

NORMAN **EndpointProtection**

Kurzanleitung für die
Netzwerkinstallation von

Norman Endpoint Manager 8.10
Norman Endpoint Protection 8.10
**Norman MailScan for Microsoft
Exchange**

Schulungshandbuch / Kurzanleitung einer Netzwerkinstallation NPro 8.1 in einer 2000 / 2003 / 2008 Domäne

Inhalt

1. Ausgangssituation	3
2. Systemvoraussetzungen	3
3. Serverinstallation.....	4
4. Erstellung eines Sicherheitsbereich (Realms)	5
5. Installation aktualisieren.....	6
6. Konfiguration von Sicherheitsbereich Admins und NIU.....	7
7. Erstellung einer Richtlinie sowie einer Gruppe für den NEM Server.....	8
8. Installation der Clients per Push Installation	9
9. Installation der Clients per MSI Datei	11
10. Installation eines Linux Clients	11
11. Topologie Filter.....	12
12. Konfiguration der Richtlinien im NEM.....	13
13. Sicherung des NEMs.....	14
14. Fernzugriff auf NEM.....	15
15. Migration von NVC 5.99 auf NPro 8.10	16
16. Hintergrundinformationen NEM.....	19
17. Tipps & Tricks	21
18. Installation von Norman MailScan for Microsoft Exchange	23


1. Ausgangssituation


!!! Es darf kein anderes Antivirenprogramm auf dem Servern oder auf den Clients installiert sein !!!


In einem Netzwerk, bestehend aus einem Windows 2000 / 2003 / 2008 Server, welcher als Domaincontroller konfiguriert ist, und mehreren Clients, wird Norman Endpoint Protection (NPRO) und Norman Endpoint Manager (NEM) installiert.

Bei Norman Endpoint Protection handelt es sich um das Clientmodul der Installation. Bei Norman Endpoint Manager handelt es sich um die Administrations- / Konfigurationsoberfläche.

In der Produktivumgebung sollte die Installation zuerst nur auf dem Distributionsrechner (z.B. dem Server) und jeweils einem 2000/XP/Win7 Client getestet werden, bis alles korrekt funktioniert. Das Serverbetriebssystem (Windows 2000, 2003, 2008) wird automatisch von der Installationsroutine erkannt.

 Hinweis, als Verteilungsserver kann auch ein XP / Vista Client genutzt werden, allerdings sollte dieser ständig verfügbar / erreichbar sein. Bitte beachten Sie ansonsten die Hardwareanforderungen im nächsten Punkt.

 Wichtig, Norman Endpoint Manager / Norman Endpoint Protection bringt seinen eigenen Netzwerktreiber mit, welcher automatisch installiert wird, damit die Kommunikation zwischen Server und Clients funktioniert. Der Treiber (Norman Network Security) wird bei bestehenden Netzwerkkadaptern hinzugefügt und eingebunden!!!

 Wichtig, Vor der Neuinstallation stellen Sie sicher, dass Ihr DNS in der Domäne fehlerfrei läuft und keine ungültigen, doppelten Einträge vorhanden sind, da es sonst zu Problemen mit der Clientzuordnung im NEM kommen kann.

2. Systemvoraussetzungen

Unterstützte Betriebssysteme:

Windows Server 2000 (SP4, Update Rollup 1 + aktuelle Patches) Windows Server 2003 32 Bit / 64 Bit (SP2, aktuelle Patches) Windows Server 2008 (auch SR2) 32-/64 Bit (aktuelle Patches) Windows SBS 2011 (aktuelle Patches) Windows 2000 (SP4, Update Rollup 1 + aktuelle Patches) Windows XP 32 Bit / 64 Bit (SP3, aktuelle Patches) Windows Vista 32 Bit / 64 Bit (SP1, aktuelle Patches) Windows 7 32 Bit / 64 Bit (aktuelle Patches)	OpenSUSE 11.3 32 Bit und 64 Bit SLES 10.02 64-Bit Debian 5.06 oder neuer 32 Bit und 64 Bit Ubuntu 8.04 oder neuer 32 Bit und 64 Bit
--	--

Hardware Voraussetzungen:

CPU: Min. 1GHz, RAM: Min. 512 MB (1GB empfohlen)

Freier Festplattenspeicher: Min. 300 MB für ein Netzwerk bis 100 Clients, dann pro 100 Clients 10 MB zusätzlich.

Unterstützte Internet Browser:

Aktuelle Mozilla Firefox 2, 3 & 4 (empfohlen). Internet Explorer 6, 7, 8 & 9 (empfohlen)

 Hinweis Generell arbeitet der Norman Endpoint Manager schneller je mehr Arbeitsspeicher zu Verfügung steht. Daher ist in größeren Netzwerken mehr Arbeitsspeicher zu empfehlen.

3. Serverinstallation

Installation auf einem 2000 / 2003 / 2008 Server

Auf dem Verteilungsserver werden folgende Dinge installiert:

- a. Norman Endpoint Protection (lokale Installation für den Server)
- b. Distributions Verzeichnisse (Verzeichnis und Module für die Verteilung)
- c. Norman Endpoint Manager (Administrationsoberfläche)

Laden Sie zunächst die Installationsdatei der aktuellen NPRO Version von unserem Internet Downloadbereich herunter:

<http://www.norman.com/downloads/sm-ent/68793/de>

Starten Sie nun die heruntergeladene Installationsdatei. Geben Sie einen Lizenzschlüssel für Netzwerkinstallationen ein.

Im benutzerdefinierten Installationsmenü wählen Sie alle Komponenten aus und die entsprechenden Sprachen **[Bild 1]**.

Bild 1:




Nach dem Fertigstellen kann es noch einige Minuten dauern, bis alle Komponenten installiert und gestartet sind. Dieses erkennen Sie daran, dass das Norman Programm Symbol in der Taskleiste mit einem Zahnrad versehen ist, solange die Aktualisierung / Installation läuft.

4. Erstellung eines Sicherheitsbereich (Realms)

Beim ersten Aufruf der NEM Oberfläche müssen Sie einen neuen Sicherheitsbereich erstellen.

Ein Sicherheitsbereich ist eine logische Übersicht des Netzwerkes sowie dessen Clients und Netzwerkgeräten auf denen Norman Endpoint Protection installiert werden kann. In der grafischen NEM Console werden die Netzwerkobjekte angezeigt. Es besteht die Möglichkeit, diese zu managen und die NEP Installation individuell zu konfigurieren.

Bitte rufen Sie dazu die NEM Oberfläche mit einem Rechtsklick auf das Norman Programm Symbol auf. Wählen Sie „**Norman Endpoint Manager**“ aus.

 **Achtung** Als Sicherheitsbereichs Name kann jeder x-beliebige Name vergeben werden. Bitte beachten Sie jedoch, dass der Sicherheitsbereich Name anschließend nicht mehr geändert werden kann.


Im NEM Assistenten werden Sie das Erste Mal gefragt, ob Sie einen neuen Sicherheitsbereich erstellen wollen oder ein vorhandenen Sicherheitsbereich wiederherstellen wollen.

Wählen Sie „**Ich richte einen neuen Sicherheitsbereich ein**“ aus.

