

mscrm-addons.com
ActivityTools for MS CRM 2013

ActivityTools für MS CRM 2013

Version 6.11 - April 2014

Installationshandbuch

(Wie man ActivityTools für MS CRM 2013 installiert/deinstalliert)

Der Inhalt dieses Dokuments kann ohne Vorankündigung geändert werden. "Microsoft" und "Microsoft CRM" sind eingetragene Warenzeichen der Microsoft Inc. Alle anderen Produkt- und Firmennamen sind Warenzeichen ihrer Inhaber.

Inhaltsverzeichnis

1	ACTIVITYTOOLS INSTALLER.....	3
2	EULA (END USER LICENSE AGREEMENT).....	3
3	INSTALLATION.....	4
4	ANMELDEINFORMATIONEN	5
5	SECURITY ROLES.....	7
6	ACTIVITYTOOLS KONFIGURATION	8
7	FERTIGSTELLUNG INSTALLATION	11
8	INSTALLATION VON ACTIVITYTOOLS IN EINER IFD/CLAIMS-BASIERENDEN UMGEBUNG.....	13
9	FEHLERBEHEBUNG	18
10	KONTAKT.....	20

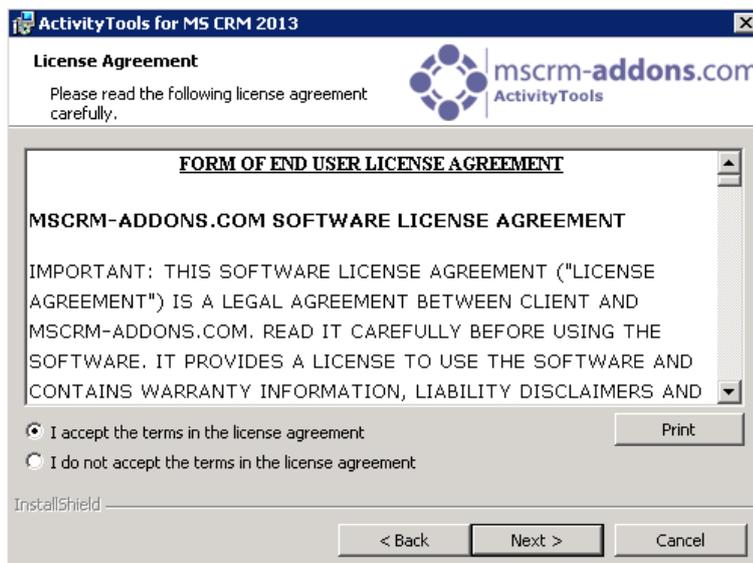
1 ActivityTools Installer

Starten Sie die ActivityTools .exe Installationsdatei mit einem Doppelklick. Das ist das Hauptfenster der Installation. Klicken sie auf [Next>] um mit der Installation fortzufahren.



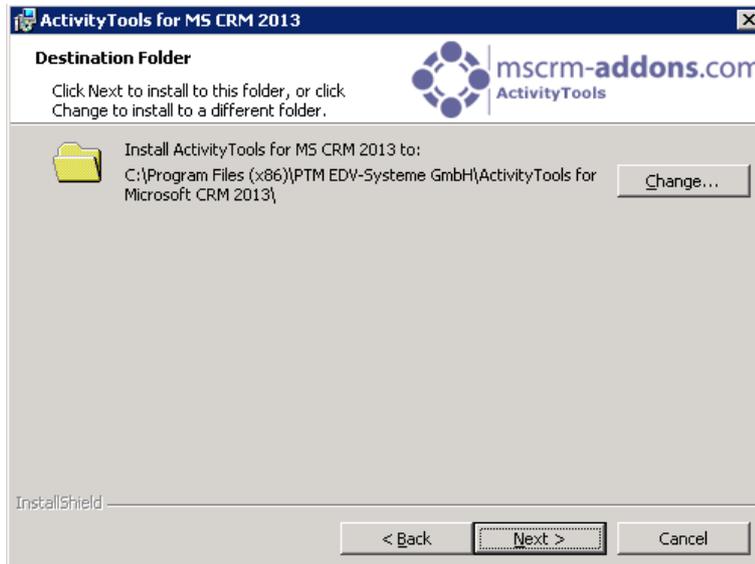
2 EULA (End User License Agreement)

Lesen Sie sich die Lizenzvereinbarung gut durch bevor Sie sie akzeptieren. Sie können nur mit der Installation fortfahren, wenn Sie die EULA akzeptieren. Sie können sich die Lizenzvereinbarung auch mit einem Klick auf die [Print]-Taste ausdrucken.

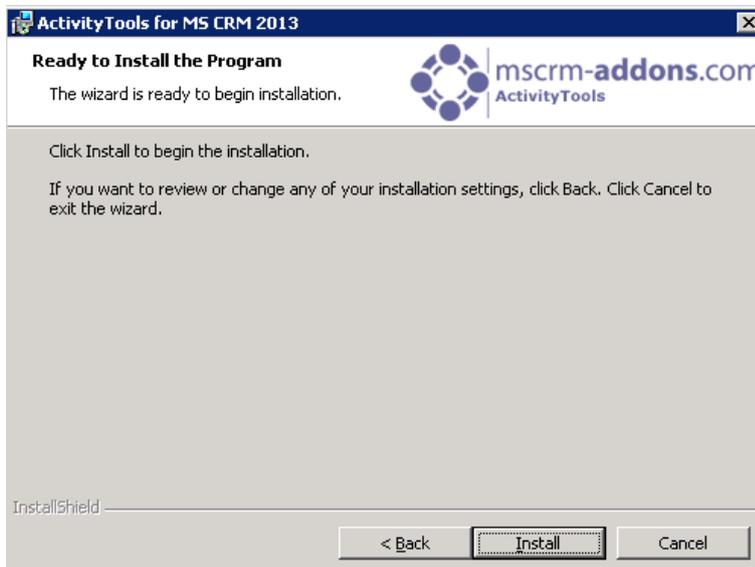


3 Installation

Nachdem Sie die Lizenzvereinbarung akzeptiert haben, klicken Sie auf den [Next >]-Button um fortzufahren.

