



AdminCamp 2012 Track 2, Session 1:

Lotus Protector - weil sicher sicher ist

Gelsenkirchen, 18. Juni 2012

Innovative Software-Lösungen.





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







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





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)





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





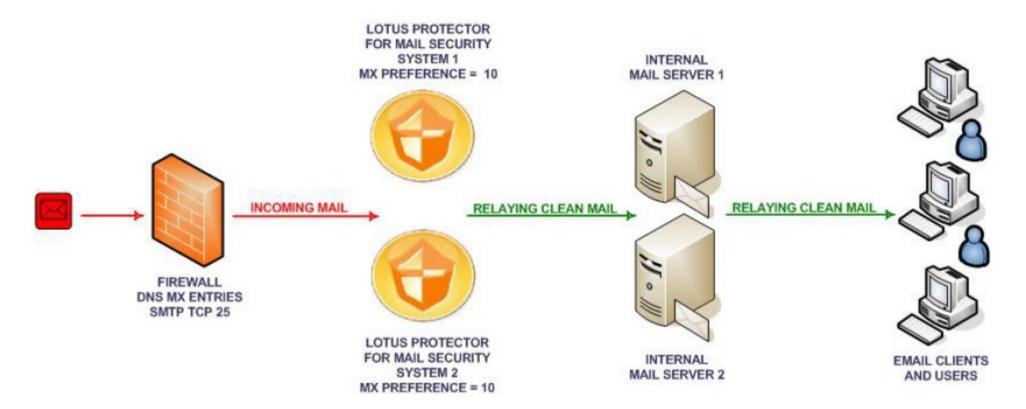
MX-Einträge (DNS)

- 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

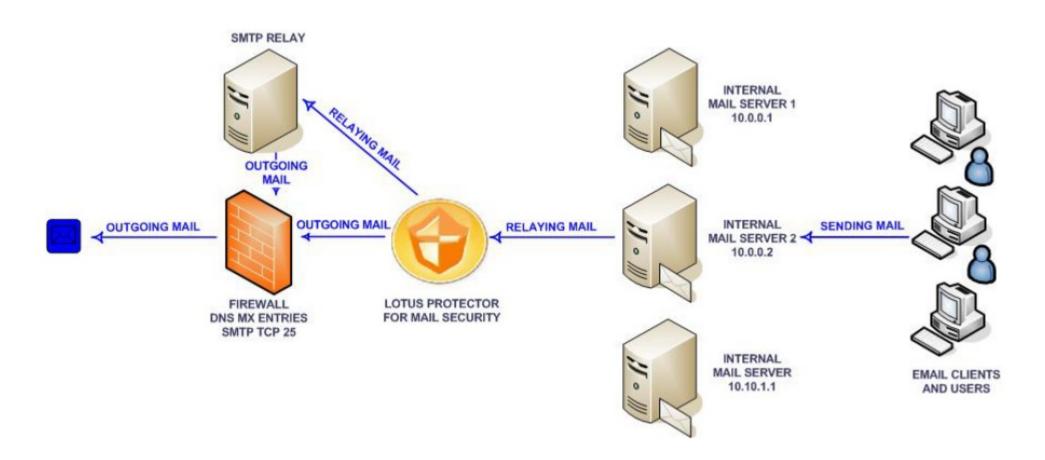


Quelle: IBM Lotus Protector for Mail Security Getting Started Guide Version 2.8 (SC27-3830-00)





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:
 Idapsearch -h Idap.tbahn.local -p 389 -D "cn=LDAP-Bind" -w ***** "maildomain=TBahn" cn





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





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





```
AC12-LPMS - VMware Player File ▼ Virtual Machine ▼ Help ▼
                                                                               _ _ ×
To start the installation enter 'install' and press <return>.
Available boot options:
  install - New installation
  rescue - Boot a rescue system
  harddisk - Boot from harddisk
  memtest86 - Test memory
boot: install_
                                            vmware<sup>*</sup>
To direct input to this virtual machine, press Ctrl+G.
```

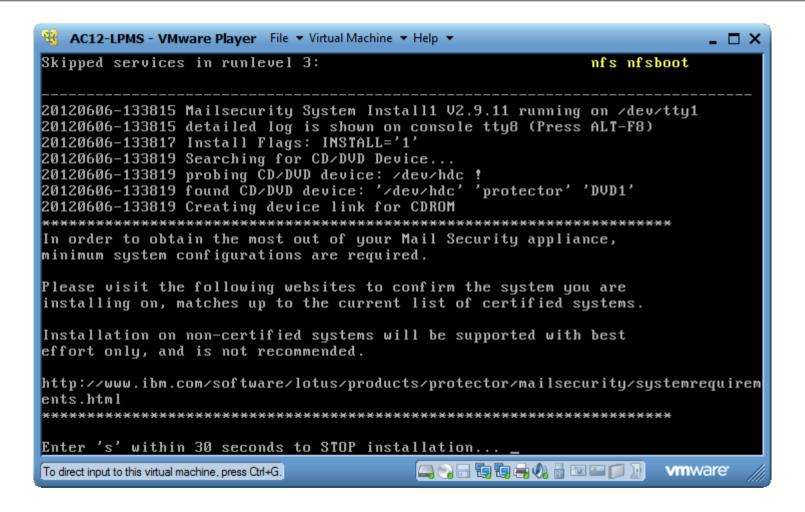




```
AC12-LPMS - VMware Player File ▼ Virtual Machine ▼ Help ▼
                                                                            _ 🗆 ×
input: ImPS/2 Generic Wheel Mouse as /class/input/input1
input: PC Speaker as /class/input/input2
md: md driver 0.90.3 MAX MD DEVS=256, MD SB DISKS=27
md: bitmap version 4.39
NET: Registered protocol family 2
IP route cache hash table entries: 32768 (order: 5, 131072 bytes)
TCP established hash table entries: 131072 (order: 8, 1048576 butes)
TCP bind hash table entries: 65536 (order: 7, 524288 bytes)
TCP: Hash tables configured (established 131072 bind 65536)
TCP reno registered
NET: Registered protocol family 1
Using IPI No-Shortcut mode
ACPI wakeup devices:
PCIO USB P2PO S1FO S2FO S3FO S4FO S5FO PE4O PE5O PE6O PE7O PE41 PE42 PE43 PE44
PE45 PE46 PE47 PE51 PE52 PE53 PE54 PE55 PE56 PE57 PE61 PE62 PE63 PE64 PE65 PE66
PE67 PE71 PE72 PE73 PE74 PE75 PE76 PE77
ACPI: (supports SØ S1 S4 S5)
Freeing unused kernel memory: 204k freed
Moving into tmpfs... done.
>>> SUSE Linux Enterprise Server 10 installation program v2.0.79 (c) 1996-2008 S
USE Linux Products GmbH <<<
Starting udev ...
... udev running
Starting hardware detection...
Activating usb devices..._
                                          vmware
To direct input to this virtual machine, press Ctrl+G.
```

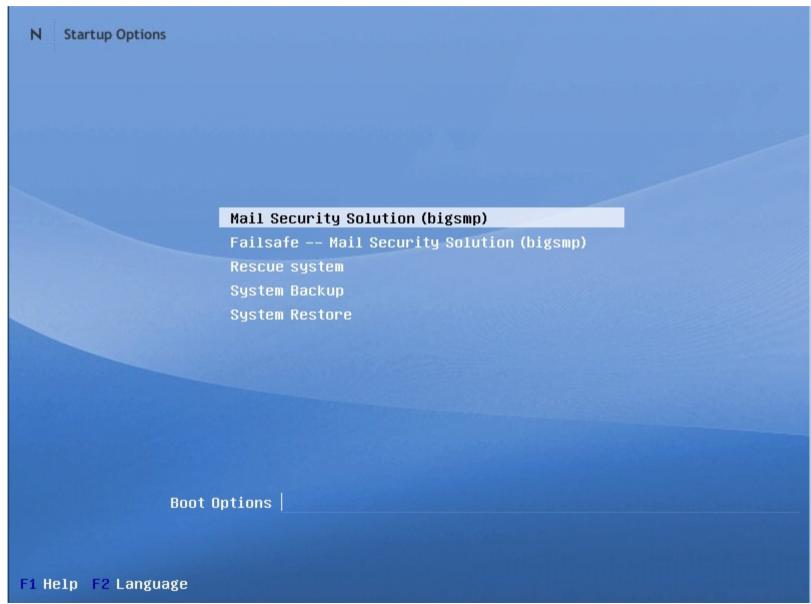
















```
AC12-LPMS - VMware Player File ▼ Virtual Machine ▼ Help ▼
                                                                            _ 🗆 X
Loading glogicfc
sd 0:0:0:0: Attached scsi generic sg0 type 0
FATAL: Error inserting glogicfc (/lib/modules/2.6.16.60-0.85.1-bigsmp/kernel/dri
vers/scsi/qlogicfc.ko): No such device
Loading serverworks
Loading sym53c8xx
Loading sata promise
Loading sata_sx4
Loading sata_via
Loading sata_qstor
Loading sata_sis
Loading sx8
Loading ips
FATAL: Error inserting ips (/lib/modules/2.6.16.60-0.85.1-bigsmp/kernel/drivers/
scsi/ips.ko): No such device
Loading ahci
Loading ata_piix
Loading jbd
Loading ext3
Waiting for device /dev/root to appear: ok
rootfs: major=8 minor=2 devn=2050
fsck 1.38 (30-Jun-2005)
[/bin/fsck.ext3 (1) -- /] fsck.ext3 -a /dev/root
ROOT (/dev/root) has gone 49710 days without being checked, check forced.
                                           vmware
To direct input to this virtual machine, press Ctrl+G.
```



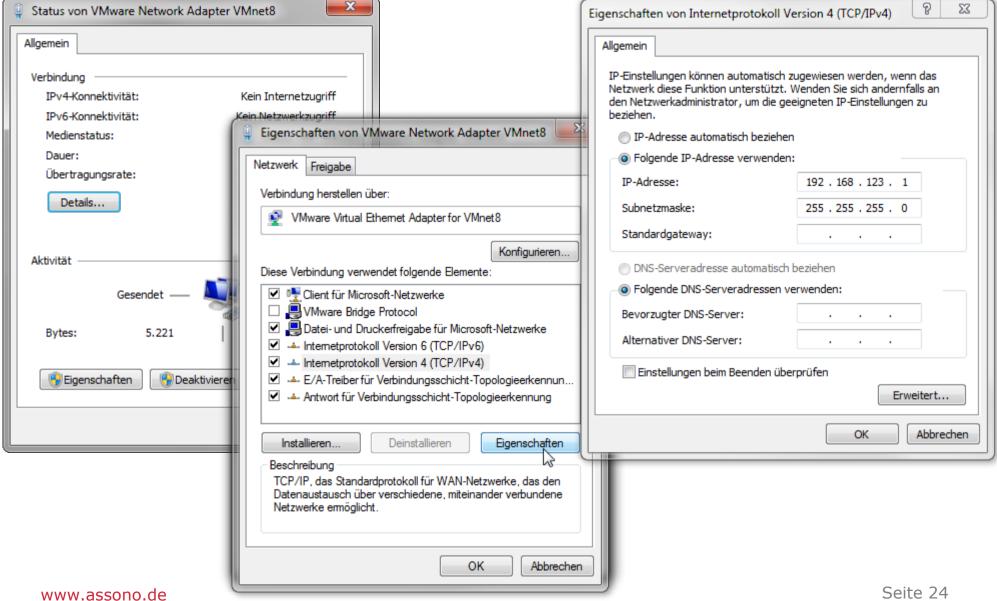


3 AC12-LPMS - VMware Player File ▼ Virtual Machine ▼ Help ▼	- □ ×
Starting ipticker daemon for ethO eth1 ok Wed Jun 6 12:00:16 UTC 2012 mounting /rescue	eth0:192.168.123.123/24 eth1:192.168.242.131/24 Mailsec: 2.8-9424
Creating Backup listfile /var/lib/backups/sysbackups.list unmounting /rescue Master Resource Control: runlevel 3 has been	reached
Skipped services in runlevel 3:	irq_balancer
20120606-120019 Mailsecurity System Install2 V2.12.4 running on /dev/tty1 20120606-120019 detailed log is shown on console tty8 (press Alt-F8) 20120606-120021 Install Flags: 20120606-120021 Current install state: 9 20120606-120021 Installation cleanup 20120606-120021 chkconfig autoinstall off 20120606-120031 ===================================	
Welcome to SUSE Linux Enterprise Server 10 SP2 (i586) Kernel 2.6.16.60-0.85.1-bigsmp (tty1)	
unconfigured login: _	
To direct input to this virtual machine, press Ctrl+G.	vmware //





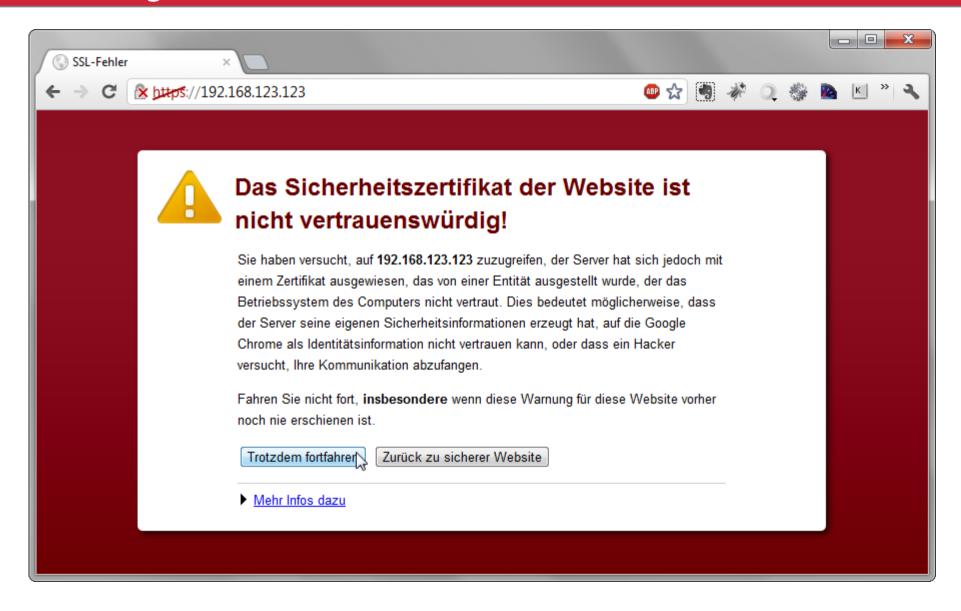
Netzwerk-Einstellungen des Clients anpassen







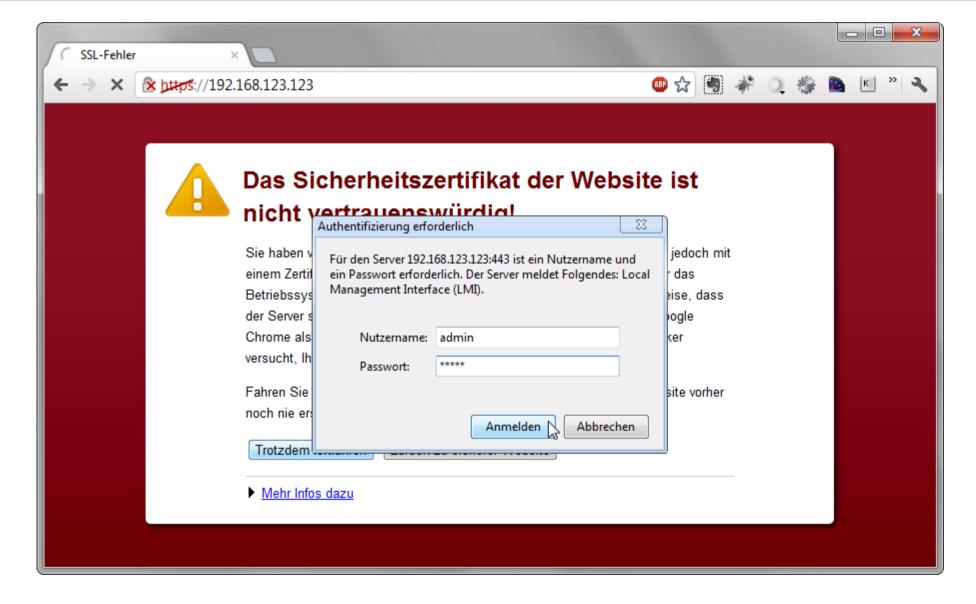
Weiter geht's im Browser





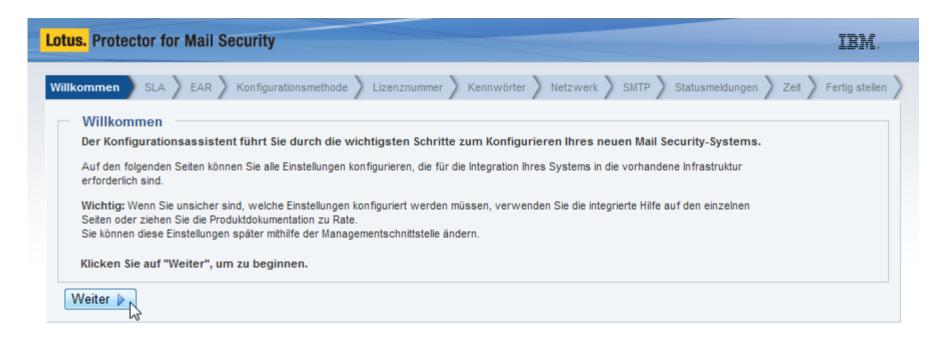


Weiter geht's im Browser



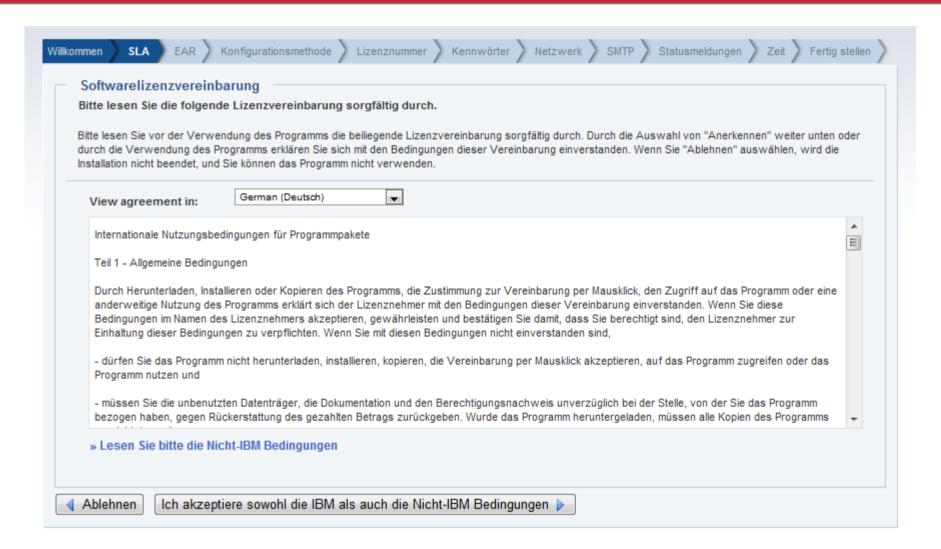






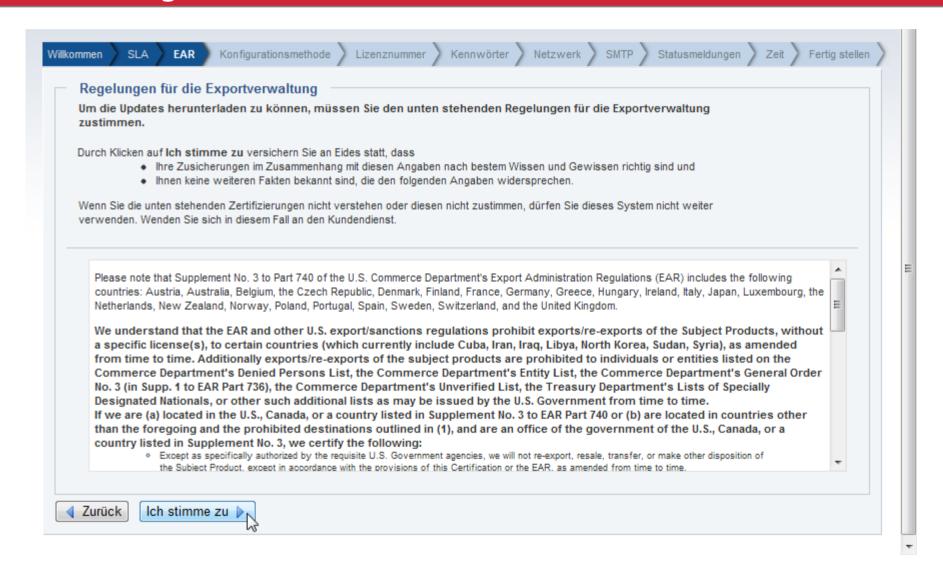












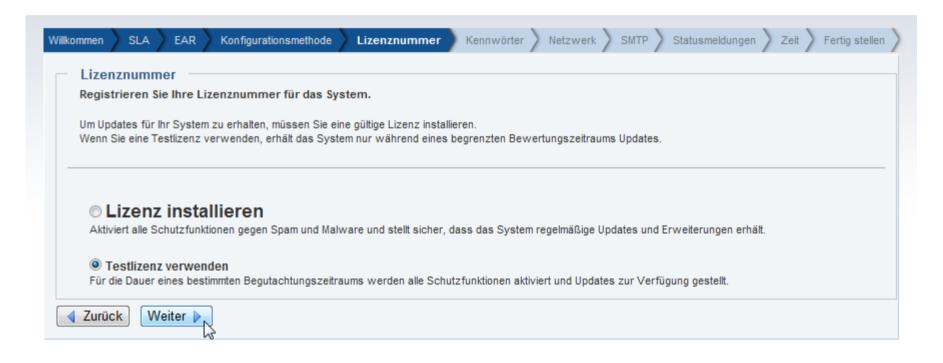






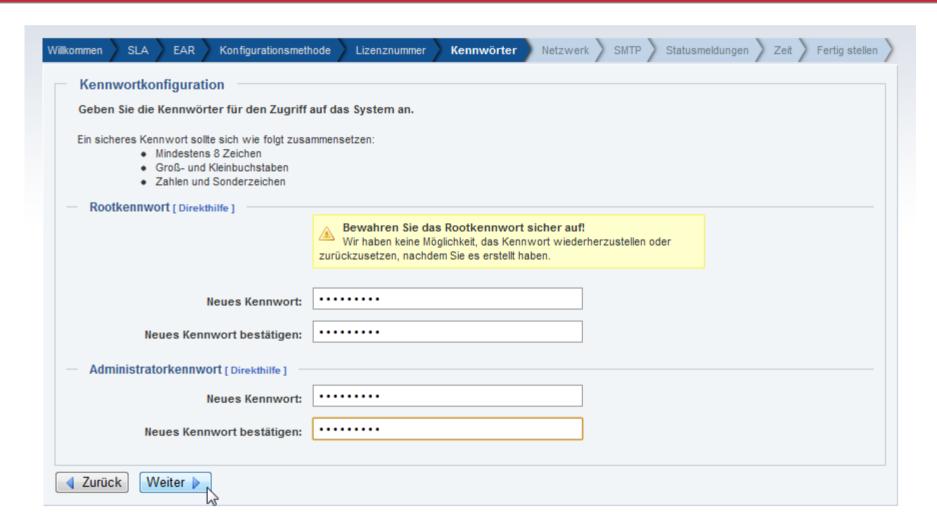












Netzwerkkonfiguration

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

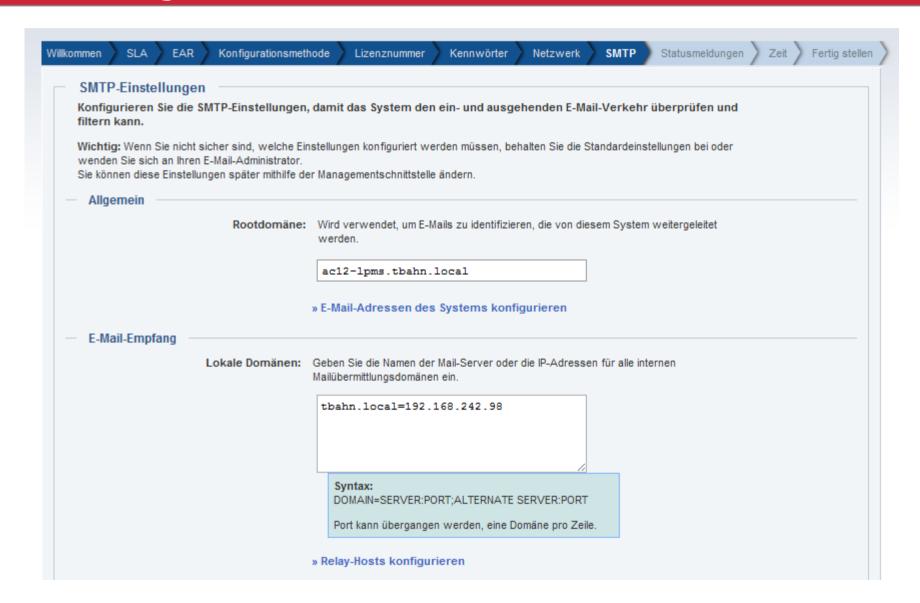
Sekundärer DNS-Server:

192.168.242.2

Tertiärer DNS-Server:

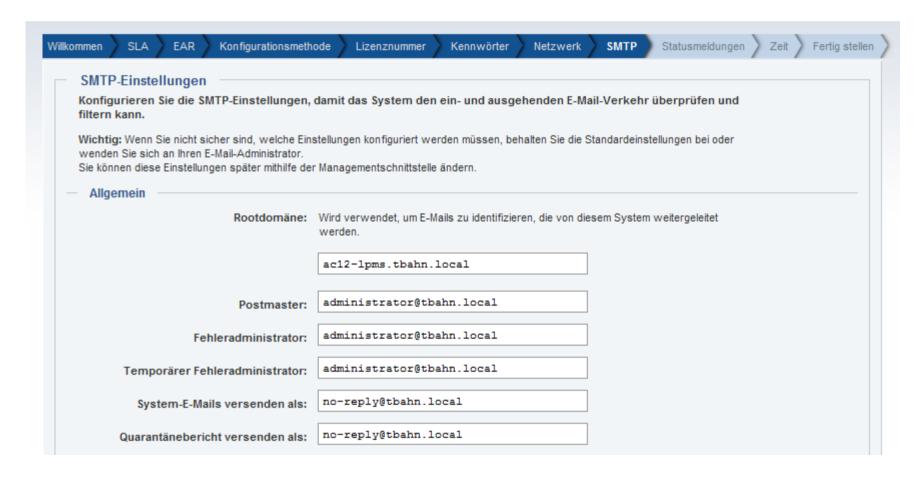












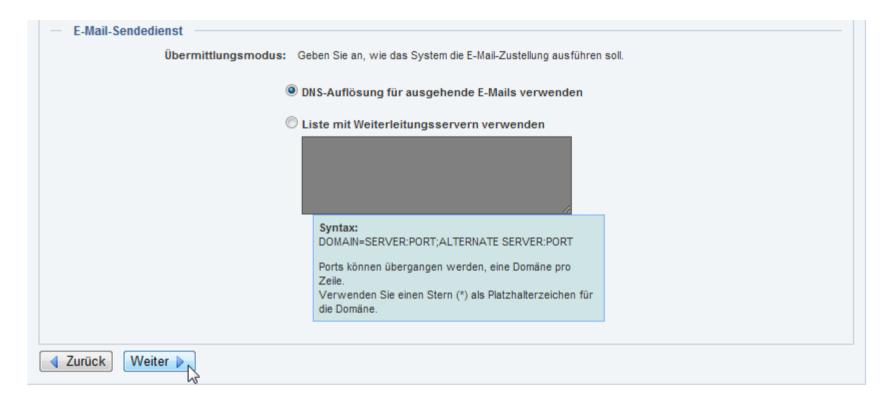






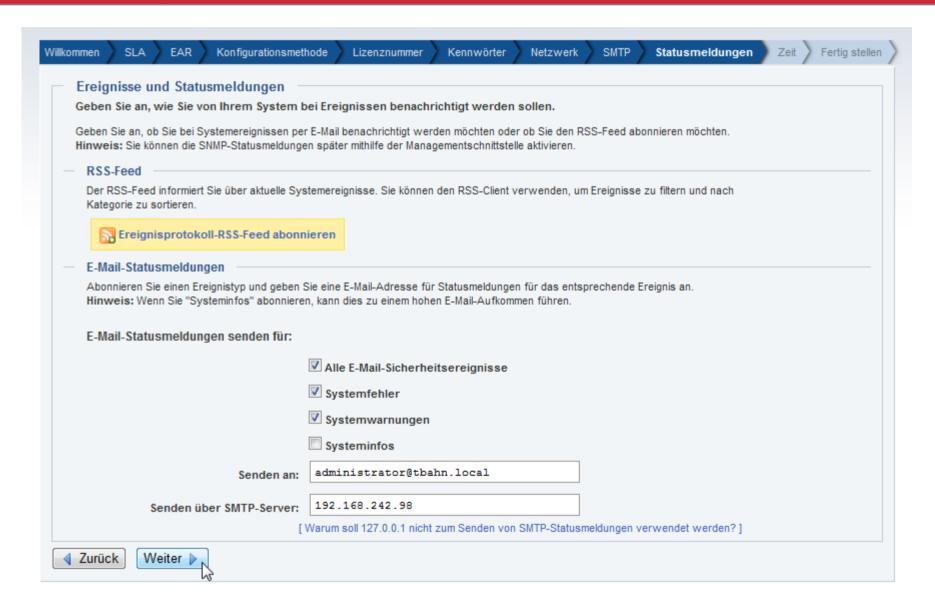












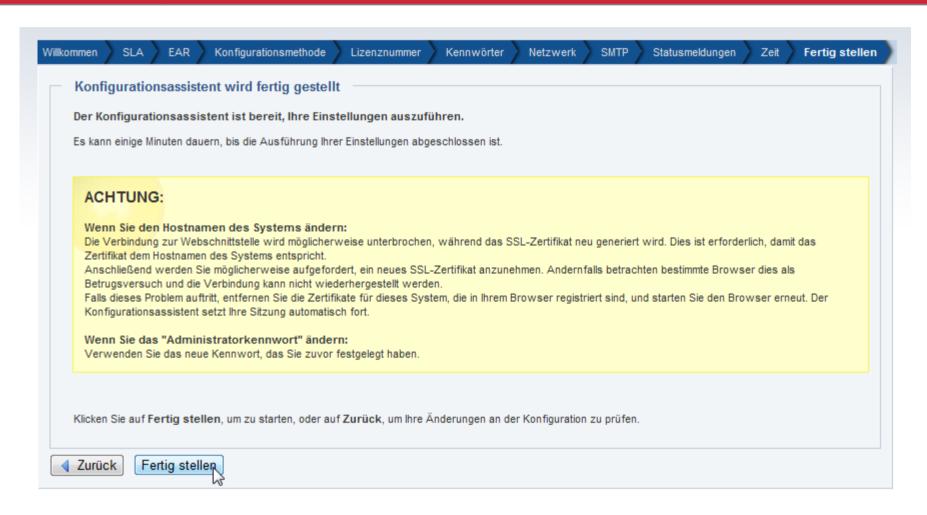


















N



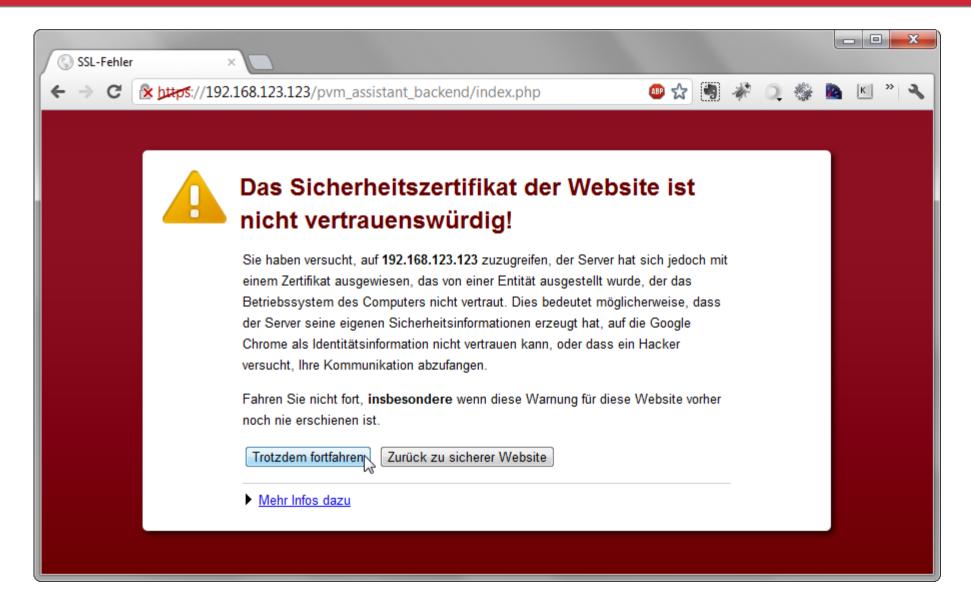








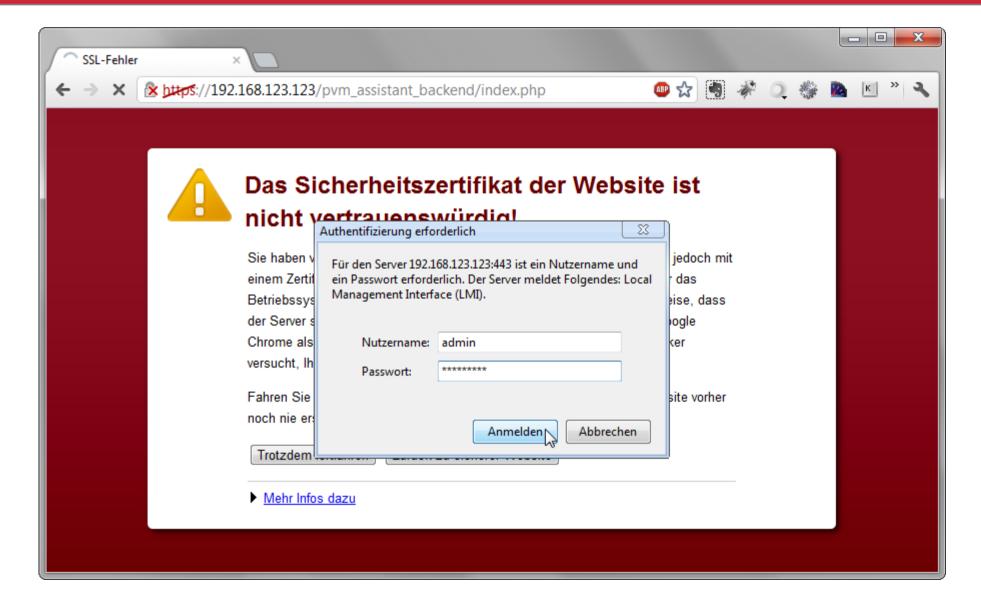
Noch einmal im Browser







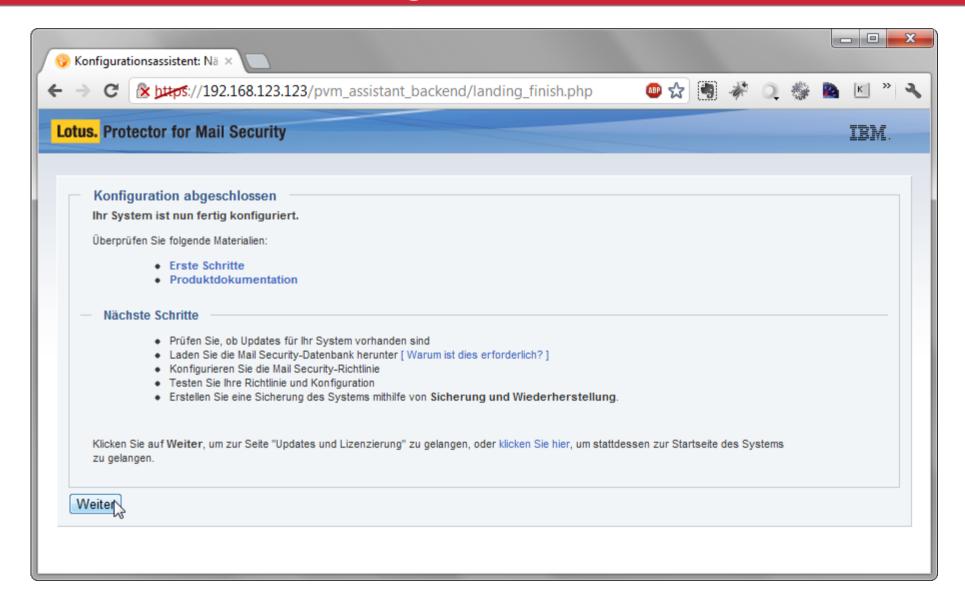
Noch einmal im Browser







Abschluss der Erstkonfiguration







Benutzeroberfläche verwendet Java







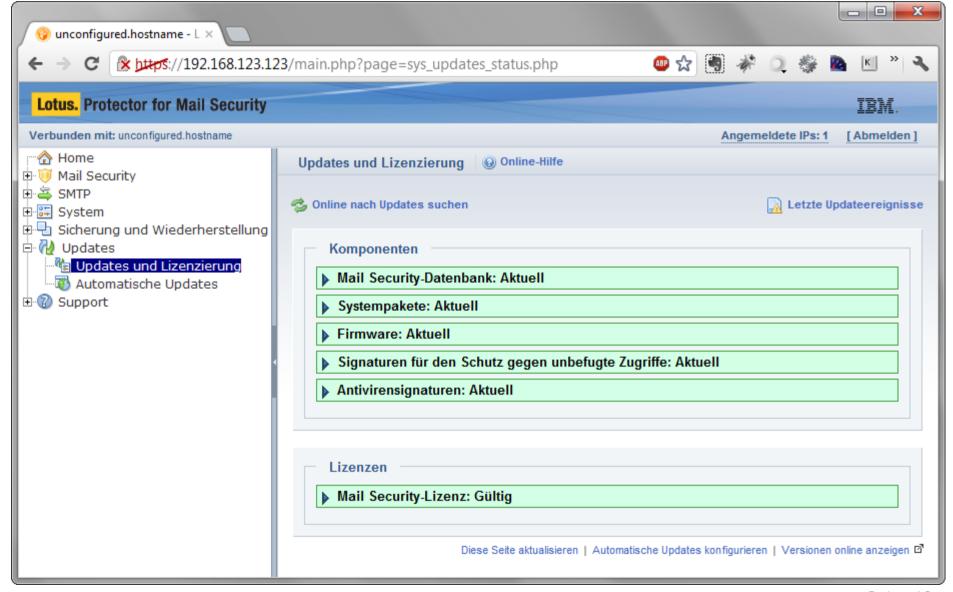
Benutzeroberfläche verwendet Java





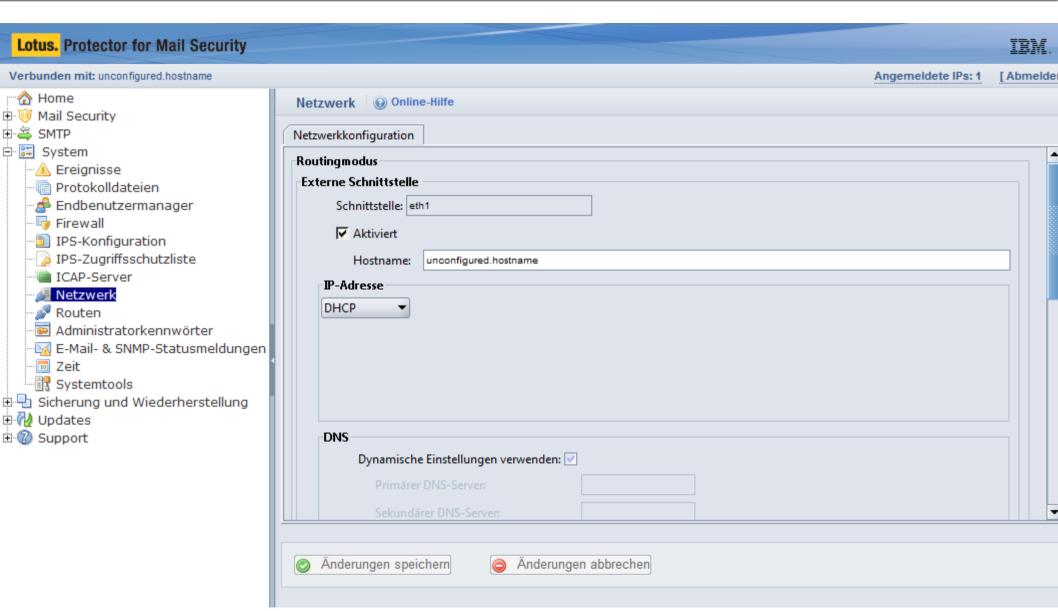


Alles im grünen Bereich...