Im erscheinenden Fenster [Bild 2] geben Sie den Sicherheitsbereichsnamen an und den Sicherheitsbereich Eigentümer Account.

 **Wichtig:** Bitte notieren Sie sich den Eigentümer Account und das entsprechende Passwort, da dieses anschließend nicht mehr geändert werden kann. **Es dürfen keine Umlaute & Sonderzeichen als Benutzername oder Passwort genutzt werden!**

Im Bereich für den Servernamen oder die IP Adresse geben Sie die Informationen des NEM Servers ein.


 **Hinweis:** Wir empfehlen Ihnen die IP Adresse zu verwenden, um Namesauflösungsproblemen vorzubeugen!

Nach Fertigstellung wird der Sicherheitsbereich entsprechend angelegt und Sie werden nun beim nächsten Starten den NEM Oberfläche nach dem Eigentümer Account gefragt.

Anschließend müssen Sie die Sprachen und die Plattformen auswählen, welche vom NEM mit aktualisiert werden sollen. Wir empfehlen Ihnen, alle Plattformen herunterzuladen, da so Probleme mit fehlenden Komponenten vermieden werden.

Glückwunsch! Sie haben nun die Basis für die Norman Endpoint Protection Verteilung geschaffen und können nun mit der Konfiguration weiter verfahren.

Bild 2:

 **Wichtig:** Bei NEM / NPro werden die Informationen, Einstellungen und Konfigurationen des Sicherheitsbereiches im sogenannten Store.nts abgespeichert. Es handelt sich dabei um eine Datenbank, welche von den Norman Diensten im ständigen Zugriff ist. Wenn Sie daher Backup Software einsetzen, welche die komplette Systemplatte sichert und sich exklusiven Zugriff auf Dateien beschafft, sollten Sie das Norman Verzeichnis von dieser Sicherung ausnehmen (Ausnahme die Norman Backupdateien), da es ansonsten zu Problemen bzw. einer defekten Datenbank kommen kann!

5. Installation aktualisieren

Nach der Erstinstallation und Einrichtung des Endpoint Managers führen Sie bitte ein Internet Update durch, damit die Lizenz validiert und die Installation mit den aktuellen Updates versorgt wird. Starten Sie dafür über das Norman Programm Symbol das „Internet Update“. Warten Sie bis die Komponenten heruntergeladen und installiert wurden. Ggf. fordert Sie die Installation zu einem Neustart des Systems auf.

Durch das anfängliche Internet Update wird sichergestellt, dass immer die aktuelle NPRO Version bei einer Erstinstallation auf die Arbeitsstationen verteilt wird.

Falls Sie über einen Proxy-Server auf das Internet zugreifen, müssen Sie diesen vorher eintragen. Wechseln Sie dazu im NEM auf den Punkt „**Richtlinien**“. Wählen Sie die Norman Endpoint Manager Richtlinie aus, wechseln Sie auf den Punkt **Produkt Manager -> Konfigurieren -> Proxy-Einstellungen**. Tragen Sie Ihren Proxy ein.

6. Konfiguration von Sicherheitsbereich Admins und NIU

Zunächst erstellen Sie einen neuen Sicherheitsbereich Administrator, mit welchem weiter gearbeitet wird. Es können verschieden Sicherheitsbereich Administratoren angelegt werden, welche z.B. für die Remoteverwaltung genutzt werden können.

Gehen Sie im Endpoint Manager in den Bereich „**Wartung**“ -> „**Sicherheitsbereich-Administratoren**“. Über „**Administrator erstellen**“ fügen Sie einen neuen Account hinzu [Bild 3]. Vergeben Sie einen Namen und das Passwort.

Bild 3:



Wichtig! Bitte beachten Sie, dass sowohl beim Benutzernamen als auch beim Passwort zwischen Groß- und Kleinschreibung unterschieden wird!

Anschließend loggen Sie sich mit dem neuen Sicherheitsbereich Administrator in den Endpoint Manager ein. Wechseln Sie in den Bereich „**Produkte**“.

Konfigurieren Sie die Sprachen und Plattformen, in denen NPRO installiert werden soll. Speichern Sie die Änderungen und machen Sie anschließend ein Internet Update.

7. Erstellung einer Richtlinie sowie einer Gruppe für den NEM Server

Bei NEM gibt es die Möglichkeiten Gruppen und Richtlinien zu erstellen.

Richtlinien: Eine Richtlinie ist eine Konfigurationsvorlage, welche einem Computer oder einer Gruppe von Computern zugewiesen werden kann.

Gruppe: Eine Gruppe wird dazu verwendet mehrere Computer zusammenzufassen um ihnen dann die gleiche Richtlinie zuzuweisen

Auch der NEM Server bekommt seine eigene Gruppe und seine eigene Richtlinie. Bei der Installation von NEM erhält der NEM Server automatisch seine eigene Richtlinie (NEM Richtlinie) und seine eigene Gruppe (NEM).

Die Richtlinie des NEM Servers kann unter dem Punkt „**Richtlinien**“ eingesehen werden. Die Gruppe des NEM wird unter „**Clients**“ angezeigt. Sie trägt den Namen „**NEM**“ und der Server wird automatisch in diese Gruppe verschoben und erhält somit seine eigene Konfiguration.

8. Installation der Clients per Push Installation

Um eine Push Installation auf den Clients in der Domäne durchführen zu können, muss zunächst ein administrativer Domänenaccount angegeben werden.

Wechseln Sie dazu in den Bereich „**Einstellungen**“ -> „**Installation in einem Netzwerk**“. Geben Sie die Account und Domäneninformationen an [Bild 6]. Speichern Sie die Änderungen.

Bild 6:


The screenshot shows the 'Einstellungen' (Settings) page with three tabs: 'Ereignisverwaltung', 'Topologiefilter', and 'Installation in einem Netzwerk'. The active tab is 'Installation in einem Netzwerk'. Below the title, there is a brief instruction: 'Installieren Sie Norman Endpoint Protection (NPRO) auf Computern in einem Netzwerk über die nötigen Anmeldeinformationen zum Verwalten von Domänen oder über die Anr...'. The form includes the following fields:

- IP/Hostname:** 192.168.100.122
- Domäne:** domäne
- Benutzername:** Administrator
- Kennwort:** Masked with six dots
- Maximale Anzahl Installationsversuche:** Kein Limit (dropdown menu)
- Verzögerung wegen fehlgeschlagener Installation:** 15 Minuten (dropdown menu)

Gehen Sie nun im Endpoint Manager in den Bereich „**Richtlinien**“. Legen Sie eine neue Regel für die Clients an. Benennen Sie die Regel „ClientPC“. Die default Einstellung der Regel können beibehalten werden.

Anschließend wechseln Sie in den Bereich „**Clients**“ und legen Sie eine neue Gruppe an. Die Gruppe benennen Sie „ClientPCs“, als Regel für die neue Gruppe wählen Sie die zuvor erstellte „ClientPC“ Regel aus.

