ActivityTools for MS CRM 2013

Version 6.10, March 2014

Installation Guide
(How to install/uninstall ActivityTools for MS CRM 2013)

The content of this document is subject to change without notice.
"Microsoft" and "Microsoft CRM" are registered trademarks of Microsoft Inc.
All other product- and company names mentioned are trademarks of their respectful owners.

Table of Contents

1 ACTIVITYTOOLS INSTALLER....3

2 EULA (END USER LICENSE AGREEMENT)....3

3 INSTALLATION....4

4 SECURITY ROLES....5

5 LOGON INFORMATION....5

6 ACTIVITYTOOLS CONFIGURATION....7

7 COMPLETE THE INSTALLATION....10

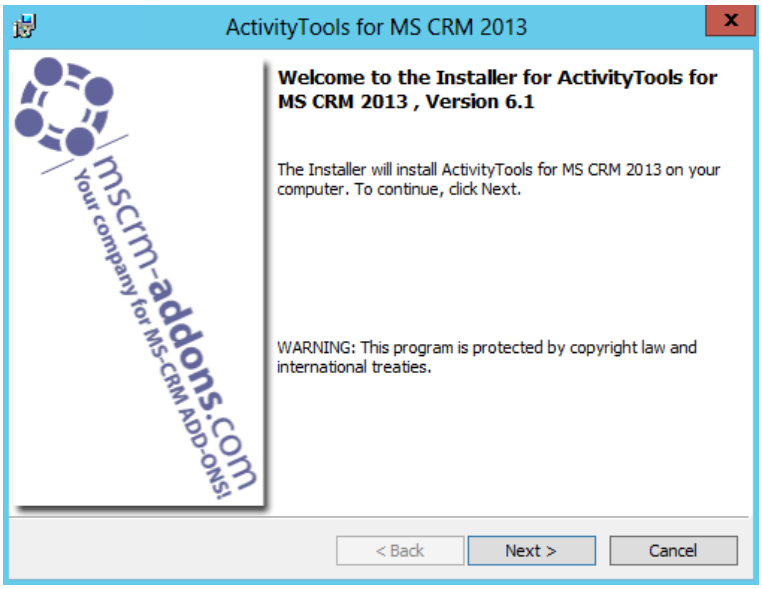
8 HOW TO INSTALL ACTIVITYTOOLS IN AN IFD/CLAIMS-BASED-ENVIRONMENT....12

9 TROUBLESHOOTING....17

10 CONTACT....19

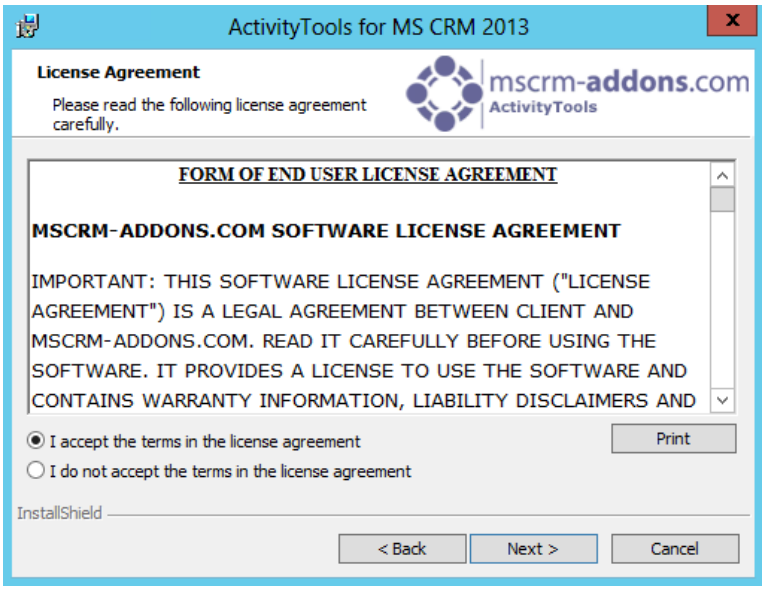
1 ActivityTools Installer

This is the main window for the installation. Click [Next] to continue the installation.



