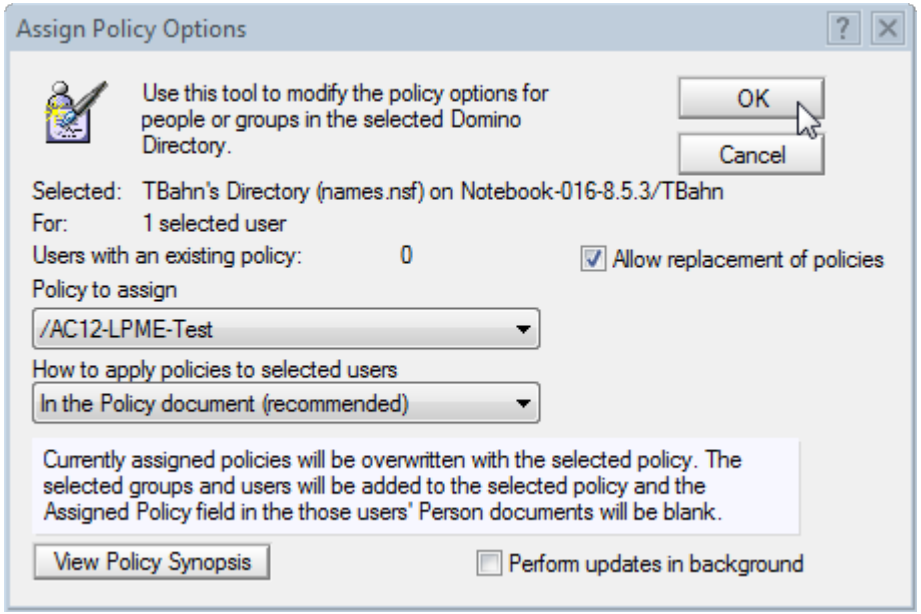
Konfiguration des Notes-Clients (via Richtlinie)

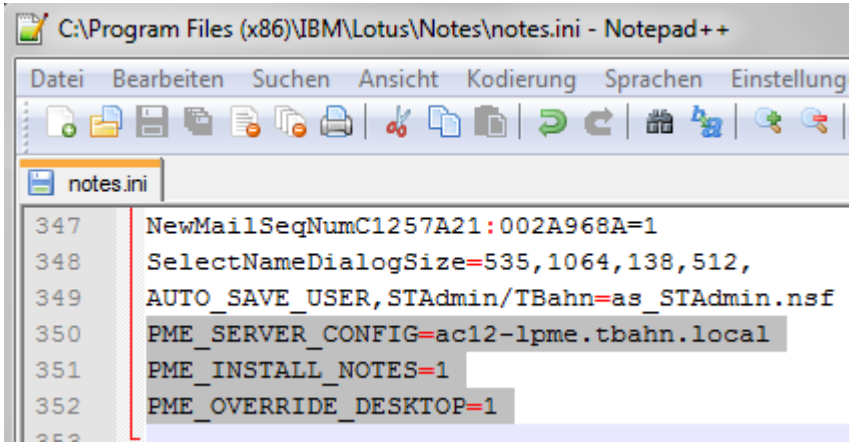


Konfiguration des Notes-Clients (via Richtlinie)



Konfiguration des Notes-Clients (via Richtlinie)