In der „**Client**“ Ansicht, wechseln Sie in den Bereich „**Objekte ohne Zuordnung**“. Wählen Sie die Clients aus, welche mit in die Verteilung aufgenommen werden sollen & verschieben Sie diese in die Gruppe „Clients“. Mehrere Clients können mit STRG Taste markiert werden und bei gedrückter STRG-Taste können diese gemeinsam per „Drag & Drop“ verschoben werden

 **Hinweis:** Norman Endpoint Manager „horcht“ mit Hilfe des eigenen Netzwerk Protokolls (Norman Network Security) den Netzwerkverkehr ab und bietet somit die Möglichkeit einer passiven Netzwerksuche.

Sollten Clients mit dieser Methode nicht angezeigt werden, gibt es auch die Möglichkeit, einen definierbaren IP Adressenbereich per „ping“ zu durchsuchen und gefundene Clients hinzuzufügen.

Dazu wechseln Sie in den Bereich „**Wartung**“ -> „**Importieren**“ -> „**Aktive Erkennung**“. Geben Sie den gewünschten IP Adressenbereich an [Bild 7] und klicken Sie auf „**Erkennen**“:

Bild 7:



Nun kann die Push Installation auf dem / den Client(s) gestartet werden. Wählen Sie in der Client Ansicht, die oder den Client aus und klicken Sie auf das „Push Install“ Symbol [Bild 8].

Bild 8:


Wenn Sie mehrere Clients auswählen wollen, halten Sie gleichzeitig die STRG Taste gedrückt, während Sie die Clients markieren.

Zur Push Installation beachten Sie bitte auch die System- / Dienstanforderung welche in unserem NPro Admin Guide beschrieben sind: http://www.norman.com/support/endpoint_protection/de

9. Installation der Clients per MSI Datei

Alternativ kann ein neuer NEP Client auch direkt mit einer MSI Datei installiert werden. Die MSI Datei kann lokal als Administrator auf dem PC installiert oder über eine Active Directory Gruppenrichtlinie eingebunden werden.

Die MSI Datei wird im Endpoint Manager unter dem Punkt „**Wartung**“ -> „**Installationsprogramme erzeugen**“ erstellt.

 Hinweis: Bei Installation eines Clients, wird für die Windows Firewall und die Norman eigene Firewall, automatisch eine Portfreigabe für den Messaging Dienst Norman Njeeves auf TCP Port 2868 eingerichtet.

Bei Peer-2-Peer Netzwerken ist das Installieren mit MSI Dateien die Standard Vorgehensweise.

10. Installation eines Linux Clients

Seit NPro 8.10 ist es möglich, Linux Clients über den Norman Endpoint Manager zu verwalten.

Die unterstützten Linux Distributionen sind im Punkt 2 (Systemanforderungen) dieser Anleitung aufgelistet.

Um einen Linux Client installieren zu können, müssen Sie sich zunächst ein Shell (SH) Skript erstellen.

Das SH Skript wird im Endpoint Manager unter dem Punkt „**Wartung**“ -> „**Installationsprogramme erzeugen**“ erstellt. Das Shell-Skript kann sowohl auf 32- als auch auf einem 64-Bit System ausgeführt werden.

Anschließend können Sie mit dem erstellten Linux Skript, den / die Linux Clients installieren. Führen Sie das Skript auf dem Linux PC als root aus.

Ein entsprechender Wizard wird Sie dann durch die NPro für Linux Installation begleiten.

11. Topologie Filter

Bei NEM haben Sie die Möglichkeit, mit Topologiefiltern zu arbeiten. Dadurch können neue Clients direkt einer Gruppe und damit vordefinierten Konfigurationen (Richtlinien) zugeordnet werden.

Der Topologiefilter wird im Endpoint Manager unter dem Menü Punkt „**Einstellungen**“ -> „**Topologiefilter**“ konfiguriert.

Einstellungen

Ereignisverwaltung | **Topologiefilter** | Installation in einem Netzwerk | Supervisorprozess

Topologiefilter

Ein gefundenes Netzwerkgerät kann automatisch nach vordefinierten Topologiegruppen gefiltert werden. Wenn ein Gerät die Filterregeln nicht erfüllt, wird es in die Standardgruppe "Objekte ohne Zuordnung" verschoben. Clients, die bereits einer bekannten Netzwerktopologie angehören, sind von den neuen Filterregeln ausgenommen.

Die allgemeine Syntax lautet: Wenn *Attribut* Gleich / Ungleich *Wert oder Teilwert* DANN verschiebe in Gruppe *Gruppe*. "Attribut" ist eine Pull-down-Liste mit gerätespezifischen Eigenschaften, z. B. ein Name oder eine IP-Adresse. Der Operator ist entweder "Gleich" (=) oder "Ungleich" (!=). Der Wert ist eine vollständige oder unvollständige Zeichenfolge, mit der das Attribut verglichen wird. Unvollständige Zeichenfolgen müssen mit einem Platzhalterzeichen beginnen oder enden. Die Filter arbeiten von oben nach unten und stoppen beim ersten Treffer. Mithilfe der Schaltfläche "Und..." können Sie Regeln mit mehreren zu erfüllenden Voraussetzungen erstellen.

Beispiel: Alle Clients, deren IP-Adressen mit 172.17 beginnen, in die Gruppe "London" verschieben: Wenn IP = 172.17* verschiebe in Gruppe "London". Außerdem kann dem Filterausdruck der Platzhalter * vorangestellt werden. Beispiel: Alle Clients, deren Namen mit "srv" enden, in Gruppe "Server" verschieben: Wenn Name = *srv verschiebe in Gruppe "Server".

WENN =

DANN verschiebe in Gruppe

Vorhandene Filter

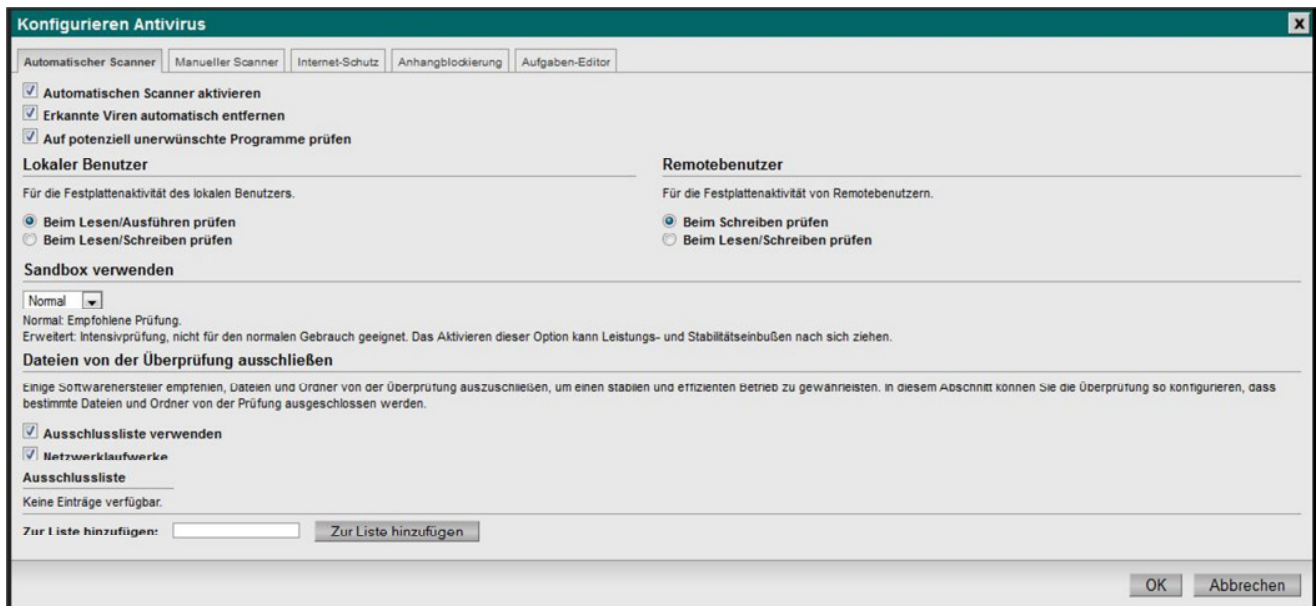
- ↑ ↓ [1] WENN IP-Adresse = 192.168.100.122 DANN verschiebe in Gruppe NEM
- ↑ ↓ [2] WENN IP-Adresse = 192.168.100.1 DANN verschiebe in Gruppe Unverwaltet