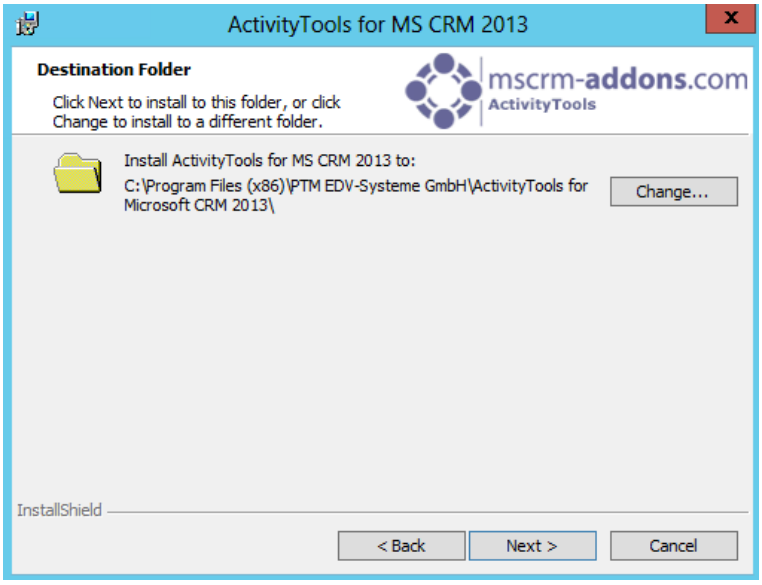
2 EULA (End User License Agreement)

Read the license agreement carefully and accept it if you agree to the terms and if you want to continue with the installation. If you do not accept the license agreement, you cannot continue with the installation. There is also a "Print"-button if you want to print the license agreement.

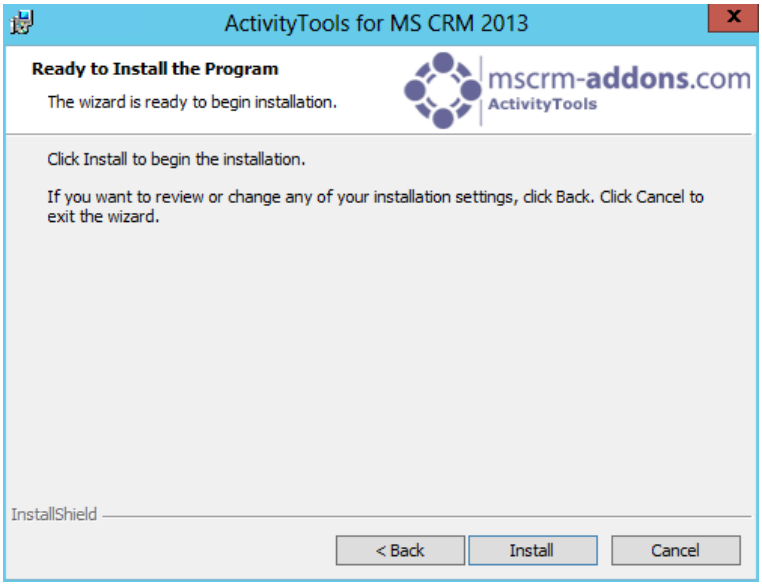


3 Installation

After accepting the EULA click on [Install] to continue with the installation. Click [Next >] to install to this suggested folder, or click [Change…] to install to a different folder.



Click [Install] to start the installation. See next screenshot:



4 Security Roles

During installation, you are asked if you want to install the Security Roles.

General security roles for all products:

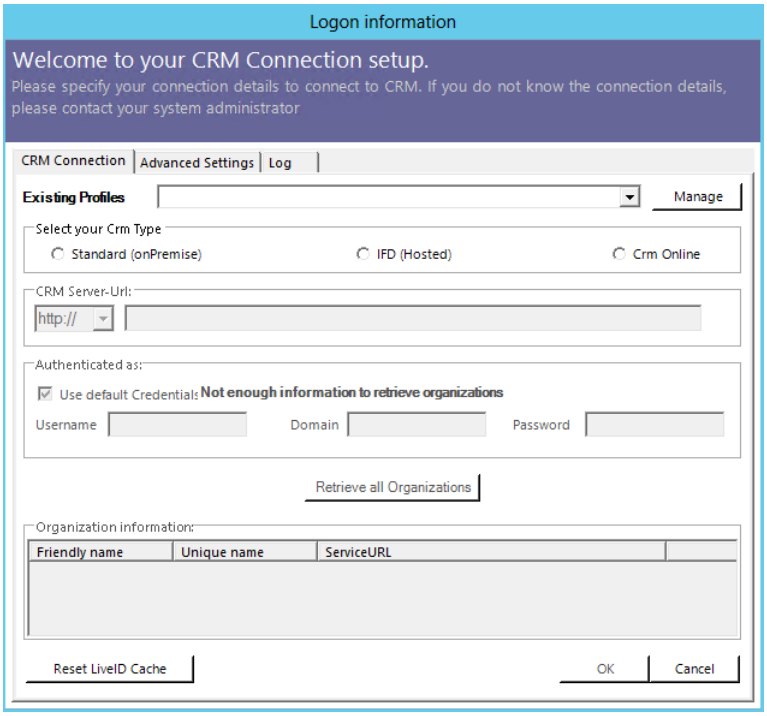
The following security role is required by all our products:

- MSCRM-Addons General Security Role

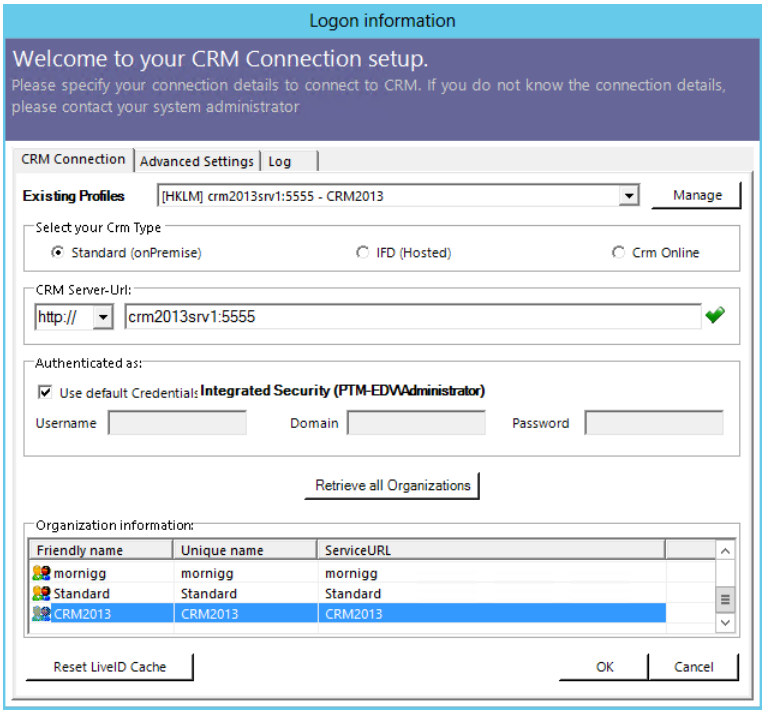
This security role contains the basic requirements for using the product itself and for being able to perform the license check.

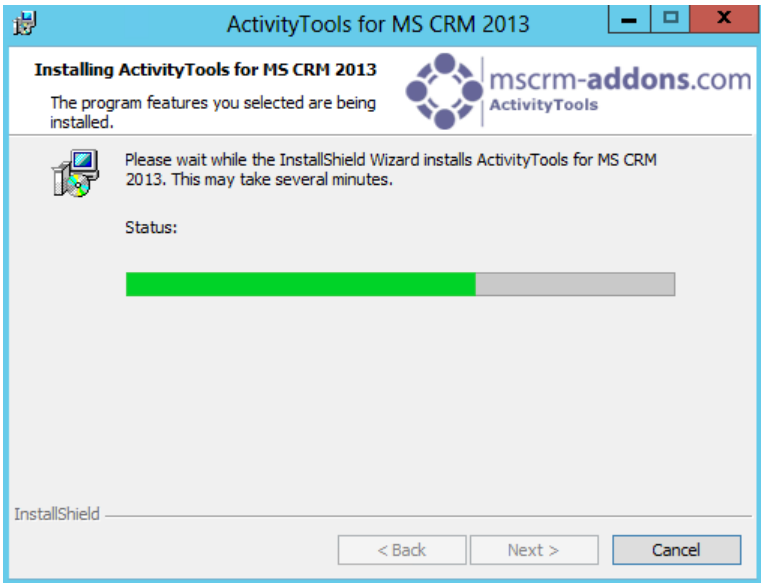
5 Logon Information

ActivityTools requires a connection to CRM. To configure your CRM Server, select an existing profile or create a new profile:



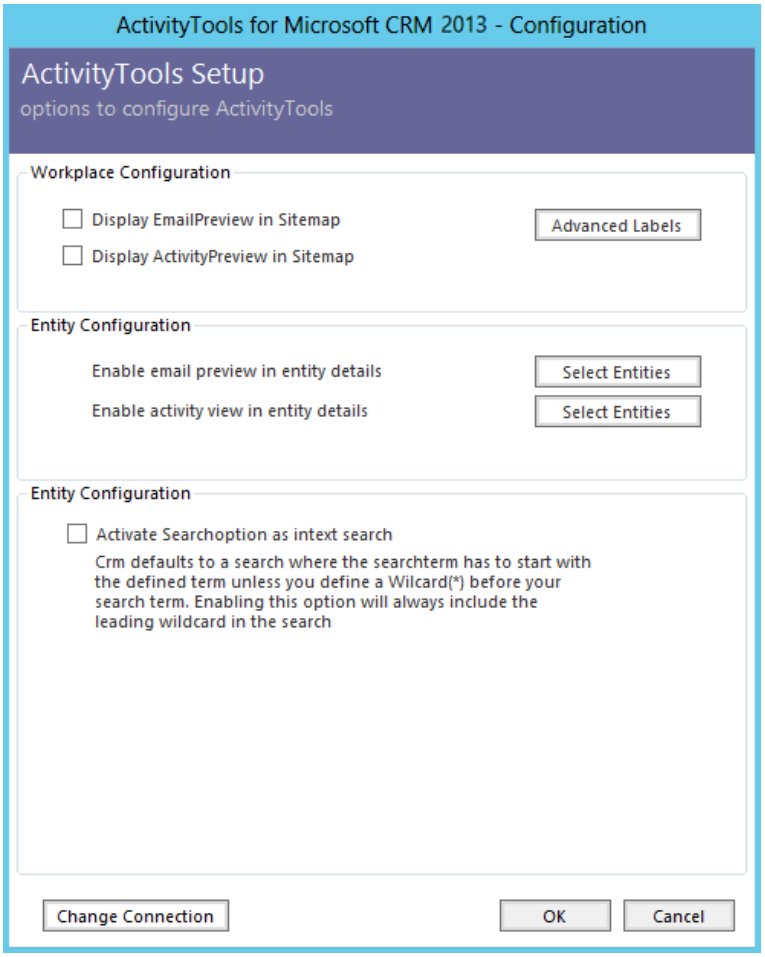
Choose the server path and add your login credentials by filling in the field's username, password and domain or choose the default credentials to connect as the currently active user. As soon as the organizations are retrieved, select the desired organization and press the [OK]-button. See next screenshot:


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] crm2013srv1:5555 - CRM2013
Manage
Select your Crm Type
Standard (onPremise)
IFD (Hosted)
Crm Online
CRM Server-Url:
http://
crm2013srv1:5555
Authenticated as:
Use default Credential: Integrated Security (PTM-EDV\Administrator)
Username
Domain
Password
Retrieve all Organizations
Organization information:
Friendly name
Unique name
ServiceURL
mornigg
mornigg
mornigg
Standard
Standard
Standard
CRM2013
CRM2013
CRM2013
Reset LiveID Cache
OK
Cancel


ActivityTools for MS CRM 2013
Installing ActivityTools for MS CRM 2013
The program features you selected are being installed.
mscrm-addons.com
ActivityTools
Please wait while the InstallShield Wizard installs ActivityTools for MS CRM 2013. This may take several minutes.
Status:
InstallShield
< Back
Next >
Cancel

6 ActivityTools Configuration

The ActivityTools for MS CRM 2013 Configuration allows you to specify the ActivityTools-Settings.



