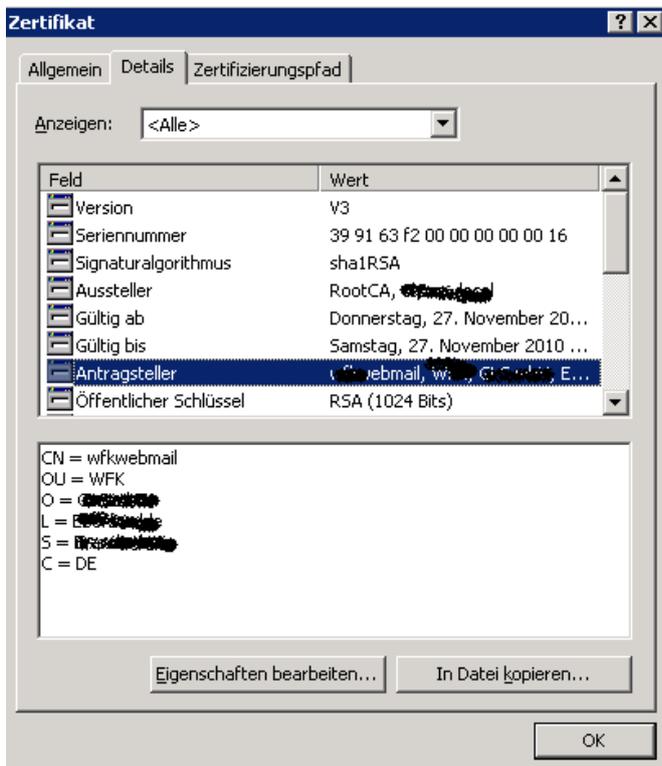
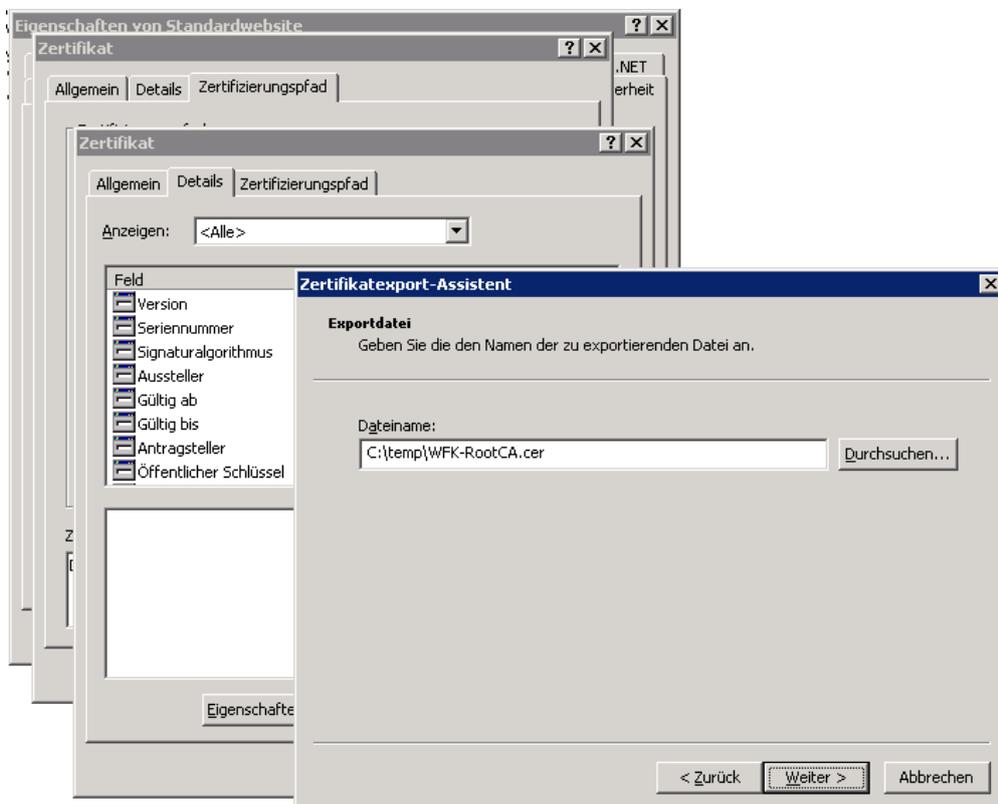