Filter erfolgreich gelöscht.

12. Konfiguration der Richtlinien im NEM

Bei NEM gibt es die Möglichkeit, verschiedene Richtlinien für verschiedene PCs bzw. Gruppen zu erstellen. So können z.B. für verschiedene Abteilungen, verschiedene Richtlinien erstellt werden. In den Richtlinien können z.B. Einstellungen für den Echtzeitscanner, Manuellen Scanner, Internet Schutz verändert werden [Bild 9].

Bild 9:



Desweiteren können in den Richtlinien folgende Sachen eingestellt werden:

Taskdateien: Taskdateien werden benutzt um in regelmäßigen Abständen (z.B. wöchentlich) auf den Clients Scans durchzuführen.

Ausschlusslisten: Auf einigen Systemen werden Ausschlusslisten für den Echtzeitscanner benötigt, damit kritische Anwendungen wie Datenbank Server, Exchange Server, ERP Systeme o.ä. nicht vom Echtzeitscanner mit gescannt werden.

Ausschlusslisten können für den Echtzeitscanner und für den Manuellen Scanner gebildet werden.

Gültige Einträge für die Ausschlussliste sind:

Wildcards z.B: *.log

Verzeichnis z.B: C:\Programme\Anwendung

Dateinamen z.B: anwendung.exe

Produkt Manager:

Hier können Sie die Sprache, Aktualisierungsintervalle und Proxy Einstellungen anpassen.

Antivirus für Exchange:

Hier können Einstellungen bezüglich des Scanverhaltens für das Norman MailScan for Exchange Plugin getätigt werden. Installationshinweise siehe Punkt 17 der Kurzanleitung.

13. Sicherung des NEMs

Der Endpoint Manager besteht aus verschiedenen Daten, welche in einer lokalen Datenbank dem sogenannten *Store* abgelegt werden. Es wird empfohlen, diese Daten in regelmäßigen Abständen zu sichern. In NEM ist eine Backuproutine integriert, bei dieser werden Informationen über die Netzwerk Topologie, Realm Logindaten und Endpoint Manager Einstellungen / Konfigurationen gesichert.

Um ein Backup zu erstellen gehen Sie in den Endpoint Manager unter den Punkt „Wartung“ -> „Sichern und wiederherstellen“. Hier können im Bereich „Sichern“ [Bild 10] Sicherungen erstellt werden und im Bereich „Wiederherstellen“ [Bild 11] können diese wiederhergestellt werden.

Bild 10:

Sichern und wiederherstellen
Wichtige Teile der Endpoint Manager-Datenbank sichern und wiederherstellen. Die Sicherung Einstellungen und Netzwerktopologie. Nach dem Einrichten eines verwalteten Sicherheitsbereichs beibehalten werden kann, selbst wenn alle Endpoint Manager verloren sind. Die Sicherung Hardwareplattformen zu verschieben. Unten kann ein regelmäßiger Sicherungsplan eingerichtet werden.

Sichern | Wiederherstellen

Letzte erfolgreiche Sicherung 2009.05.15 10:01:47

Ziel
C:\Programme\Norman\backups\noc\ Durchsuchen

Max. Anzahl Sicherungen
30

Geplante Sicherungen zulassen

Unten den/die Wochentag(e) auswählen:
Mo Di Mi Do Fr Sa So

Startzeit 15 : 00

Bild 11:

Sichern und wiederherstellen
Wichtige Teile der Endpoint Manager-Datenbank sichern und wiederherstellen. Die Sicherung Einstellungen und Netzwerktopologie. Nach dem Einrichten eines verwalteten Sicherheitsbereichs beibehalten werden kann, selbst wenn alle Endpoint Manager verloren sind. Die Sicherung Hardwareplattformen zu verschieben. Unten kann ein regelmäßiger Sicherungsplan eingerichtet werden.

Sichern | Wiederherstellen

Daten aus Sicherungsdatei importieren und wiederherstellen.

Wiederherstellen aus...
C:\Programme\Norman\backups\noc\ Durchsuchen

Wiederherstellungsstrategie
Einstellungen und Topologie

Aktuelle Werte beibehalten

Hinweis: Bei einer Neuinstallation eines NEM Sicherheitsbereichs kann statt einem neuen Sicherheitsbereich, ein Sicherheitsbereich aus einem Backup wiederhergestellt werden. Dieses ist nützlich, falls ein Server ersetzt wurde oder durch einen Hardwaredefekt ausgetauscht wurde. Entscheidend ist das DNS Name, IP Adresse und Netzwerk Einstellungen des Servers mit den vorherigen identisch sind.

14. Fernzugriff auf NEM

Bei NEM gibt es die Möglichkeit per Remote Zugriff auf die Endpoint Manager Oberfläche von frei zu definierenden Arbeitsstationen zuzugreifen. Damit dies möglich ist, muss diese Funktion zunächst freigeschaltet werden.

Die Freischaltung erfolgt in der NEM Oberfläche unter dem Menüpunkt

„Wartung“ -> „Fernzugriff“.

Dort wird die Option über die Checkbox „**Fernzugriff zulassen**“ freigeschaltet. Als IP Adressen können individuelle IP Adressen angegeben werden.