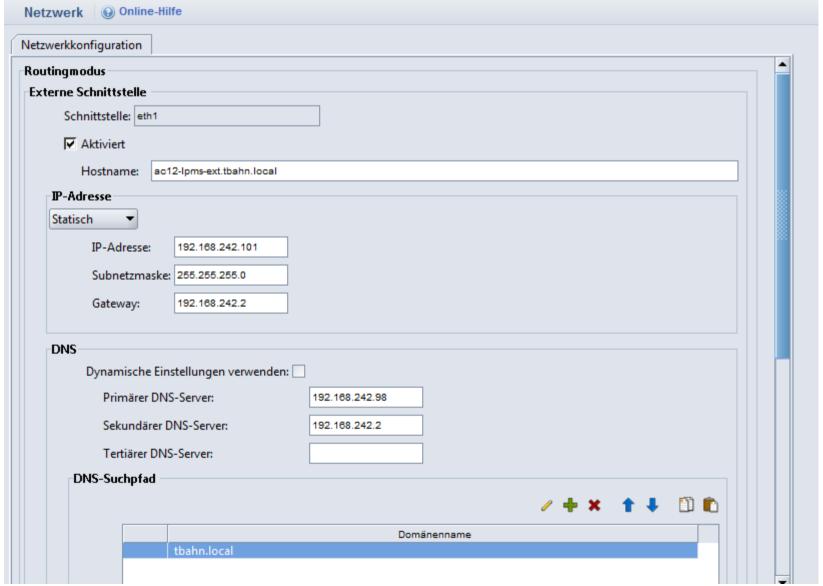






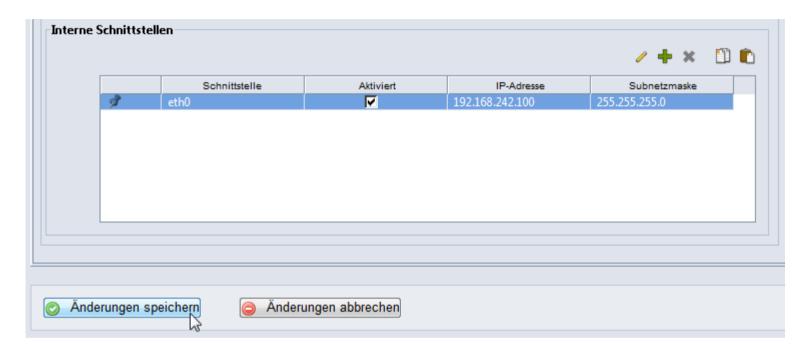






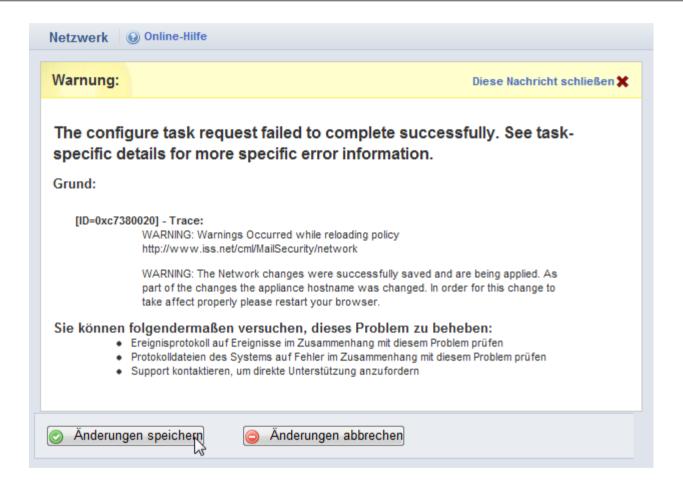
















3 AC12-LPMS - VMware Player File ▼ Virtual Machine ▼ Help ▼	- □ ×
reate IPv6 socket: Address family not supported by protoceth0:192.16 eth1:192.16	68.242.100/24 68.242.101/24
Starting SSH daemon Mailsec: 2.	8-9424
Starting Mail Security:	done
20120606-190620 N replicator[5074] Starting Replication service: gro	config
20120606-190620 N replicator[5074] Start rc=0	J
20120606-190620 N replicator[5153] Starting Replication service: gra	lata
20120606-190620 N replicator[5153] Start rc=0	
20120606-190620 N replicator[5172] Starting Replication service: gr	nail
20120606-190620 N replicator[5172] Start rc=0	
Starting slpd	done
Starting httpd2 (prefork)	done
Starting CRON daemon	done
Starting ipticker daemon for ethO eth1 ok	
Wed Jun 6 19:06:24 UTC 2012	
mounting /rescue	
Creating Backup listfile /var/lib/backups/sysbackups.list	
unmounting /rescue	
Master Resource Control: runlevel 3 has been	reached
Skipped services in runlevel 3: irq_bala	incer
Welcome to SUSE Linux Enterprise Server 10 SP2 (i586)	
Kernel 2.6.16.60-0.85.1-bigsmp (tty1)	
unconfigured login: _	
To direct input to this virtual machine, press Ctrl+G.	vmware //





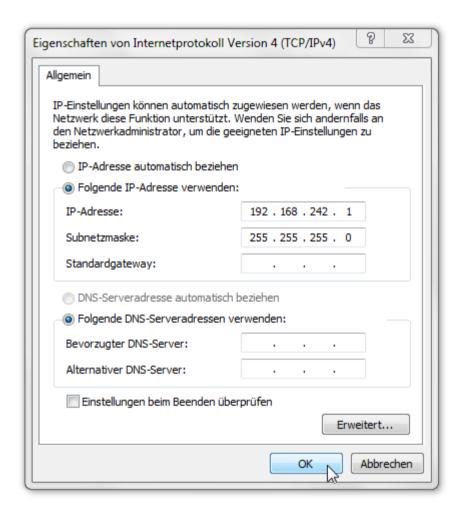
Änderungen über Konsole oder SSH

- 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



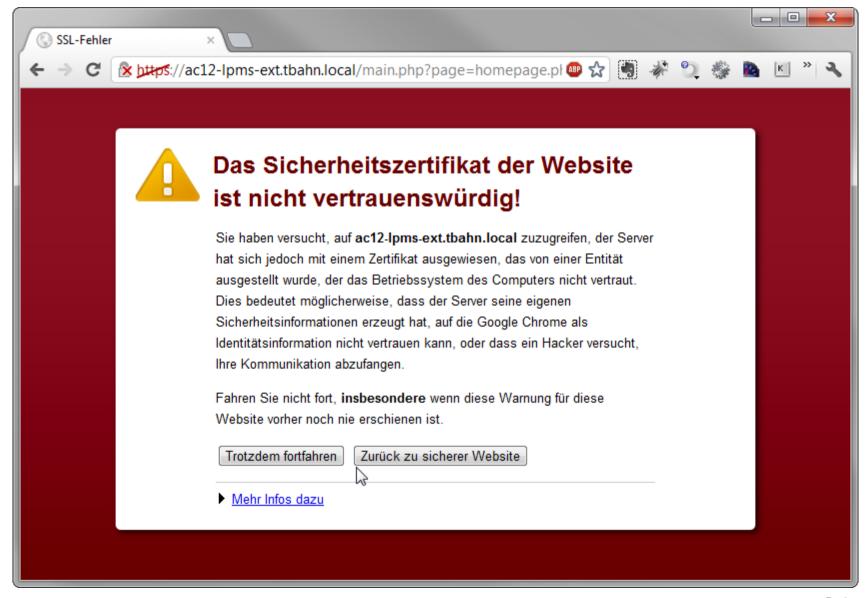


Netzwerk-Einstellungen des Clients wiederherstellen



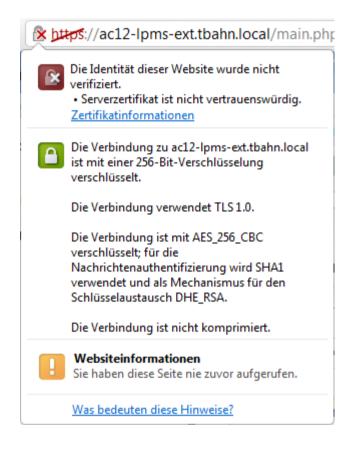












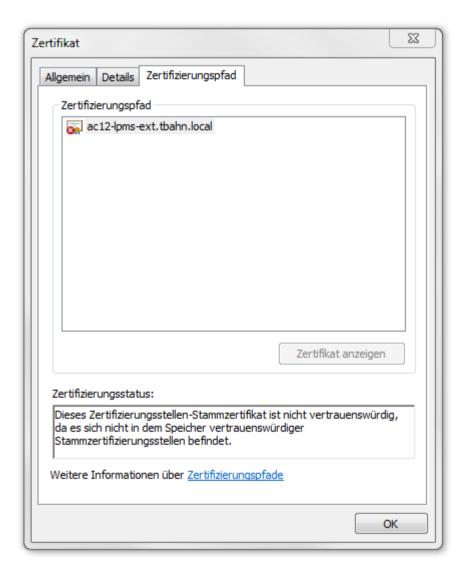






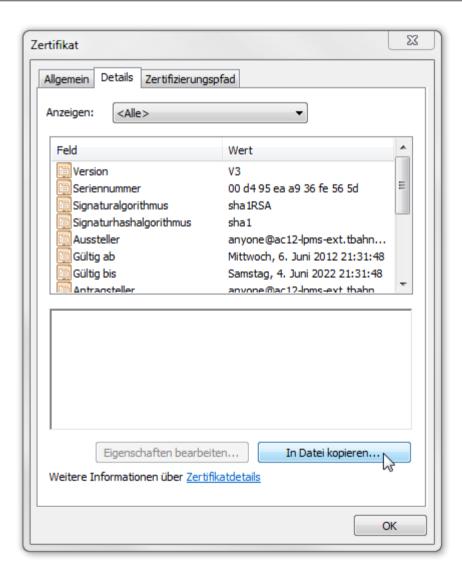












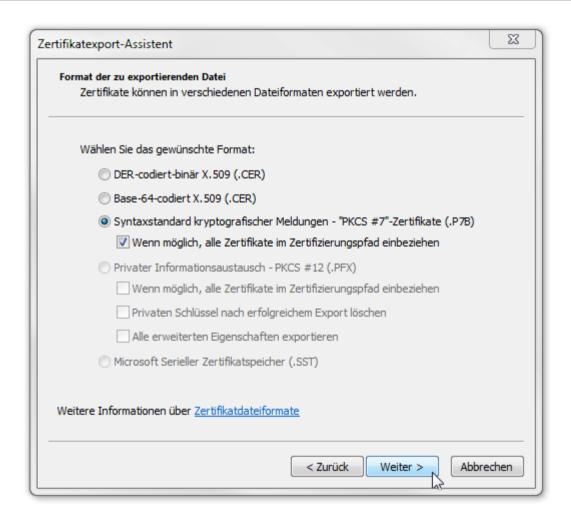






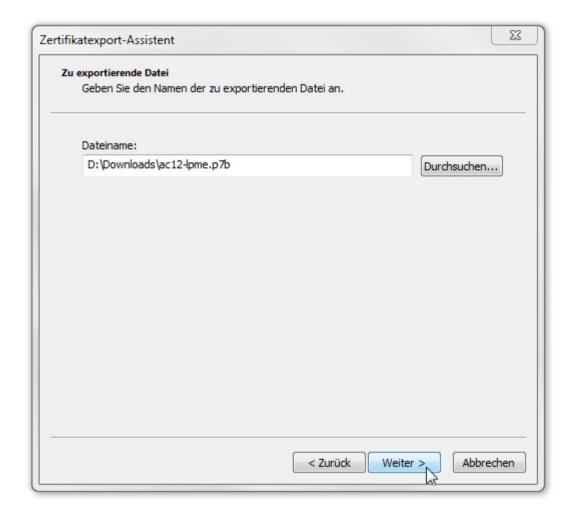












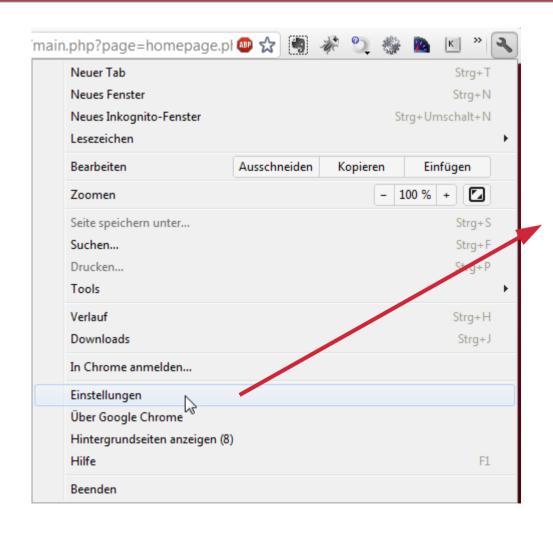


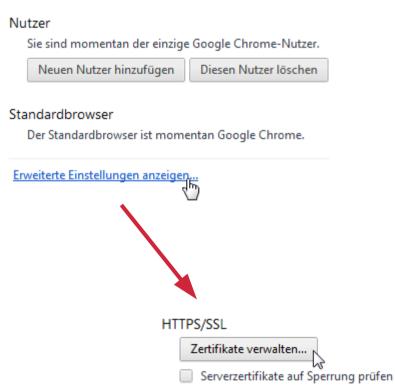






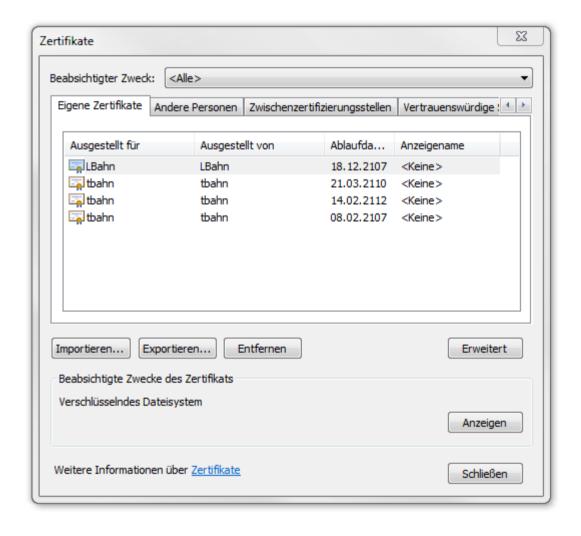






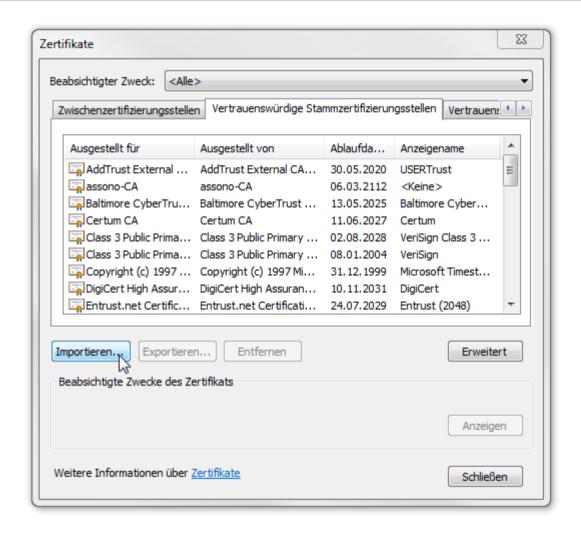












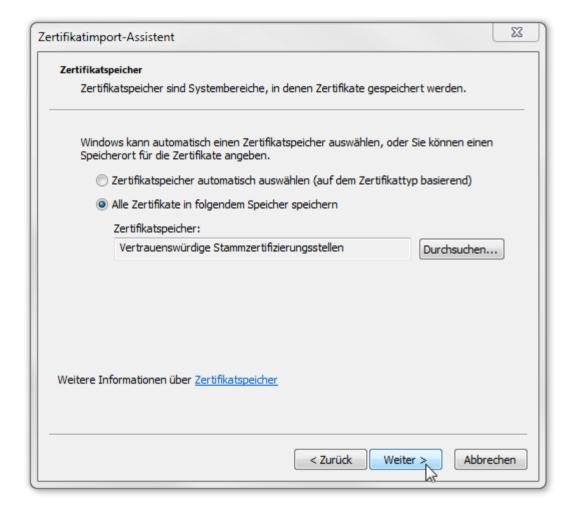












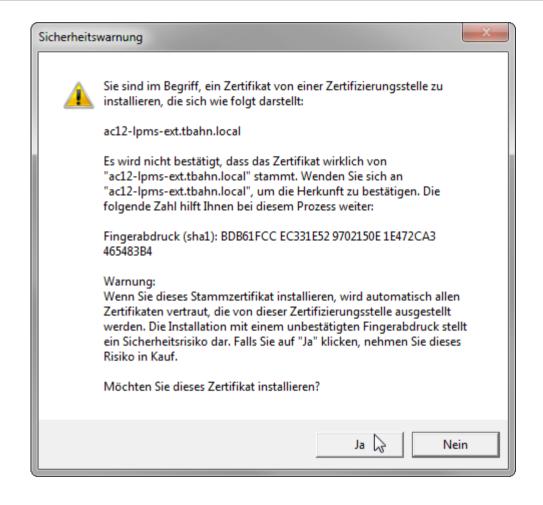






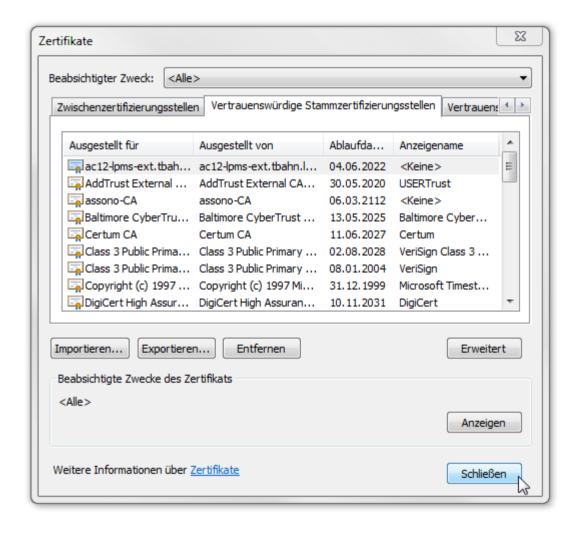








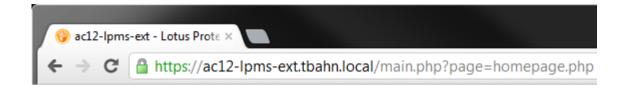








Warnung wegen des SSL-Zertifikats







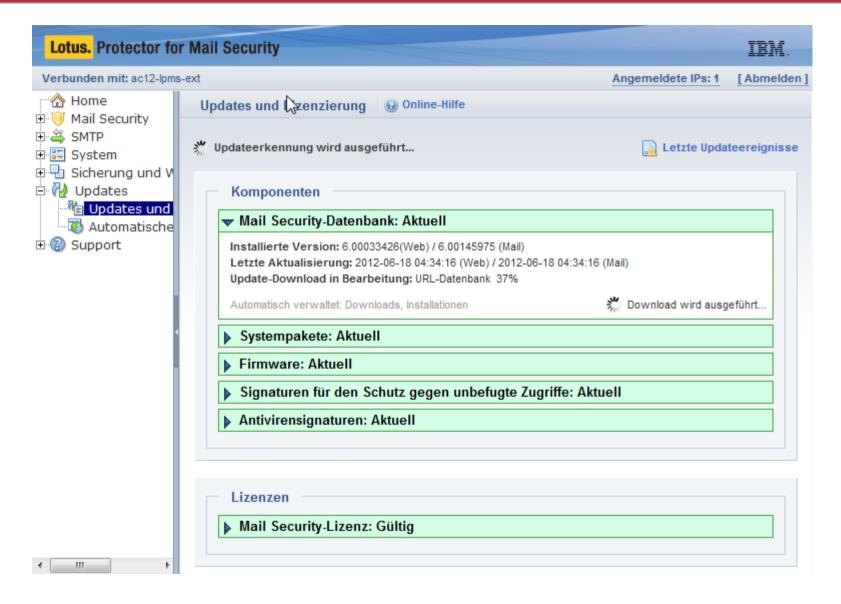
Automatische Aktualisierungen konfigurieren







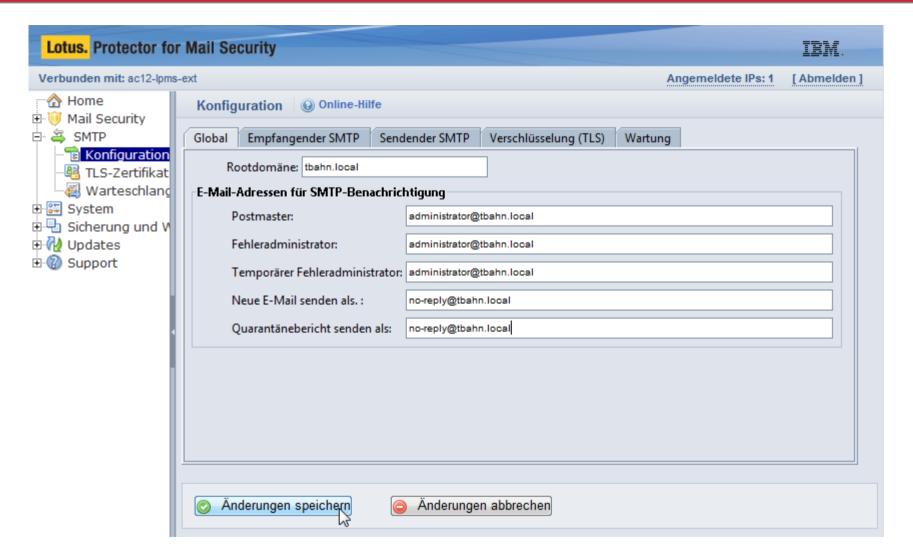
Aktualisierungsstatus und Mail Security-Datenbank







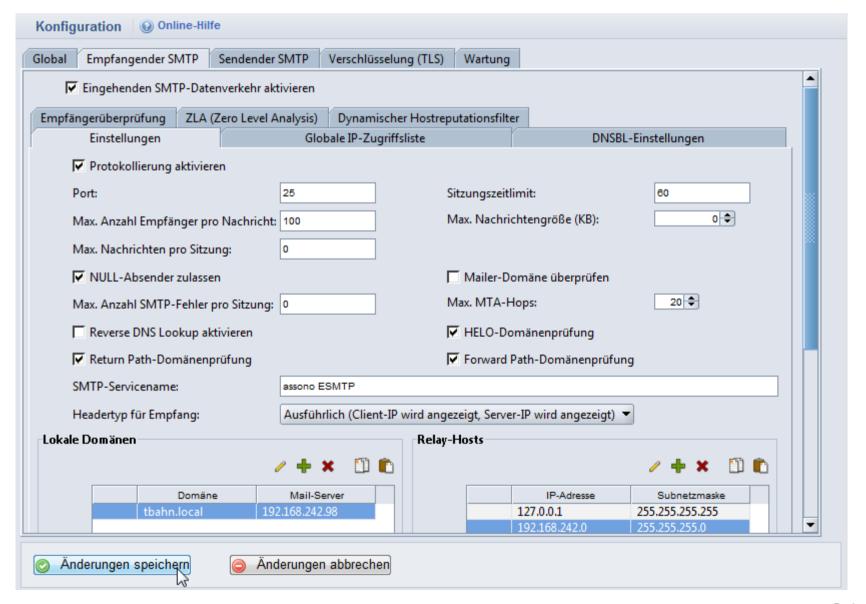
SMTP-Konfiguration







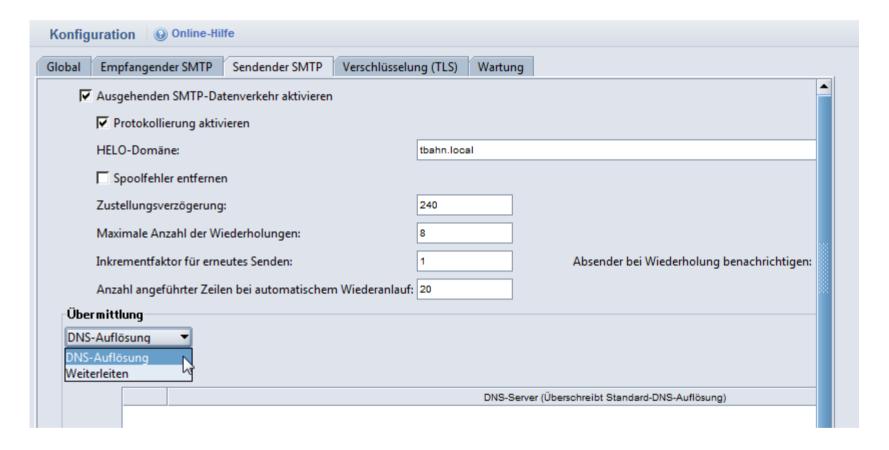
SMTP-Konfiguration





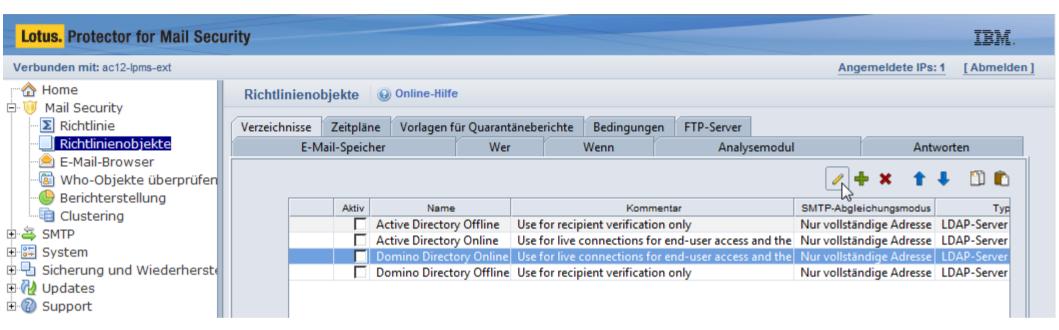


SMTP-Konfiguration



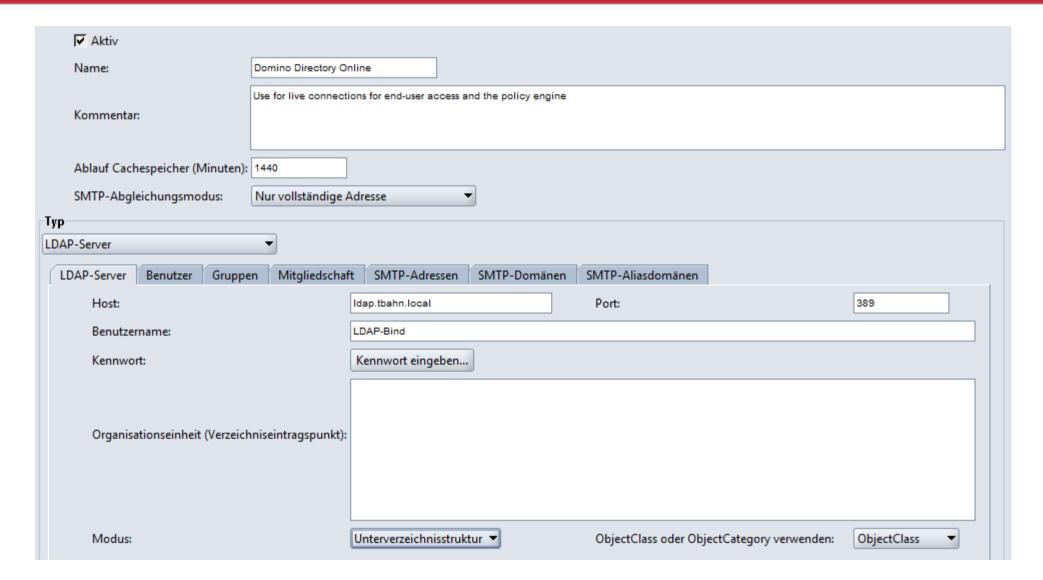






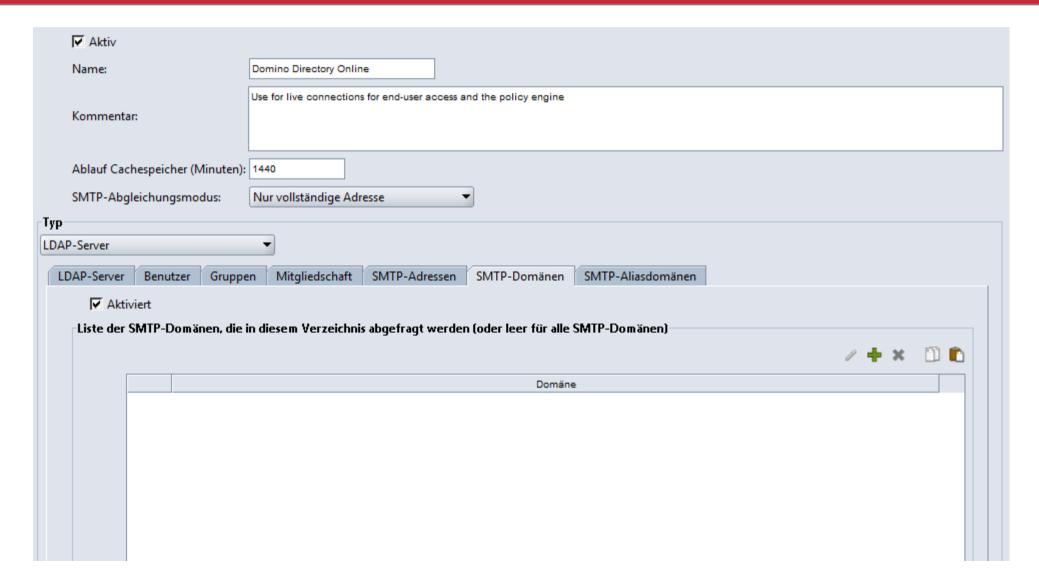






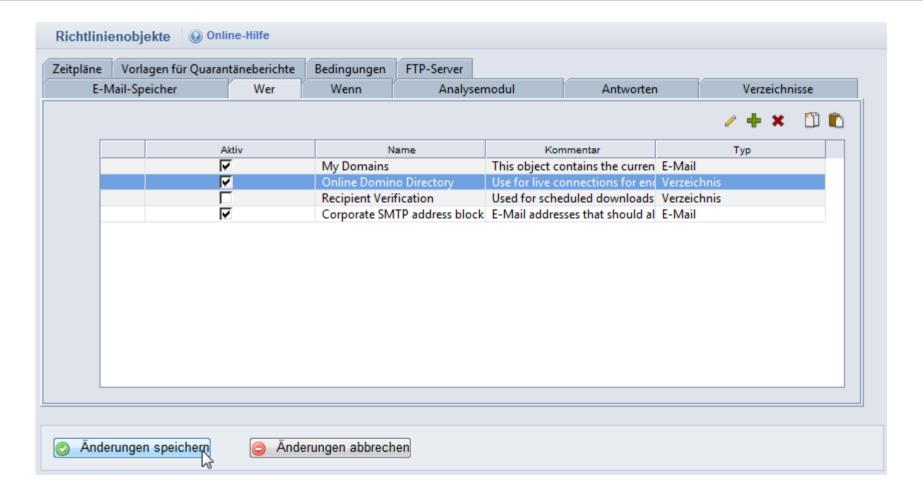






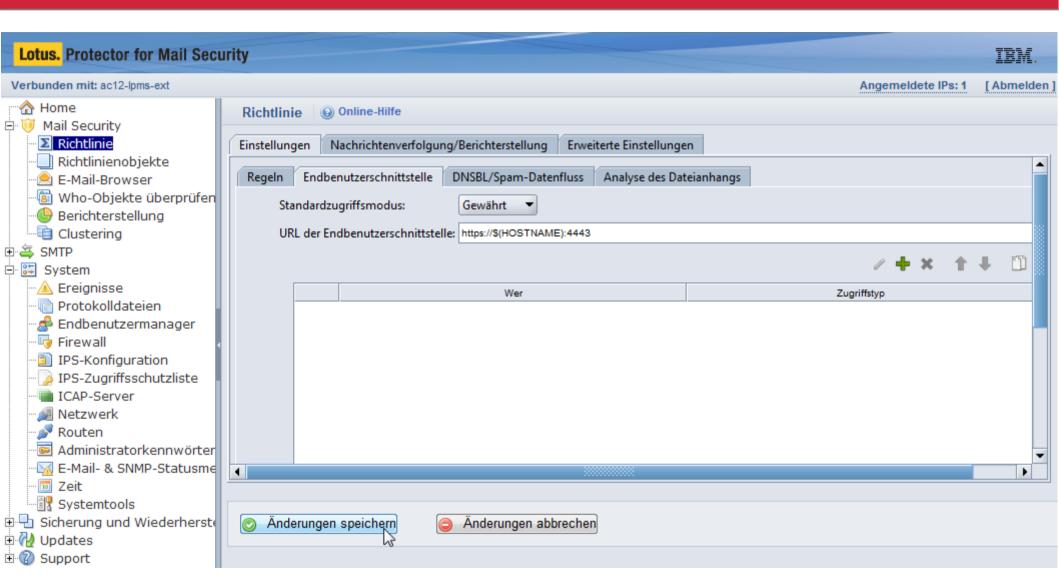






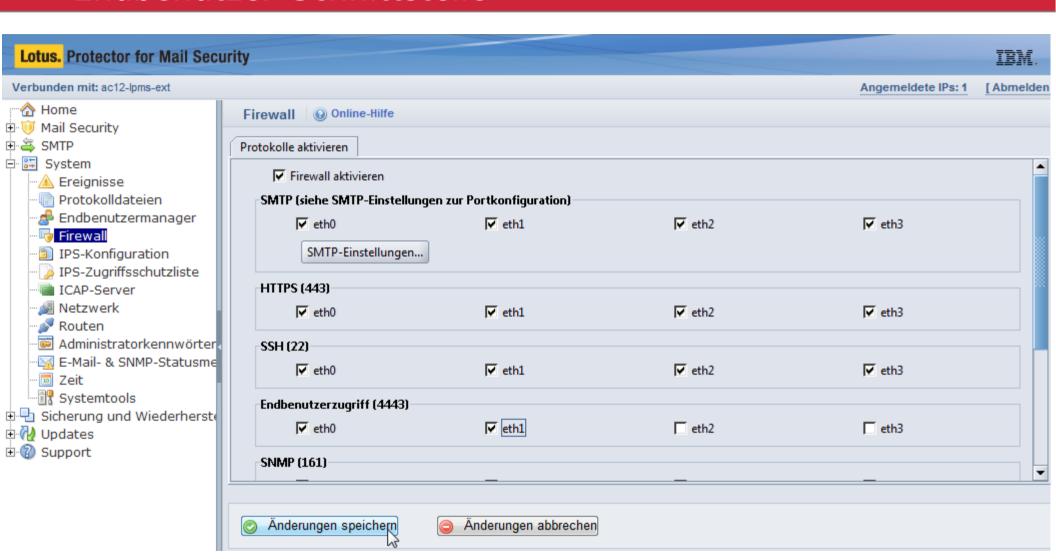






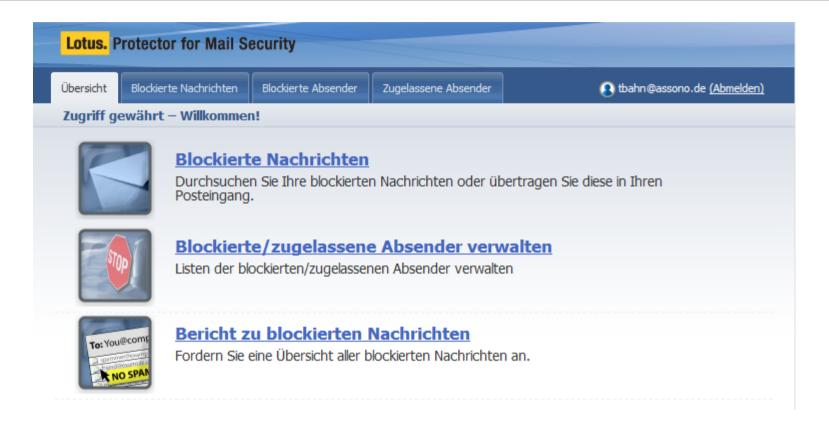






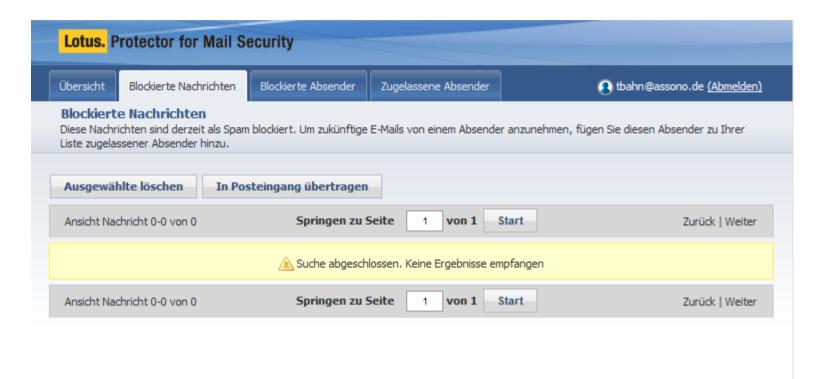




























Konfiguration des Domino-Servers

Konfigurationseins	tellungen : Notebook-016-8.5.3/TE	Bahn 600
Allgemein Sicherheit Client-U	pgrade Router/SMTP MIME NOTES.INI-Einste	llungen Lotus iNotes IMAP SNMP
Allgemein Beschränkungen un	d Steuerungen Ausschlussklauseln Mailverfolge	ung Nachrichtenrückruf Erweitert
Router/SMTP allgemein		
Anzahl der Mailboxen:	7 2	
SMTP wird zum Senden von Nachrichten an Empfänger außerhalb der lokalen Internetdomäne verwendet:	[©] Aktiviert 』▼	
SMTP ist innerhalb der lokalen Internetdomäne zulässig:	□ Deaktiviert □ ▼	
Server innerhalb der lokalen Notes-Domäne sind via SMTP über TCP/IP erreichbar:	^r Immer 』▼	
Adresssuche:	[™] Vollst. Name dann lokaler Teil 』 ▼	
Ausführliche Suche:	[□] Deaktiviert <u> </u> •	
Relaishost für Nachrichten, die die lokale Internetdomäne verlassen:	ac12-lpms.tbahn.local <u>a</u>	





Desktopeinstel	lungen	
Allgemein Smart Upgrad	de Anwendungen Widgets Wählverbindungen Konten Namensserv	er
Allgemein		
Name:	『AC12-LPMS-Test』	
Beschreibung:		

Optionen für Lotus Protector		Übernehmen von übergeordneter Richtlinie:	untergeordneten
Geben Sie die URL für den Zugriff auf Protector-Server 『ac12-lpms-ext.tbahn.local:4443』 an:	☐ Wert nicht festlegen	Übernehmen	Zwingend

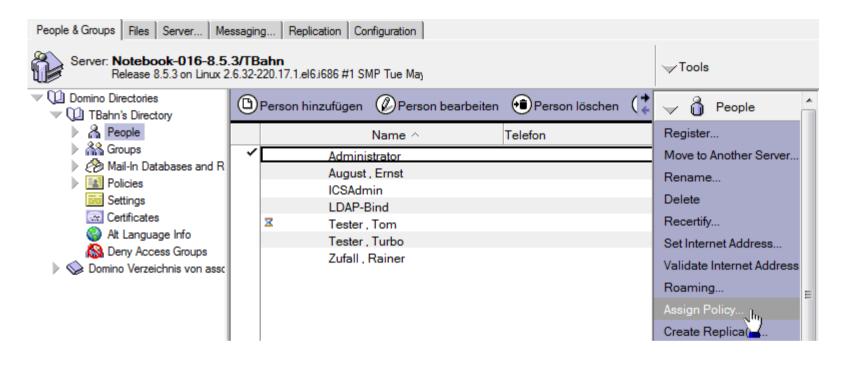




Richtlinie : /AC12-LPMS-Test		
Allgemein Richtlini	ienzuweisung Richtlinienpriorität Komme	ntare Administration
Allgemein		
Richtlinienname:	『/AC12-LPMS-Test』	Untergeordnete Richtlinie erstellen
Typ der Richtlinie:	Explizit =	
Beschreibung:	r	
Kategorie:	r _1	
Einstellungstyp	Einstellungsname	
Registrierung:		Neu
Einrichtung:		Neu
Archivierung:	°▼	Neu
Desktop:	『AC12-LPMS-Test』▼	Neu
Sicherheit:	° . ▼	Neu
Mail:	r _ •	Neu



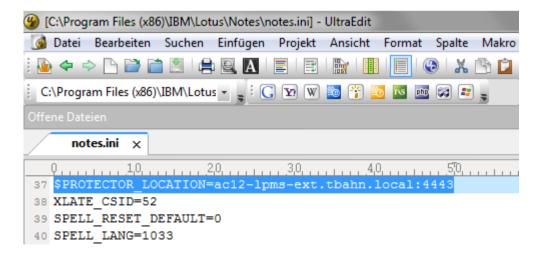








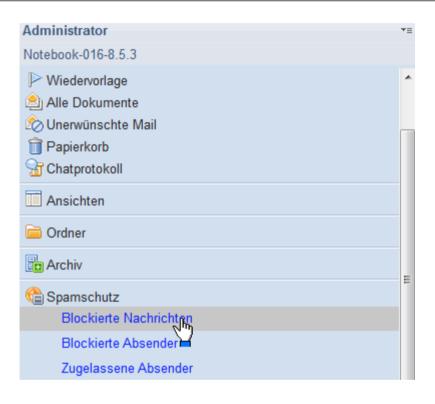
Assign Poli	icy Options	? 🗙	
M	Use this tool to modify the policy options for people or groups in the selected Domino Directory.	OK	
	TBahn's Directory (names.nsf) on Notebook-01	6-8.5.3/TBahn	
For:	1 selected user		
Users with	an existing policy:	Allow replacement of policies	
Policy to a	ssign		
/AC12-LP	PMS-Test ▼		
How to ap	ply policies to selected users		
In the Poli	licy document (recommended)		
selected	Currently assigned policies will be overwritten with the selected policy. The selected groups and users will be added to the selected policy and the Assigned Policy field in the those users' Person documents will be blank.		
View Po	olicy Synopsis Perform	updates in background	







LPMS aus Benutzersicht im Notes-Client

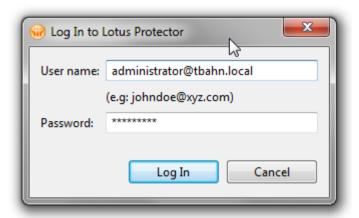






LPMS aus Benutzersicht im Notes-Client

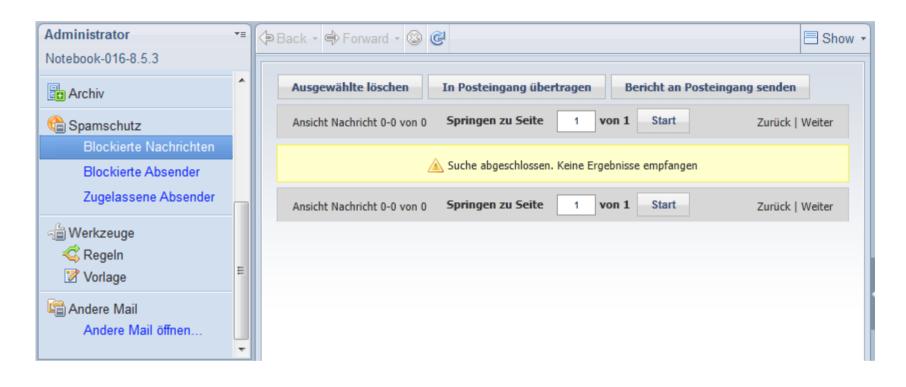
Issue Cross Certificate	? ×
Certifier Server	Thomas Bahn/assono Local
Subject name	EMAIL=anyone@ac124pms-ext.tbahn.local/CN=ac12 ▼
Subject alternate names	
Fingerprint	196A 5297 6651 2EEC 88BC 8DC4 072B 72DD
Expiration date	18.06.2022 11:11:30
	Cross certify Cancel







LPMS aus Benutzersicht im Notes-Client









Testen mit Telnet

```
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...
```





Testergebnis

```
Page Source for Test vom Telnet-Cli... ×

☆ Home ×
역장 역장 역장 역장 역장 열장 역장 계약 기 위험 시청 시청 시청 시청 시 예 시 시 📜 🔡
  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...
```