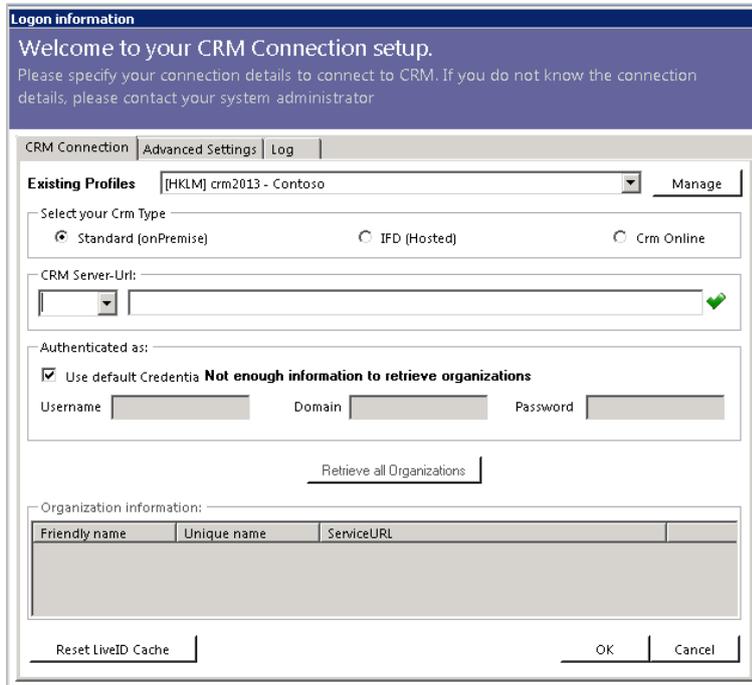


Klicken Sie auf [Install] um die Installation zu starten. (Siehe nächstes Bild)



4 Anmeldeinformationen

ActivityTools benötigt eine CRM-Verbindung. Um Ihren CRM Server zu konfigurieren, wählen Sie ein bestehendes Profil oder erstellen Sie ein neues Profil:



Logon information
Welcome to your CRM Connection setup.
Please specify your connection details to connect to CRM. If you do not know the connection details, please contact your system administrator

CRM Connection | Advanced Settings | Log

Existing Profiles: [HKLM] crm2013 - Contoso [Manage]

Select your Crm Type:
 Standard (onPremise)
 IFD (Hosted)
 Crm Online

CRM Server-Url: [] [] ✓

Authenticated as:
 Use default Credentia **Not enough information to retrieve organizations**
 Username [] Domain [] Password []

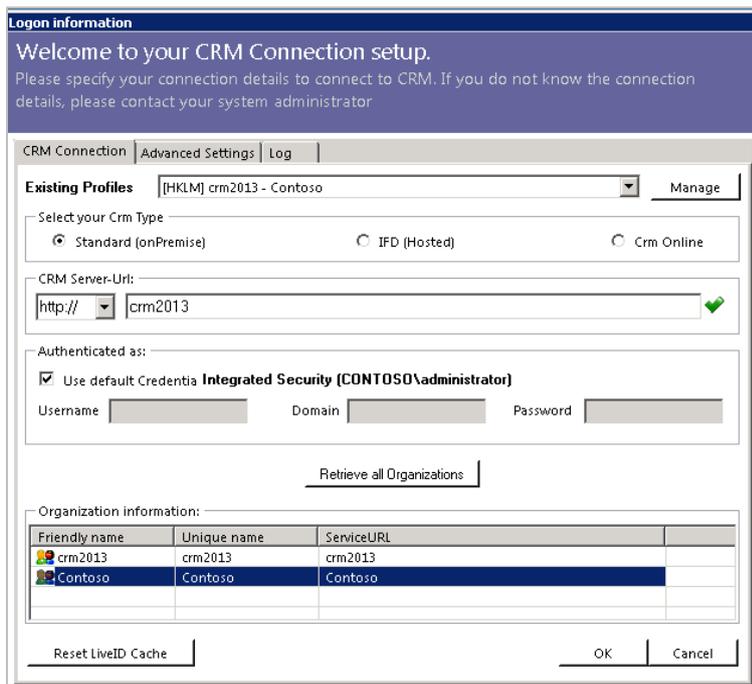
[Retrieve all Organizations]

Organization information:

Friendly name	Unique name	ServiceURL

[Reset LiveID Cache] [OK] [Cancel]

Wählen Sie einen Serverpfad und geben Sie Ihre Anmeldedaten, Benutzername, Passwort und Domäne ein oder wählen Sie die Standard-Anmeldedaten. Sobald die Organisationen abgerufen wurden, klicken Sie auf [OK]. (Siehe nächstes Bild)



Logon information
Welcome to your CRM Connection setup.
Please specify your connection details to connect to CRM. If you do not know the connection details, please contact your system administrator

CRM Connection | Advanced Settings | Log

Existing Profiles: [HKLM] crm2013 - Contoso [Manage]

Select your Crm Type:
 Standard (onPremise)
 IFD (Hosted)
 Crm Online

CRM Server-Url: [http://] [crm2013] ✓

Authenticated as:
 Use default Credentia **Integrated Security (CONTOSO\administrator)**
 Username [] Domain [] Password []

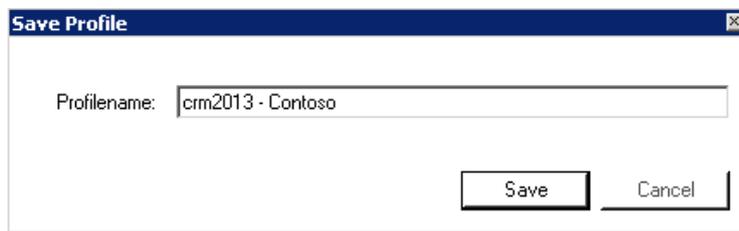
[Retrieve all Organizations]

Organization information:

Friendly name	Unique name	ServiceURL
crm2013	crm2013	crm2013
Contoso	Contoso	Contoso

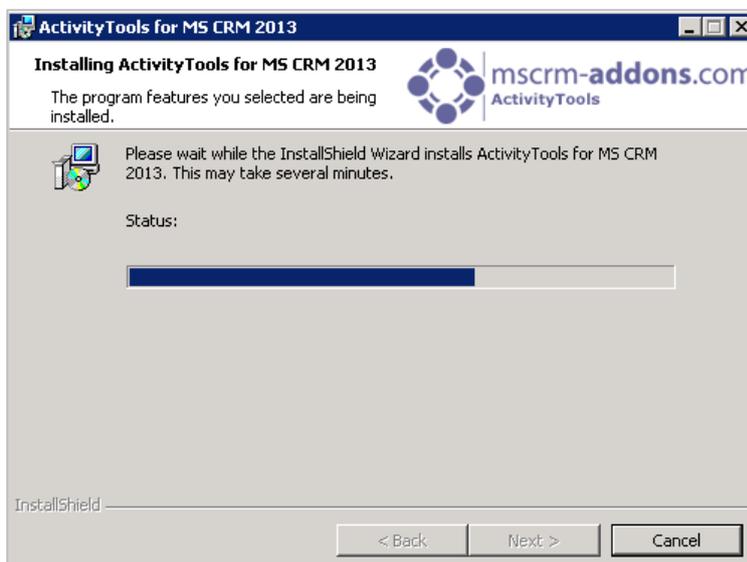
[Reset LiveID Cache] [OK] [Cancel]

Wenn Sie ein Profil zum ersten Mal anlegen, erscheint folgendes Fenster:



Hier können Sie das neue Profil speichern. Vergeben Sie einen Profilnamen und klicken Sie auf [Save] um das Profil zu speichern.

Folgendes Fenster erscheint:



5 Security Roles

Während der Installation werden Sie gefragt, ob sie die Security Roles installieren möchten.