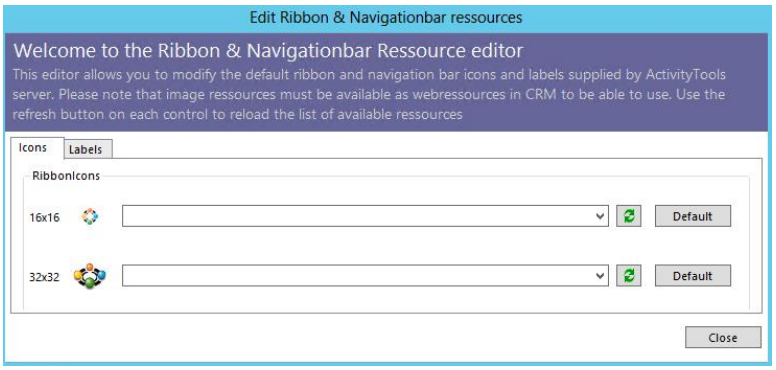
1 Workplace Configuration

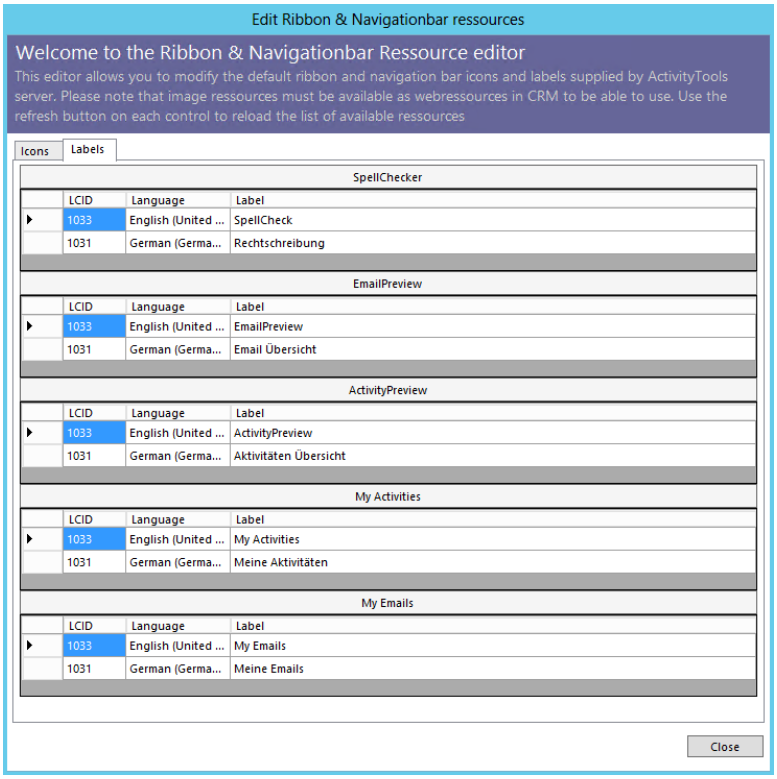
Display EmailPreview in Sitemap:
Check this option if you want to display "EmailPreview" in the CRM-Sitemap.

Display ActivityPreview in Sitemap:
Check this option if you want to display "ActivityPreview" in the CRM-Sitemap.

Advanced Labels:

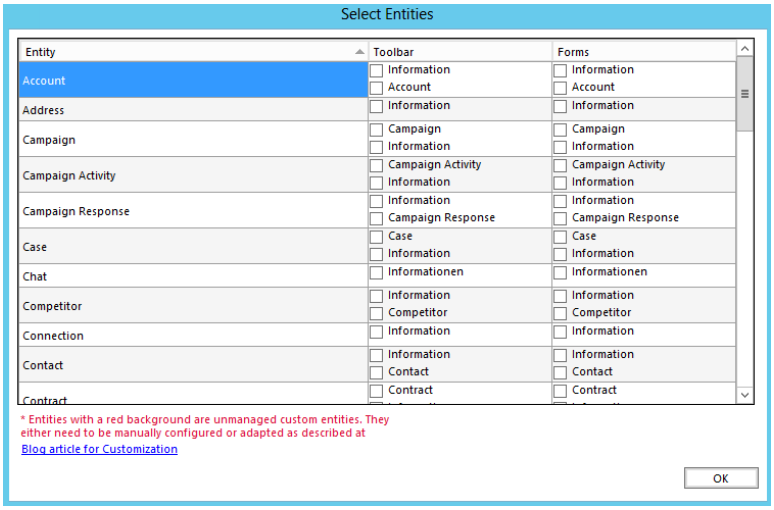
The Advanced Labels button allows you to modify the default ribbon and navigation bar icons and labels supplied by ActivityTools server. Note: the Image ressources must be available as webressources in CRM to be able to use. Click on the refresh button on each control to reload the list of available ressources. See screenshots below:





2 Entity Configuration

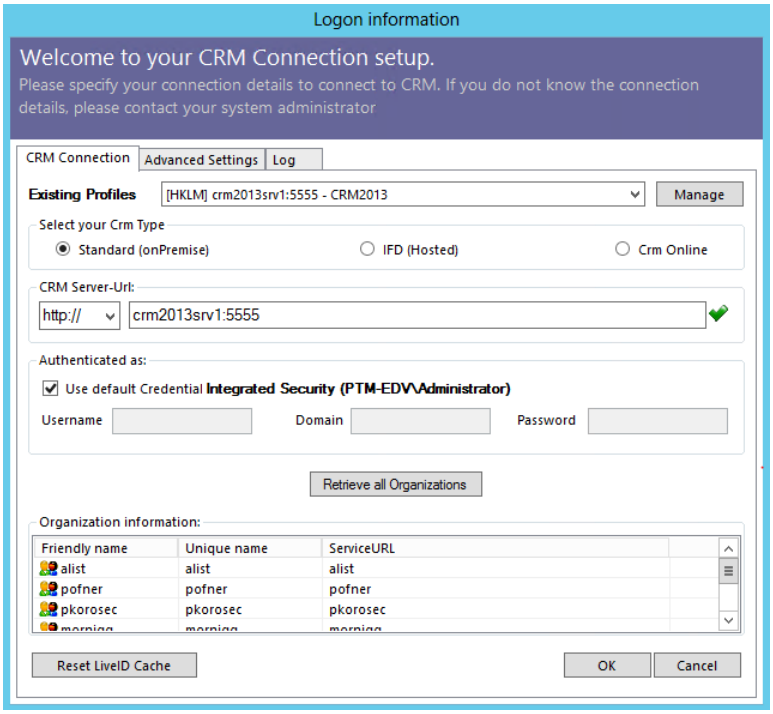
Enable the email preview/ activity preview in entity details:
Here you can specify which entities should display the email or activity preview in the entity details. Following window will appear. Check your entities:



Activate the search-option as index search:
CRM defaults to a search where the search-term has to start with the defined term unless you define a wildcard (*) before your search term. Enabling this option will always include the leading wildcard in the search.

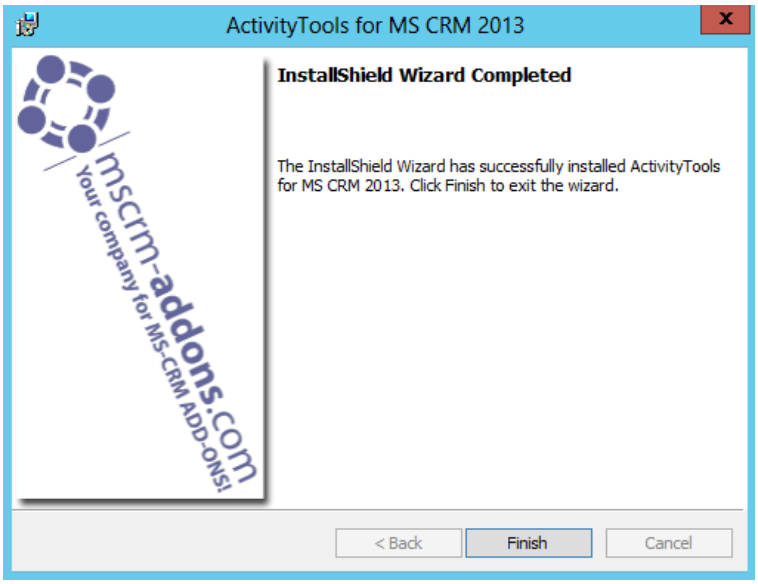
3 Change Connection

Click here to change your CRM-connection details. Please enter your system administrator if you don't know the connection details.