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





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





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

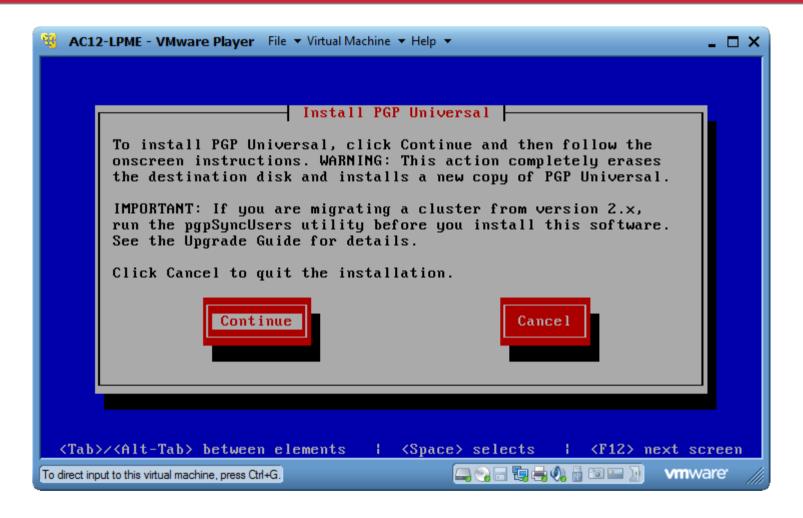






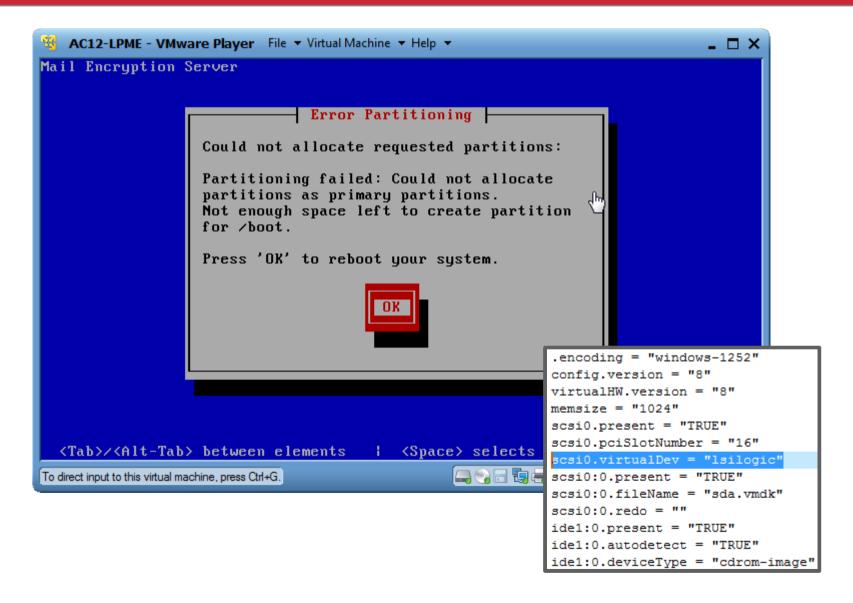






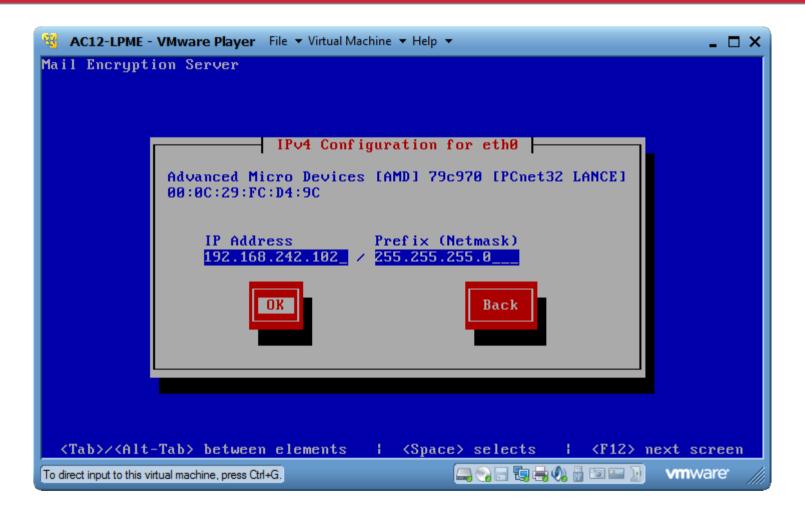












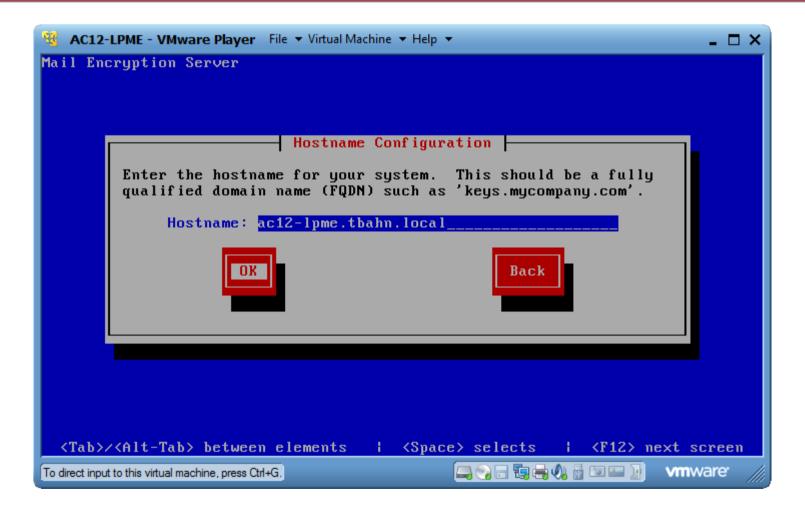




3 AC12-LPME - VMware Player File ▼ Virtual Machine ▼ Help ▼	_ 🗆 ×
Mail Encryption Server	
Miscellaneous Network Settings	
Gateway: 192.168.242.2	
Primary DNS: 192.168.242.98	
OK Back	
<tab>/<alt-tab> between elements <space> selects <f12> next</f12></space></alt-tab></tab>	screen
	mware //











AC12-LPME - VMware Player File ▼ Virtual Machine ▼ Help ▼	- □ ×
Mail Encryption Server	
Formatting Formatting / file system 63%	
<tab>/<alt-tab> between elements <space> selects <f12> next :</f12></space></alt-tab></tab>	screen
To direct input to this virtual machine, press Ctrl+G.	ware //





	- 🗆 ×
Mail Encryption Server	
Package Installation	
Name : Size : Summary:	
Starting install process. This may take several minutes	
Total Comple Remaini	
0%	
<tab>/<alt-tab> between elements <space> selects <f12> next</f12></space></alt-tab></tab>	screen
To direct input to this virtual machine, press Ctrl+G.	ware //





AC12-LPI	ME - VMware Player File ▼ Vi	rtual Machine 🔻 Help 🔻			_ 🗆 ×		
Mail Encry	uption Server						
	P	ackage Installat	ion -				
	Name : glibc-common-2.5-34-i386 Size : 65087k Summary: Common binaries and locale data for glibc						
	98%						
	Total : Completed: Remaining:	Packages 301 7 294	Bytes 1123M 12M 1111M	Time 0:01:46 0:00:01 0:01:45			
		1×					
<pre><tab>/<alt-tab> between elements <space> selects <f12> next screen</f12></space></alt-tab></tab></pre>							
To direct input to this virtual machine, press Ctrl+G.							





```
AC12-LPME - VMware Player File ▼ Virtual Machine ▼ Help ▼
                                                                             _ 🗆 ×
sending termination signals...done
sending kill signals...done
disabling swap...
        /tmp/sda3
unmounting filesystems...
        /mnt/runtime done
        disabling /dev/loop0
        /proc/bus/usb done
        /proc done
        /dev/pts done
        ∕sys done
        /tmp/ramfs done
        /selinux done
        /mnt/sysimage/boot done
        /mnt/sysimage/sys done
        /mnt/sysimage/proc/sys/fs/binfmt_misc done
        /mnt/sysimage/proc done
        /mnt/sysimage/dev done
        /mnt/sysimage done
rebooting system
Restarting system.
                                                To direct input to this virtual machine, press Ctrl+G.
                                                                        vmware
```











```
AC12-LPME - VMware Player File ▼ Virtual Machine ▼ Help ▼
                                                                                        _ 🗆 X
Starting udev:
Loading default keymap (us):
                                                                         OK 1
Setting hostname ac12-lpme.tbahn.local:
                                                                      \mathbf{I} = \mathbf{O}\mathbf{K} = \mathbf{I}
No devices found
Setting up Logical Volume Management: /dev/hdc: open failed: No medium found
                                                                      \mathbf{I} = \mathbf{O}\mathbf{K} = \mathbf{I}
Checking filesustems
/: clean, 39997/7841280 files, 639023/7837711 blocks
/boot: clean, 39/26104 files, 20092/104388 blocks
                                                                        OK 1
Remounting root filesystem in read-write mode:
                                                                      \mathbf{I} = \mathbf{O}\mathbf{K} = \mathbf{I}
Mounting local filesystems:
                                                                      \mathbf{I} = \mathbf{O}\mathbf{K} = \mathbf{I}
Enabling local filesystem quotas:
                                                                     [ OK ]
Enabling /etc/fstab swaps:
                                                                      I OK 1
INIT: Entering runlevel: 3
Entering non-interactive startup
Starting sysstat: Calling the system activity data collector (sadc):
                                                                         OK 1
Checking for hardware changes
                                                                        OK 1
Bringing up loopback interface:
                                                                       OK 1
Bringing up interface eth0:
                                                                      \Gamma OK 1
Starting auditd:
Running the Mail Encryption Server first time boot configuration:
                                                      vmware
To direct input to this virtual machine, press Ctrl+G.
```





AC12-LPME - VMware Player File ▼ Virtual Machine ▼ Help ▼	- □ ×
Mail Encryption Server 2.1.0.1 Build(78.3.0.1.4323) Kernel 2.6.18-128.4.1.el5PAE on an i686	
Mail Encryption Server Administration is available via web interface Connect to https://192.168.242.102:9000	
ac12-lpme login: _	
To direct input to this virtual machine, press Ctrl+G.	vare ///

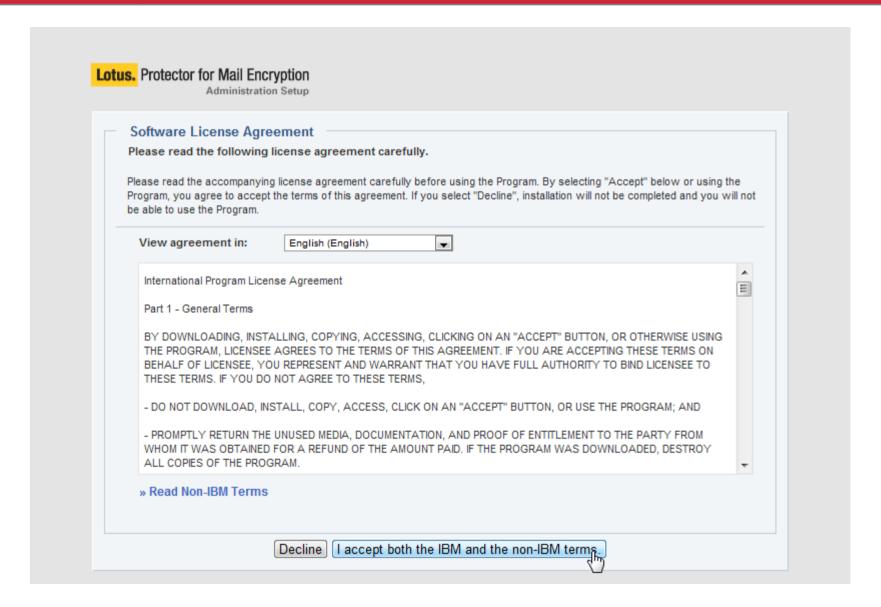






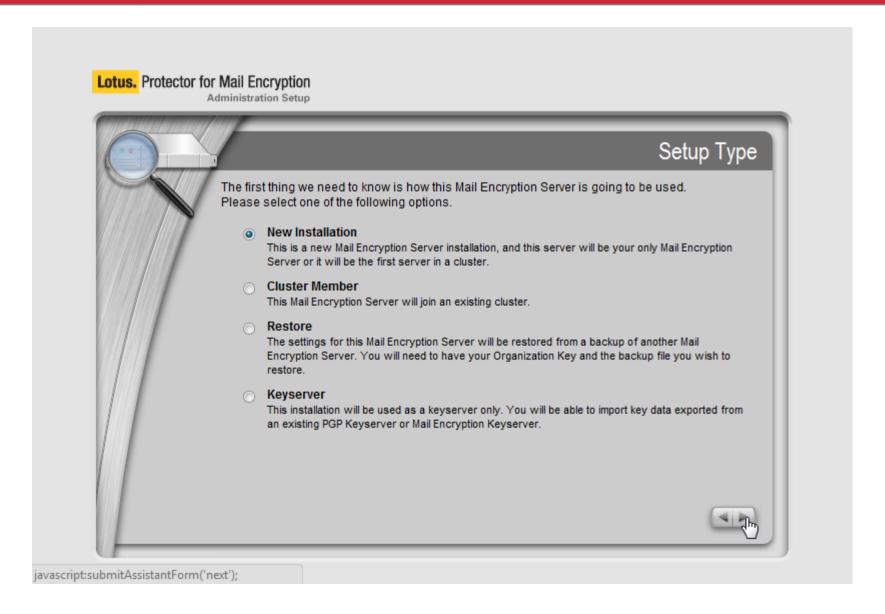






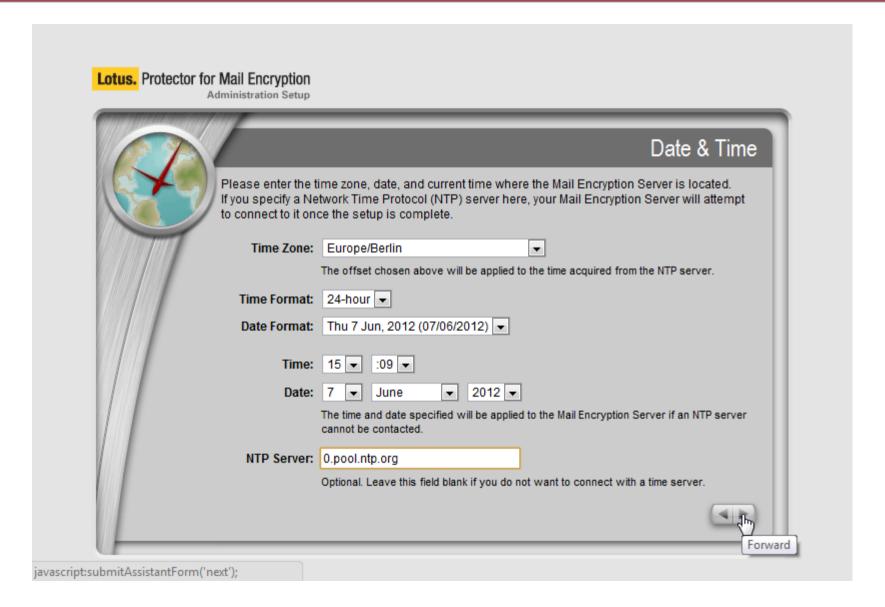






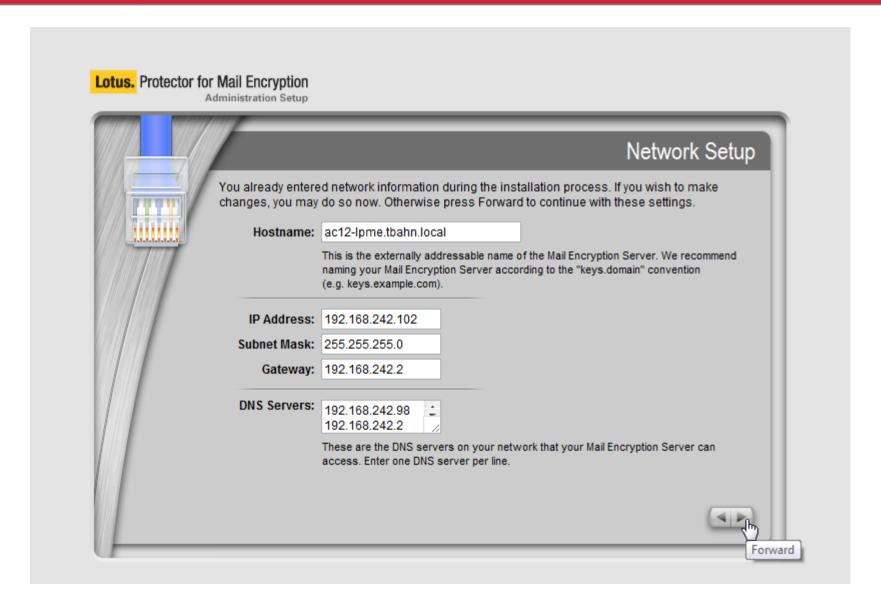






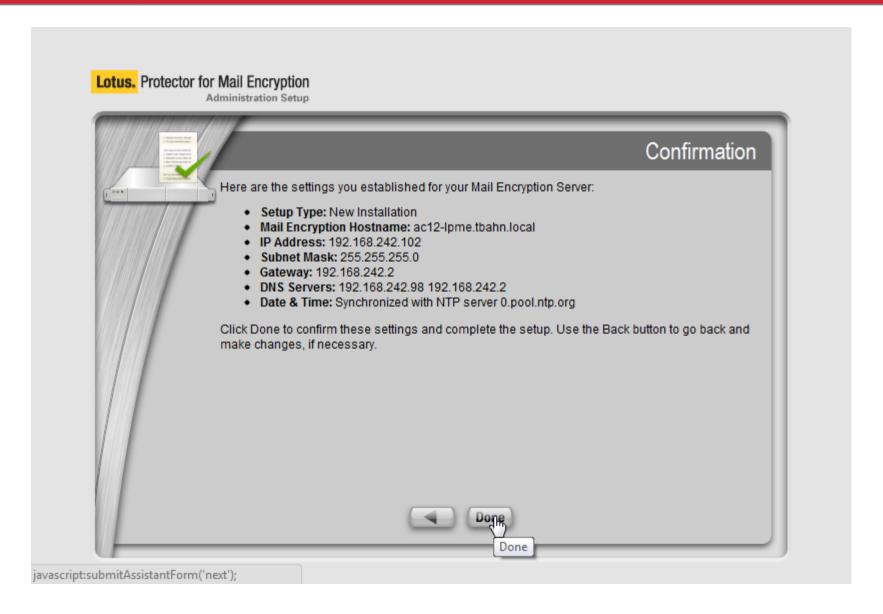


















Network Configuration Changed

You have changed the IP address or another network setting on this Mail Encryption Server.

The Mail Encryption Server is currently restarting to implement these changes. You will automatically be redirected to the proper IP address in approximately 75 seconds.

If the operation does not finish in that time frame, please wait another minute or two and then manually reload the next page in your Web browser.

If you just uploaded a backup to restore, the restore operation is happening now. This restore could potentially take a long time if your backup file is large. Please be patient.

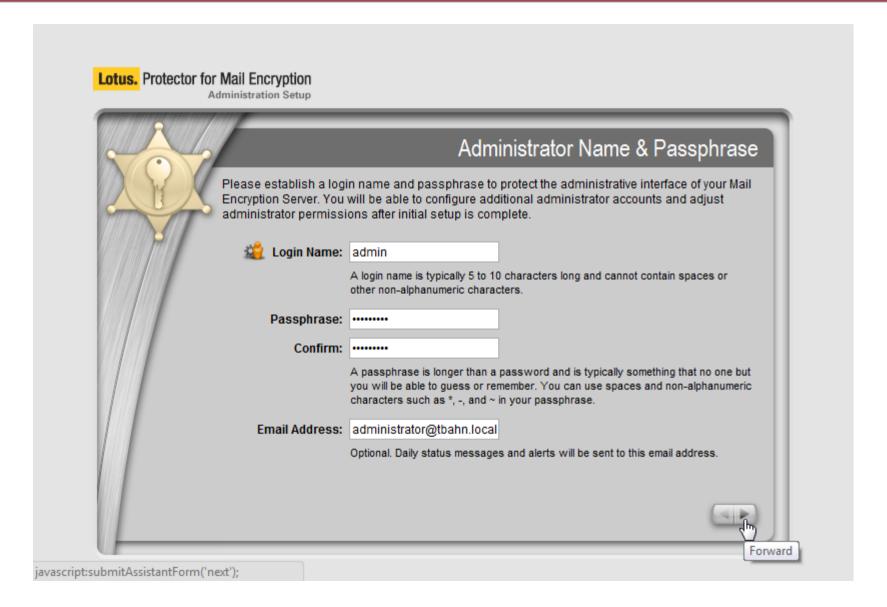
If you are not automatically redirected, you may redirect manually.