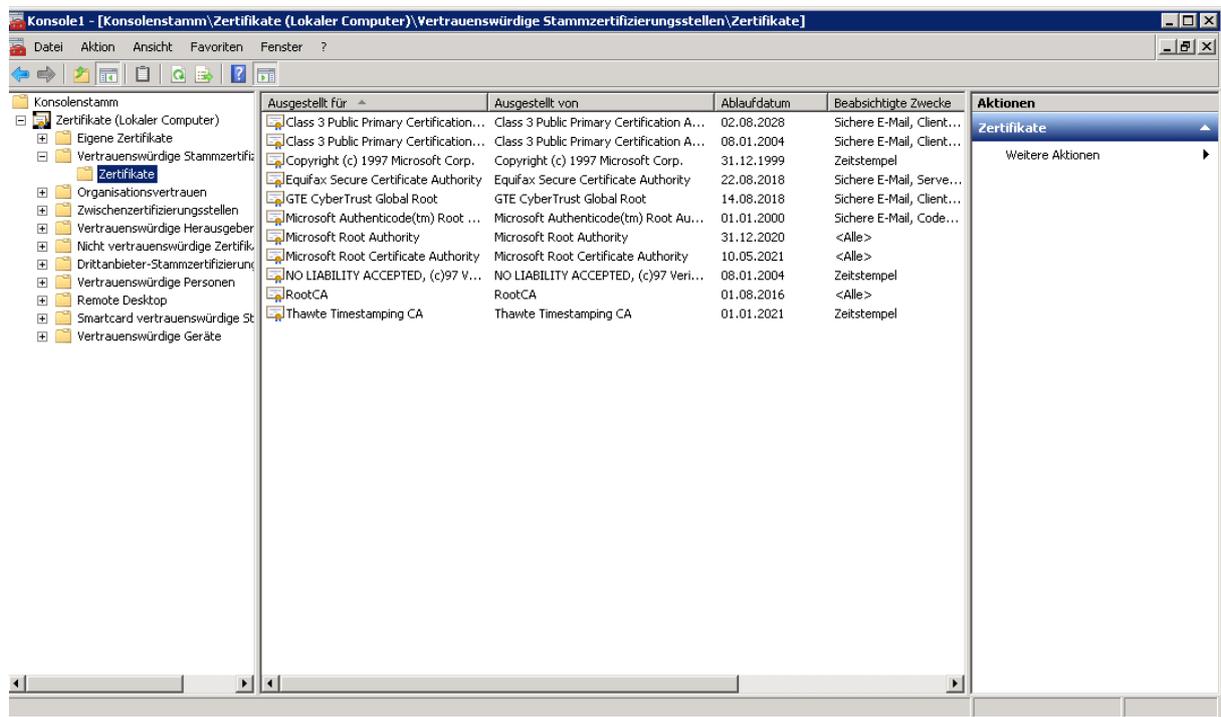
Ausgestellt auf WFKWEBMAIL



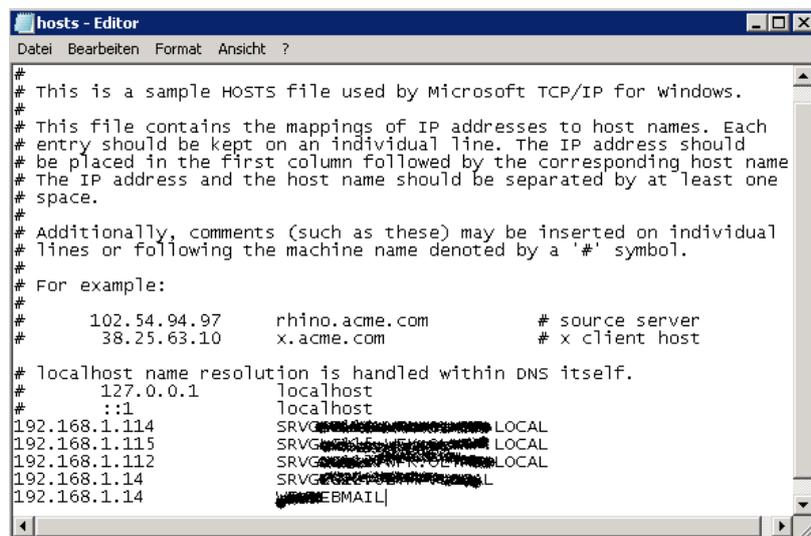
Root CA Zertifikat exportieren und am TMG importieren, da der TMG Mitglied einer Arbeitsgruppe ist



## RootCA Zertifikat am TMG importieren



## Namensauflösung am TMG fuer den Mailserver und Active Sync setzen



## .KEY Zertifikat von RAPIDSSL in .PFX umwandeln

SSL Converter - Convert SSL Certificates to different formats - Windows Internet Explorer

https://www.sslshopper.com/ssl-converter.html

File Edit View Favorites Tools Help

SSL Converter - Convert SSL Certificates to different ...

SSL Converter

Most Popular

- How to use SSL Certificates with Exchange 2007
- SSL Host Headers in IIS 7
- More Discussion About How Firefox 3 Handles SSL Certificates
- Free SSL Certificates from a Free Certificate Authority
- SSL Certificate for Mozilla.com Issued Without Validation

SSL Quick Search

- Cheap SSL Certificates
- Cheapest Unchained Certificates
- Cheapest EV Certificates
- UC Certificates
- Special Deals
- Best SSL Wildcard Certificates

There was a problem converting that certificate. It may be corrupt or it may be in a different format than the one you selected. You can try using a different format or running the OpenSSL commands on your own machine. The private key also may not match the certificate that you uploaded.

Certificate File to Convert: C:\Temp\2010\_...de.crt Browse...

Private Key File: C:\Temp\2010\_...de.key Browse...

Chain Certificate File (optional): Browse...

Chain Certificate File 2 (optional): Browse...

Type of Current Certificate: Standard PEM Detected type from file extension

Type To Convert To: PFX/PKCS#12

PFX Password: .....

Convert Certificate

⚠ Your private key is intended to remain on the server. While we try to make this process as secure as possible by using SSL to encrypt the key when it is sent to the server, for complete security, we recommend that you manually convert the certificate on your server using the OpenSSL commands below.

Da ist es:

File Download

Do you want to open or save this file?

Name: 2010\_...pfx  
Type: Personal Information Exchange  
From: [www.sslshopper.com](http://www.sslshopper.com)

Open Save Cancel

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. [What's the risk?](#)

## Das neue Zertifikat am TMG importieren

**Zertifikatimport-Assistent**

**Kennwort**

Der private Schlüssel wurde mit einem Kennwort geschützt, um die Sicherheit zu gewährleisten.

Geben Sie das Kennwort für den privaten Schlüssel ein.

Kennwort:  
[.....]

Hohe Sicherheit für den privaten Schlüssel aktivieren. Wenn Sie diese Option aktivieren, werden Sie immer dann, wenn der private Schlüssel von einer Anwendung verwendet wird, zur Kennworteingabe aufgefordert.

Schlüssel als exportierbar markieren. Dadurch können Sie Ihre Schlüssel zu einem späteren Zeitpunkt sichern bzw. überführen.

Alle erweiterten Eigenschaften mit einbeziehen.