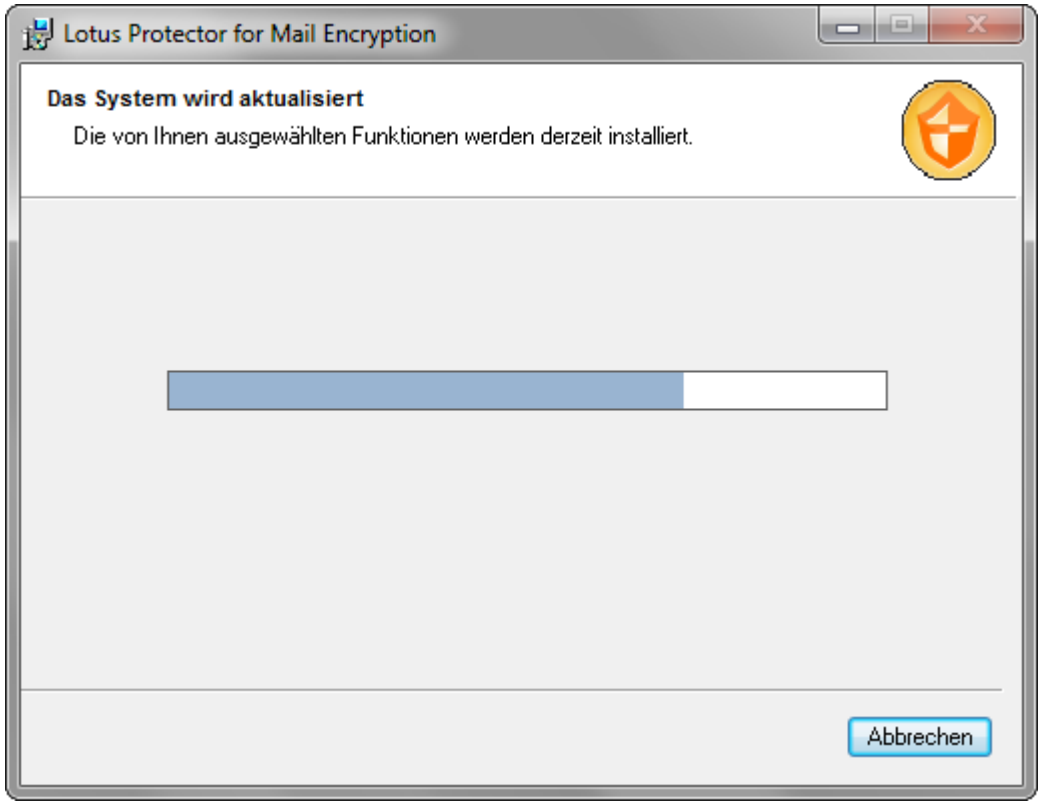




Installation des LPME-Clients

Installation des LPME-Clients

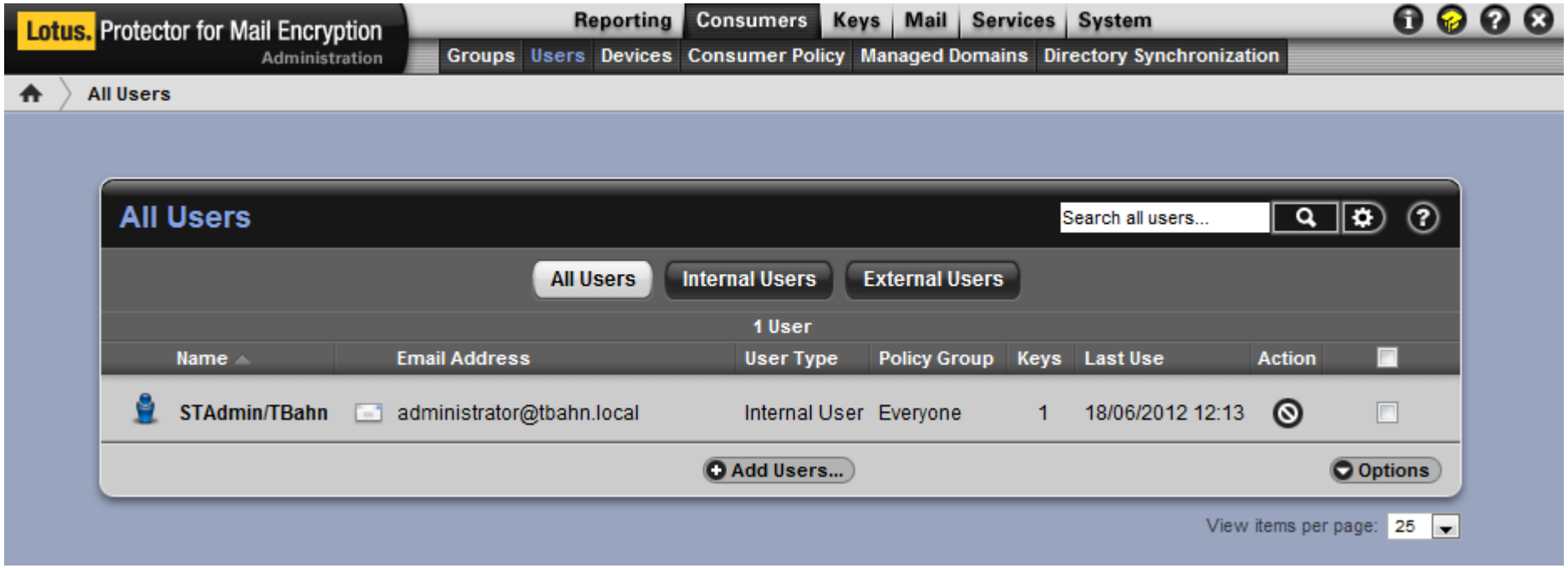
Installation des LPME-Clients



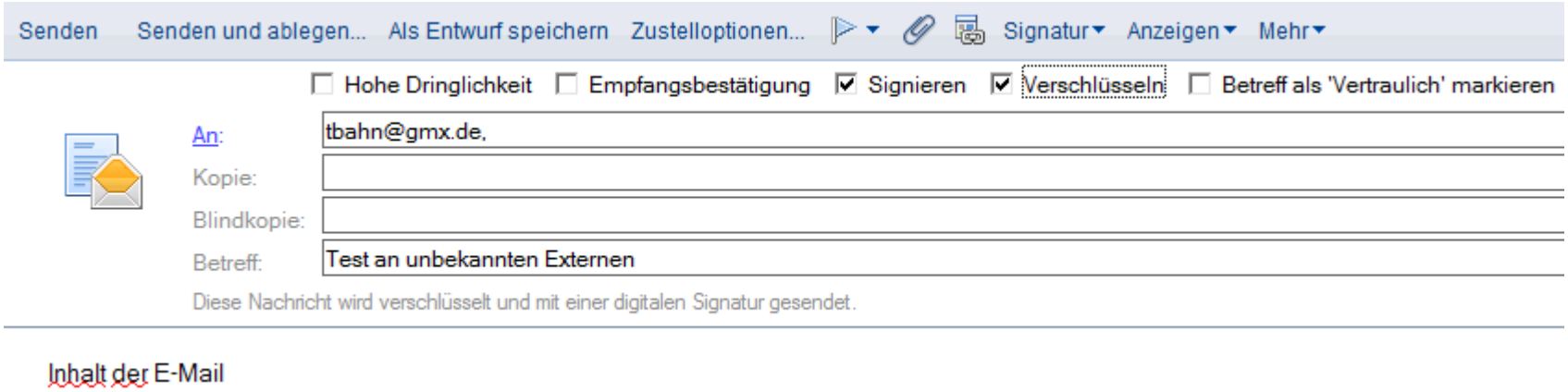