The URL for the Mail Encryption Server is: https://ac12-lpme.tbahn.local:9000/

Z

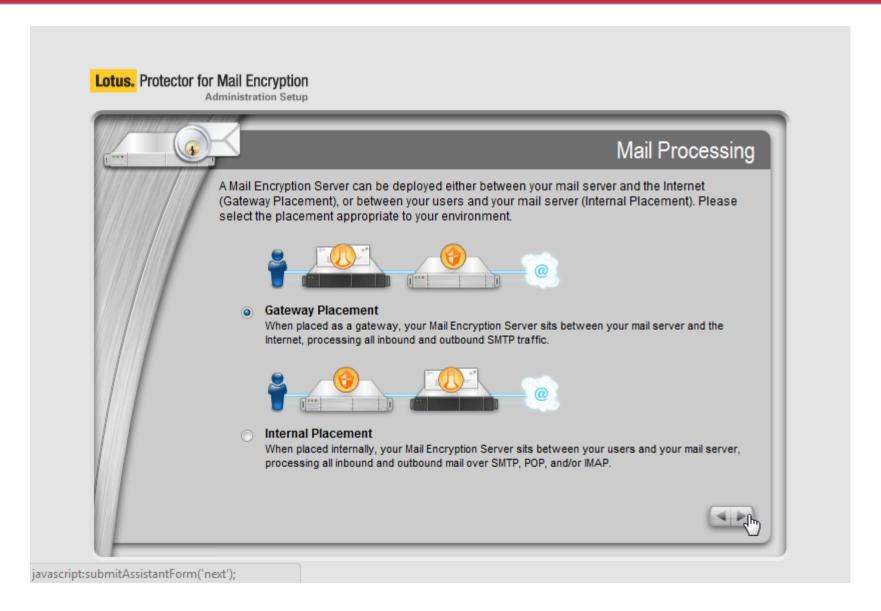






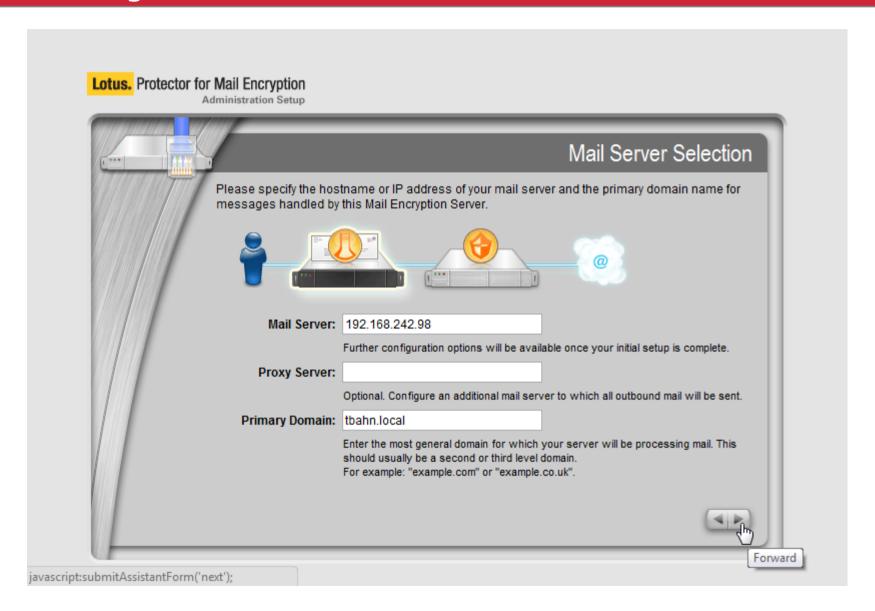






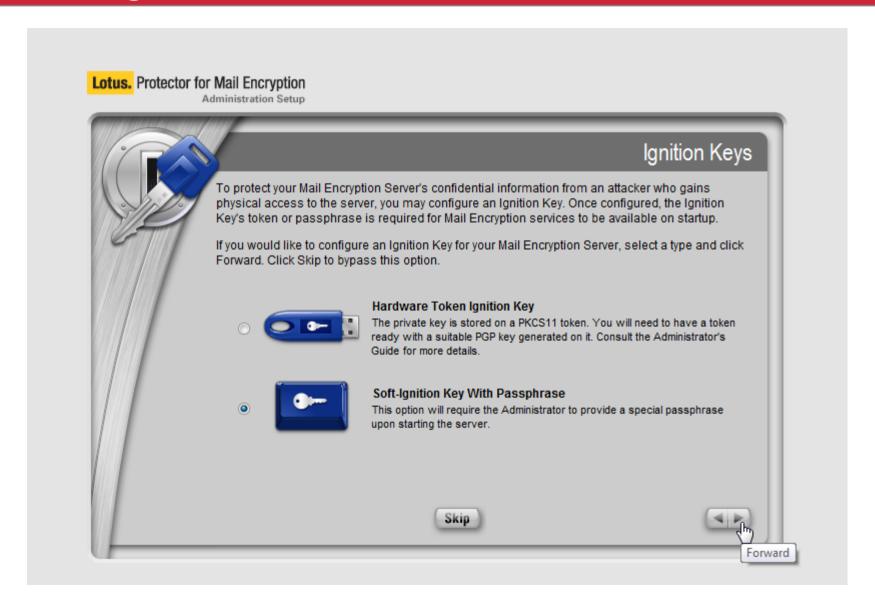






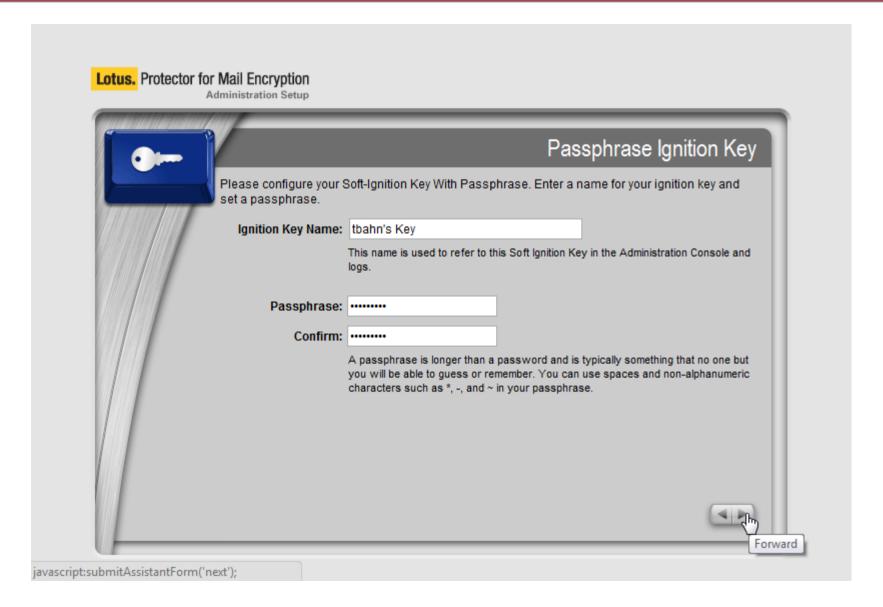






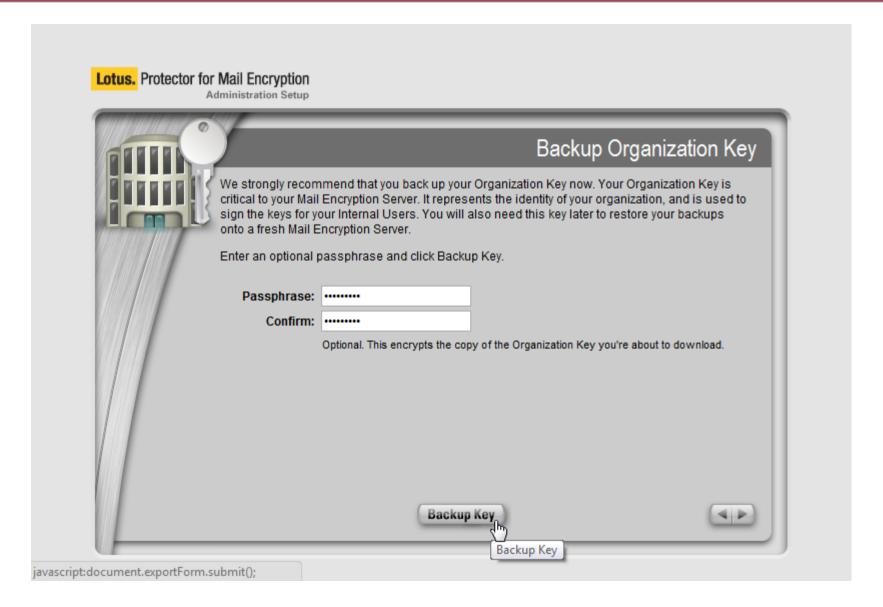






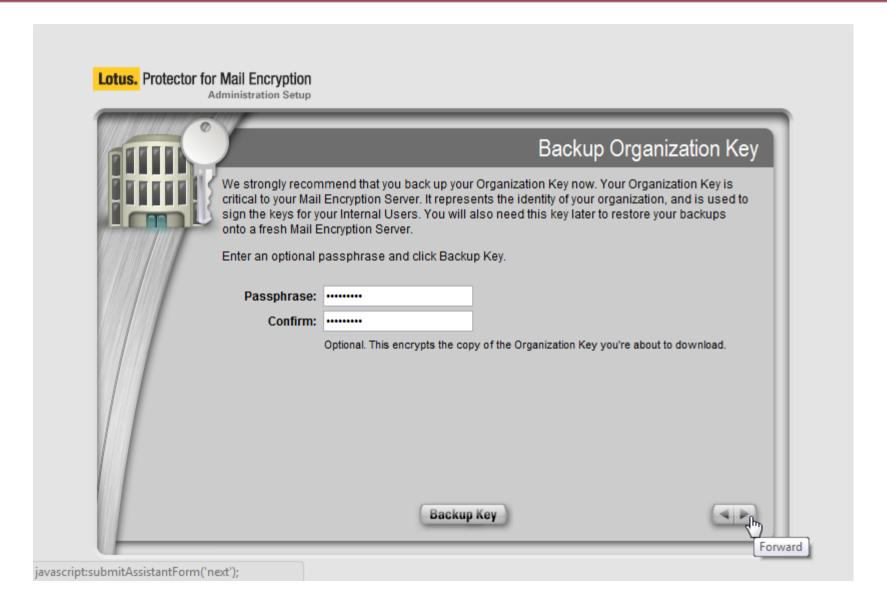






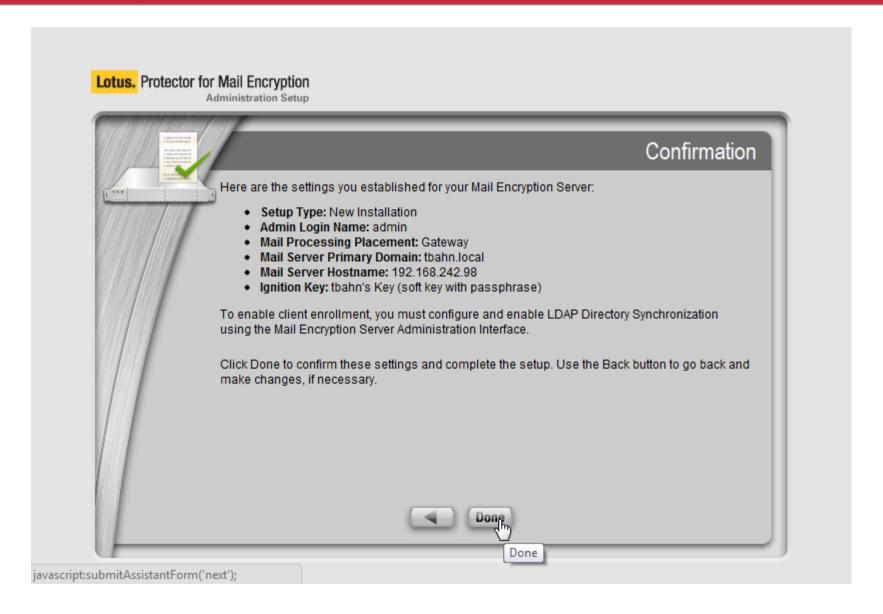


















Configuration Changed

You have changed certain Mail Encryption Server settings.

The Mail Encryption Server is currently restarting to implement these changes. You will automatically be redirected to the proper IP address in approximately 90 seconds.

If the operation does not finish in that time frame, please wait another minute or two and then manually reload the next page in your Web browser.

If you just uploaded a backup to restore, the restore operation is happening now. This restore could potentially take a long time if your backup file is large. Please be patient.

If you are not automatically redirected, you may redirect manually.

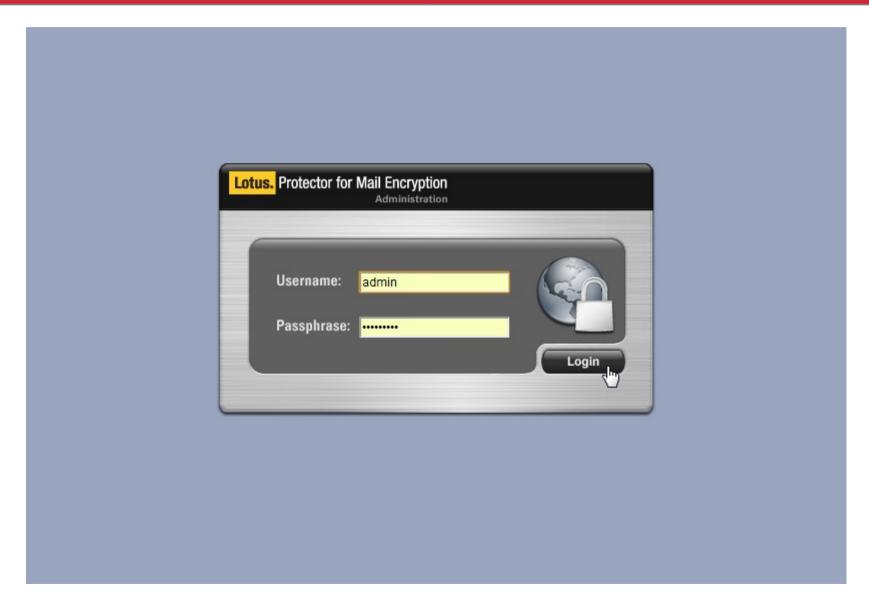
The URL for the Mail Encryption Server is: https://ac12-lpme.tbahn.local:9000/

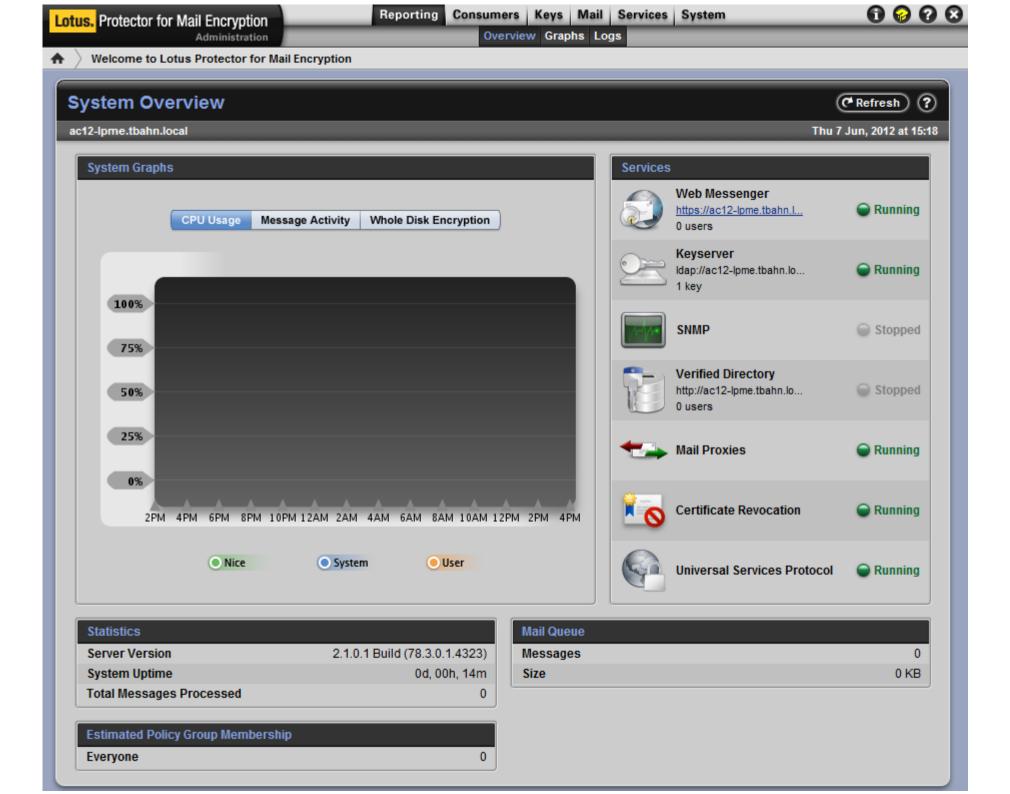
S

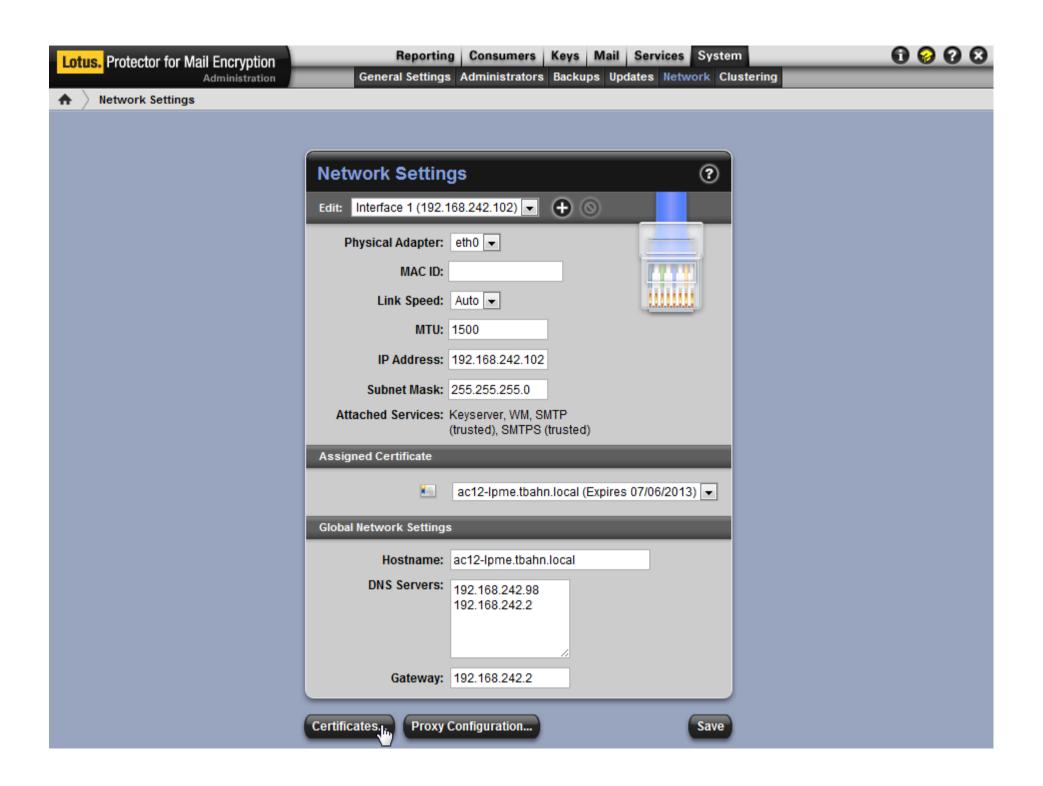




Erster Start (Neuanmeldung im Browser)

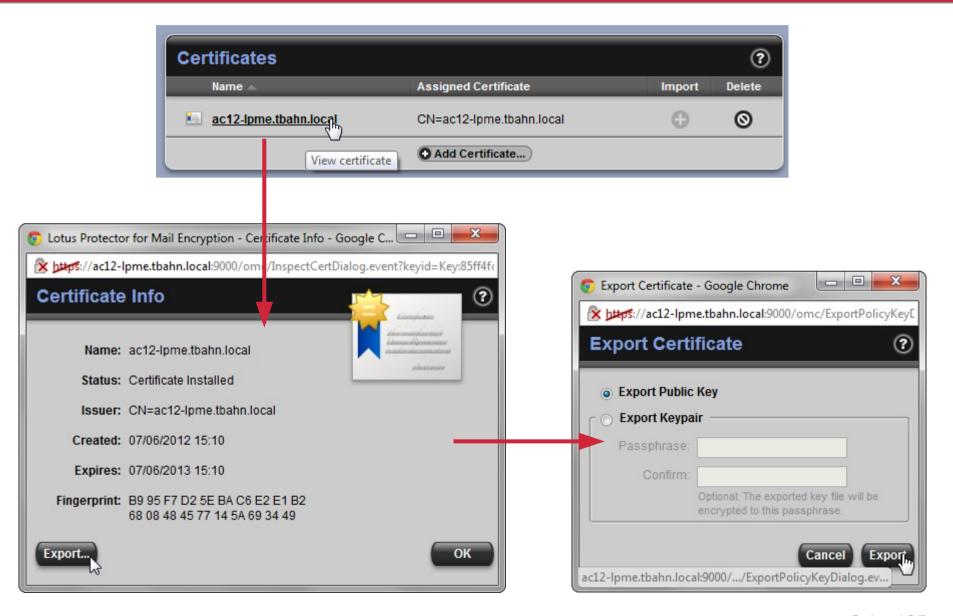






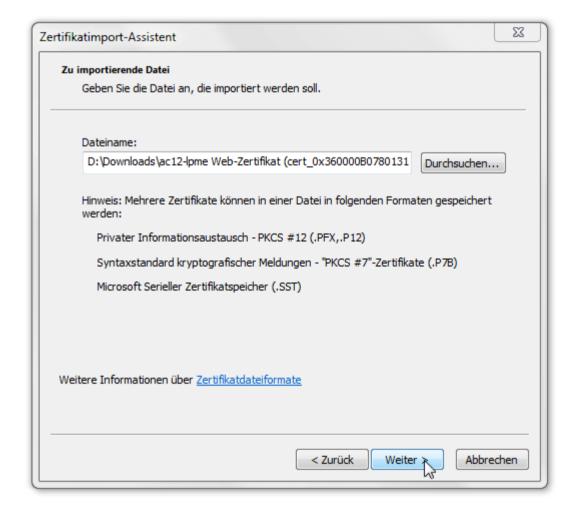






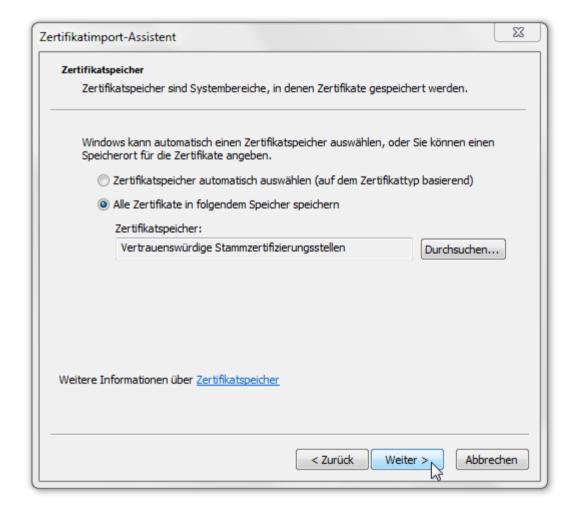












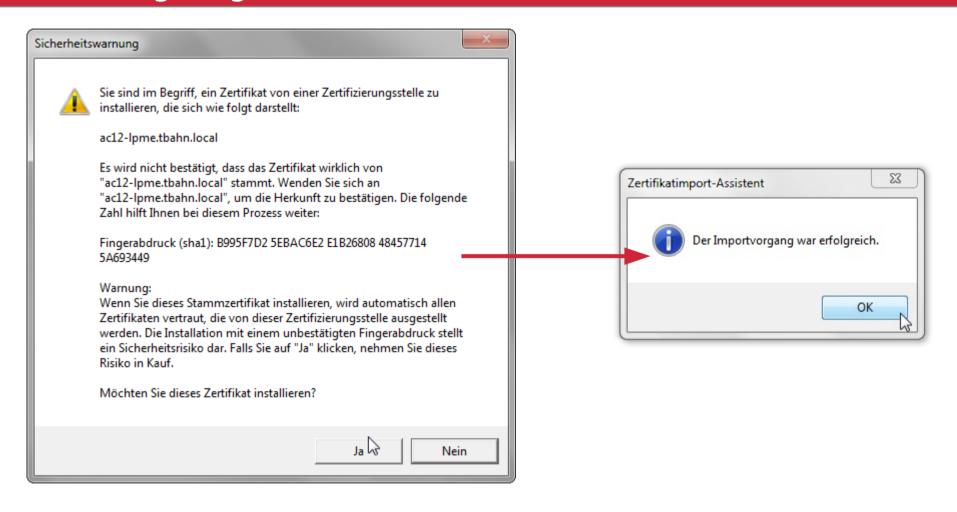






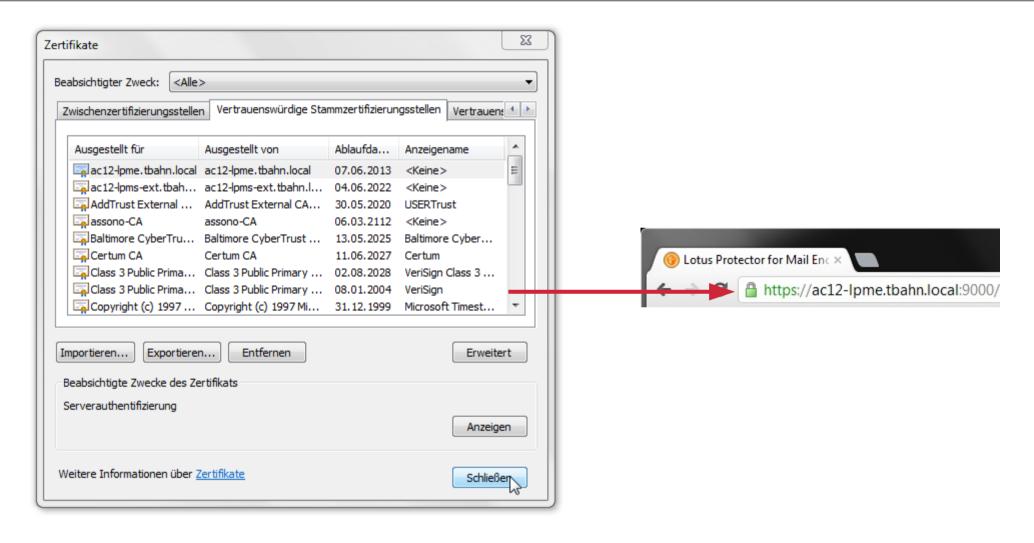








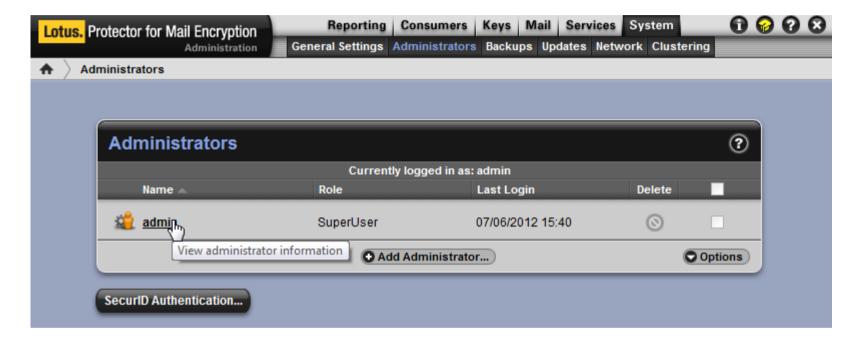








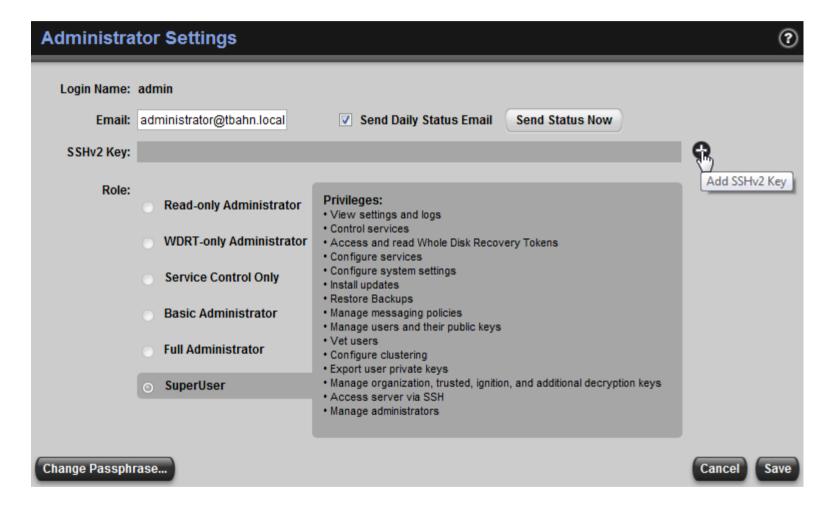
SSH-Zugriff (Public Key)