Weitere Informationen über [das Sichern privater Schlüssel](#)

< Zurück   Weiter >   Abbrechen

Da ist es

Konsole1 - [Konsolenstamm\Zertifikate (Lokaler Computer)\Eigene Zertifikate\Zertifikate]

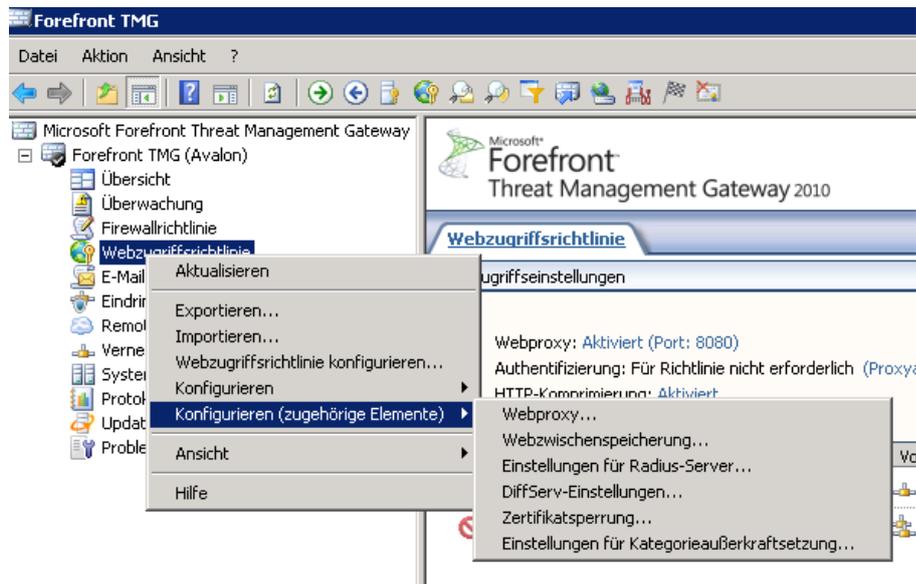
Datei   Aktion   Ansicht   Favoriten   Fenster   ?

Ausgestellt für	Ausgestellt von	Ablaufdatum	Beabsichtigte Zwecke	Aktionen
*.class	Equifax Secure Certificate Authority	01.04.2011	Serverauthentifizieru...	Zertifikate Weitere Aktionen

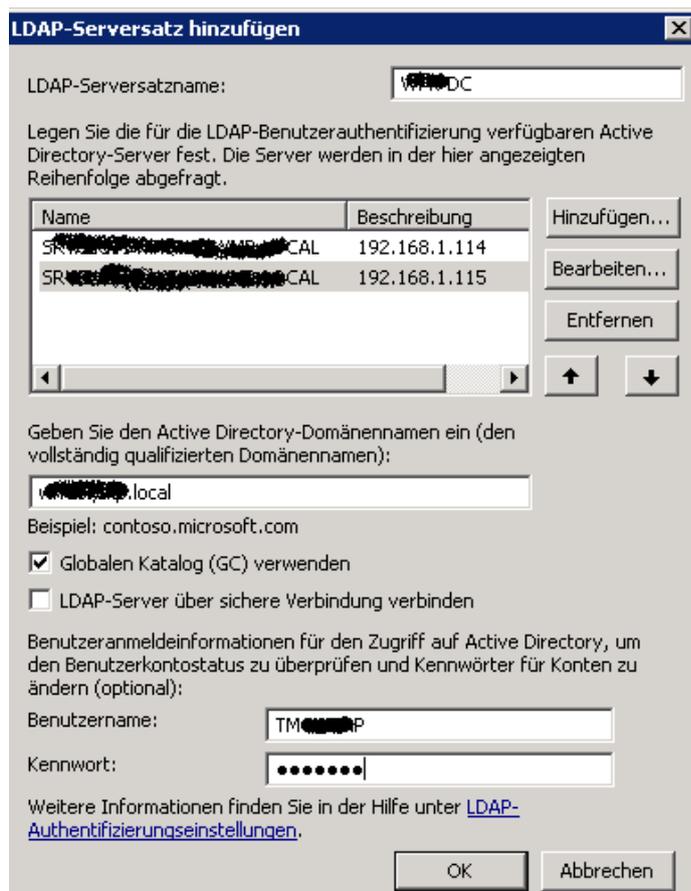
Konsolenstamm

- Zertifikate (Lokaler Computer)
  - Eigene Zertifikate
    - Zertifikate
      - Vertrauenswürdige Stammzertif...
      - Organisationsvertrauen
      - Zwischenzertifizierungsstellen
      - Vertrauenswürdige Herausgeber
      - Nicht vertrauenswürdige Zertifik...
      - Drittanbieter-Stammzertifizierung
      - Vertrauenswürdige Personen
      - Remote Desktop
      - Zertifikatregistrierungsanforderu...
      - Smartcard vertrauenswürdige St...
      - Vertrauenswürdige Geräte

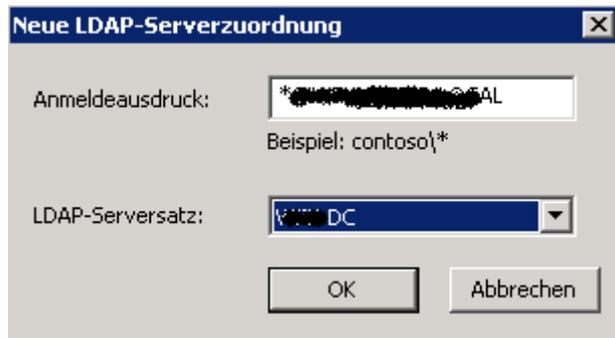
## LDAP(S)-Server fuer TMG konfigurieren