Installation des LPME-Clients

Installation des LPME-Clients

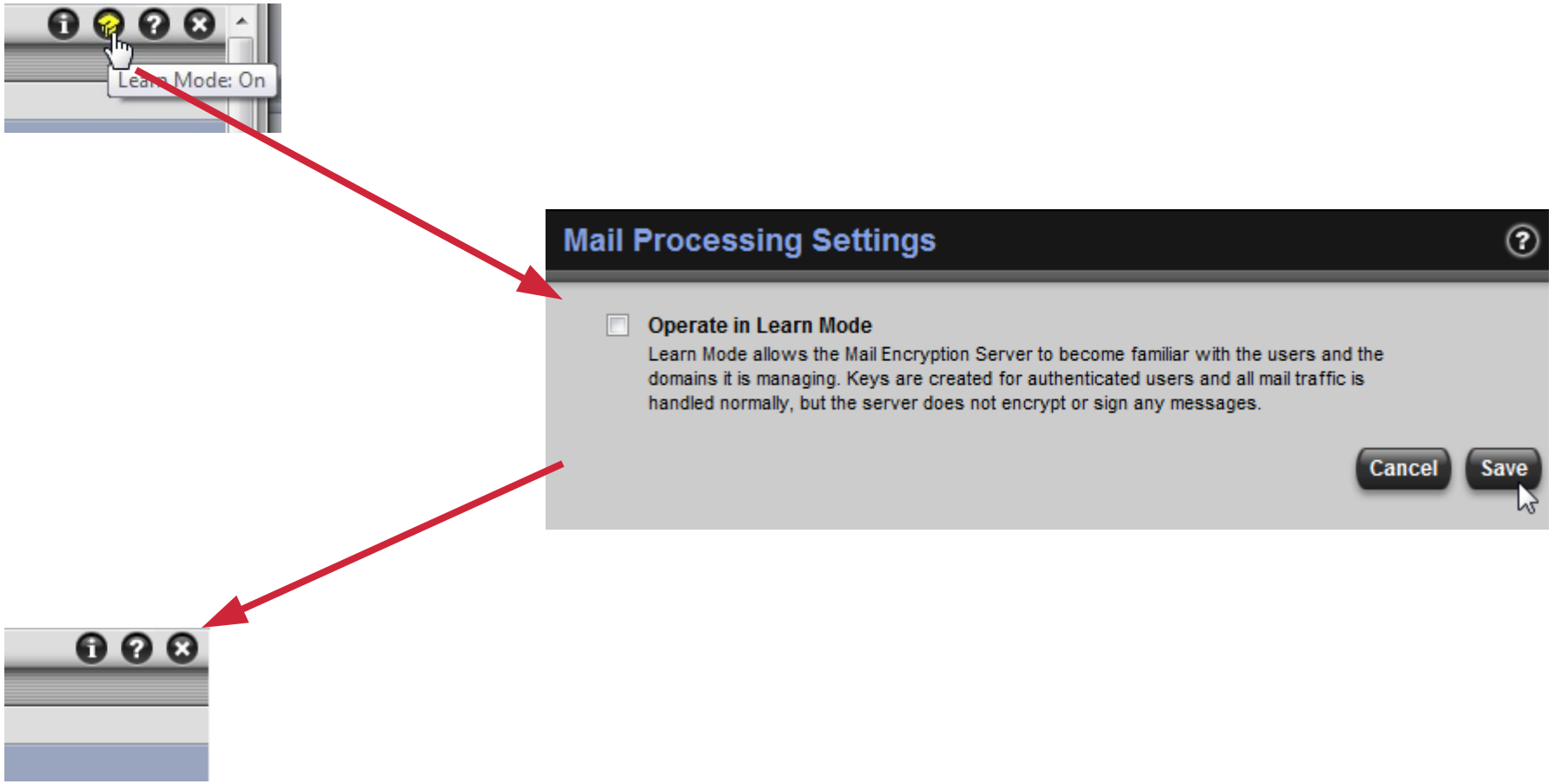
Installation des LPME-Clients



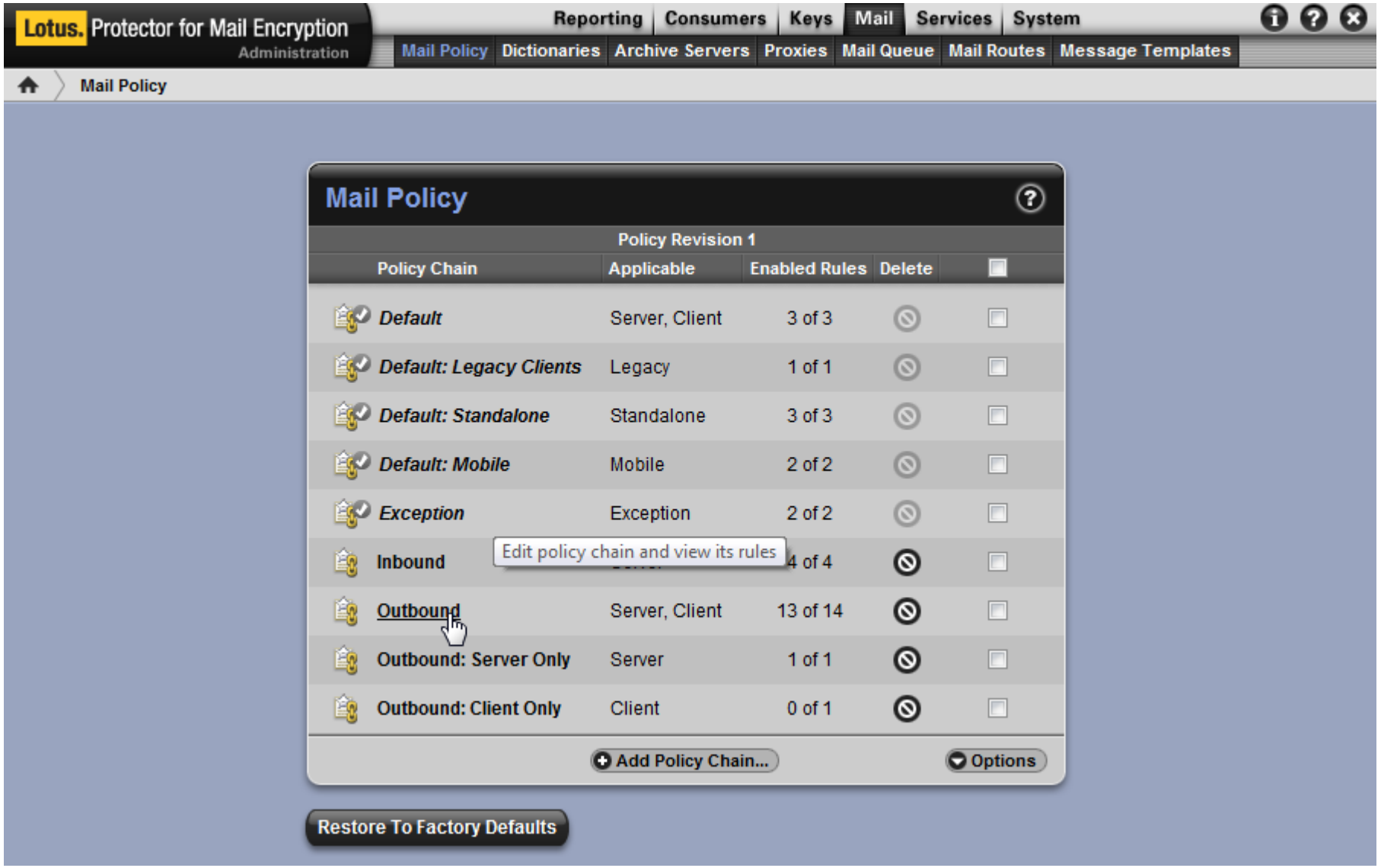
Benutzung des LPME-Clients