SSH-Zugriff (Public Key)



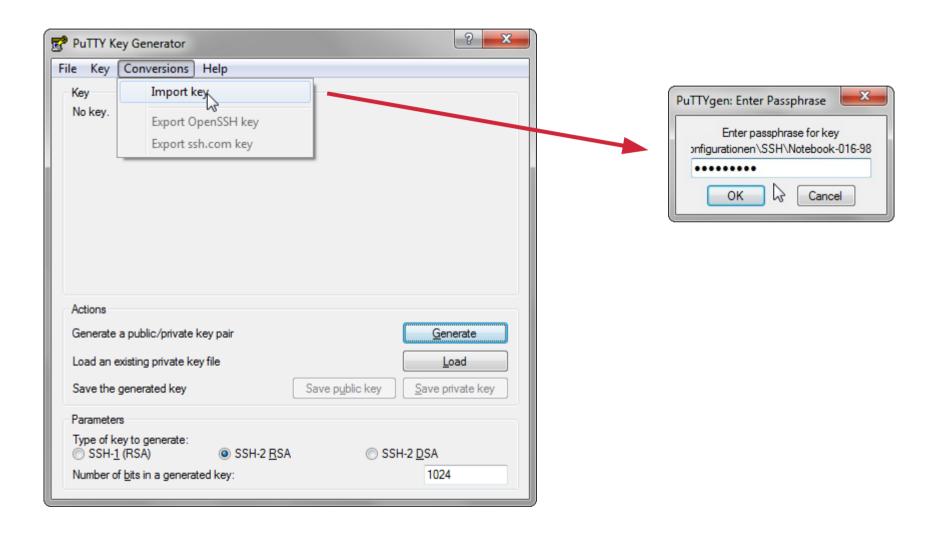




```
[administrator@notebook-016-98 ~]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/administrator/.ssh/id rsa):
Created directory '/home/administrator/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification 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:
Of: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]----+
              ο.
           . 0.0
        . + 0.0
       . S +.. E .
        . = .0...0
           .. . 0.
               + .
              0.0.
```

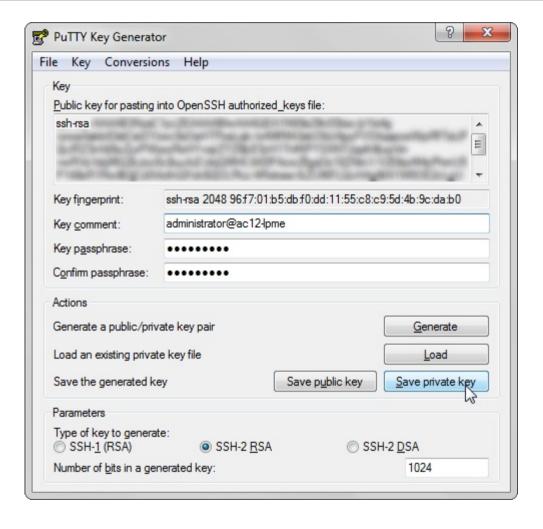






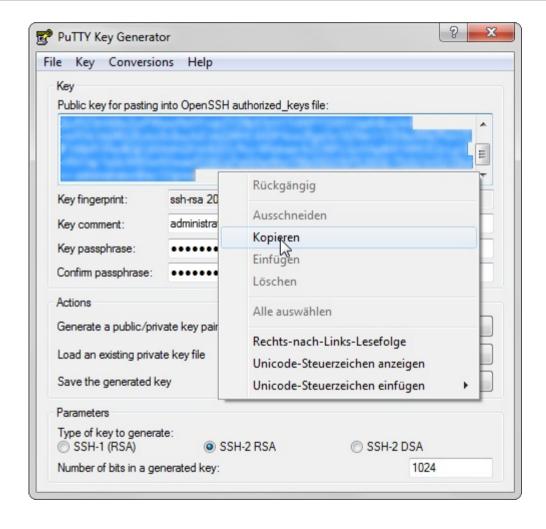












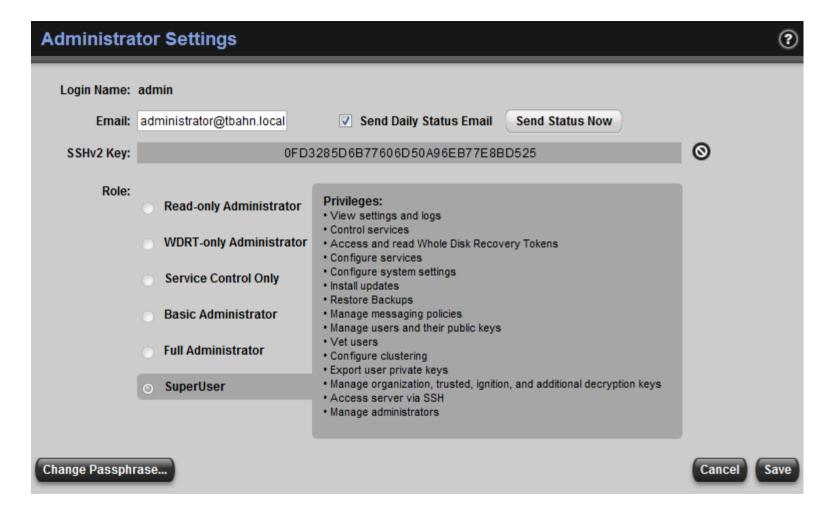












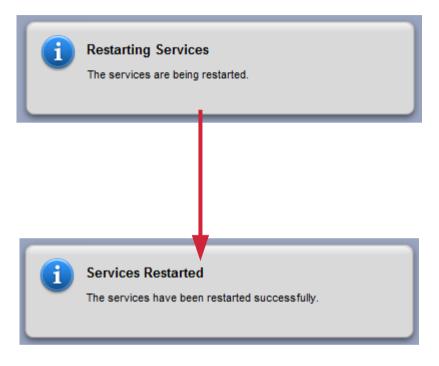






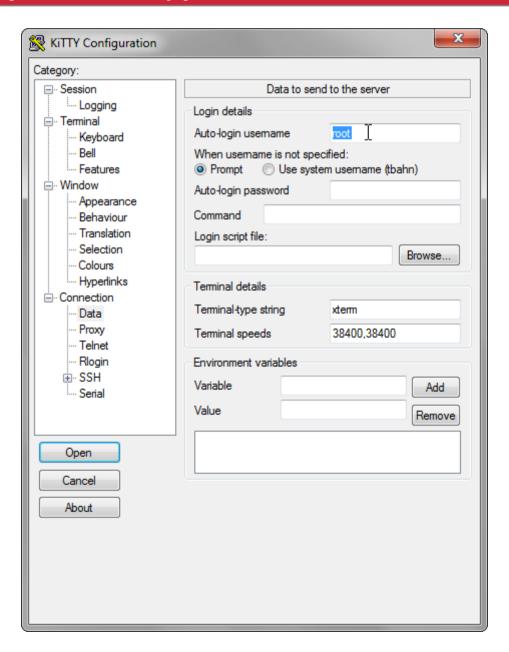






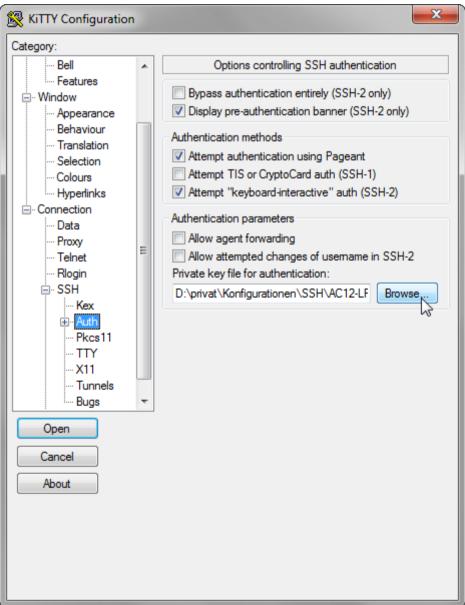






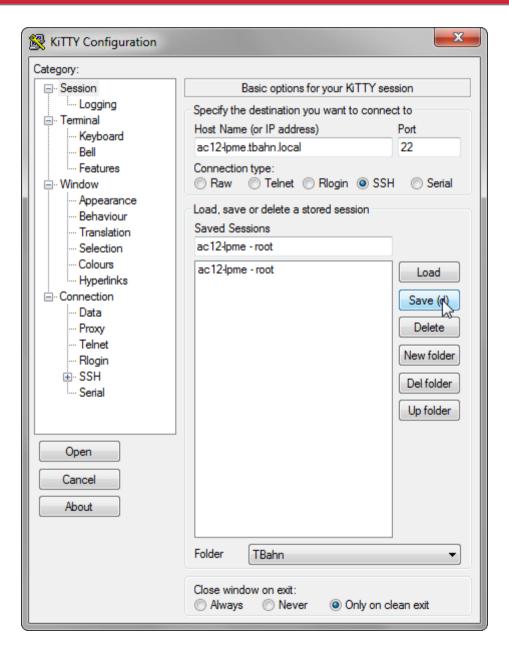






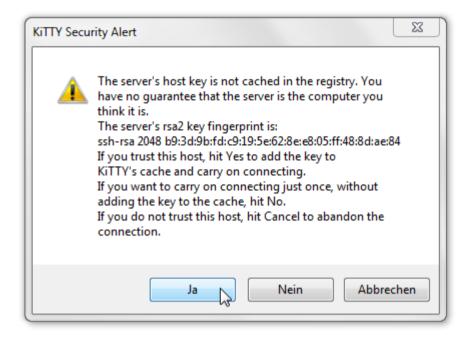
















```
- 0
root@ac12-lpme:~
Using username "root".
Authenticating with public key "administrator@ac12-lpme"
Passphrase for key "administrator@ac12-lpme":
[root@ac12-lpme ~]#
```





[root@ac12-lpme	~l# chk	config -	_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	2:011 2:01	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_cffent dc server	0:off	1:off	2:off	3:off	4:off	5:off	6:off
gpm	0:off	1:off	2:011 2:01	3:on	4:on	5:on	6:off
ypm haldaemon	0:off	1:off	2:off	3:on	4:on	5:on	6:off
httpd	0:off	1:off	2:011 2:01	3:on	4:on	5:on	6:off
iptables	0:off	1:off	2:on	3:on	4:on	5:on	6:off
jexec	0:011 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	2:011 2:01	3:on	4:on	5:on	6:off
luap 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
murcipathu netconsole	0:off	1:off	2:011 2:0ff	3:off	4:off	5:off	6:off
netfs	0:off	1:off	2:011 2:0ff	3:011 3:on	4:011 4:0n	5:011 5:0n	6:off
netplugd	0:off	1:off	2:011 2:0ff	3:off	4:off	5:off	6:off
netprugu network	0:off	1:off	2:011 2:0n	3:011 3:on	4:011 4:0n	5:011 5:0n	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
ntpd ntpdate	0:off	1:off	2:on	3:on	4:on	5:on	6:off
ncpdate	0:off	1:011 1:0ff	2:on	3:on	4:on	5:on	6:off
pesca pgpconfigure	0:off	1:011 1:0ff	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
pgpdatalayer pgpdbinit	0:off	1:off	2:on	3:on	4:on	5:on	6:off
	0:off	1:off	2:on	3:on	4:on	5:on	6:off
pgpfixsystem							6:off
pgpgroupd	0:off	1:off	2:on	3:on	4:on	5:on	
pgprep pgpsdkrmi	0:off 0:off	1:off 1:off	2:on	3:on	4:on	5:on	6:off 6:off
	0:off	1:011 1:0ff	2:on	3:on	4:on	5:on	6:off
pgptcpwrapper			2:on	3:on	4:on	5:on	
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



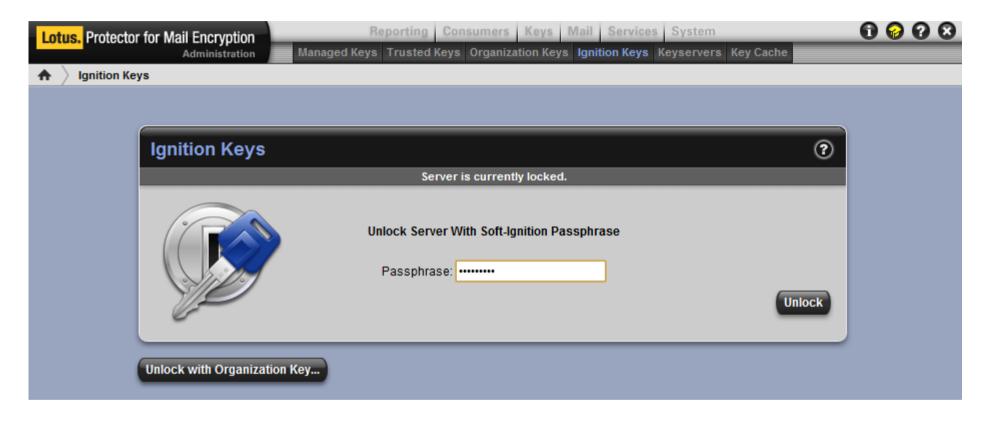


```
login as: root
Using keyboard-interactive authentication.
Password:
Last login: Thu Jun 7 15:24:29 2012 from 192.168.242.1
ac12-lpms-ext:~ # cd .ssh
ac12-lpms-ext:~/.ssh # ls -1
total 8
-rw----- 1 root root 1192 Jun 6 13:31 id dsa
-rw-r--r-- 1 root root 1119 Jun 6 13:31 id dsa.pub
ac12-lpms-ext:~/.ssh # 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 ves
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
```





Nach jedem Neustart...







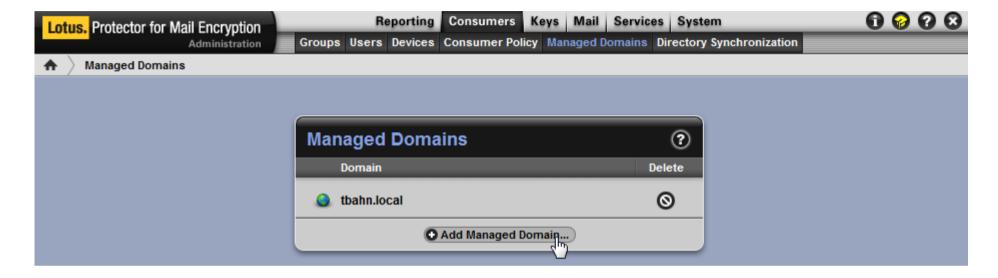
Nach jedem Neustart...

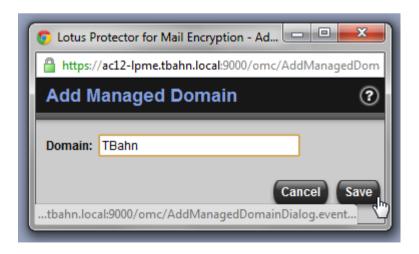






Domino-Domäne hinzufügen

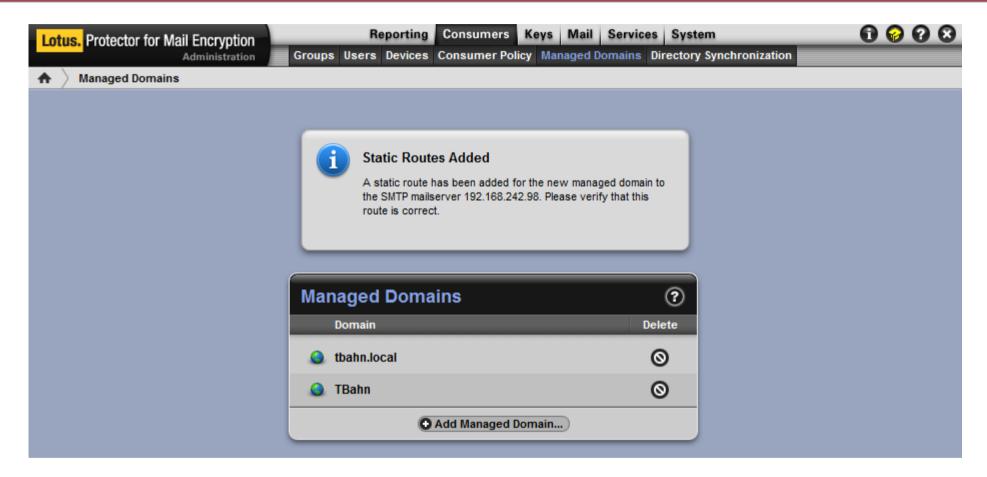






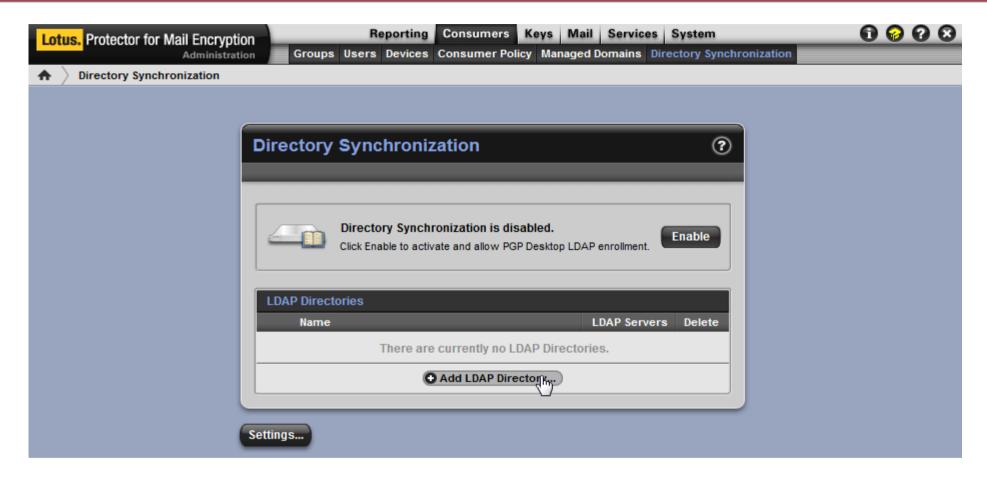


Domino-Domäne hinzufügen



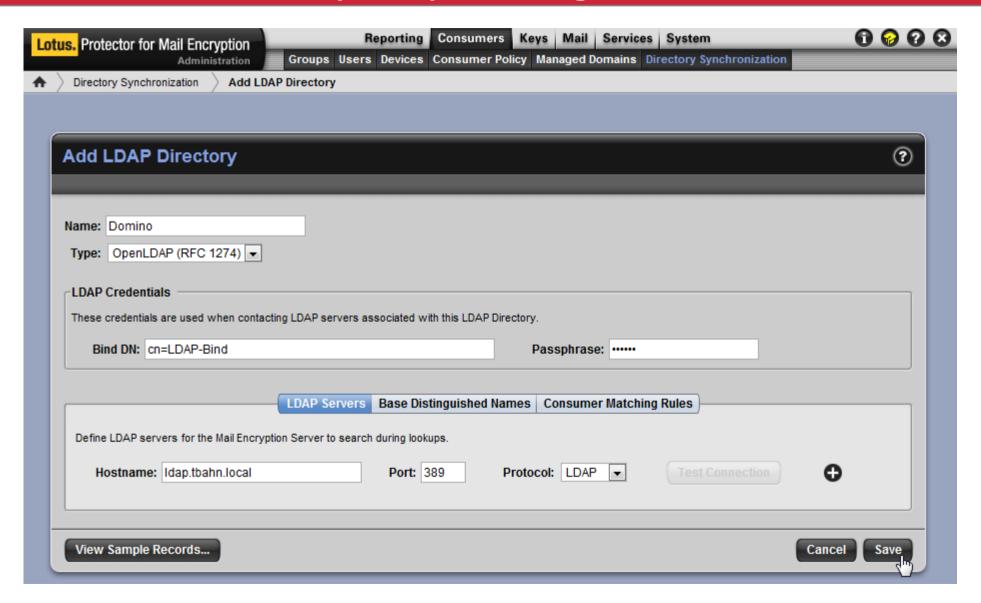






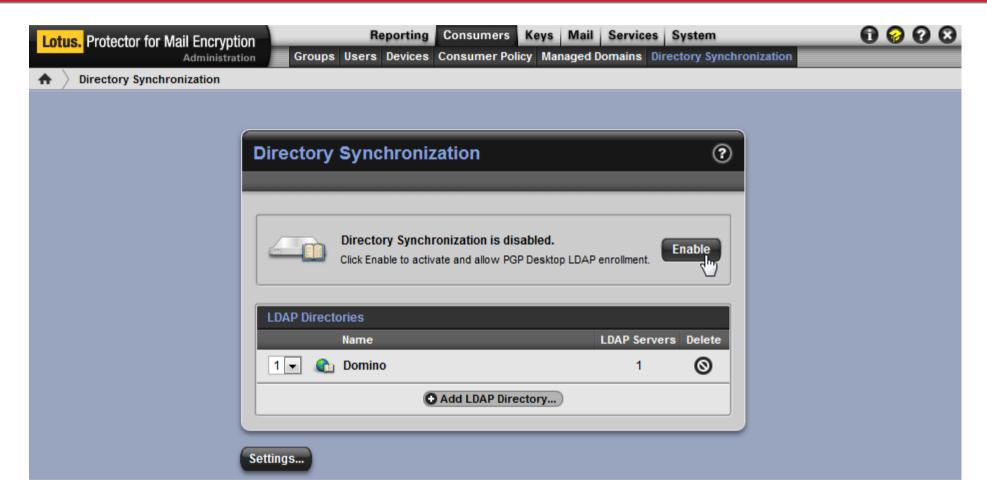


















Configuration Changed

You have changed certain Mail Encryption Server settings.