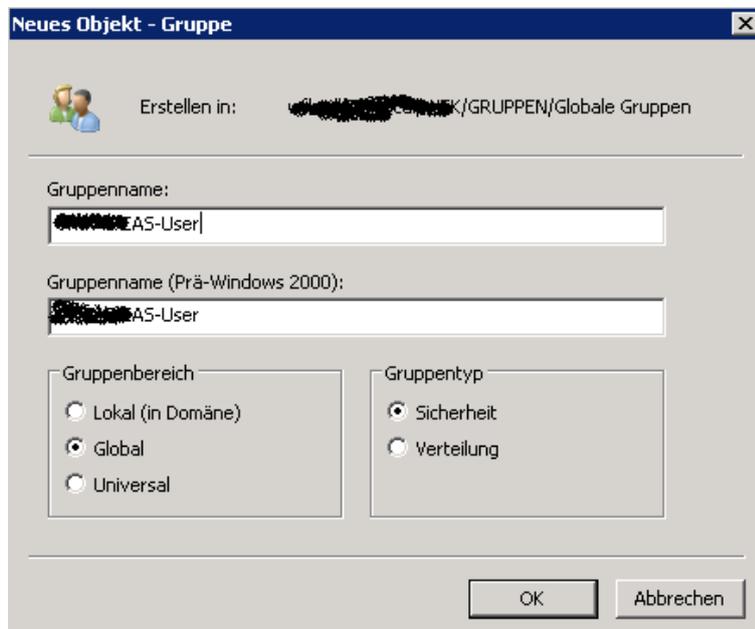
## LDAP Server Set + User angeben



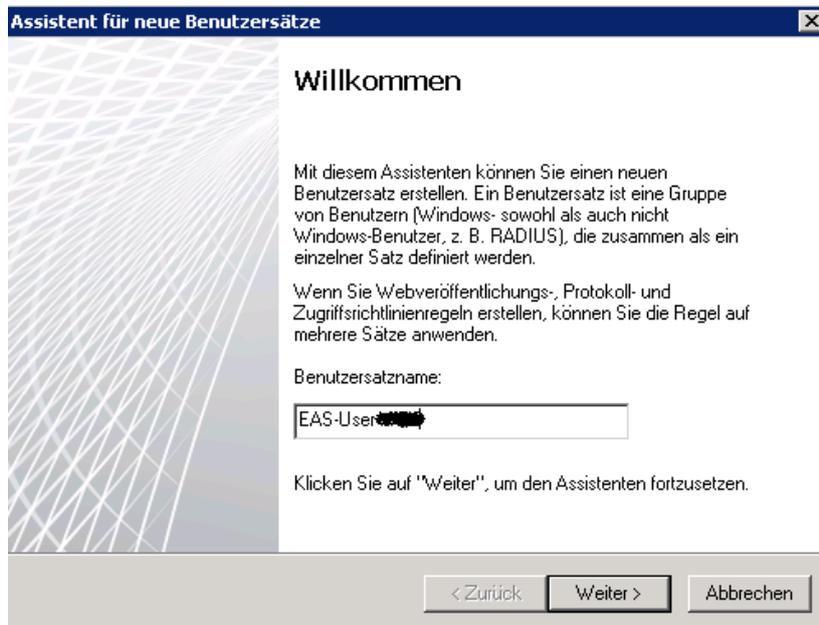
Anmeldeausdrücke für UPN und NT-Style konfigurieren



Windows Gruppe zur Nutzung von EAS anlegen und die berechtigten Benutzer hinzufügen



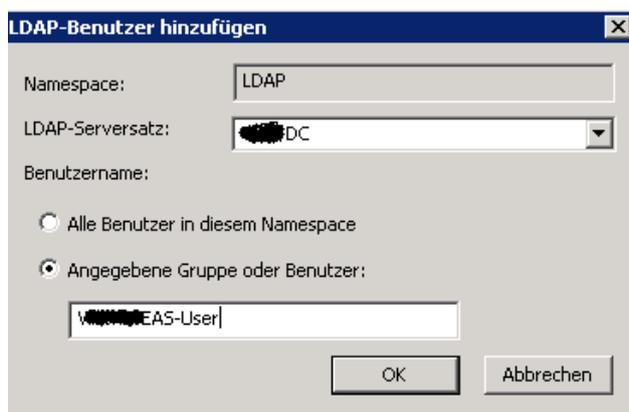
## Neue LDAP-Benutzergruppe am TMG Server anlegen



## LDAP Namespace



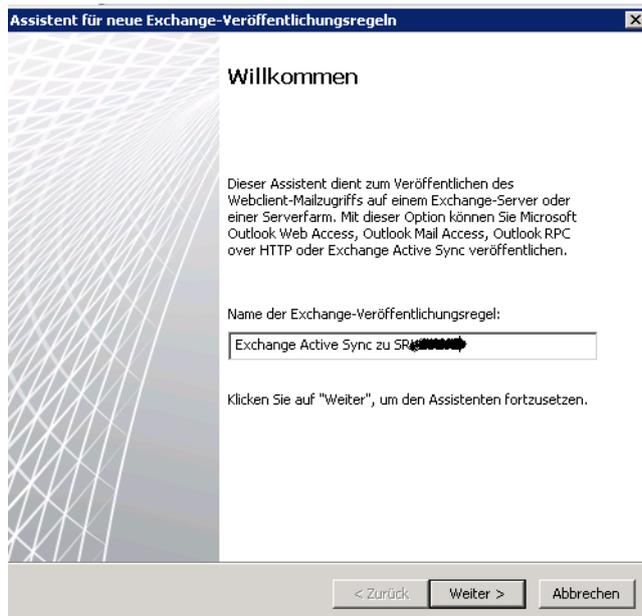
## Globale AD-Gruppe angeben



## Abfrage ins AD mit dem LDAP Account



## Neue Veröffentlichungsregel fuer Exchange Webclientzugriff und RPC ueber HTTPS



**Assistent für neue Exchange-Veröffentlichungsregeln**

**Dienste auswählen**  
Wählen Sie die Dienste aus, die auf diesem Mailserver veröffentlicht werden sollen.

Exchange-Version: Exchange Server 2003

Webclient-E-Mail-Dienste:

- Outlook Web Access
- Outlook RPC/HTTP(s)
  - Zusätzliche Ordner auf Exchange Server for Outlook 2007-Clients veröffentlichen
- Outlook Mobile Access
- Exchange ActiveSync

< Zurück Weiter > Abbrechen

Einzelne Webseite oder Lastenausgleich veröffentlichen

SSL verwenden

Interner Sitename

**Assistent für neue Exchange-Veröffentlichungsregeln**

**Interne Veröffentlichungsdetails**  
Geben Sie den internen Namen der Exchange-Site oder des Exchange-Servers an, auf der/dem die Veröffentlichung erfolgen soll.