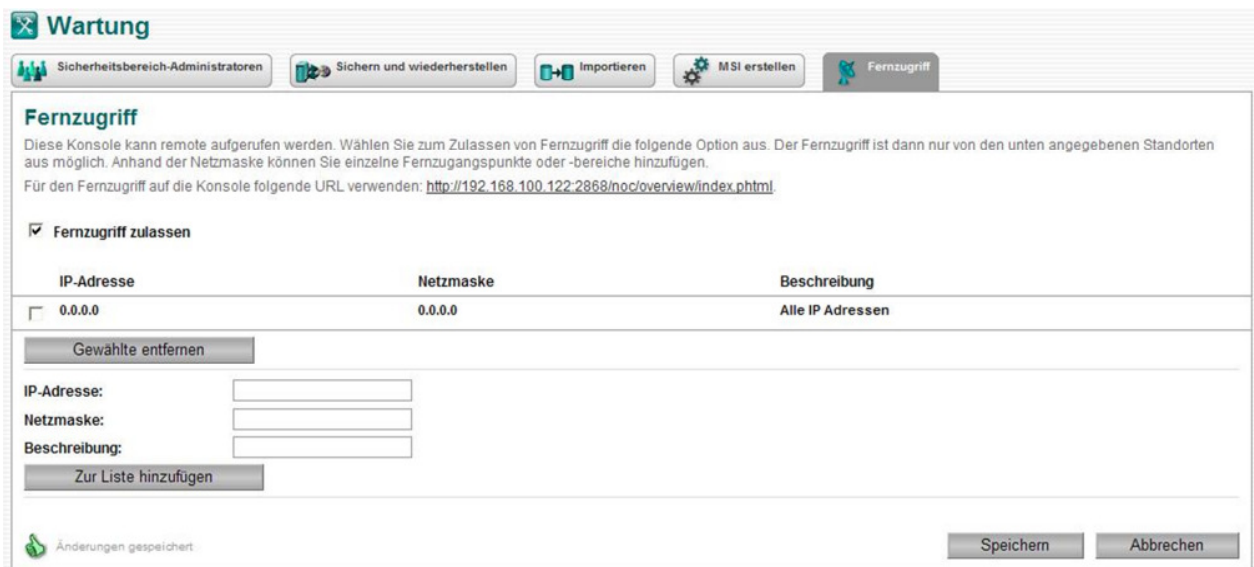
 Hinweis: Soll der Remote Zugriff für alle Arbeitsstationen im Netzwerk möglich sein, geben Sie als IP Adresse ein 0.0.0.0 und als Netzmaske 0.0.0.0 [Bild 12].

Bild 12:



Wartung

Sicherheitsbereich-Administratoren | Sichern und wiederherstellen | Importieren | MSI erstellen | **Fernzugriff**

Fernzugriff

Diese Konsole kann remote aufgerufen werden. Wählen Sie zum Zulassen von Fernzugriff die folgende Option aus. Der Fernzugriff ist dann nur von den unten angegebenen Standorten aus möglich. Anhand der Netzmaske können Sie einzelne Fernzugangspunkte oder -bereiche hinzufügen.
Für den Fernzugriff auf die Konsole folgende URL verwenden: <http://192.168.100.122:2868/noc/overview/index.phtml>.


Fernzugriff zulassen

IP-Adresse	Netzmaske	Beschreibung
<input type="checkbox"/> 0.0.0.0	0.0.0.0	Alle IP Adressen

IP-Adresse:

Netzmaske:

Beschreibung:

 Änderungen gespeichert

Die Remote URL setzt sich wie folgt zusammen:

<http://127.0.0.1:2868/noc/overview/index.phtml>.

Anstatt von 127.0.0.1 tragen Sie direkt die IP Adresse des NEM Servers ein.


15. Migration von NVC 5.99 auf NPro 8.10

Bei NEM gibt es die Möglichkeit, eine bestehende Norman Virus Control Installation zu migrieren. Hierbei können sowohl Konfigurationen direkt in Richtlinien übernommen als auch bestehende Installation von NVC auf NPro aktualisiert werden.

Wir empfehlen allerdings eine komplette Neuinstallation der Server und Clients durchzuführen, um eventuelle, Fehler und Probleme bei der Migration vorzubeugen bzw. zu vermeiden. Bei der Neuinstallation muss Norman Virus Control auf den Clients zunächst deinstalliert werden. Wichtig ist, dass nach der Deinstallation das alte, verbleibende Norman Verzeichnis gelöscht wird, damit keine alten Dateien mehr vorhanden sind.

Sollten Sie sich für eine Migration entscheiden, ist es wichtig, dass NVC und NEM / NPRO nicht parallel auf dem gleichen System installiert sein dürfen.

Vor der Deinstallation von NVC auf dem Verteilungsserver kopieren Sie sich zunächst das NVC DISTRIB Verzeichnis mit Unterordnern (z.B. c:\programme\norman\distrib). Anschließend machen Sie die Deinstallation von NVC (wenn NVC für Exchange mit installiert ist, deinstallieren Sie das Plugin zuerst, als zweites dann NVC). Nach einem Serverreboot, löschen Sie das verbleibende Norman Verzeichnis und installieren dann NEM / NPro.

 Hinweis: Beachten Sie dazu bitte auch die Hinweise im NPro Adminguide: http://www.norman.com/support/endpoint_protection/de. Sie können auch das Migrationstool **PushMig** nutzen, welches Sie unter: http://www.norman.com/support/support_tools/70875/de finden.

Windows XP, Vista, 200x x86 Umgebung (Migration geht nicht unter 64Bit)

Bei Windows XP, Vista, 200x kann die NEM / NPro integrierte Migrationsfunktion genutzt werden. Diese ist im Endpoint Manger unter „Wartung“ -> „Importieren“ -> „Migrieren“ zu finden.



Wartung

Sicherheitsbereich-Administratoren Sichern und wiederherstellen Importieren

Importieren

Die Importfunktionen stellen Methoden zum Füllen Ihrer Topologiekarte bereit. Mit "Importieren" können anhand der alten Verteilerhierarchie zu erstellen. Mit "Migrieren" werden Migrationsdaten in einen von NSS-verwalteten Sicherheitsbereich zu migrieren. Mit der Option "Aktive Erkennung" können Sie eine weiteren Verwaltung importieren.

Importieren Migrieren Aktive Erkennung

Geben Sie den Pfad zu einem NVC-v5-Verteilerpunkt an (Ordner \distrib), um die Topologie zu importieren (Dateien) Richtlinien zu erstellen. Das Ergebnis und die importierte Topologie finden Sie unter Client

Pfad des NVC 5-Verteilerpunkts

Durchsuchen

Über die Schaltfläche „**Durchsuchen**“ kann das bisherige NVC DISTRIB Verzeichnis ausgewählt werden. Man muss entsprechen das alte ...\\Norman\\Distrib Verzeichnis des NVC Servers auswählen und dann auf Migrate klicken. Melden Sie sich mit einem Administrativen Account am Share an oder wählen Sie das Verzeichnis lokal aus.

Nach klicken auf die Schaltfläche „Migrate“ kopiert NEM nun in das gewählte ...\\Norman\\Distrib\\Download die NSA Dateien für NPro und in das ...\\Norman\\Distrib\\nvc\\config Verzeichnis wird die Datei migns7.nts kopiert.


Alle Clients in der Verteilung werden sich nun aus dem ...\\Norman\\Distrib\\Download die NSA Dateien kopieren und somit auf NPro migrieren /aktualisieren.

Die Client NVC Installation kopiert sich zunächst die NSA Dateien welche der lokalen NVC Installation entsprechen. Ist NVC z.B. Deutsch werden die deutschen NSA Komponenten Dateien kopiert und damit installiert. Nach dem ersten Neustart des Clients kopiert dieser die Policy vom Server und wenn dort eine andere Sprache ausgewählt ist z.B. werden diese Komponenten vom NEM Server kopiert. Anschließend wird der Client erneut einen Neustart fordern um die Sprachmodule endgültig zu übernehmen.