The Mail Encryption Server is currently restarting to implement these changes. You will automatically be redirected to the proper IP address in approximately 30 seconds.

If the operation does not finish in that time frame, please wait another minute or two and then manually reload the next page in your Web browser.

If you just uploaded a backup to restore, the restore operation is happening now. This restore could potentially take a long time if your backup file is large. Please be patient.

If you are not automatically redirected, you may redirect manually.

The URL for the Mail Encryption Server is: https://ac12-lpme.tbahn.local:9000/





Konfiguration des Domino-Servers

Konfigurationseins	tellungen : Notebook-016-8.5.3/TBah
Allgemein Sicherheit Client-U	pgrade Router/SMTP MIME NOTES.INI-Einstellung
Allgemein Beschränkungen und	d Steuerungen Ausschlussklauseln Mailverfolgung
Router/SMTP allgemein	
Anzahl der Mailboxen:	r
SMTP wird zum Senden von Nachrichten an Empfänger außerhalb der lokalen Internetdomäne verwendet:	『Aktiviert』▼
SMTP ist innerhalb der lokalen Internetdomäne zulässig:	Deaktiviert . •
Server innerhalb der lokalen Notes-Domäne sind via SMTP über TCP/IP erreichbar:	『Immer』▼
Adresssuche:	[©] Vollst. Name dann lokaler Teil <u></u>
Ausführliche Suche:	□ Deaktiviert 』 ▼
Relaishost für Nachrichten, die die lokale Internetdomäne verlassen:	ீ ac12-lpme.tbahn.local ு
Beim Senden von Nachrichten an den Relaishost Authentifizierung verwenden:	Deaktiviert . •





Konfiguration des Domino-Servers

Konfigurationseins	tellungen : Notebook-016-8.5.3/TBah
Allgemein Sicherheit Client-U	pgrade Router/SMTP MIME NOTES.INI-Einstellung
Allgemein Beschränkungen un	d Steuerungen Ausschlussklauseln Mailverfolgung
Router/SMTP allgemein	
Anzahl der Mailboxen:	
SMTP wird zum Senden von Nachrichten an Empfänger außerhalb der lokalen Internetdomäne verwendet:	[™] Aktiviert <u></u>
SMTP ist innerhalb der lokalen Internetdomäne zulässig:	『 Deaktiviert 』▼
Server innerhalb der lokalen Notes-Domäne sind via SMTP über TCP/IP erreichbar:	『Immer』▼
Adresssuche:	[®] Vollst. Name dann lokaler Teil 』▼
Ausführliche Suche:	[®] Deaktiviert 』▼
Relaishost für Nachrichten, die die lokale Internetdomäne verlassen:	ି ac12-lpme.tbahn.local ୁ
Beim Senden von Nachrichten an den Relaishost Authentifizierung verwenden:	Deaktiviert •



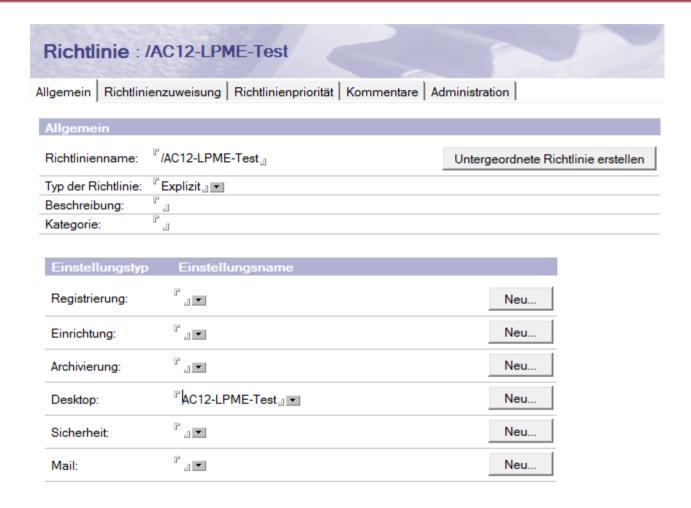


Deskt	opeinstellungen		
Allgemein	Smart Upgrade Anwendungen V	Vidgets Wählverbindungen	Konten Namensserver
Allgeme	in		
Name:	『AC12-LPME-Test』	I	
Beschreib	oung:		

Desktopeinstellungen : AC12-LPME-Test	100		and a
Allgemein Smart Upgrade Anwendungen Widgets Wählverbindungen	Konten Na	amensserver	Benutzerdefinierte Einstellungen
Notes.ini Arbeitsumgebungen Verwaltete Einstellungen Diese NOTES.INI-Einstellungen auf die Systeme der Benutzer übertragen:			
PME_SERVER_CONFIG=Ipme.tbahn.local PME_INSTALL_NOTES=1 PME_OVERRIDE_DESKTOP=1			
Computerspezifische Formel eingeben Liste bearbeiten			

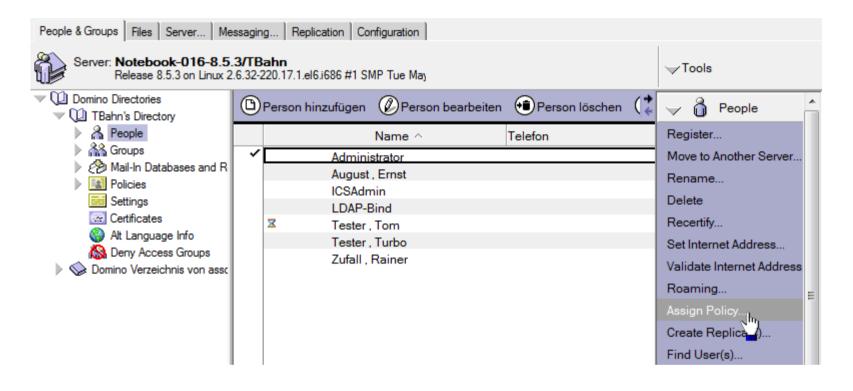






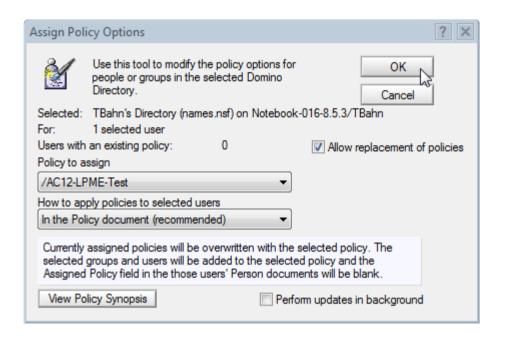


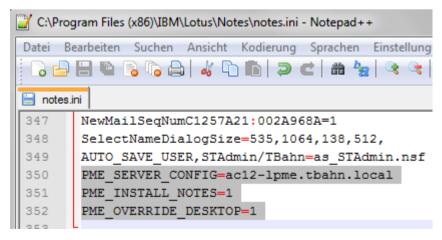












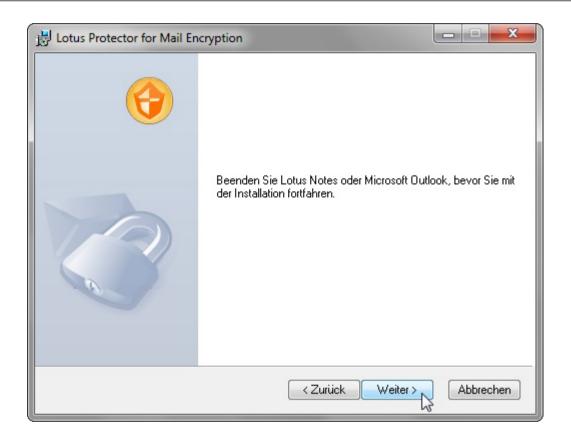






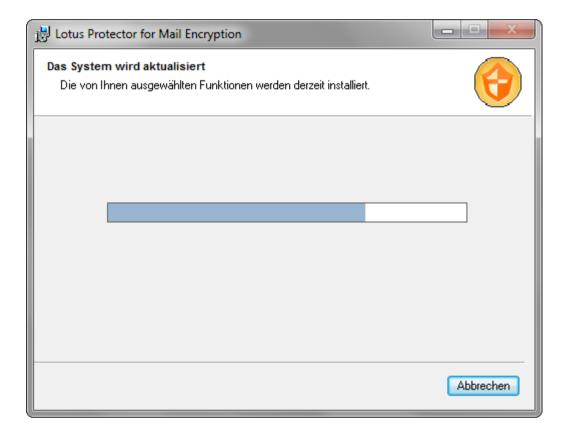


















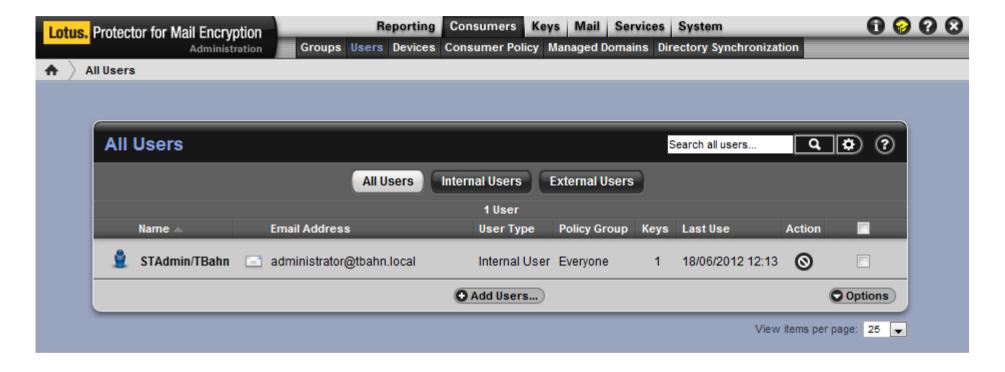
















Benutzung des LPME-Clients

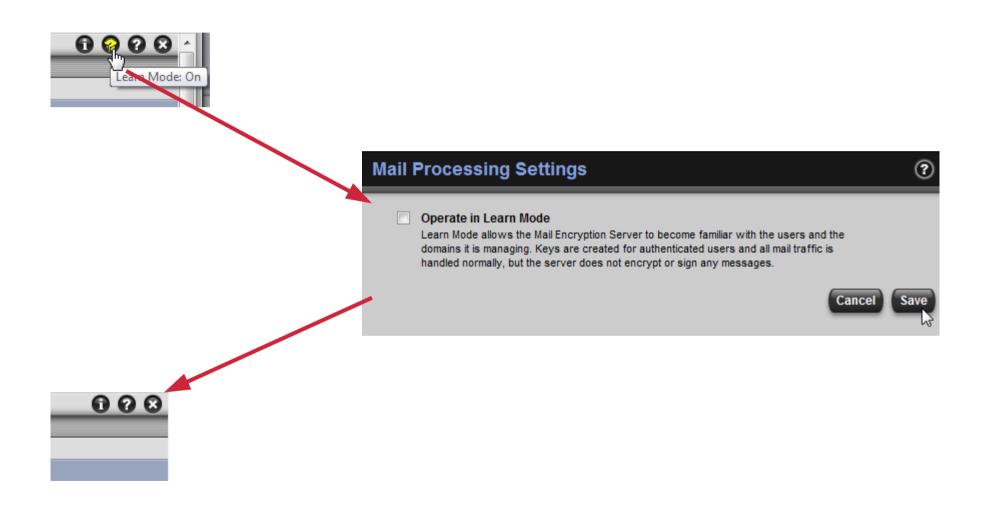
Senden Sen	iden und able	gen Als Entwurf speichern Zustelloptionen ▶ ▼ 🖉 踢 Signatur▼ Anzeigen▼ Mehr▼
		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
	I	□ Hohe Dringlichkeit □ Empfangsbestätigung ☑ Signieren ☑ Verschlüsseln □ Betreff als 'Vertraulich' markieren
	<u>An</u> :	tbahn@gmx.de,
	Kopie:	
	Blindkopie:	
	Betreff:	Test an unbekannten Externen
	Diese Nachric	ht wird verschlüsselt und mit einer digitalen Signatur gesendet.

Inhalt der E-Mail



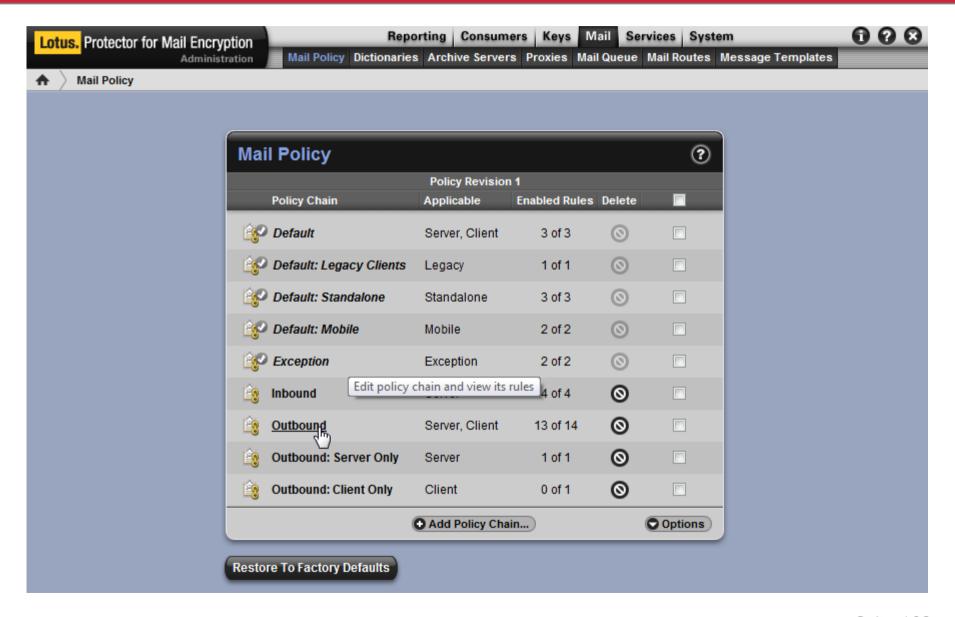


LPME "scharf" schalten









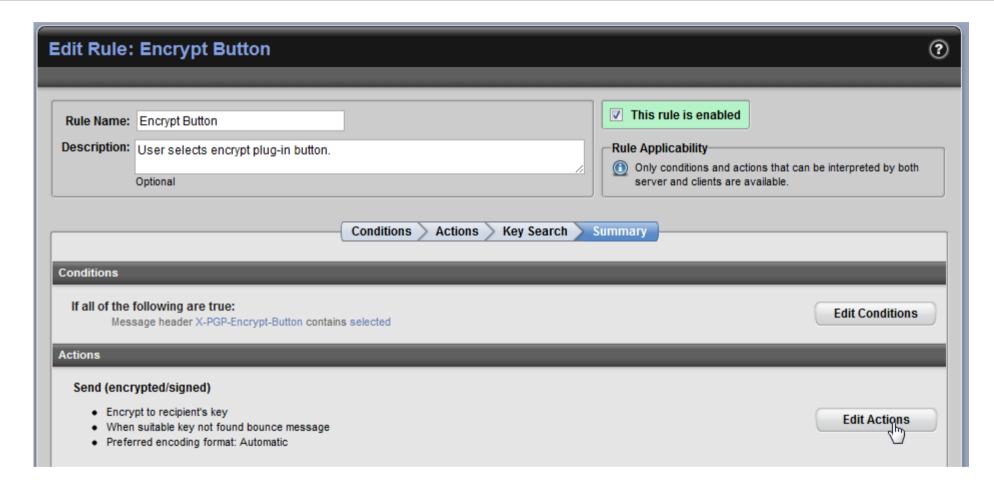




Policy Chain: Outbound				?
	This Policy Chain is applicable to Server, Client			
Rule	Description	Status	Delete	
9 🔽 🖄 Always Encrypt Sensitive Messages	Encrypt messages with high sensitivity before sending.	Enabled	0	
10 🔻 🧏 Sign + Encrypt Buttons	User selects both sign and encrypt plug-in buttons.	Enabled	0	
11 🔻 😤 Sign Button	User selects sign plug-in button.	Enabled	0	
12 Encrypt Button	User selects encrypt plug-in button.	Enabled	0	
13 Application Is Edit rule	If this rule is executed on the server, route the message to the "Outbound: Server Only" chain.	Enabled	0	

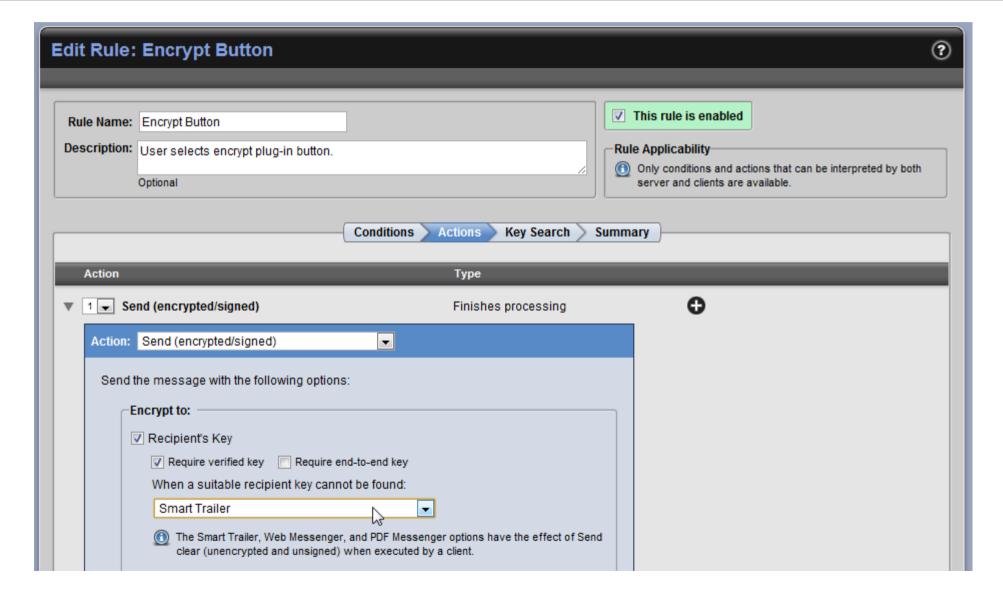














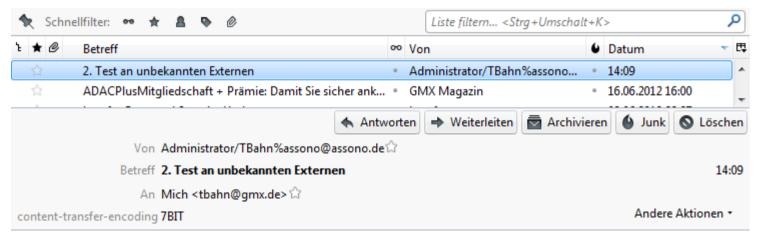


Senden Sen	den und able	gen Als Entwurf speichern Zustelloptionen ▼ 🔗 🐻 Signatur ▼ Anzeigen ▼ Mehr ▼
	I	☐ Hohe Dringlichkeit ☐ Empfangsbestätigung 🔽 Signieren 🔽 Verschlüsseln ☐ Betreff als 'Vertraulich' markieren
	An:	tbahn@gmx.de,
	Kopie:	
	Blindkopie:	
	Betreff:	2. Test an unbekannten Externen
	Diese Nachric	ht wird verschlüsselt und mit einer digitalen Signatur gesendet.

Inhalt, Inhalt, Inhalt...







Inhalt, Inhalt, Inhalt...

This message could have been secured by Lotus Protector for Mail Encryption. To secure future messages from this sender, please click this link:

https://ac12-lpme.tbahn.local/b/b.e?r=tbahn%40gmx.de&n=OG%2FA4REgHvwXqPn7FtG%2BUw%3D%3D







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.





Fragen?

jetzt stellen – oder später:

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



Folien unter:

www.assono.de/blog/d6plinks/AC12-Lotus-Protector