Allgemeine Security Roles für alle unsere Produkte:

Für unsre Produkte sind folgende Security Roles erforderlich:

- MSCRM-Addons General Security Role

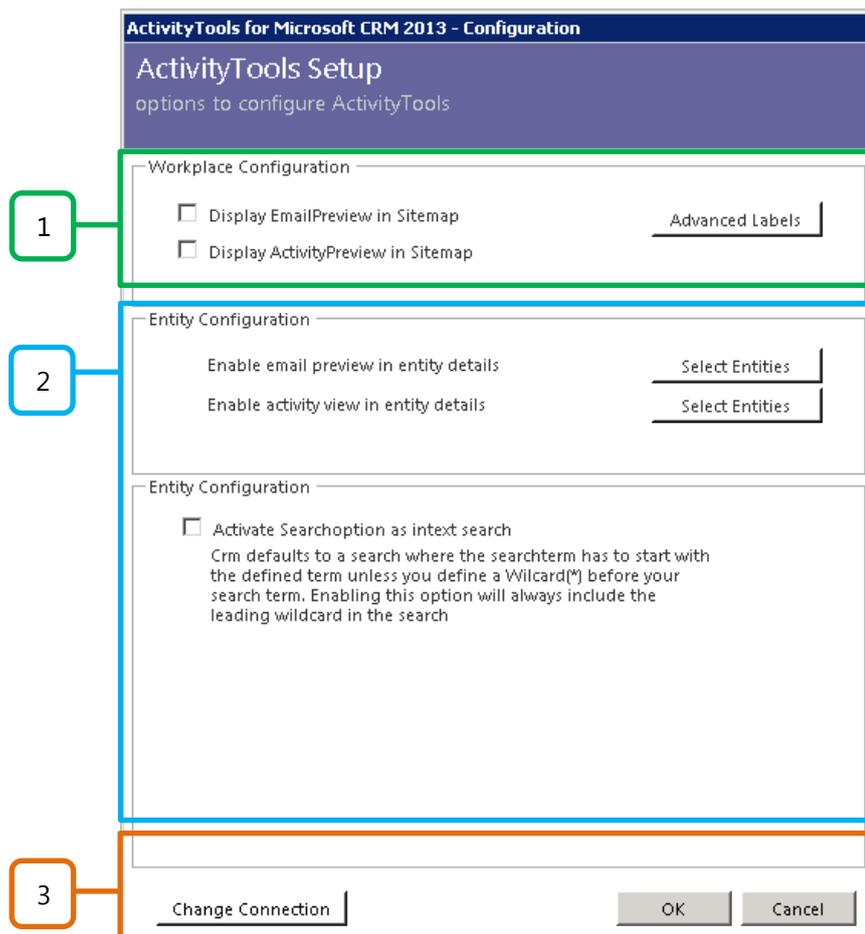
Diese Security Role beinhaltet die grundlegenden Anforderungen zur Verwendung des Produktes selbst und zur Befähigung, den Lizenz-Check auszuführen.

Klicken Sie auf [Yes] um allen Benutzern die Sicherheitsrolle zuzuweisen.

Achtung: Wenn dieser Schritt übersprungen wird, muss die Sicherheitsrolle manuell allen Benutzern zugewiesen werden oder die benötigten Rechte muss den bestehenden Sicherheitsrollen hinzugefügt werden.

6 ActivityTools Konfiguration

Die ActivityTools für MS CRM 2013 Konfiguration, ermöglicht es Ihnen die ActivityTools Einstellungen zu spezifizieren.



1. Workplace Configuration / Konfiguration Arbeitsbereich

Display EmailPreview in Sitemap:

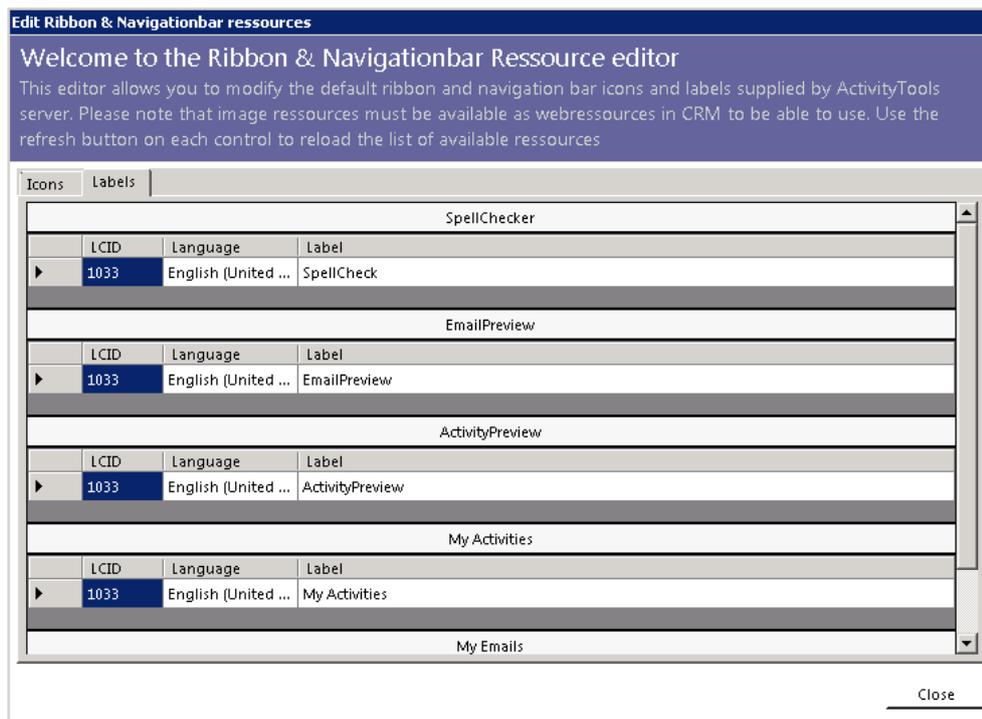
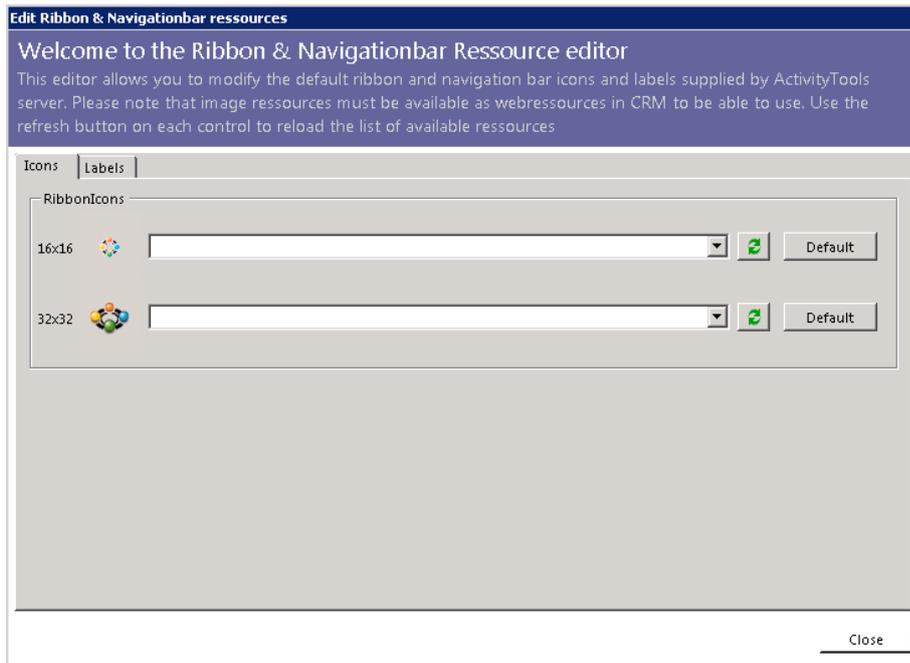
Wählen Sie diese Option aus um den Menüpunkt „Meine Emails“ in der oberen CRM-Navigationsleiste anzuzeigen.