Interner Sitename:

Der interne Sitename ist der Name der Website, die Sie, so wie sie intern angezeigt wird, veröffentlichen möchten. Normalerweise handelt es sich hierbei um den Namen, den interne Benutzer zum Aufrufen der Website in die Browser eingeben.

 Der interne Sitename muss mit dem allgemeinen Namen oder dem alternativen Antragstellernamen (Subject Alternative Name, SAN) für das Zertifikat übereinstimmen, das an die zu veröffentlichen Website gebunden ist.

Wenn Forefront TMG den internen Sitenamen nicht auflösen kann, kann Forefront TMG mithilfe des Computernamens oder der IP-Adresse des Servers eine Verbindung herstellen, der als Host für die Site dient.

Name oder IP-Adresse eines Computers verwenden, um eine Verbindung zum veröffentlichten Server herzustellen

Computername oder IP-Adresse:

< Zurück Weiter > Abbrechen

## Oeffentlicher Name

**Assistent für neue Exchange-Veröffentlichungsregeln**

**Details des öffentlichen Namens**  
Geben Sie den öffentlichen Domännennamen (FQDN) oder die IP-Adresse an, die Benutzer eingeben sollen, um die veröffentlichte Site zu erreichen.

Anforderungen annehmen für:    
Nur Anforderungen für diesen öffentlichen Namen oder diese IP-Adresse werden an die veröffentlichte Site weitergeleitet.

Öffentlicher Name:   
Beispiel: www.contoso.com

< Zurück Weiter > Abbrechen

## Neuer Weblistener

**Assistent für neue Exchange-Veröffentlichungsregeln**

**Weblistener auswählen**  
Der Weblistener bestimmt die IP-Adressen und den Port, auf dem der Forefront TMG eingehende Webanforderungen abhört.

Weblistener:   
  
Listeneigenschaften:

Eigenschaft	Wert

Von / Listener Nach  
Alle Netzwerk... Alle

**Assistent für neue Weblistenerdefinition**

**Willkommen**

Mit diesem Assistenten können Sie einen neuen Weblistener erstellen. Weblistener legen fest, wie Forefront TMG eingehende Webanforderungen von den Clients empfangen und authentifizieren soll.

Weblistenname:

Klicken Sie auf "Weiter", um den Assistenten fortzusetzen.

< Zurück Weiter > Abbrechen

## SSL verwenden

**Assistent für neue Weblistenereffinition**

**Sicherheit der Clientverbindung**  
Wählen Sie die Art der Verbindungen aus, die dieser Weblistener mit Clients herstellen soll.

Sichere SSL-Verbindungen mit Clients erforderlich

Forefront TMG veröffentlicht die Server ausschließlich über HTTPS an die Clients (empfohlen).

Keine sicheren SSL-Verbindungen mit Clients erforderlich

Forefront TMG veröffentlicht die Server über HTTP. Clientanmeldeinformationen werden unverschlüsselt an den Forefront TMG-Computer gesendet.

 Bei der Veröffentlichung über SSL muss ein SSL-Serverzertifikat mit der entsprechenden Bezeichnung auf dem Forefront TMG-Computer installiert sein.

< Zurück   Weiter >   Abbrechen

## Weblistener ist INTERN bei Single NIC Szenario

**Assistent für neue Weblistenereffinition**

**Weblistener-IP-Adressen**  
Geben Sie die Forefront TMG-Netzwerke und die IP-Adressen dieser Netzwerke an, die für eingehende Webanforderungen empfängsbereit sein sollen.

In diesen Netzwerken auf eingehende Webanforderungen achten:

Name	Ausgewählte IPs
<input type="checkbox"/> Extern	<Alle IP-Adressen>
<input checked="" type="checkbox"/> Intern	<Alle IP-Adressen>
<input type="checkbox"/> Lokaler Host	<Alle IP-Adressen>
<input type="checkbox"/> Quarantäne-VPN-Clients	<Alle IP-Adressen>
<input type="checkbox"/> VPN-Clients	<Alle IP-Adressen>

IP-Adressen auswählen...