Da NEM / NPro nur die alte NVC Distrib Verzeichnisstruktur überprüft, kann direkt nur das Verzeichnis genutzt werden. Somit kann NEM / NPro auf dem bisherigen NVC Distrib Server installiert werden. Dabei geht man wie folgt vor:

1. Sicherung des ...\\Norman\\Distrib Verzeichnisses der NVC Installation
2. Eine Neue Freigabe auf das ...\\Norman\\Distrib. Freigabe Namen und Berechtigungen wie vorher.
3. Deinstallieren von NVC
4. Installieren, Konfigurieren von NPro / NEM
5. Migration wie oben beschrieben.

Macht man diese Migration mit zwei verschiedenen Servern, also einem NVC Verteilungsserver und einem NEM Server, wird sich der NVC Verteilungsserver nicht automatisch auf NPro aktualisieren. Dieses muss manuell gemacht werden.

 **Wichtig:** Bei dieser Migrationsmethode wird probiert alle Clients, die der NVC Verteilung angehören, auf NPro zu aktualisieren. Sollen nur vereinzelt Clients auf NPro migriert werden, können die NSA Dateien vom NEM Server und die Migrationsdatei migns7.nts manuell kopiert werden.

Die NSA Dateien müssen in das lokale ...\\Norman\\Download Verzeichnis kopiert werden. Die Datei migns7.nts in das lokale ...\\Norman\\config Verzeichnis des NVC Clients. Nach ein paar Minuten wird dieser sich aktualisieren.

Netware / Firebreak Umgebung

Bei einem NVC Netzwerk mit Firebreak muss zusätzlich zwingend ein Windows Server (2000, 2003) als NEM / NPro Server eingesetzt werden. Dieser Windows Server wird als neuer NEM Verteilungsserver installiert. Nach der Installation des NEM Verteilungsserver müssen vom NEM Verteilungsverzeichnis ...\\norman\\distrib\\download alle NSA Dateien auf das alte Firebreak NVC Download Verteilungsverzeichnis kopiert werden. Zusätzlich zu den NSA Dateien muss noch die Migrationsdatei migns7.nts aus dem ...\\Norman\\Distrib\\nvc\\config Verzeichnis auf das alte Firebreak Config Verzeichnis kopiert werden.

Windows 9x / ME / NT Umgebung

Diese Betriebssysteme können nicht mit NPro bestückt werden. Bei einer Mischinstallation mit XP, Vista PC und Windows 9x, Me, NT PCs werden zwei Distrib Server benötigt. Einer für NVC und einer für NPro. Diese beiden können nicht auf der gleichen Maschine sein.

Import von Konfigurationsdateien, Topologie:

Wie bereits erwähnt, können Konfigurationsdateien und somit auch z.B. Ausschlusslisten von NVC übernommen werden.

Dieses machen Sie in der NEM Oberfläche unter dem Punkt:

Maintenance -> Import -> Import.

The screenshot shows the 'Wartung' (Maintenance) section of the Norman Endpoint Manager interface. At the top, there are several navigation buttons: 'Sicherheitbereich-Administratoren', 'Sichern und wiederherstellen', 'Importieren' (highlighted), 'MSI erstellen', and 'Fernzugriff'. Below these is the 'Importieren' section, which includes a description of the import function and three sub-buttons: 'Importieren', 'Migrieren', and 'Aktive Erkennung'. The main area contains a text box for the path to the NVC 5 distribution folder, a 'Durchsuchen' (Search) button, and an 'Importieren' button at the bottom right.

Über den Button „**Durchsuchen**“ können die Konfigurationsdateien aus dem ...\\Norman\\Distrib\\nvc\\Config Verzeichnis des NVC Verteilungsserver in den NEM importiert werden. Als Verzeichnispfad muss nur ...\\Norman\\Distrib angegeben werden. Auch hier muss sich wieder mit einem administrativen Account am Share angemeldet werden oder das Verzeichnis von einem lokalen Pfad ausgewählt werden.

16. Hintergrundinformationen NEM

NPro 7.20 besitzt mehrere `..bin` Verzeichnisse. Die wichtigsten Verzeichnisse und Komponenten werden hier im Detail erläutert:

...\`Norman\npm\bin` Verzeichnis:

<code>DeINVC5.exe</code>	Deinstallations- und Reparaturprogramm: Wenn Sie dieses Programm starten können Sie zwischen Reparatur und Deinstallation wählen. Rufen Sie von der Kommandozeile <code>delnvc5 /repair</code> aus, so wird die Reparatur ohne Benutzereingriff gestartet.
<code>Elogger.exe</code>	Protokollierungsprogramm in welchem Norman Programmmodule Informationen anzeigen
<code>Elogsvc.exe</code>	Dienst welcher die Protokollierungsfunktion für die Norman Komponenten und den Elogger bereitstellt.
<code>LicWiz.exe</code>	Norman's Lizenz Wizard. Enthält Informationen zur installierten Lizenz, deren Produkte und Laufzeiten.
<code>Lnq.exe</code>	Kommandozeilenprogramm zur Abfrage des lokalen Installationsstatus. Es werden keine Parameter verwendet.
<code>NBrowser.exe</code>	Norman's eigener Browser, wird verwendet zur Darstellung der lokalen Einstellungen, Konfigurationen etc. Alternativ wird der Internet Explorer oder der Mozilla Firefox genutzt.
<code>Niu.exe</code>	Norman Internet Update. Das Programm ist über das Norman Traymenü und das Startmenü verknüpft.
<code>Njeeves.exe</code>	Kommunikationsdienst von NEM / NPro. Versendet lokale und Netzwerkmeldungen. Die Meldungen werden über das verschlüsselte Norman Protokoll NIX (Norman Information Exchange) verschickt. TCP/IP Port 2868 wird hierbei genutzt. Njeeves stellt auch die Norman Internet Service Engine (NISE) zur Verfügung. NISE wird als http Server verwendet, welcher auf die Dateien, Datenbank Komponenten und GUI Inhalte des Endpoint Managers zugreift.
<code>Nvoy.exe</code>	Norman Resource Provider.
<code>Scheduler.exe</code>	Norman Scheduler Service. Taskplannerdienst. Startet mit dem Taskeditor vordefinierte Scantasks.
<code>Zanda.exe</code>	Das Kernstück der NEM / NPro Installation. Zanda ist der Installationsagent (Z ero A dministration N etwork D istribution A gent). Dieser Dienst startet automatisch und startet alle anderen NEM / NPro Dienste.
<code>Zlh.exe</code>	Z anda's L ittle H elper ist ein Hilfsmodul, welches unter anderem alle NEM / NPro Komponenten des Benutzermodus startet. Es stellt auch das Tray Menü zur Verfügung.

...\Norman\nse\bin Verzeichnis:

Nsesvc.exe Norman Scanner Engine Service. Dieser Dienst stellt den Norman Scan Komponenten (Echtzeitscanner, Manueller Scanner, Internetschutz) die Virensignatur zur Verfügung. Dieses ermöglicht einen schnelleren Zugriff auf die Virensignatur und verringert den Arbeitsspeicher Bedarf. Sollte der NSESVC Dienst nicht gestartet sein, werden die Norman Scan Komponenten selbstständig die Virensignatur in den Arbeitsspeicher laden.