Display ActivityPreview in Sitemap:

Wählen Sie diese Option aus um den Menüpunkt „Meine Aktivitäten“ in der oberen CRM-Navigationsleiste anzuzeigen.

Advanced Icons/Labels:

Die Advanced Labels Registerkarte ermöglicht die Anpassung der oberen Standard-CRM-Navigationsleiste und Navigationsleisten-Symbole und CRM-Menüpunkte die von ActivityTools Server unterstützt werden. **Notiz:** Die Bild-Ressource muss als CRM-Webressource verfügbar sein um genutzt werden zu können. Klicken Sie auf die „refresh“-Taste jeder Steuerung um eine Liste der verfügbaren Ressourcen zu laden. (Siehe nächsten Bilder)



2. Entity Configuration / Konfiguration Entitäten

Wie man die Email Vorschau / Aktivitäten Vorschau in den Entitäten Details aktiviert:

Hier können Sie definieren, welche Entitäten in der Aktivitäten Vorschau und in den Entitäten Details angezeigt werden sollen. Folgendes Fenster erscheint:

Entity	Toolbar	Forms
Account	<input type="checkbox"/> Account	<input type="checkbox"/> Account
Address	<input type="checkbox"/> Information	<input type="checkbox"/> Information
Campaign	<input type="checkbox"/> Campaign	<input type="checkbox"/> Campaign
Campaign Activity	<input type="checkbox"/> Campaign Activity	<input type="checkbox"/> Campaign Activity
Campaign Response	<input type="checkbox"/> Campaign Response	<input type="checkbox"/> Campaign Response
Case	<input type="checkbox"/> Case	<input type="checkbox"/> Case
Competitor	<input type="checkbox"/> Competitor	<input type="checkbox"/> Competitor
Connection	<input type="checkbox"/> Information	<input type="checkbox"/> Information
Contact	<input type="checkbox"/> Contact	<input type="checkbox"/> Contact
Contract	<input type="checkbox"/> Contract	<input type="checkbox"/> Contract
Contract Line	<input type="checkbox"/> Contract Detail	<input type="checkbox"/> Contract Detail
Duplicate	<input type="checkbox"/> Information	<input type="checkbox"/> Information
Email	<input type="checkbox"/> Email	<input type="checkbox"/> Email
	<input type="checkbox"/> Wizard	<input type="checkbox"/> Wizard
	<input type="checkbox"/> Information	<input type="checkbox"/> Information

* Entities with a red background are unmanaged custom entities. They either need to be manually configured or adapted as described at [Blog article for Customization](#)

OK

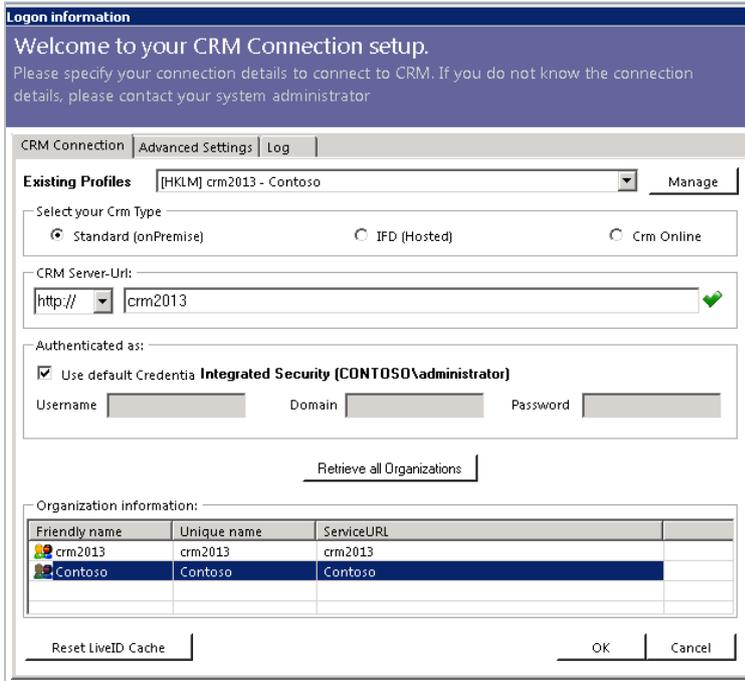
Im oben gezeigten Fenster können Sie Ihre Entitäten definieren.

Wie man die Suchoption als Index Suche aktiviert:

CRM hat standardmäßig eine Suche, bei der der Suchbegriff mit einem bestimmten Begriff anfangen muss, es sei denn, Sie definieren einen Platzhalter (*) vor Ihrem Suchbegriff. Wenn Sie diese Option aktivieren wird der Platzhalter immer in die Suche inkludiert.

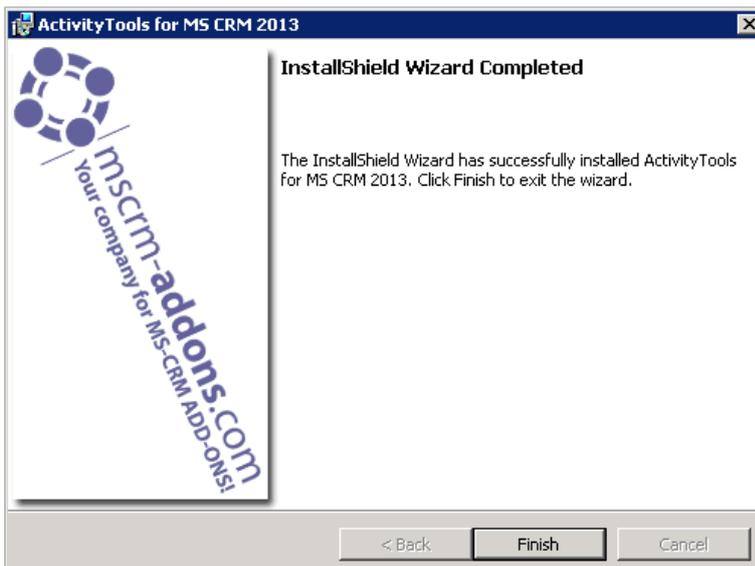
3. Change Connection / Verbindungseinstellungen Ändern

Hier können Sie Ihre CRM-Verbindungsdetails ändern. Bitte fragen Sie Ihren Systemadministrator, wenn Sie die Verbindungsdetails nicht kennen.