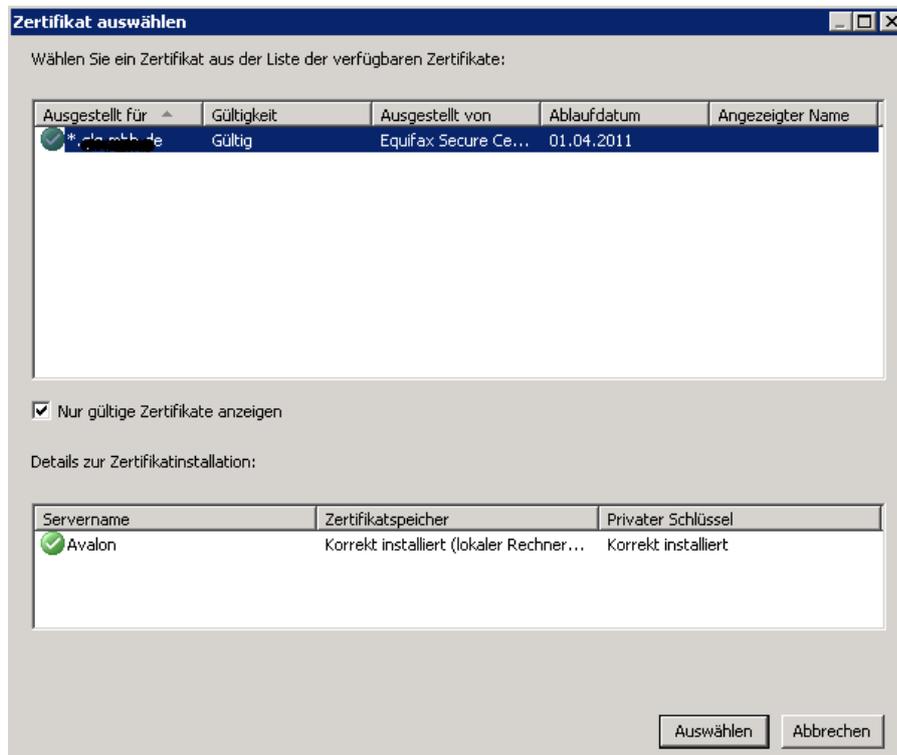
Forefront TMG komprimiert die Inhalte, die über diesen Weblistener an die Clients gesendet werden, sofern die Clients, die die Inhalte angefordert haben, die Komprimierung unterstützen.

< Zurück   Weiter >   Abbrechen

Oeffentliche IP-Adresse auswaehlen, falls in Zukunft mehrere IP gebunden sind



Zertifikat auswaehlen



## HTTP Basic Authentication mit LDAP

**Assistent für neue Weblistenereinstellung** ✕

**Authentifizierungseinstellungen**  
Legen Sie fest, wie Clients die Authentifizierung bei Forefront TMG vornehmen sollen und wie Forefront TMG die Anmeldeinformationen überprüfen soll.

Legen Sie fest, wie die Clients die Anmeldeinformationen an Forefront TMG übermitteln

HTTP-Authentifizierung

Standard     Digest     Integriert

Legen Sie fest, wie Forefront TMG die Client-Anmeldeinformationen überprüfen soll:

Windows (Active Directory)     RADIUS OTP  
 LDAP (Active Directory)     RSA SecurID  
 RADIUS

< Zurück    Weiter >    Abbrechen

## Basic Authentication

**Assistent für neue Exchange-Veröffentlichungsregeln** ✕

**Authentifizierungsdelegierung**  
Authentifizierungsdelegierung ist die Methode, mit der Forefront TMG die Sitzung authentifiziert, die mit der veröffentlichten Site geöffnet wird.

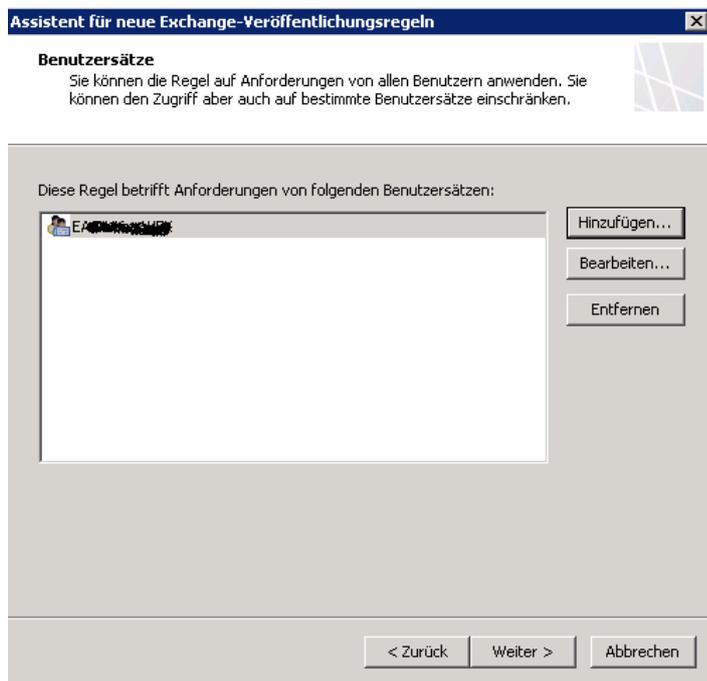
Legen Sie die Methode fest, mit der Forefront TMG sich beim veröffentlichten Webserver authentifizieren soll:

Standardauthentifizierung

Beschreibung  
Forefront TMG verwendet die Standardauthentifizierung, um den Client beim veröffentlichten Webserver zu authentifizieren. Der veröffentlichte Webserver muss so konfiguriert sein, dass die Standardauthentifizierung akzeptiert wird.

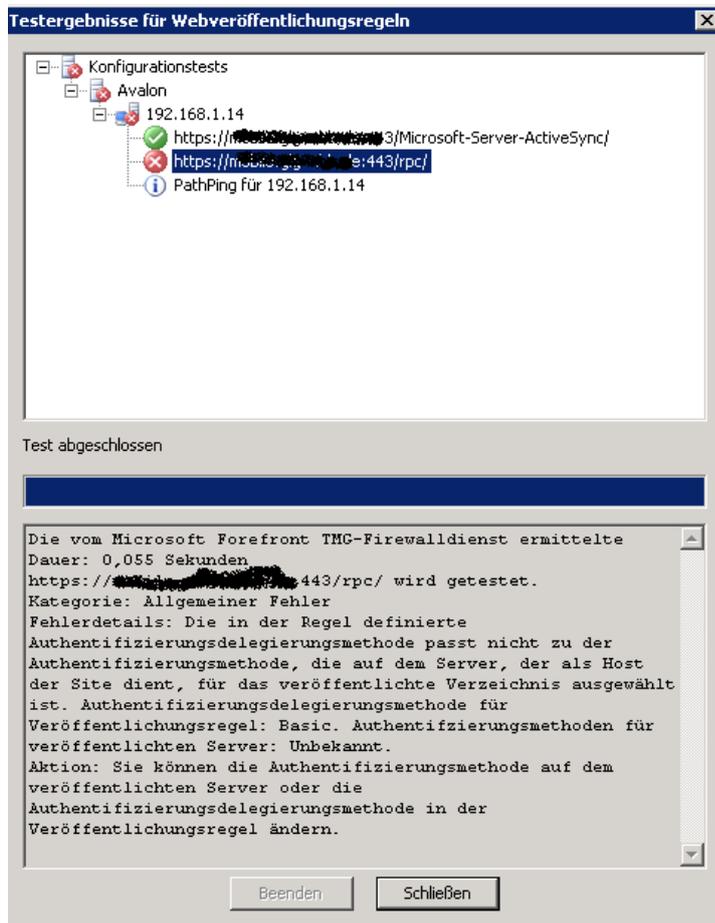
< Zurück    Weiter >    Abbrechen

## LDAP Benutzersatz auswahlen



## Konfiguration uebernehmen

## Regel testen

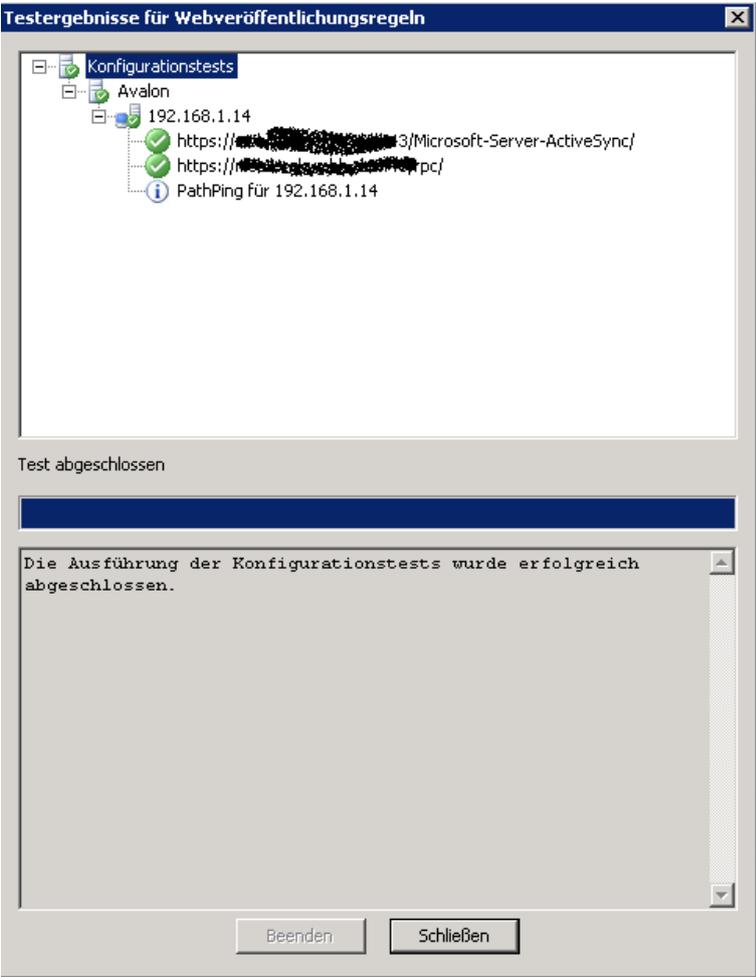


# Basic Authentication im RPC Verzeichnis auf dem Exchange Server erlauben

The screenshot displays the IIS Manager interface with the following components:

- Internetinformationsdienste-Manager:** The main application window showing a tree view on the left with 'Rpc' selected under 'Webdienste'.
- Eigenschaften von Rpc:** A dialog box with tabs for 'Benutzerdefinierte Fehler', 'BITS-Servererweiterungen', and 'ASP.NET'. The 'Authentifizierung und Zugriffsteuerung' section is active, showing options for anonymous access, IP restrictions, and secure communication.
- Authentifizierungsmethoden:** A dialog box where 'Anonymen Zugriff aktivieren' is checked. Under 'Authentifizierter Zugriff', 'Standardauthentifizierung (Kennwort wird als Klartext gesendet)' is selected. The 'Standarddomäne' and 'Bereich' fields are empty.
- IIS-Manager:** A warning dialog box with a yellow triangle icon. The text reads: 'Mit der ausgewählten Authentifizierungsmethode werden Kennwörter ohne Datenverschlüsselung im Netzwerk übertragen. Die Systemsicherheit kann gefährdet werden, wenn ein anderer Benutzer versucht, ein Protokollanalyseprogramm zu verwenden, um Benutzerkennwörter während der Authentifizierung zu ermitteln. Weitere Informationen zur Benutzerauthentifizierung finden Sie in der Hilfe. Diese Warnung gilt nicht für HTTPS- oder SSL-Verbindungen.' Below the text, it asks 'Möchten Sie den Vorgang wirklich fortsetzen?' with 'Ja', 'Nein', and 'Hilfe' buttons.

# Erneuter Test nach Aenderung der Authentifizierung



# EAS Test

Microsoft Exchange Server Remote Connectivity Analyzer - Windows Internet Explorer

https://www.testexchangeconnectivity.com/Default.aspx

File Edit View Favorites Tools Help

Favorites TN\_FOREFRONT Forum MCSEBoard XING TV MCT Banking

Microsoft Exchange Server Remote Connectivity Anal...

## Microsoft® Exchange Remote Connectivity Analyzer

Select the test you want to run:

- Microsoft Exchange ActiveSync Connectivity Tests
  - Exchange ActiveSync
  - ActiveSync AutoDiscover
- Microsoft Exchange Web Services Connectivity Tests
  - Synchronization, Notification, Availability, and OOF
  - Service Account Access (Developers)
- Microsoft Office Outlook Connectivity Tests
  - Outlook: Anywhere (RPC over HTTP)
  - Outlook: AutoDiscover
- Internet Email Tests
  - Inbound SMTP Email
  - Outbound SMTP Email

[Next](#)

© 2009 Microsoft | [Forum](#) | [Version 1.0](#) | [Feedback](#) | [Privacy](#) | [Legal](#)

# Testen

Microsoft Exchange Server Remote Connectivity Analyzer - Windows Internet Explorer

https://www.testexchangeconnectivity.com/Default.aspx

File Edit View Favorites Tools Help

Favorites TN\_FOREFRONT Forum MCSEBoard XING TV MCT Banking

Microsoft Exchange Server Remote Connectivity Anal...

## Microsoft® Exchange Remote Connectivity Analyzer

### Exchange ActiveSync

Use Autodiscover to detect settings

Email Address:

Manually Specify Server Settings

ActiveSync Server:

Domain\Username (or UPN):

Password:

Confirm Password:

Synchronize All Items in Inbox folder

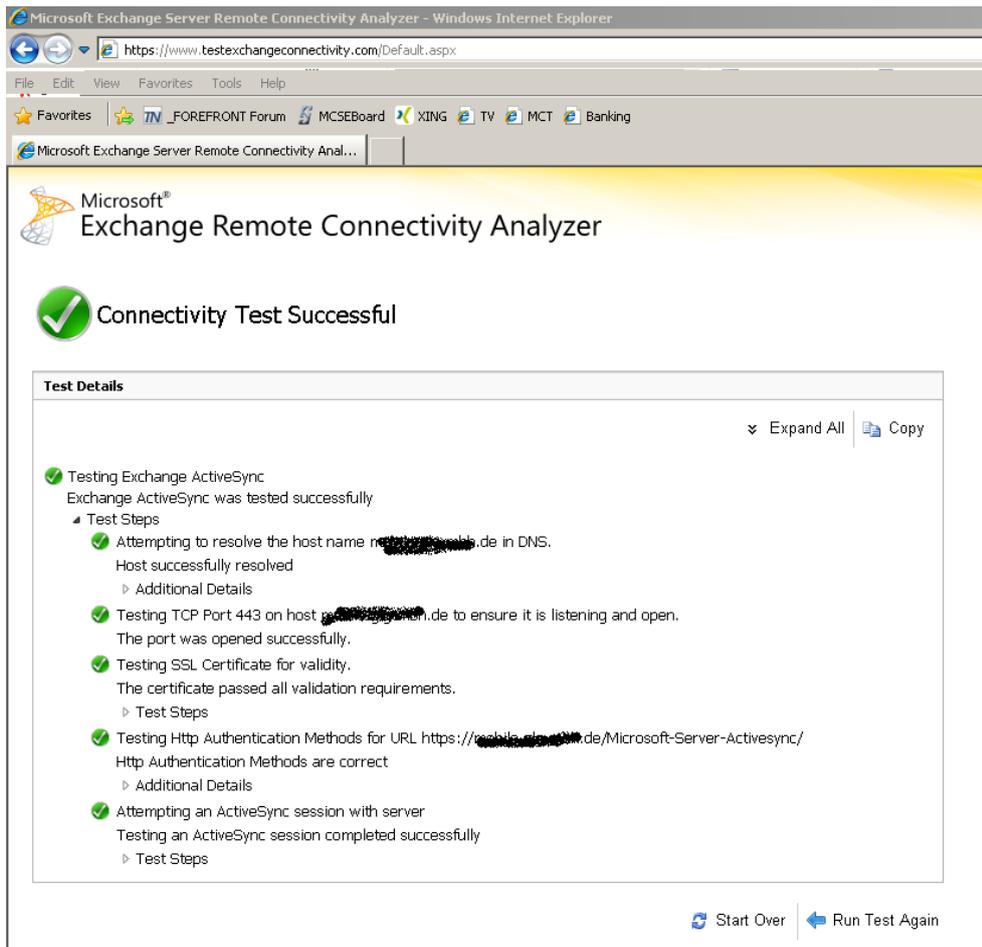
Ignore Trust for SSL

I understand that I must use the credentials of a working account from my Exchange domain to be able to test connectivity to it remotely; I acknowledge that I am responsible for the management and security of this account.

### Verification

 Enter the verification code from the left:

# Connectivity Test erfolgreich



The screenshot shows the Microsoft Exchange Remote Connectivity Analyzer interface in a Windows Internet Explorer browser. The browser's address bar displays the URL <https://www.testexchangeconnectivity.com/Default.aspx>. The page title is "Microsoft Exchange Server Remote Connectivity Analyzer".

The main heading of the page is "Microsoft Exchange Remote Connectivity Analyzer". Below this, a large green checkmark icon is followed by the text "Connectivity Test Successful".

A "Test Details" section is visible, containing the following information:

- Testing Exchange ActiveSync**  
Exchange ActiveSync was tested successfully
- Test Steps**
  - Attempting to resolve the host name **mobileclient101.de** in DNS.  
Host successfully resolved  
▷ Additional Details
  - Testing TCP Port 443 on host **mobileclient101.de** to ensure it is listening and open.  
The port was opened successfully.
  - Testing SSL Certificate for validity.  
The certificate passed all validation requirements.  
▷ Test Steps
  - Testing Http Authentication Methods for URL <https://mobileclient101.de/Microsoft-Server-Activesync/>  
Http Authentication Methods are correct  
▷ Additional Details
  - Attempting an ActiveSync session with server  
Testing an ActiveSync session completed successfully  
▷ Test Steps

At the bottom right of the "Test Details" section, there are two buttons: "Start Over" and "Run Test Again".