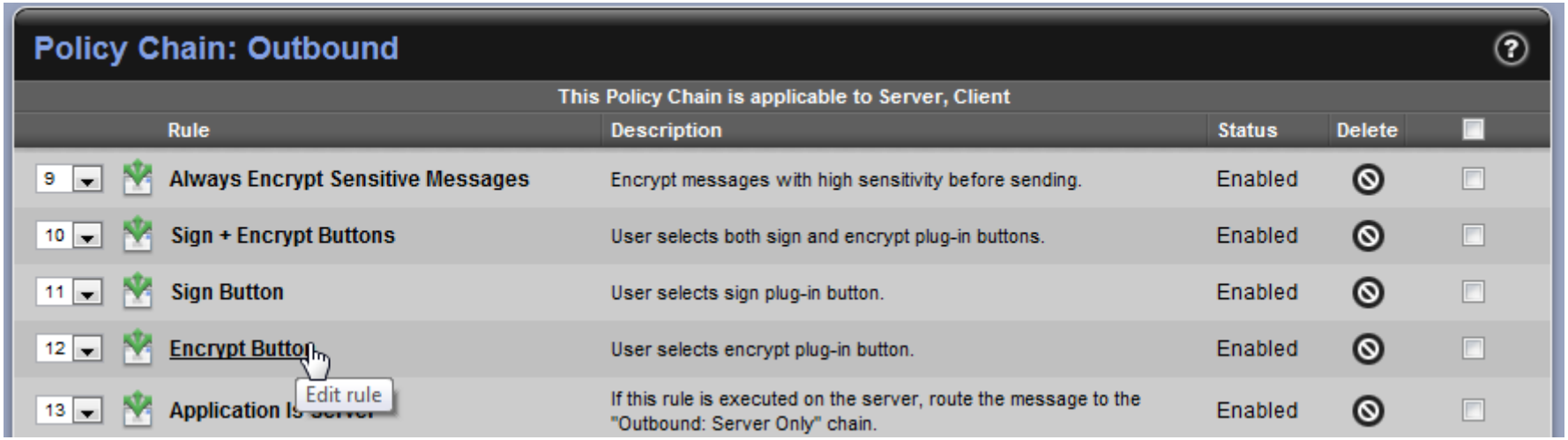
LPME „scharf“ schalten



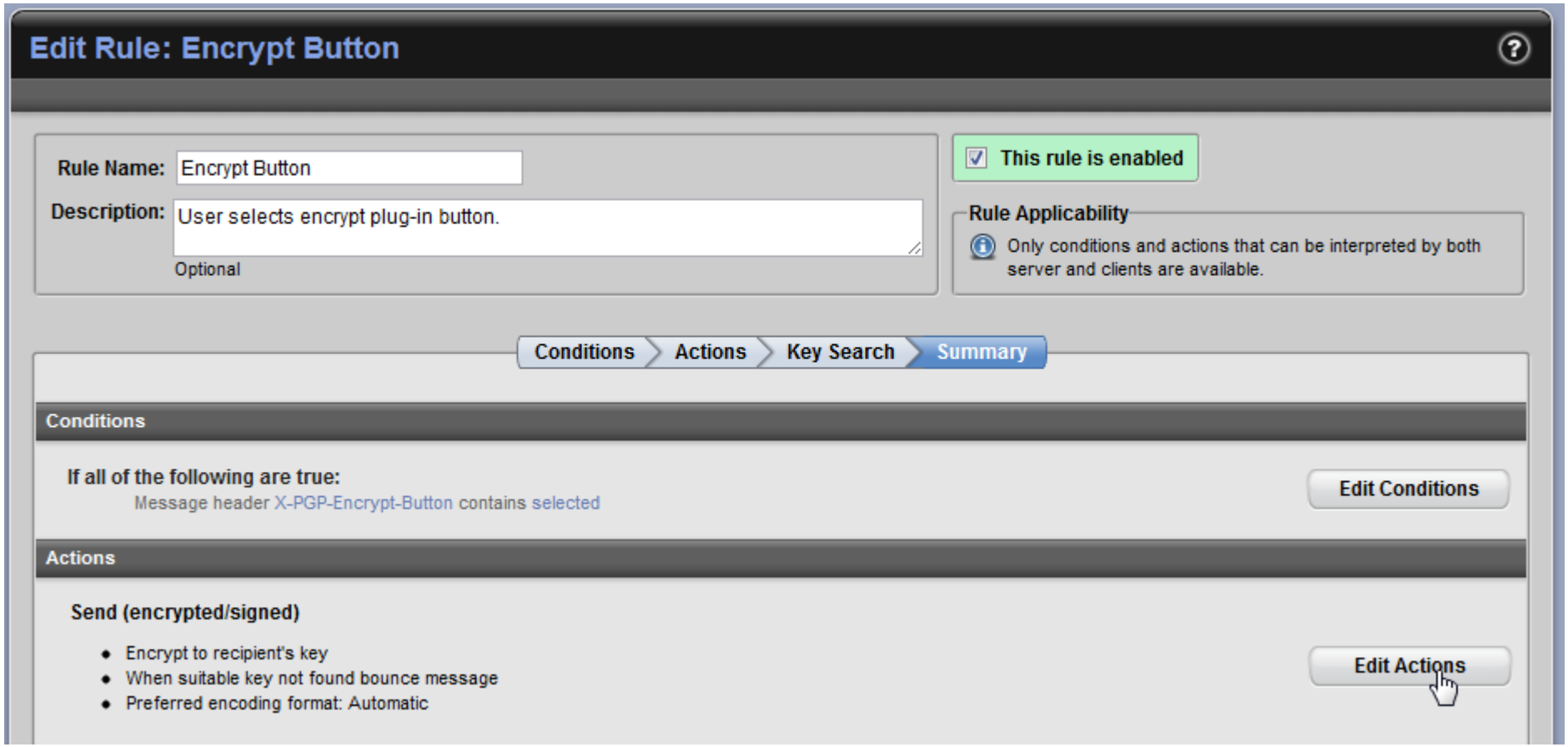
Ausgangsregel auf Smart Trailer stellen



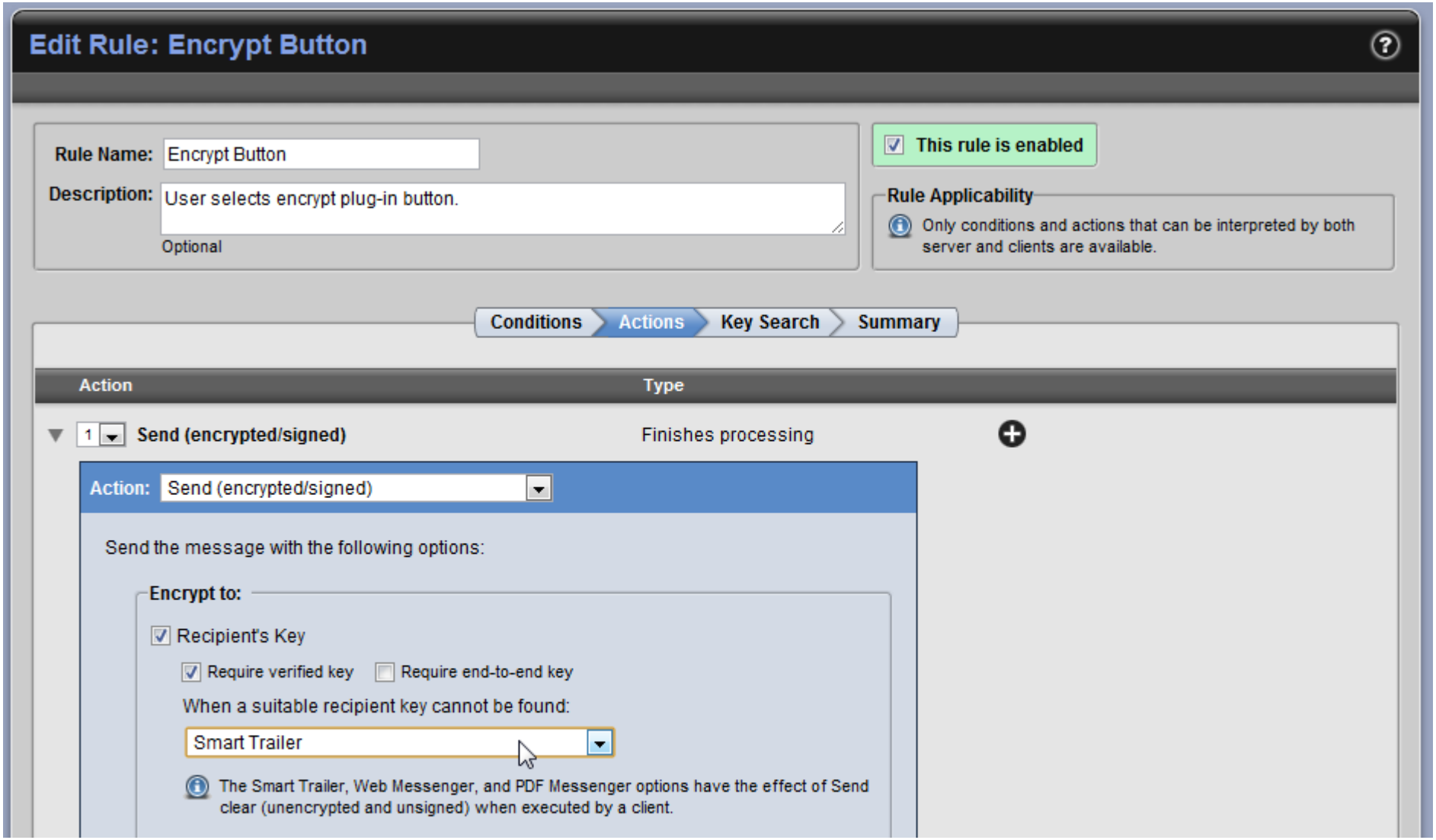
Ausgangsregel auf Smart Trailer stellen