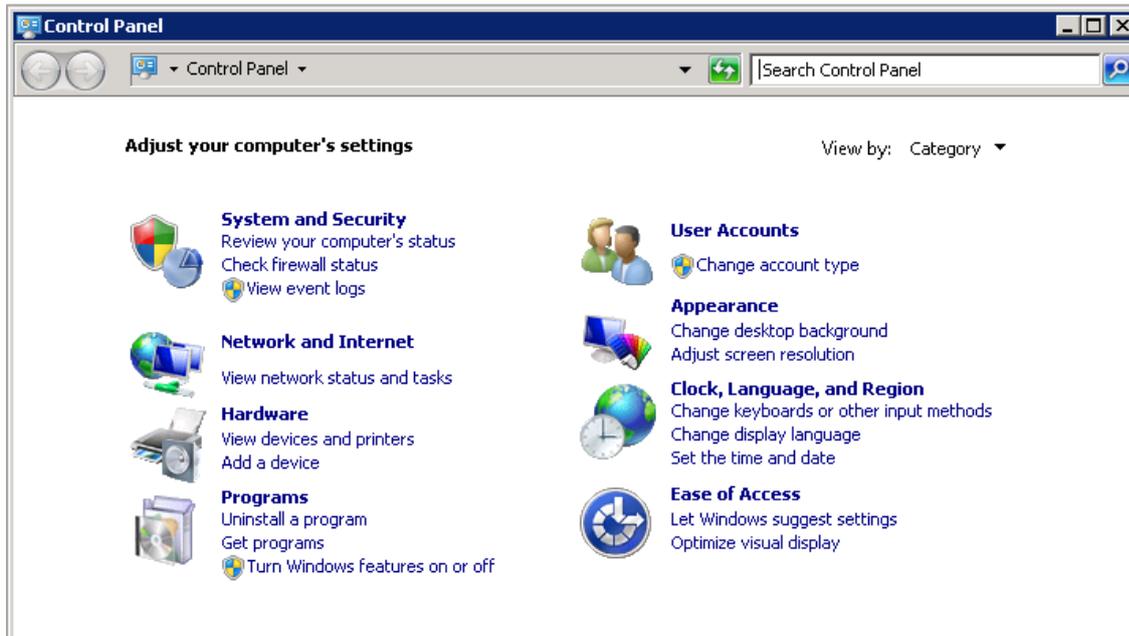
7 Fertigstellung Installation

Wenn die Installation erfolgreich war, erscheint unteres Fenster. Klicken Sie auf [Finish] um die Installation fertig zu stellen.

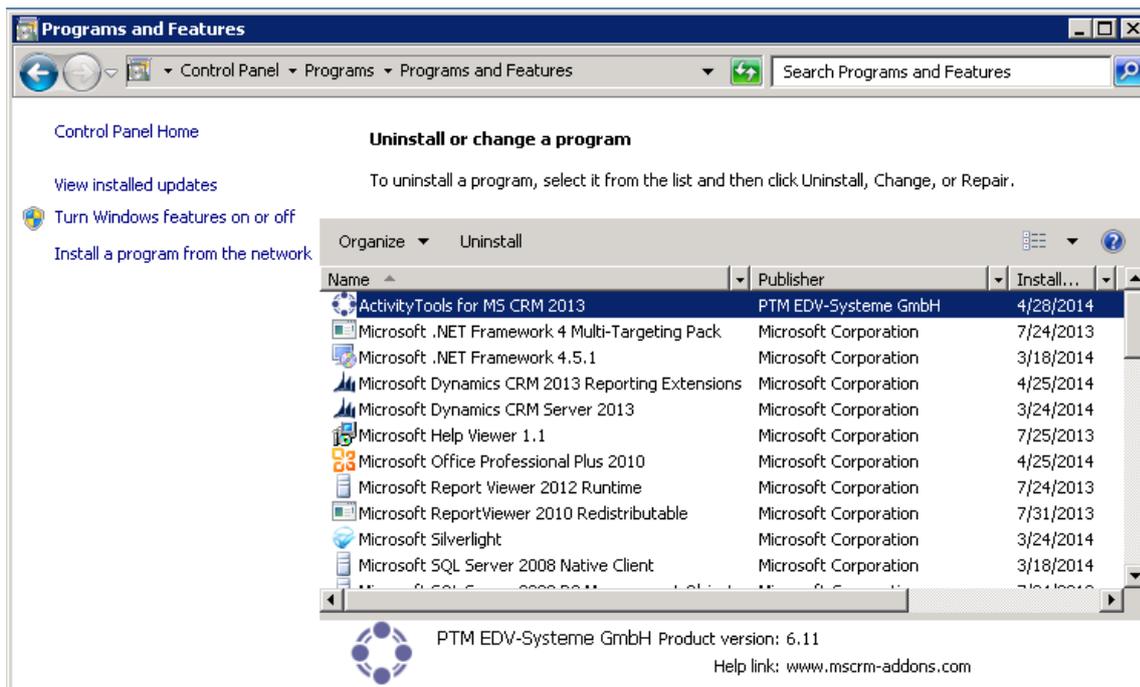


8 Deinstallieren

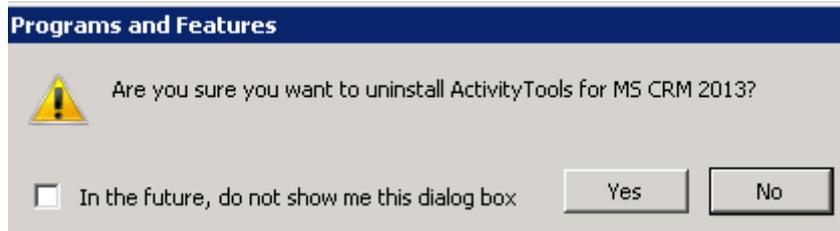
Um ActivityTools zu deinstallieren, öffnen Sie Systemsteuerung vom Startmenü und wählen Sie den Menüpunkt „Programme und Einstellungen“.



Suchen Sie nach ActivityTools for CRM 2013 und klicken Sie auf "Deinstallieren" um folgen Sie den Deinstallationsanweisungen. (Siehe nächstes Bild).



Folgendes Fenster erscheint:



Klicken Sie auf [Yes] um ActivityTools for MS CRM 2013 zu Deinstallieren.

8 Installation von ActivityTools in einer IFD/Claims-basierenden Umgebung

In diesem Kapitel werden die einzelnen Schritte, die für eine Installation von ActivityTools in einer IFD/Claims-Based Umgebung nötig sind, erläutert.

Sie benötigen folgende Downloads um das Addon erfolgreich installieren zu können:

1. IFD-Tool -> [Download Link](#), Sie müssen sich auf unserer Homepage anmelden.
2. Für die Installation von ActivityTools benötigen Sie zumindest die Version 5.13 (Link zum [Download Bereich](#))

Bevor Sie mit der Installation beginnen ist es erforderlich, dass MS CRM fehlerfrei für IFD/Claims konfiguriert wurde (inkl. Ihr ADFS).