...\Norman\nvc\bin Verzeichnis:

CCLaw.exe Komponente des Zugriffsscanners (lokale Benutzer)

Nip.exe Norman Internet Protection (Internetschutz)

Nvcc.exe Kommandozeilenscanner für Win32 (Windows 2000 / XP / 2003). **Nvcc /?** zeigt alle Parameter an.z.B. scannt: **nvcc /ald /cl /o /u /l:2** alle lokalen Laufwerke, mit automatischer Bereinigung und speichert unter ...\

Nvcoa.exe Steuerungsmodul des Zugriffsscanners. Wird nur geladen wenn kein Benutzer angemeldet ist. Der Befehl **nvcoa -unloadx** entlädt alle Zugriffsscannerkomponenten während **Nvcoa -loadx** sie wieder startet. So können Sie z.B. skriptgesteuert den Zugriffsscanner anhalten, um Software im Netzwerk zu verteilen und danach den Scanner wieder zu starten. Beachten Sie, dass Sie dafür lokale Administrationsrechte besitzen müssen.

Nvcoas.exe Zugriffsscannerdienst.

Nvcod.exe Manueller Scanner. Ihn starten Sie über das Kontextmenü des Explorers, oder zeitgesteuert über Taskdateien.

17. Tipps & Tricks

Zugriff auf Norman Endpoint Manger per URL:

Die Norman Endpoint Manager Oberfläche ist Browser basiert und kann daher auch direkt per URL aufgerufen werden. Die URL der NEM Oberfläche lautet <http://localhost:2868/noc/index.phtml>. Statt localhost kann auch die IP Adresse des Norman Endpoint Manager's Computers angegeben werden.

Ausschlussliste Konfigurieren:

Auf Servern oder Computern auf denen z.B. Datenbanken, ein Exchange Server oder andere kritische Anwendungen installiert sind, sollte mit Ausschlusslisten gearbeitet werden.

Die Ausschlussliste wird in NPro in den einzelnen Richtlinien konfiguriert (In der Richtlinie über die Option „Konfigurieren Antivirus“ im Bereich für den Echtzeit- und OnDemand Scanner.

Bezüglich der Thematik Exchange und Ausschlussliste beachten Sie bitte den MS Knowledge Base Artikel 328841 (<http://support.microsoft.com/kb/328841>) und 823166 (<http://support.microsoft.com/kb/823166>)

Datensicherung Unload / Load Skript für Norman Echtzeitscanner:

Bei einem Backup / einer Datensicherung gilt generell, dass der Echtzeitscanner ausgeschaltet werden sollte, da es immer wieder zu Problemen kommt, wenn dieser während des Backups läuft. Dieses ist unabhängig von der Backupsoftware.

Backup Programme bieten in der Regel die Möglichkeit, eine Batchdatei vor und nach dem Backup durchzuführen. Mit Hilfe einer Batchdatei kann der Echtzeitscanner angehalten werden.

Eine Batchdatei zum stoppen / unload des Echtzeitscanner würde z.B wie folgt aussehen:

```
start c:\programme\norman\npm\bin\Zanda -unload  
start c:\programme\norman\nvc\bin\invcoa -unloadx
```

Eine Batchdatei zum starten / load des Echtzeitscanner würde z.B. wie folgt aussehen:

```
start c:\programme\norman\npm\bin\Zanda -load
```

Kommandozeilenbefehle für Norman Dienste:

In manchen Fällen ist es notwendig auf gemanagten NPro Clients im Netzwerk, die Dienste manuell über die Kommandozeile zu starten / stoppen etc.

Generell gültige Kommandozeilenschalter für die Norman Komponenten (zanda, zlh, nip, elogsvc, nsesvc etc.) sind:

```
-unload (stoppen)  
-uninstall (deinstallieren)  
-install (installieren)  
-load (starten)
```

Der Schalter wird hinter der eigentlichen Komponente mit angegeben z.B. *zanda -unload*

Bei der Installation von NPro wird auf den Clients automatisch eine Systemvariable (NpmLib) angelegt, welche auf das ...**Norman\npm\bin** Verzeichnis zeigt.

Daher können für folgende Komponenten die Kommandos direkt in der Eingabeaufforderung eingegeben werden und es muss nicht zu nächst in das ...**Norman\npm\Bin** Verzeichnis gewechselt werden:

```
Elogger (öffnet den Elogger direkt)  
Zlh
```

Elogsvc

Nip

Lnq (listet die lokalen Komponenten und deren Status auf)

Zusätzliche Kommandozeilenschalter:

Zanda -updatenow (Auf Verteilungsserver nach Updates schauen bzw. den nächsten Timer überspringen)

Zanda -installnow (wenn neue Komponenten herunter geladen wurden, wird die Installation dieser sofort gestartet)

Zanda -test (Listet die Timer bis zum nächsten Update auf)

Zanda -repair (Reparatur von NVC starten)

Um z.B. den Echtzeitscanner anzuhalten, wechseln Sie in der Kommandozeile in das ...**Norman\ncv\bin** Verzeichnis:

Die Befehle hier lauten:

Nvcoa -unloadx (Echtzeitscanner stoppen)

Nvcoa -loadx (Echtzeitscanner starten)

Sicherheitshinweise:

Virulente Dateien können auf unterschiedlichen Wegen auf die Computer gelangen. Dieses kann z.B. durch infizierte Webseiten, durch ungepatchte Sicherheitslücken in Windows oder anderen Anwendungen geschehen.

Durch USB Sticks, CDs oder anderen externen Medien können auch virulente Dateien in das Netzwerk / auf die Arbeitsstation eingeschleust werden.

Daher ist es wichtig dass neben einem aktuellen Virenschutz auch Windows und andere Anwendungen (z.B. Adobe Acrobat, Flash, Quicktime, Internet Explorer, Mozilla Firefox usw.) ständig aktualisiert werden, damit bekannte Lücken geschlossen werden und nicht ausgenutzt werden können.

Das Produkt Portfolio von Norman umfasst unter anderem Sicherheitslösungen um Ihr Netzwerk auf aktuellem Software Aktualisierungsstand zu halten, den Umgang mit Wechselmedien einzuschränken und somit die Gefahr von ungewollten Infektionen und Datenverlust zu minimieren.

Gerne unterstützen wir Sie dabei, Ihr Netzwerk sicherer vor derartigen Angriffen zu machen. Bei Bedarf und Interesse zögern Sie bitte nicht, uns zu kontaktieren.

Desweiteren sollte der Benutzer mit welchem gearbeitet wird, mit normalen Windows Benutzer Berechtigungen ausgestattet werden, damit sich nicht unerlaubt Programme, Anwendungen etc. installieren können!

Da wir tagtäglich zwischen 4000 - 14000 neue Malware Objekte in unserer Signaturdatenbank erfassen, sollten Sie in regelmäßigen Abständen einen Scan über das System laufen lassen, damit Dateien, welche erst in ein oder zwei Tage später in der Signatur auftauchen, vom System gelöscht werden können, damit diese sich nicht aktivieren können.

18. Installation von Norman MailScan for Microsoft Exchange

Aktuelle Systemvoraussetzungen:

Prozessor mit 1 GHz oder mehr.