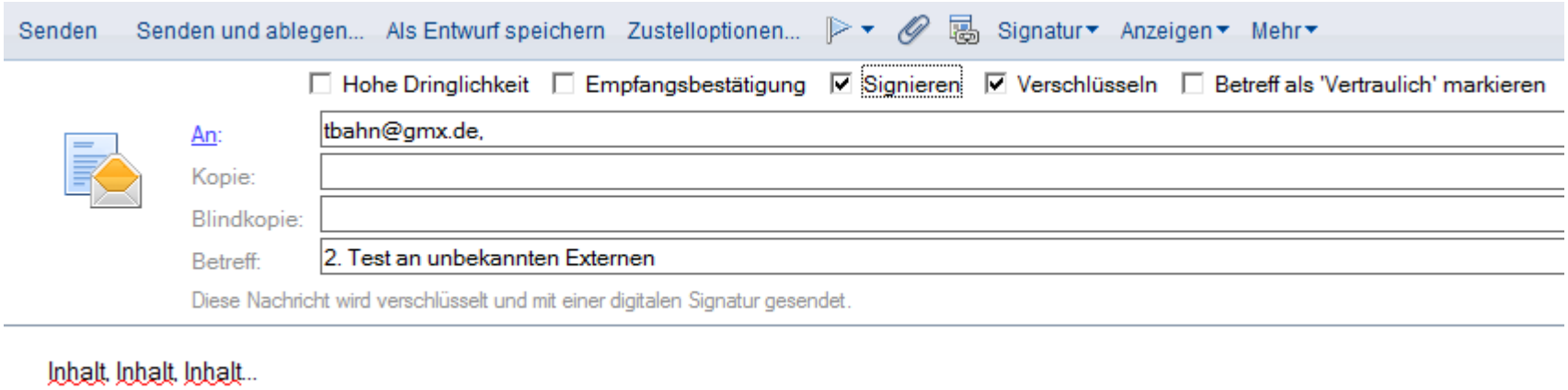
Ausgangsregel auf Smart Trailer stellen



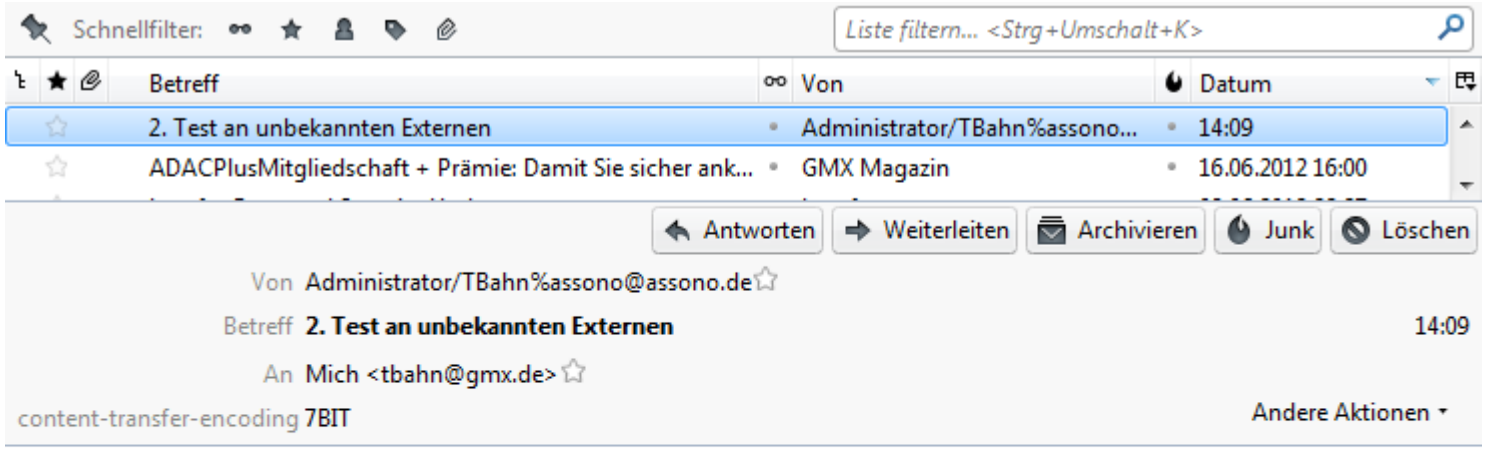
Ausgangsregel auf Smart Trailer stellen



Ausgangsregel auf Smart Trailer stellen



Ausgangsregel auf Smart Trailer stellen



Ausgangsregel auf Smart Trailer stellen

Vielen Dank, dass Sie sich entschieden haben, Ihre Nachrichten mit Lotus Protector for Mail Encryption zu sichern.

Damit Ihre Sicherheit gewährleistet ist, senden wir eine E-Mail-Nachricht an den Empfänger dieses Links. Klicken Sie auf den Link in der Nachricht, um eine Passphrase zu erstellen und zukünftig Nachrichten zu sichern.

Weitere Informationen finden Sie auf unserer Website unter www.pgp.com.

assono

Fragen?

jetzt stellen – oder später:

tbahn@assono.de
http://www.assono.de/blog
04307/900-401

assono
IT-Consulting & Solutions

Folien unter:
www.assono.de/blog/d6plinks/AC12-Lotus-Protector