Mehr Details über die Konfiguration von IFD/Claims finden Sie im Microsoft Guide im Bereich „Configuring Claims-based Authentication for Microsoft Dynamics CRM 2013“. [Download](#)

Die folgende Systemkonfiguration ist die Basis für unseren Guide. Ihr Setup wird Unterschiede bezüglich folgender URLs aufzeigen. Stellen Sie daher sicher, dass Sie die folgenden URLs durch Ihre eigenen URLs ersetzen wenn Sie unserem Guide folgen!

ActivityTools muss mit einem http UND einem https Port konfiguriert sein.

Interne URL um auf MS Dynamics CRM zuzugreifen:

<https://internalcrm.rc1ifd.ptm-edv.at>

Externe URL um auf MS Dynamics CRM zuzugreifen:

[https://\[orgname\].rc1ifd.ptm-edv.at](https://[orgname].rc1ifd.ptm-edv.at)

AD FS Server:

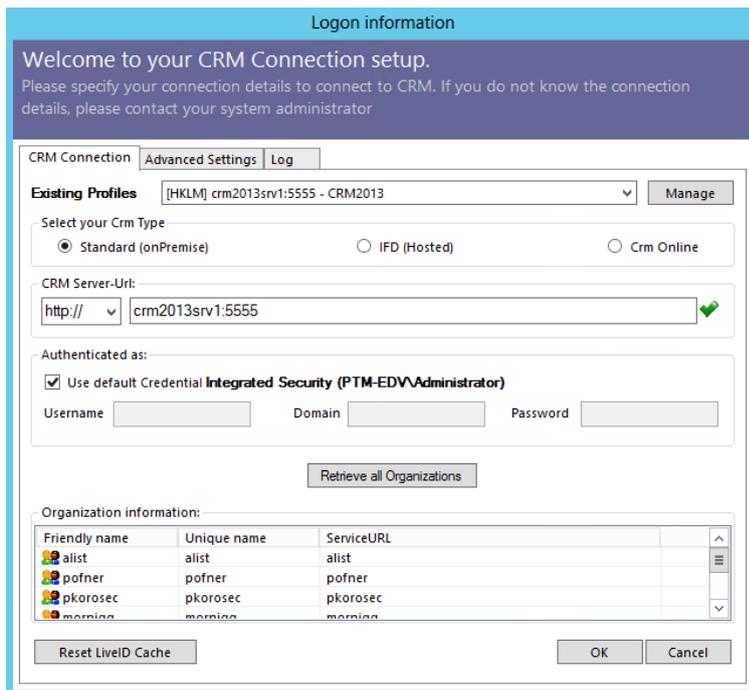
<https://win2008domain.ptm-edv.at>

Auch das Addon selbst benötigt einen DNS Namen:

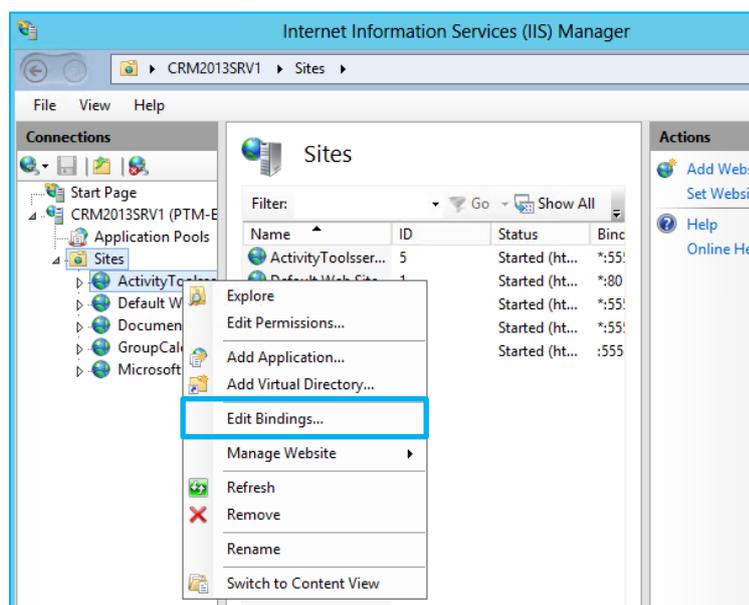
<https://activitytoolsserver.rc1ifd.ptm-edv.at>

ActivityTools Basis Installation/Konfiguration:

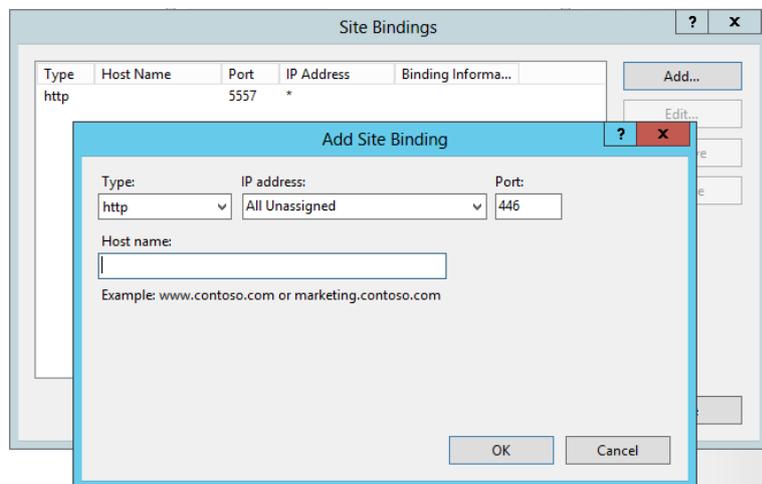
1. Installieren Sie das Addon auf dem CRM Server.
2. Sie werden nach den Logon Informationen gefragt. Tragen Sie den internen IFD Namen Ihres CRM Systems ein. In unserem Fall ist dieser „internalcrm.rc1ifd.ptm-edv.at“. Wählen Sie die Organisation, auf der Sie das Addon installieren möchten, und klicken Sie auf [OK].



3. Nachdem die Installation abgeschlossen ist, müssen Sie die IIS (inetmgr.exe) öffnen. Gehen Sie zu ‚Sites‘ -> Addon WebSite. Klicken Sie mit der rechten Maustaste auf die ActivityTools Server – WebSite und wählen Sie "Edit Bindings...".