512 MB RAM, zusätzlich zum erforderlichen Arbeitsspeicher für Microsoft Exchange Server (1 GB empfohlen).

300 MB verfügbarer Festplattenspeicher

32-Bit-Systeme:

Microsoft Exchange Server 2000/2003 SP2

Windows Server 2000/2003

64-Bit-Systeme:

Microsoft Exchange Server 2007 SP2

Microsoft Exchange Server 2010

Windows Server 2008

Windows Server 2008 R2

Windows Small Business Server 2011


Vor der Installation des Norman MailScan für Exchange Plugins sind folgende Dinge zu erledigen:

Installieren Sie Norman Endpoint Protection auf dem Exchange Server.

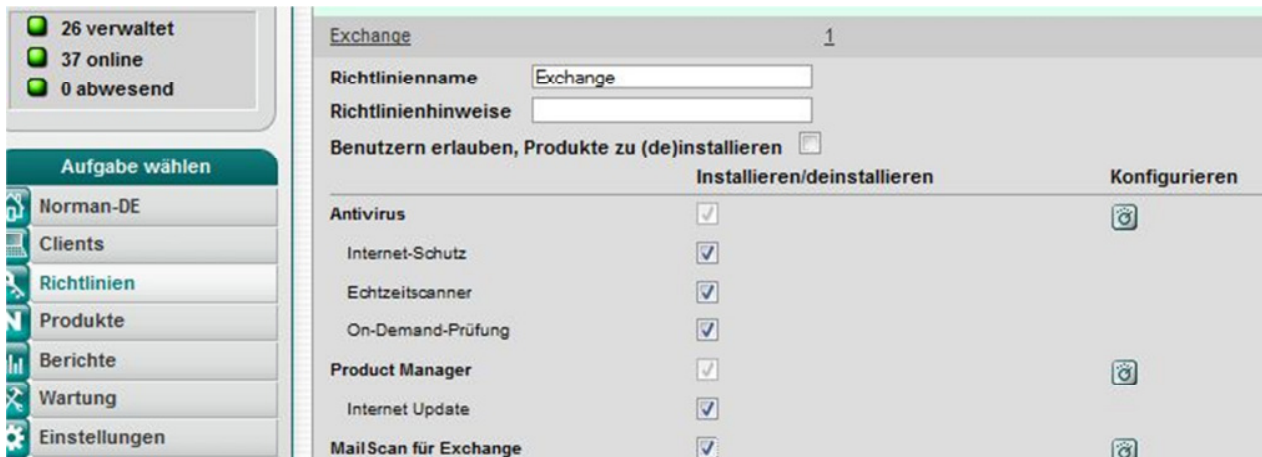
Vergewissern Sie sich zunächst, dass im Endpoint Manager unter „**Produkte**“ -> „**Lizenzen**“ „MailScan für Exchange“ ausgewählt ist. Setzen Sie ggf. den Haken und machen Sie ein Internet Update ihrer Installation. Sollte der Punkt „MailScan für Exchange“ nicht auftauchen, ist die genutzte Norman Lizenz nicht dafür gültig. Kontaktieren Sie in einem solchen Fall bitte Ihren zuständigen Vertriebspartner oder Händler.

The screenshot shows the Norman Endpoint Manager web interface. On the left, there is a sidebar with a 'Risikostufe' (Risk Level) indicator, an 'Aktueller Status' (Current Status) section showing 0 Alarms, 0 Fehler, 0 Warnungen, 1 nicht aktualisiert, and 6 offline, and an 'Aufgabe wählen' (Select Task) section with options like 'Norman-DE' and 'Clients'. The main content area is titled 'Produkte' (Products) and has tabs for 'Lizenzen' (Licenses), 'Sprachen' (Languages), and 'Plattformen' (Platforms). The 'Lizenzen' tab is selected, showing instructions to use the Internet Update function and a list of products with checkboxes. The products listed are: Antivirus, Product Manager, Norman Endpoint Manager, Network Protection, and MailScan für Exchange. A button 'Ausgewählte Produkte aktualisieren' is located below the list.




Prüfen Sie nun, das Sie für den Exchange Server am Norman Endpoint Manager Server eine eigene Richtlinie erstellen und diese dem Server zu zu weisen (Siehe auch Punkt 11 der Kurzanleitung).

 Hinweis: Wenn der Exchange Server auch der Norman Endpoint Manager (NEM) Verteilungsserver ist, nutzen Sie die Richtlinie des NEM Server.

In der Richtlinie des Exchange Servers vergewissern Sie sich, dass der Haken bei "MailScan für Exchange" gesetzt ist, damit das Plugin auf dem Exchange Server installiert wird.




The screenshot shows the Norman Endpoint Manager interface. On the left, there is a sidebar with navigation options: 'Norman-DE', 'Clients', 'Richtlinien', 'Produkte', 'Berichte', 'Wartung', and 'Einstellungen'. The main area displays the configuration for an 'Exchange' policy. The 'Richtlinienhinweise' field is empty. Below, there is a table with columns for 'Antivirus', 'Product Manager', and 'MailScan für Exchange'. The 'MailScan für Exchange' checkbox is checked, and there are 'Installieren/deinstallieren' and 'Konfigurieren' buttons for each category.

	Installieren/deinstallieren	Konfigurieren
Antivirus	<input checked="" type="checkbox"/>	
Internet-Schutz	<input checked="" type="checkbox"/>	
Echtzeitscanner	<input checked="" type="checkbox"/>	
On-Demand-Prüfung	<input checked="" type="checkbox"/>	
Product Manager	<input checked="" type="checkbox"/>	
Internet Update	<input checked="" type="checkbox"/>	
MailScan für Exchange	<input checked="" type="checkbox"/>	

Sobald der Exchange Server den Richtlinien Haken für „Mailscan für Exchange“ aktiviert hat, wird das Plugin auf ihm installiert. Der Norman Zanda Dienst prüft zunächst, ob auf dem Server eine unterstützte Exchange Version installiert ist, ist dieses der Fall, wird Mailscan für Exchange installiert. Wenn der Haken aus der Richtlinie entfernt wird, wird das Plugin wieder deinstalliert. Achten Sie auch darauf, dass der Haken in der Richtlinie bei „**Benutzern erlauben, Produkte zu (de)installieren**“ nicht gesetzt ist, da die Plugin Installation ansonsten nicht startet.

Nach der Installation werden die Einstellungen des Exchange Plugins vom Norman Endpoint Manager über die Exchange Server Richtlinie gemanaged.

 Hinweis: Bitte beachten Sie, dass die Einstellungen für die Exchange Richtlinie welche Sie für „MailScan für Exchange“ tätigen, Auswirkungen auf den kompletten Store von Exchange haben, da das Plugin in der VSAPI für MS Exchange hängt. Das bedeutet, dass die Einstellungen nicht nur auf neue eMails greift, sondern auf alle bisher im Store vorhandenen eMails.

Weiter Hinweise zu Norman MailScan für Microsoft Exchange finden Sie in unserem Norman Endpoint Protection Admin Handbuch unter:

http://www.norman.com/support/endpoint_protection/de

Notizen:
