Net at Work
Building IT-Excellence.

NoSpamProxy Web Portal 11.1

Installationsanleitung

- Protection
- Encryption
- Large Files



Impressum

Alle Rechte vorbehalten. Dieses Handbuch und die darin beschriebenen Programme sind urheberrechtlich geschützte Erzeugnisse der Net at Work GmbH, Paderborn, Bundesrepublik Deutschland. Änderungen vorbehalten. Die in diesem Handbuch enthaltenen Informationen begründen keine Gewährleistungs- und Haftungsübernahme seitens der Net at Work GmbH. Die teilweise oder vollständige Vervielfältigung ist nur mit schriftlicher Genehmigung der Net at Work GmbH zulässig.
Copyright © 2015 Net at Work GmbH
Net at Work GmbH
Am Hoppenhof 32a
D-33104 Paderborn

Handelsmarken

Microsoft®, Windows®, Windows Server 2008®, Windows Server 2012® und Windows Server 2012 R2® sind eingetragene Handelsmarken der Microsoft Corporation. NoSpamProxy® ist eine eingetragene Handelsmarke der Net at Work GmbH. Alle anderen verwendeten Handelsmarken gehören den jeweiligen Herstellern / Inhabern.

15.10.2016

Inhalt

1. Einführung 4
   - Zertifikatslose Verschlüsselung mit dem Web Portal 4
   - Passwörter für PDF Mail 4
   - Large Files 4
2. Voraussetzungen und Vorbereitung der Installation 5
   - Voraussetzungen 5
   - Vorbereitungen 5
3. Hilfe und Unterstützung 6
4. Installation des Web Portals 7
   - Starten der Installation 7
     - Installationsordner 8
     - Konfiguration der Datenbank 8
     - IIS Konfiguration 9
     - Fehlende Windows Features 10
     - Ablauf der Installation 10
     - Abschluss der Installation 11
5. Installation eines SSL-Zertifikats im IIS 13
   - Kontrolle eines bestehenden Zertifikats 13
6. Nach der Installation 17
7. Upgrades 18
   - Upgrade Pfade 18
     - Updates von Version 11 auf Version 11.1 18
     - Updates von Version 10.1 auf Version 11 18
     - Updates von Version 10 auf Version 10.1 18
8. Fehlerbehandlung 19
   - Anmeldeseite nicht erreichbar - Fehler 500.21 19
9. Anhang 20
   - Anzeige des Zertifikatsspeichers des lokalen Computers 20

1. Einführung

Das Web Portal ist eine Erweiterung von NoSpamProxy Encryption und der "Large Files"-Funktion.

Zertifikatslose Verschlüsselung mit dem Web Portal

Beim Einsatz von NoSpamProxy Encryption können Sie das Web Portal über ein eigenes Setup installieren. Das Web Portal dient zur verschlüsselten Kommunikation mit Partnern, die keinen eigenen Verschlüsselungsschlüssel, wie zum Beispiel Zertifikate oder PGP-Schlüssel, besitzen. Die Nachrichten können über verschlüsselte PDF-Dokumente zum Empfänger gesandt werden. Antworten auf die Nachricht werden direkt über das Web Portal verfasst und zum ursprünglichen Sender zurückgesandt. Das Web Portal kommuniziert dabei mit der Intranet Rolle und kann so alle notwendigen Information erhalten, die es für die einwandfreie Funktion benötigt.

Passwörter für PDF Mail

Die Passwörter für PDF Mail können jetzt im Partner Knoten der Management Konsole hinterlegt werden. Diese Passwörter werden zu allen verbundenen Gateway Rollen und Web Portalen repliziert. Wenn das Passwort geändert wird, wird dem Partner eine E-Mail-Benachrichtigung über diese Änderung zugesandt. Falls kein Passwort für PDF Mail zur Verfügung steht, wird die ausgehende E-Mail in eine Warteschleife gesetzt.

Large Files

Große Dateien einfach, sicher und ohne Medienbruch versenden. Das Erweiterungsmodul Large Files erlaubt es Nutzern, beliebig große Dateien direkt aus Outlook heraus zu versenden. Anwender können auf diese Weise auch große Dateien, welche Beschränkungen des Mail-Programms überschreiten, ohne Medienbruch mit einem einzigen Klick versenden. Der Einsatz ist unkompliziert und mit dem Versand herkömmlicher Dateianhänge vergleichbar. Im Gegensatz zu den weit verbreiteten Cloud-basierten File-Transfer-Diensten werden die Daten über einen eigenen Web-Server des Kunden bereitgestellt und via SSL verschlüsselt übertragen. Das Sicherheitsniveau der Lösung wird damit auch kritischen Business-Anforderungen jederzeit gerecht.

2. Voraussetzungen und Vorbereitung der Installation

Voraussetzungen

Für die Installation des Web Portals sind die folgenden Voraussetzungen notwendig.

- Windows Server 2008 R2 oder höher.
- .NET Framework 4.5.2. Wird bei Bedarf während der Installation mit installiert.
- Microsoft SQL Server. Hier kann während der Installation entweder die kostenlose Microsoft SQL Server 2012 Express Edition installiert werden oder ein bereits vorhandener SQL Server genutzt werden. Das Web Portal unterstützt Microsoft SQL Server 2008 oder später in den Editionen Express, Standard oder Enterprise.

Vorbereitungen

In Abhängigkeit der geplanten Installationsumgebungen sind unterschiedliche Vorbereitungen notwendig.

- **Portfreigaben auf der Firewall**
  Wenn Sie eine Firewall verwenden, muss der für das Web Portal von NoSpamProxy vorgesehene Port freigegeben sein. In der Regel ist dies Port 443.
- **IIS auf einer Gateway Rolle**
  Wenn der IIS auf dem gleichen System wie eine der Gateway Rollen installiert ist, deaktivieren Sie bitte die SSL-Loopbackprüfung. Das Verfahren wird in der Microsoft Knowledge Base beschrieben http://support.microsoft.com/kb/896861. Bitte nutzen Sie die 'Methode 2'.
- **Web Portal in der DMZ / nicht im Active Directory**
  Wenn das Web Portal auf einem Rechner in der DMZ bzw. nicht im Active Directory installiert ist, deaktivieren Sie bitte die UAC-Remote-Restrictions. Das Verfahren wird in der Microsoft Knowledge Base beschrieben http://support.microsoft.com/kb/951016.

3. Hilfe und Unterstützung

Hilfe und Unterstützung für die Installation und den Betrieb von NoSpamProxy bekommen Sie von Net at Work in vielen Formen.

- **Trainingsvideos**
  Die Trainingsvideos bieten einen Überblick über verschiedene Bereiche und zeigen Konfigurationen, Schritt für Schritt, im konkreten Anwendungsfall.
- **Blog**
  Das Blog bietet tagesaktuelle Hinweise auf neue Produktversionen, Änderungsvorschläge für Ihre Konfiguration, Warnungen vor Kompatibilitätsproblemen und viele weitere Hinweise, die sie unterstützen. Die neuesten Nachrichten aus dem Blog werden auch auf der Startseite der NoSpamProxy Konfigurationskonsole eingeblendet, so dass Sie keine wichtigen Hinweise verpassen.
- **Knowledge Base**
  Die Knowledge Base enthält weiterführende technische Informationen zu speziellen Problemstellungen.
- **Support**
  Wenn Sie weitergehende Unterstützung brauchen, besuchen Sie unser Support-Webseite.

4. Installation des Web Portals

In diesem Kapitel wird die Installation des Web Portals für NoSpamProxy beschrieben.



Für Upgrades sollten Sie zusätzlich das Kapitel über Upgrades lesen, da sonst die einwandfreie Funktionalität nicht gewährleistet werden kann.

Starten der Installation

Vor dem Beginn der Installation sollten alle Windows-Programme geschlossen sein. Nach dem Start ermittelt die Installationsroutine die vorhandene Systemkonfiguration und schlägt automatisch Standardeinstellungen für die Installation vor (Bild 1). Die jeweiligen Einstellungen können sie am Ende jeder Zeile durch Anklicken von **Modify** einsehen und gegebenenfalls ändern.

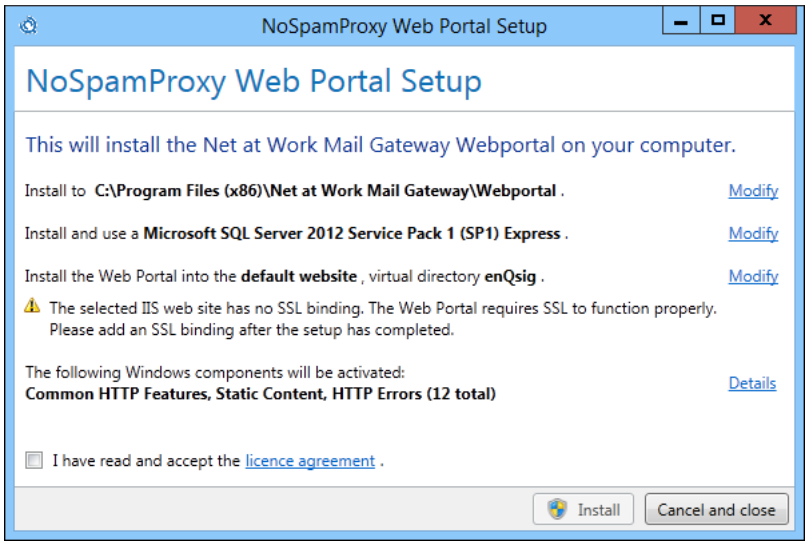


Bild 1: Zusammenfassung der Installationsoptionen bei Erstinstallation

Bei erneuter Installation des Web Portals oder bereits eingerichtetem Internet Information Server (IIS) zeigt die Übersicht andere Einstellungen an (Bild 2).

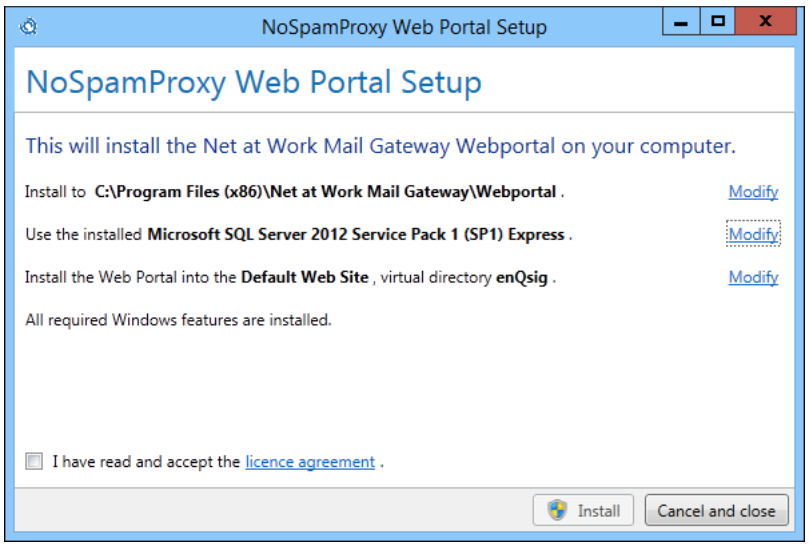


Bild 2: Zusammenfassung der Installationsoptionen bei bereits eingerichtetem IIS

Installationsordner

Legen Sie den Installationsordner für das Web Portal fest (Bild 3).

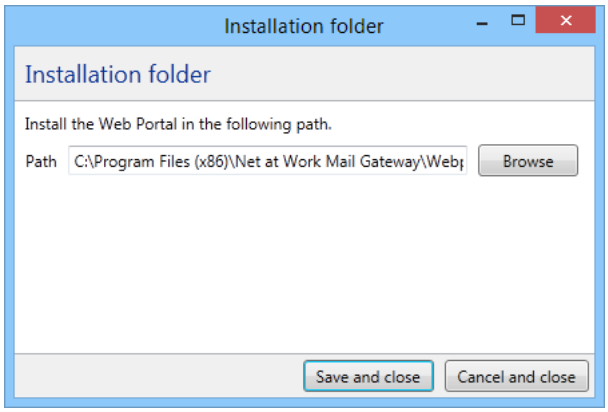


Bild 3: Auswahl des Installationsordners

Konfiguration der Datenbank

Das Web Portal benötigt eine Datenbank. Es kann entweder eine bestehende SQL-Server-Instanz verwendet werden oder das Setup installiert eine Microsoft SQL Server 2012 Express Edition (Bild 4).

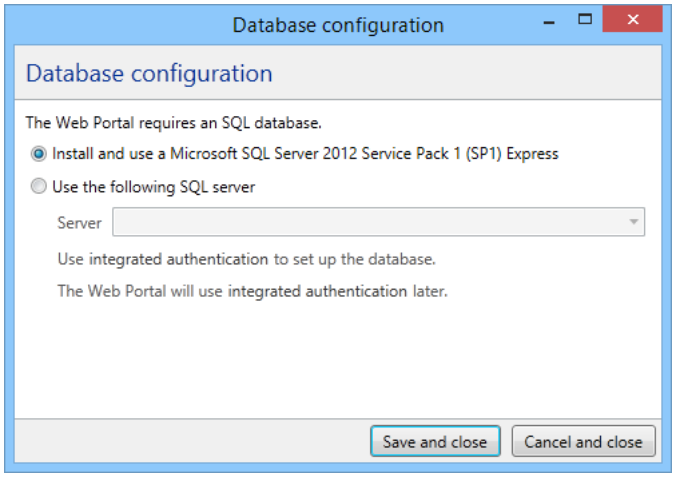


Bild 4: Auswahl der Datenbank

IIS Konfiguration

Wenn Sie das Web Portal in eine bestimmte Website oder ein bestimmtes virtuelles Verzeichnis installieren möchten, benötigen Sie dafür die "IIS Management Tools". Falls diese noch nicht installiert sind, bietet Ihnen das Setup die Installation in das virtuelle Verzeichnis "enQsig" innerhalb der Standard-Website an (Bild 5).

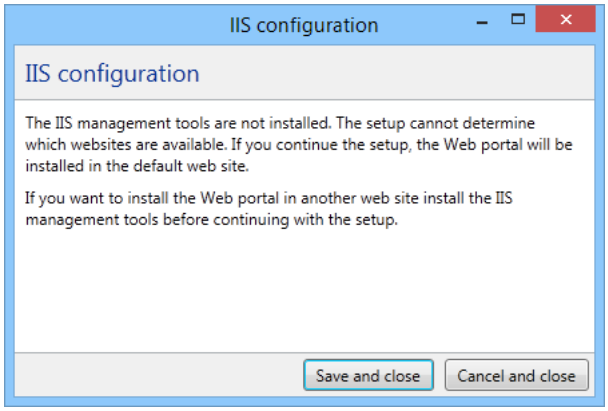


Bild 5: Anzeige, dass die Standardeinstellungen verwendet werden müssen

Wenn das Web Portal in eine andere Website oder ein anderes virtuelles Verzeichnis installiert werden soll, müssen Sie zuerst diese Installation abbrechen und die "IIS Management Tools" installieren. Danach können Sie die Website und das virtuelle Verzeichnis auswählen (Bild 6). Für jede der ausgewählten Websites wird angezeigt ob SSL bereits konfiguriert ist oder ob weitere Schritte notwendig sind.

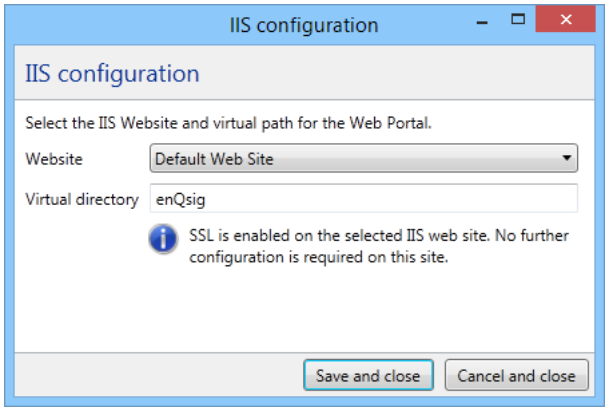


Bild 6: Auswahl der Website und des virtuellen Verzeichnisses in das das Web Portal installiert werden soll

Fehlende Windows Features

Wenn für die Installation Windows Features fehlen, werden diese automatisch aktiviert. Über **Details** können Sie alle Windows Features einsehen, die beim Abschluss der Installation aktiviert werden.

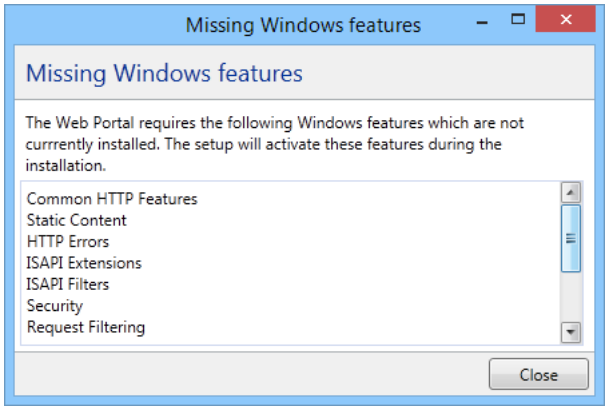


Bild 7: Anzeige der Windows Features die aktiviert werden

Ablauf der Installation

Nach dem Lesen und dem Akzeptieren der Lizenzbedingungen können Sie über **Install** die Installation starten. Jetzt werden alle, in der Übersicht angezeigten Schritte durchgeführt (Bild 8).

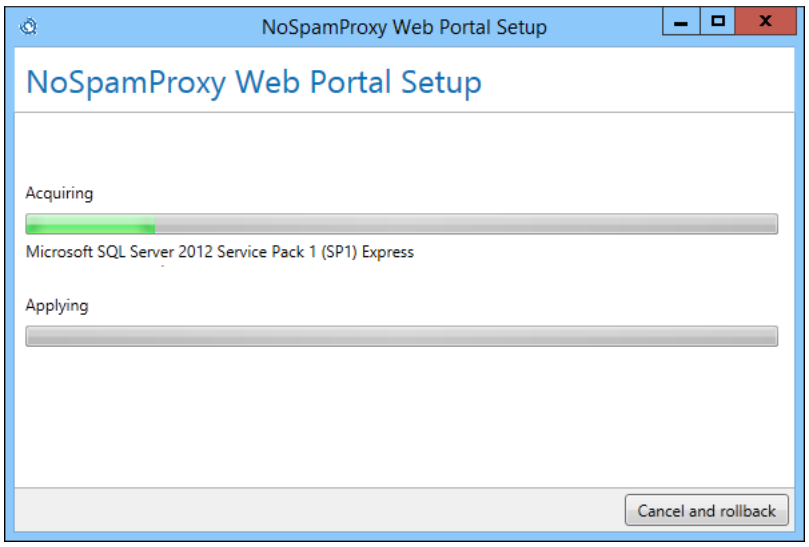


Bild 8: Anzeige des Installationsfortschritts

Abschluss der Installation

Nach der erfolgreichen Durchführung der Installation informiert Sie das Programm über weitere durchzuführende Schritte. Hier kann es noch notwendig sein einen SSL-Zugang für das Web Portal zu konfigurieren (Bild 9) oder, falls die Konfiguration schon durchgeführt wurde, nur noch den Rechner neu zu starten (Bild 10).

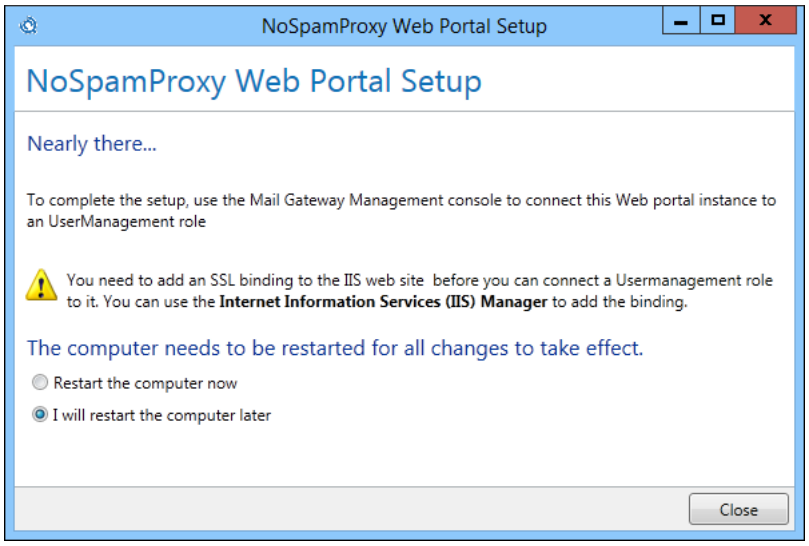


Bild 9: Abschluss der Installation ohne Bindung von SSL

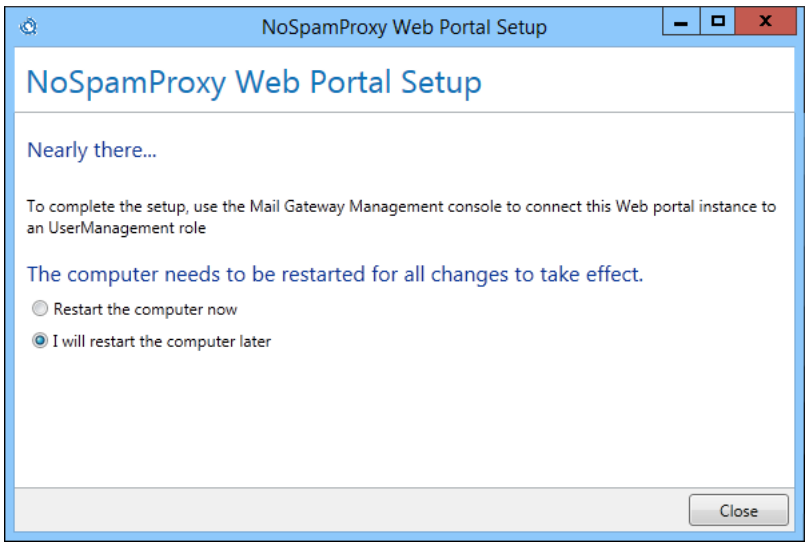


Bild 10: Abschluss der Installation mit erfolgreicher Bindung von SSL

5. Installation eines SSL-Zertifikats im IIS

Um den SSL-Zugang für das Web Portal zu konfigurieren, öffnen Sie bitte den "Internet Information Services (IIS) Manager" (Bild 11). Wählen Sie dort "Server Certificates" mit einem Doppelklick aus. Es öffnet sich die Liste der Server-Zertifikate (Bild 12). Sie können hier kontrollieren ob Ihr eigenes Zertifikat für den SSL-Zugang angezeigt wird.

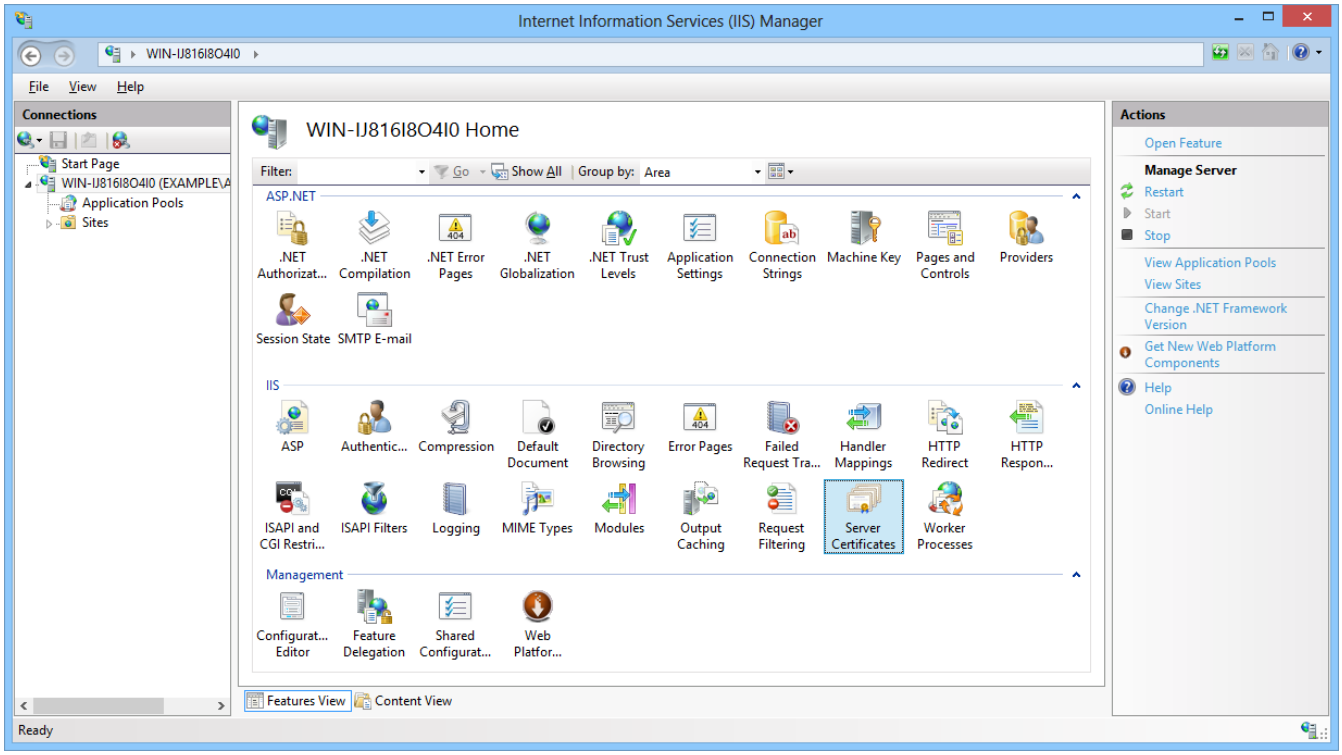


Bild 11: Der IIS-Manager

Kontrolle eines bestehenden Zertifikats

Die Server-Zertifikate müssen im Zertifikatsspeicher des lokalen Computer-Kontos hinterlegt sein. Hier liegen Sie im Speicher **Persönliche Zertifikate** / **Personal**. Alle für SSL nutzbaren Zertifikate werden in der Liste **Server Certificates** des IIS-Managers aufgeführt (Bild 12). Kontrollieren Sie in der Liste, ob Ihr Zertifikat darin aufgeführt wird.

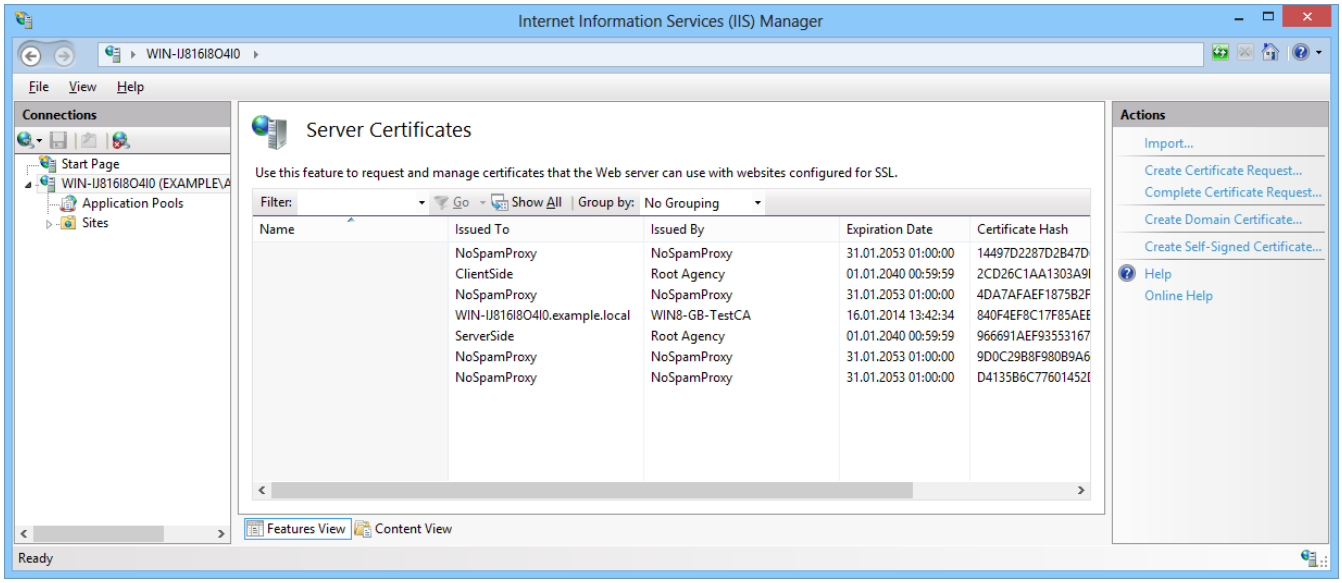


Bild 12: Die Liste aller Server-Zertifikate

Stellen Sie sicher, dass das verwendete SSL-Zertifikat unter anderem den exakten FQDN enthält, den Sie für den Aufruf des Web Portals verwenden. Wenn Sie das Web Portal zum Beispiel unter Verwendung der URL `https://portal.example.com/enqsig` betreiben wollen, muss der Name `portal.example.com` als Name im SSL-Zertifikat auftauchen. Des Weiteren muss sichergestellt sein, dass der Aussteller dieses Zertifikats auf dem Server der Intranet Rolle als vertrauenswürdige Stammzertifizierungsstelle eingetragen ist. Die Liste der vertrauenswürdigen Stammzertifizierungsstellen können sie im Zertifikatsspeicher des lokalen Computer-Kontos einsehen. Für einen schnellen Test, öffnen Sie auf dem Server der Intranet Rolle den Internet Explorer und geben die URL des Web Portals ein, in unserem Beispiel `https://portal.example.com/enqsig`. Die Seite muss sich ohne Fehlermeldungen öffnen. Wenn das der Fall ist, kann die Verbindung zum Web Portal in der Intranet Rolle ebenfalls erfolgreich hinzugefügt werden.

Wählen Sie jetzt im Baum des IIS-Managers unter **Sites** die Webseite, in die das Web Portal installiert wurde. Bei einer Standardinstallation heißt sie **Default Web Site**. (Bild 13) Wählen Sie auf der Seite über einen Rechtsklick **Edit Bindings...** oder über das **Actions**-Menü die Option **Bindings...**.

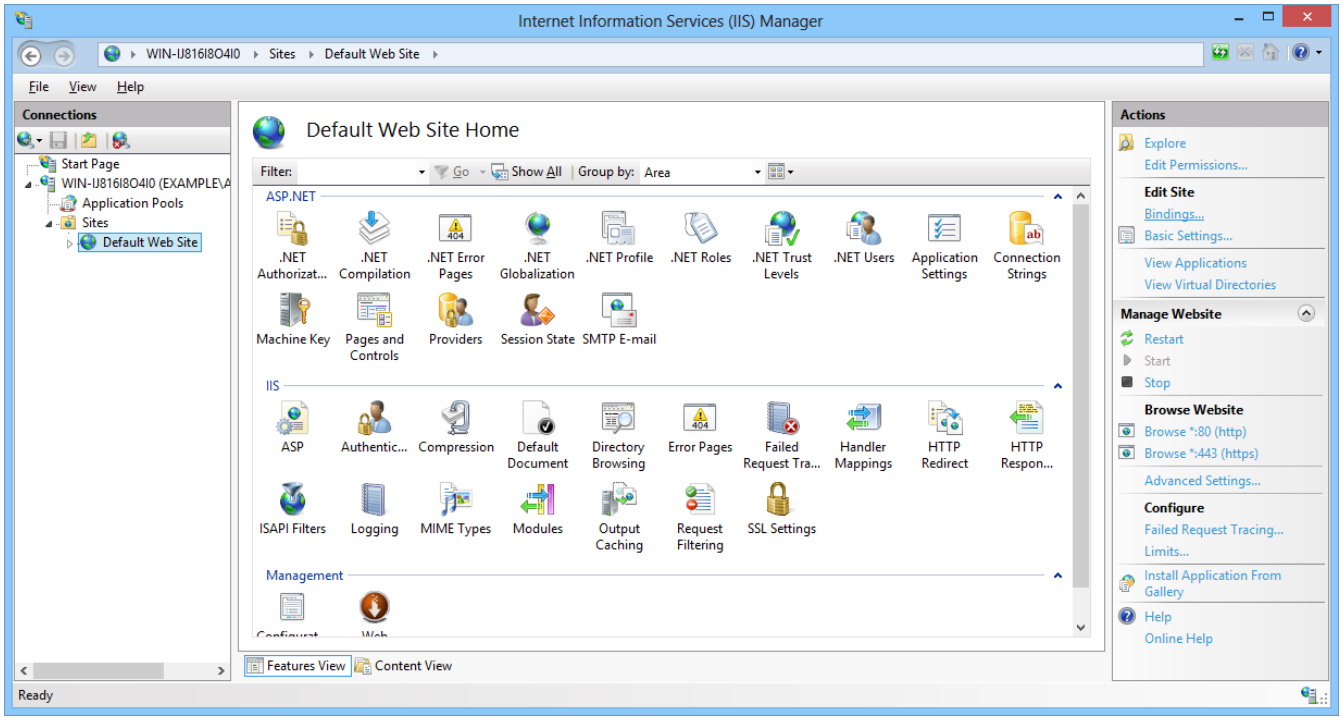


Bild 13: Die Konfiguration der Website des Web Portals

Fügen Sie jetzt über **Add** eine neue Bindung hinzu (Bild 14).

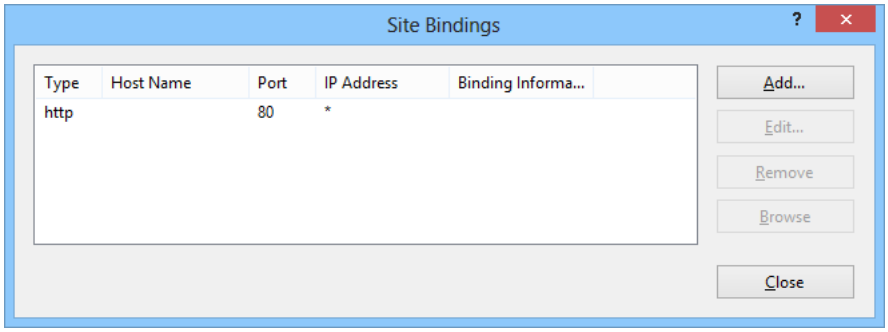


Bild 14: Die Liste aller Bindungen

Wählen Sie die gegebenenfalls eine bestimmte IP-Adresse, den Port 443 und das zuvor kontrollierte SSL-Zertifikat (Bild 15).

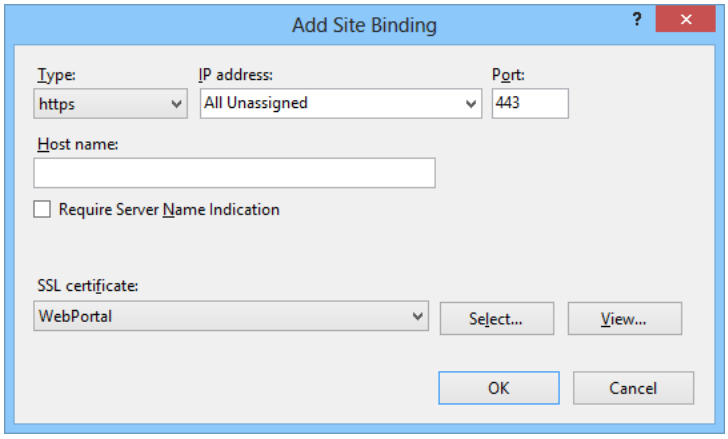


Bild 15: Erstellen einer neuen HTTPS-Bindung

Nach Abschluss des Dialogs erscheint die neue Site-Bindung in der Liste aller Bindungen der Website (Bild 16).

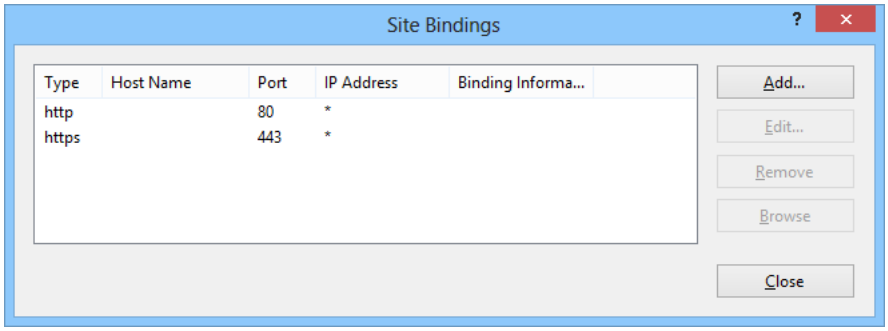


Bild 16: Die Liste aller Bindungen mit der neu erstellten HTTPS-Bindung

6. Nach der Installation

Nach Abschluss der Installation können Sie die Webseite des Web Portals über die bei der Installation angegebene Adresse aufrufen. Bei einer Standardinstallation ist diese:

```
https://<Rechnername>/enqsig
```

Sollte die Seite nicht aufrufbar sein, überprüfen Sie bitte die Konfiguration des Internet Information Servers. Schauen Sie danach in das Kapitel Fehlerbehandlung.

Bei erfolgreicher Installation erscheint die Anmeldeseite des Web Portals (Bild 17)

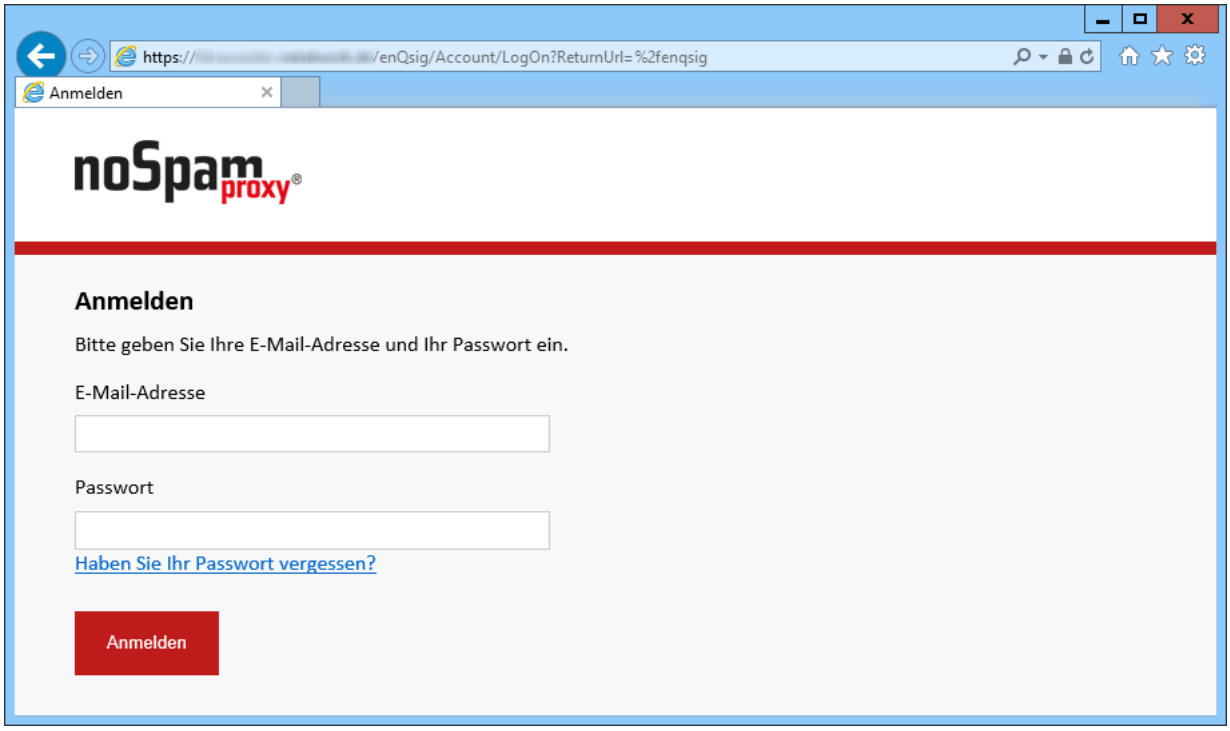


Bild 17: Der Anmeldebildschirm des Web Portals

Nun können Sie das Web Portal mit Ihrer Intranet Rolle verbinden. Öffnen Sie dazu die Verwaltungsoberfläche von NoSpamProxy. Im Knoten **Konfiguration**, **Gateway Komponenten** finden Sie den Abschnitt **Web Portal**. Dort können Sie die Verbindung konfigurieren.

Wenn Sie die Large Files für hochgeladene Dateien nutzen möchten und diese Dateien durch den CYREN-Dienst auf Viren überprüft werden sollen, ist noch ein weiterer Schritt notwendig. Dieser darf erst ausgeführt werden, wenn eine Verbindung zur Intranet Rolle hergestellt wurde. Öffnen sie einen Browser und navigieren Sie zu der folgenden Seite: `https://servername/enqsig/admin/configurecyren`. Geben Sie auf dieser Seite den Benutzernamen und das Kennwort eines Administratorenkontos ein. Durch diese Aktion wird der CYREN-Dienst konfiguriert. Das Portal ist nun einsatzbereit.

7. Upgrades



Wenn Sie ein Update von einer vorherigen Version des Web Portals durchführen, beachten Sie bitte unbedingt die folgenden Punkte.

- Sie müssen in den meisten Fällen einer Aktualisierung vor und nach der Installation manuelle Schritte durchführen, da sonst der reibungslose Betrieb des Web Portals nicht mehr gewährleistet ist. Beachten Sie dazu die Schritte im Abschnitt Upgrade Pfade. Die Abschnitte sind kumulativ, das heißt, dass Sie nacheinander die Abschnitte von Ihrer derzeit installierten Version bis zur aktuellen Version beachten müssen.
- Bitte kontrollieren Sie nach der Durchführung einer Programmaktualisierung in jedem Fall die Konfiguration Ihres Web Portals.

Upgrade Pfade

Je nachdem von welcher vorherigen Version Sie auf die aktuelle Version des Web Portals aktualisieren, müssen unterschiedliche Schritte durchgeführt werden.

Updates von Version 11 auf Version 11.1

Mit der Version 11.1 wird als SQL Server die Version 2008 vorausgesetzt. Aktualisieren Sie bitte Ihren SQL Server 2005 auf mindestens die Version 2008, bevor Sie das NoSpamProxy Update starten.

Beim Update von der Version 11 auf die Version 11.1 bleiben während des Updates alle Einstellungen und Benutzerinformationen erhalten.

Updates von Version 10.1 auf Version 11

Beim Update von der Version 10.1 auf die Version 11 bleiben während des Updates alle Einstellungen und Benutzerinformationen erhalten.

Updates von Version 10 auf Version 10.1

Beim Update von der Version 10 auf die Version 10.1 bleiben während des Updates alle Einstellungen und Benutzerinformationen erhalten.

8. Fehlerbehandlung

Anmeldeseite nicht erreichbar - Fehler 500.21

Falls die Anmeldeseite nicht angezeigt wird, sondern stattdessen der HTTP Fehler 500.21 ist wahrscheinlich ASP.NET 4.5.2 im IIS nicht richtig installiert bzw. registriert.



Bevor Sie das ASP.NET Framework 4.5.2 auf Ihrem Internet Server neu registrieren, überprüfen Sie bitte, ob das Framework mit eventuellen anderen Internetseiten, die über diesen Server bereitgestellt werden, kompatibel ist. Sichern Sie Ihr System und speziell die IIS-Konfiguration bevor Sie fortfahren.

Führen Sie eine erneute Installation mit dem folgenden Befehl durch:

```
%windir%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -i
```

9. Anhang

Anzeige des Zertifikatsspeichers des lokalen Computers

Um die Zertifikate des lokalen Computers anzuzeigen sind die folgenden Schritte notwendig:

Starten Sie eine neue MMC-Konsole (Start -> Ausführen -> mmc.exe) (Bild 18).

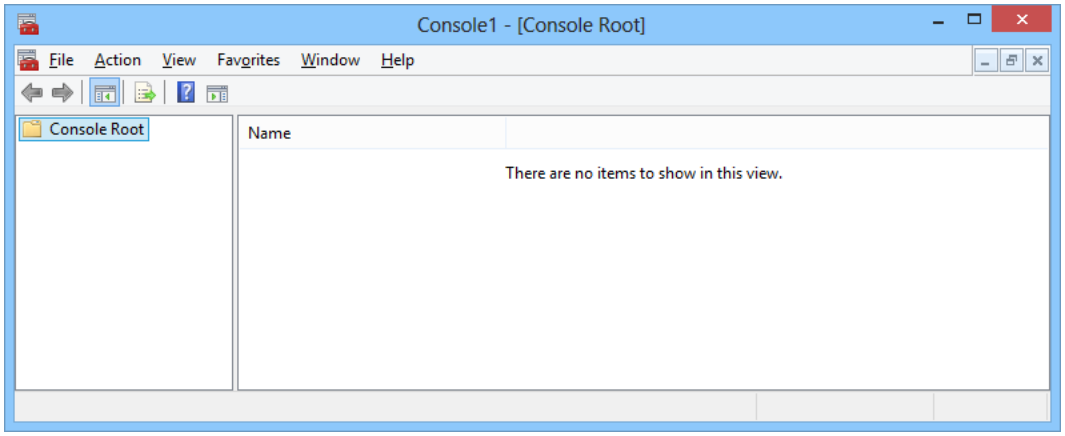


Bild 18: Eine leere MMC

Klicken Sie im Menü **Datei** / **File** auf **Snap-In hinzufügen/entfernen** / **Add/Remove Snap-in**. Wählen Sie das **Zertifikate** / **Certificates** Snap-In aus und klicken Sie auf **Hinzufügen** / **Add** (Bild 19).

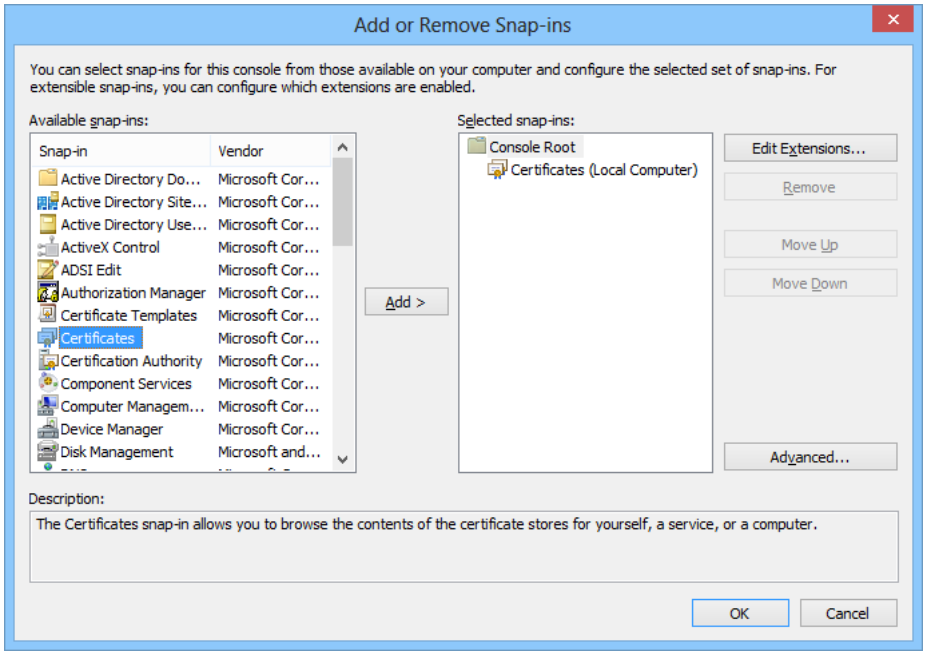


Bild 19: Ein Dialog zum Hinzufügen von Snap-Ins

Es erscheint der Konfigurationsassistent für das Snap-In **Zertifikate**. Wählen Sie hier zuerst das **Computer Konto** / **Computer account** (Bild 20) und im nächsten Schritt **Lokaler Computer** / **Local computer** (Bild 21) lokalen Computer aus und klicken Sie auf **Beenden** / **Finish**.

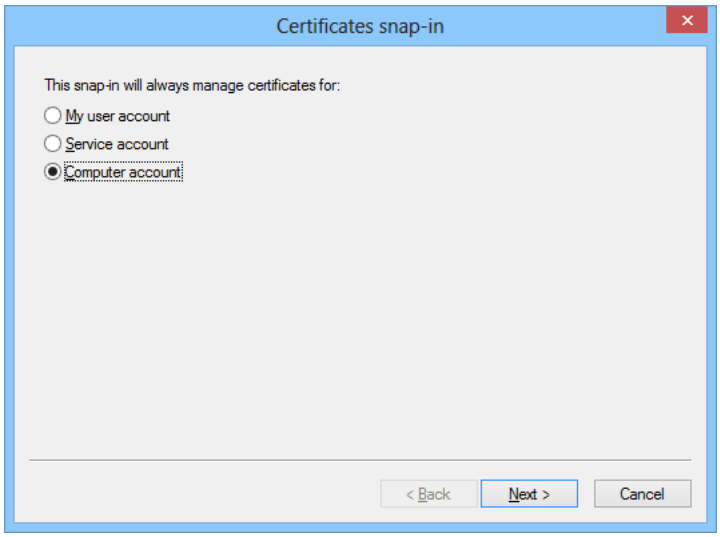


Bild 20: Auswahl des Computer Kontos

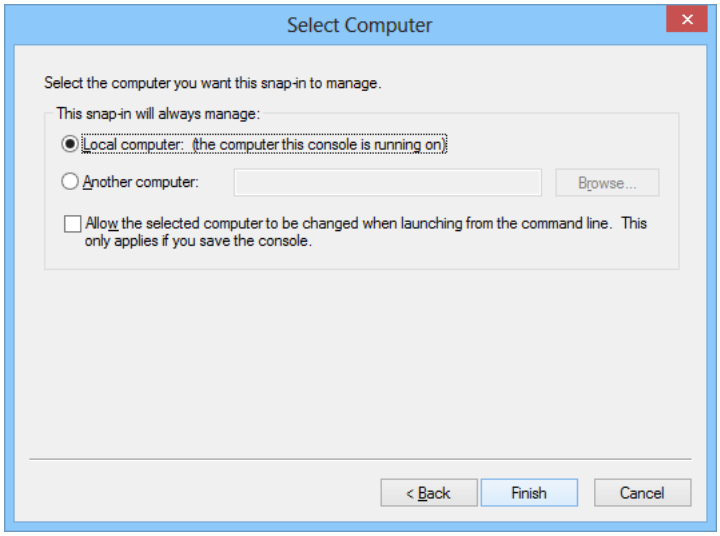


Bild 21: Auswahl des lokalen Computers

Schließen sie den Dialog **Snap-In hinzufügen oder entfernen / Add or Remove Snap-ins** mit **OK**. Klicken Sie im Fenster **Konsolenstamm** / **Console Root** auf **Zertifikate (Lokaler Computer)** / **Certificates (Local Computer)**, um die Zertifikatspeicher für den Computer anzuzeigen.