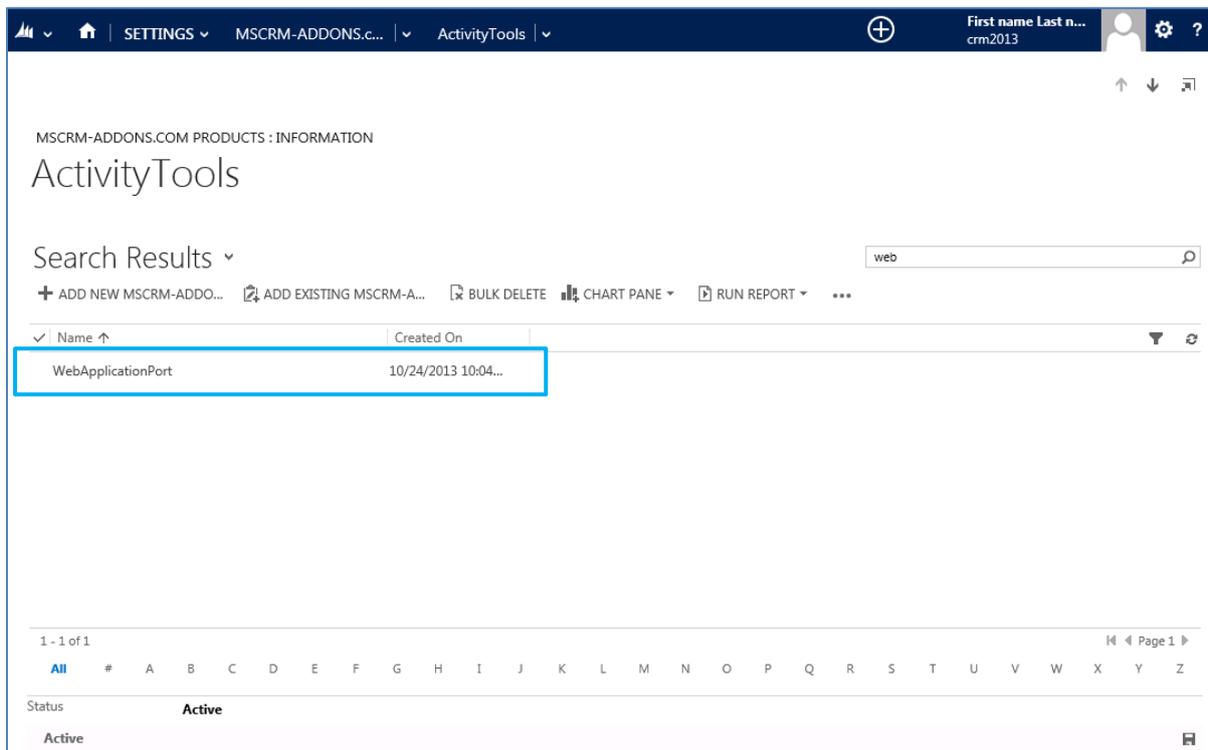


Klicken Sie bei den Bindings auf [Add...] und wählen Sie bei „Add Site Binding“ den Typ „https“. Weiters müssen Sie den Port spezifizieren. In unserem Fall verwenden wir 4446.



Somit haben wir die Website für https verfügbar gemacht. Klicken Sie auf [OK].

4. Gehen Sie erneut auf die Addon Website und doppel-klicken Sie auf "Authentication". Bestätigen Sie, dass die Optionen „Anonymous“ und „ASP.Net Impersonation“ Settings aktiviert sind.
5. Die Addon URL muss zu Ihrem DNS Server hinzugefügt werden. Ihre DNS Server müssen den activitytoolsserver.[your-domain] Namen korrekt auflösen. Das heißt, dass diese den Namen mit derselben IP Adresse wie die Ihres CRM Servers auflösen müssen. Sollten Sie außerdem einen externen DNS verwenden, stellen Sie sicher, dass sowohl der externe, als auch der interne DNS in der Lage sind, die URL aufzulösen.
6. Extrahieren Sie das IFD-Tool (zip-File) welches Sie zuvor heruntergeladen haben und führen Sie die IFDSetupWizard.exe aus. Folgen Sie den Schritten im IFD Setup.
7. Öffnen Sie Ihr CRM System im Internet Explorer und gehen Sie zu den "Settings" -> "MSCRM-ADDONS.com Products" -> Öffnen Sie ActivityTools -> in der MSCRM-ADDONS.com Products Form, wählen Sie die MSCRM-ADDONS.com Settingskeys und suchen Sie nach dem "WebApplicationPort" Eintrag.



- Öffnen Sie den WebApplicationPort und ersetzen Sie den vorhandenen Key/Value folgendermaßen: [httpsPort]|[httpPort]|[claimsbased]|[addonname]|[debugging], z.B.: 4446|5557|true|activitytoolsserver|false

Die Konfiguration des CRM-Teils ist fertiggestellt. Nun müssen Sie den **AD FS konfigurieren**.

NOTIZ: Wenn Sie AD FS benutzen, muss der IFD Wizard neu durchgeführt werden, wenn das https Zertifikat und/oder das TokenSignal Zertifikat am AD FS ablaufen.

- Melden Sie sich bitte bei Ihrem AD FS Server an und starten Sie "AD FS 2.0 Management".
- Klicken Sie im „Actions“-Menu, welches Sie in der rechten Spalte finden, auf "Add Relying Party Trust".
- Im „Add Relying Party Trust“-Assistenten, klicken Sie auf [Start].
- Klicken Sie auf "Import data about the relying party published online or on a local network" auf der "Select Data Source" Seite und geben Sie dann die URL ein um die „federationmetadata.xml file“ zu lokalisieren.

Die „federation metadata“ werden mit Hilfe des IFD-Tools auf dem CRM Server erstellt z.B.
<https://activitytoolsserver.rc1ifd.ptm-edv.at:4446/FederationMetadata/2007-06/FederationMetadata.xml>

Geben Sie diese URL in Ihren Browser ein und stellen Sie sicher, dass keine Zertifikat-bezogenen Warnmeldungen auftreten.

- Klicken Sie auf [Next>].

6. Geben Sie einen Anzeigenamen auf der "Specify Display Name" Seite ein (z.B. ActivityTools IFD) und klicken Sie auf [Next>].
 7. Auf der "Choose Issuance Authorization Rules" Seite, belassen Sie die "Permit all users to access this relying party"-Option ausgewählt und klicken Sie auf [Next>].
 8. Auf der "Ready to Add Trust" Seite, klicken Sie zunächst auf [Next>] und dann auf [Close].
 9. Sollte der "Rules Editor" aufscheinen, klicken Sie auf "Add Rule". Andernfalls, gehen Sie zur "Relying Party Trusts list", klicken Sie mit der rechten Maustaste auf das "relying party object" welches Sie erstellt haben, klicken Sie auf "Edit Claims Rules" und danach auf "Add Rule". Wichtig: Stellen Sie sicher, dass das "Issuance Transform Rules"-Tab ausgewählt ist.
 10. Wählen Sie in der "Claim rule template list" das "Pass Through or Filter an Incoming Claim template" und klicken Sie auf [Next>].
 11. Erstellen Sie die folgende Regel:
 - Claim rule Name: Pass Through UPN (oder etwas Beschreibendes)
 - Fügen Sie folgendes Mapping hinzu:
 - i. Incoming claim type: UPN
 - ii. Pass through all claim values
 12. Klicken Sie auf [Finish].
 13. Klicken Sie auf "Add Rule" im "Rules Editor" und wählen sie das "Pass Through or Filter an Incoming Claim template" in der "Claim rule template list". Danach klicken Sie auf [Next>]:
 - Claim rule Name: Pass Through Primary SID (oder etwas Beschreibendes)
 - Fügen Sie folgendes Mapping hinzu:
 - i. Incoming claim type: Primary SID
 - ii. Pass through all claim values
 14. Klicken Sie auf [Finish].
 15. Im "Rules Editor", klicken Sie auf "Add Rule".
 16. Wählen Sie das "Transform an Incoming Claim template" in der "Claim rule template list" und klicken Sie auf [Next>].
 17. Erstellen Sie folgende Regel:
 - Claim rule Name: Transform Windows Account Name to Name (oder etwas Beschreibendes)
 - Fügen Sie folgendes Mapping hinzu:
 - i. Incoming claim type: Windows account name
 - ii. Outgoing claim type: Name
 - iii. Pass through all claim values
 18. Klicken Sie auf [Finish]. Wenn Sie alle drei Regeln erstellt haben, klicken Sie auf [OK] um den „Rules Editor“ zu schließen.
- Sie haben die Konfiguration nun abgeschlossen und sollten nun in der Lage sein das Addon in Ihrem IFD/Claims Umfeld zu nützen.

9 Fehlerbehebung

Sollten Sie folgende Fehlermeldung bekommen, könnte dies aus 2 Gründen passieren:

Server Error in '/' Application.

ID4175: The issuer of the security token was not recognized by the IssuerNameRegistry. To accept security tokens from this issuer, configure the IssuerNameRegistry to return a valid name for this issuer.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.IdentityModel.Tokens.SecurityTokenException: ID4175: The issuer of the security token was not recognized by the issuerNameRegistry. To accept security tokens from this issuer, configure the IssuerNameRegistry to return a valid name for this issuer.

Source Error:

An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.

Stack Trace:

```
[SecurityTokenException: ID4175: The issuer of the security token was not recognized by the IssuerNameRegistry. To accept security tokens from this issuer, configure the IssuerNameRegistry to return a valid name for this issuer.]
Microsoft.IdentityModel.Tokens.Saml11.Saml11SecurityTokenHandler.CreateClaims(SamlSecurityToken samlSecurityToken) +739
Microsoft.IdentityModel.Tokens.Saml11.Saml11SecurityTokenHandler.ValidateToken(SecurityToken token) +644
Microsoft.IdentityModel.Tokens.SecurityTokenHandlerCollection.ValidateToken(SecurityToken token) +117
Microsoft.IdentityModel.Web.TokenReceiver.AuthenticateToken(SecurityToken token, Boolean ensureBearerToken, String endpointUri) +151
Microsoft.IdentityModel.Web.WSFederationAuthenticationModule.SignInWithResponseMessage(HttpRequest request) +615
Microsoft.IdentityModel.Web.WSFederationAuthenticationModule.OnAuthenticateRequest(Object sender, EventArgs args) +521
System.Web.SyncEventExecutionStep.System.Web.HttpApplication.IExecutionStep.Execute() +80
System.Web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean& completedSynchronously) +270
```

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.0.30319.237

Grund 1:

Ein möglicher Grund für diese Fehlermeldung könnte die Verwendung eines falschen Zertifikates für das "ADFS signing" sein. Stellen Sie daher sicher, dass der thumbprint in der web.config zu demjenigen im "Token Signing Certificate in ADFS" passt.

```
<issuerNameRegistry type="Microsoft.IdentityModel.Tokens.ConfigurationBasedIssuerNameRegistry,
Microsoft.IdentityModel, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35">
  <trustedIssuers>
    <add thumbprint="37a59abae1a394ffd8f0fd750c2e38e98069e349"
name="http://win2008domain.ptm-edv.at/adfs/services/trust" />
  </trustedIssuers>
</issuerNameRegistry>
```

Wenn diese Fehlermeldung aufscheint:

Server Error in '/' Application.

Keyset does not exist

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Security.Cryptography.CryptographicException: Keyset does not exist

Source Error:

An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.

Stack Trace:

```
[CryptographicException: Keyset does not exist]
System.Security.Cryptography.Utils.CreateProvHandle(CspParameters parameters, Boolean randomKeyContainer) +5557310
System.Security.Cryptography.Utils.GetKeyPairHelper(CspAlgorithmType keyType, CspParameters parameters, Boolean randomKeyContainer, Int32 dwKeySize, SafeProvH
System.Security.Cryptography.RSACryptoServiceProvider.GetKeyPair() +221
System.Security.Cryptography.X509Certificates.X509Certificate2.get_PrivateKey() +516
System.IdentityModel.Tokens.X509AsymmetricSecurityKey.get_PrivateKey() +101
System.IdentityModel.Tokens.X509AsymmetricSecurityKey.DecryptKey(String algorithm, Byte[] keyData) +25
System.IdentityModel.Selectors.SimpleTokenResolver.TryResolveSecurityKeyCore(SecurityKeyIdentifierClause keyIdentifierClause, SecurityKey& key) +319
Microsoft.IdentityModel.Tokens.EncryptedSecurityTokenHandler.ReadToken(XmlReader reader) +290
Microsoft.IdentityModel.Tokens.SecurityTokenHandlerCollection.ReadToken(XmlReader reader) +125
Microsoft.IdentityModel.Web.TokenReceiver.ReadToken(String tokenXml, XmlDictionaryReaderQuotas readerQuotas) +360
Microsoft.IdentityModel.Web.WSFederationAuthenticationModule.SignInWithResponseMessage(HttpRequest request) +417
Microsoft.IdentityModel.Web.WSFederationAuthenticationModule.OnAuthenticateRequest(Object sender, EventArgs args) +521
System.Web.SyncEventExecutionStep.System.Web.HttpApplication.IExecutionStep.Execute() +80
System.Web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean& completedSynchronously) +165
```

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.0.30319.17929

Grund 2:

Ein weiterer Grund für die Fehlermeldung könnten auch Zugriffsrecht-Probleme mit dem "Certificate Private Key" sein (Hauptsächlich ein Aspekt bei „self-signed certificates“.)

Öffnen Sie Ihren "Certificate Store" auf dem Server (MMC, fügen Sie den "Certificate Snapin for local computer" hinzu) und suchen Sie Ihr HTTPS Zertifikat. Wählen Sie die "manage private keys" Option im Kontextmenü unter "All tasks" und erlauben Sie den Zugriff für jeden.

Checkliste für allgemeine Fehlerbehebung:

- Ist der "Setting WebApplicationPort" intakt?
- Existieren not-http/https-Bindings im CRM?
- Existieren not-http/https-Bindings auf der Produkt-Website?
- Löst der DNS die Produktlinks korrekt auf?
- Wurde das "ConnectionProfile" mit "IFD" als Verbindungstyp ausgewählt?

10 Kontakt

Wenn Sie Probleme oder Fragen zu unserem Produkt haben, senden Sie uns eine E-Mail an support@mscrm-addons.com

oder besuchen Sie unseren Blog
<http://blogs.mscrm-addons.com>

PTM EDV-Systeme GmbH
Bahnhofgürtel 59
A-8020 Graz, Austria

Tel US +1 404.720.6066
Tel Austria +43 316 680-880-0
Fax +43 316 680-880-25
www.ptm-edv.at
www.mscrm-addons.com