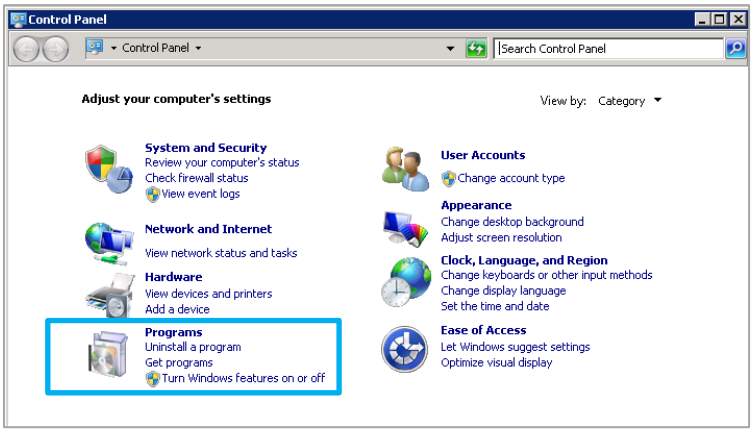
7 Complete the installation

The installation was successful. Click on [Finish] to finish the installation and to exit the installer.

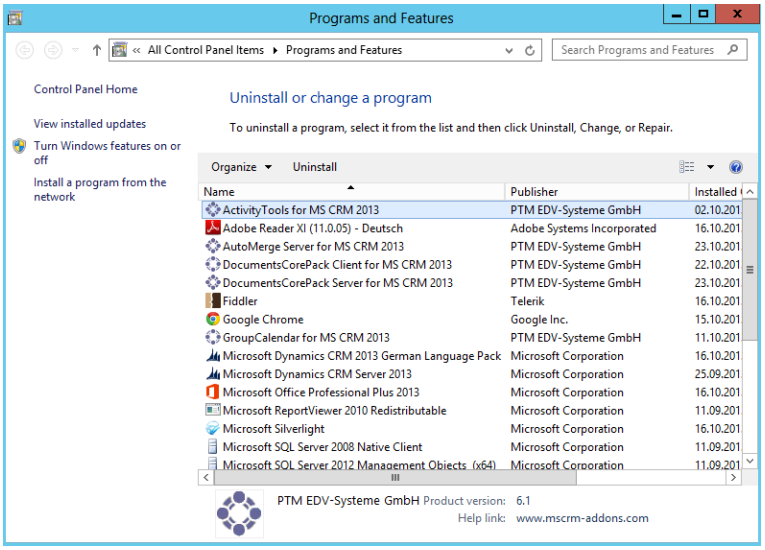


8 Uninstall

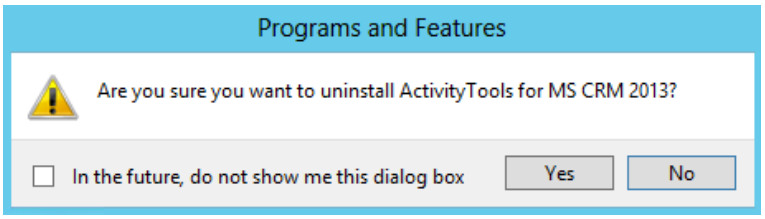
To uninstall ActivityTools select Programs in Control Panel.



Search for ActivityTools CRM 2013 in “Uninstall or change a program” to uninstall ActivityTools. Follow the instructions to uninstall the addon. See screenshots below:



Click on [Yes] to uninstall ActivityTools for MS CRM 2013.



8 How to install ActivityTools in an IFD/Claims-Based-Environment

This chapter will walk you through the required steps to install ActivityTools in an IFD/Claims-Based-Environment.

You need to have the following downloads present to successfully setup the Addon:

1. IFD-Tool -> Download Link, you need to have a login on our web site
2. For installing ActivityTools you need at least version 5.13 from our Download Section

Before you start installing, MS CRM is required to be working correctly in IFD/Claims-Mode, including your ADFS, which should be installed correctly and configured to work with MS CRM.

More details on how to configure MSCRM for IFD/Claims can be found in the Microsoft Guide "Configuring Claims-based Authentication for Microsoft Dynamics CRM 2011" Download.

The following system configuration is the basis for our guide. Your setup will differ in these URLs, make sure you are replacing the URLs with your own URLs when following the guide. ActivityTools has to be configured with an http AND an https port.

Internal Url used to access Microsoft Dynamics CRM:
https://internalcrm.rc1ifd.ptm-edv.at

External Url used to access Microsoft Dynamics CRM:
https://[orgname].rc1ifd.ptm-edv.at

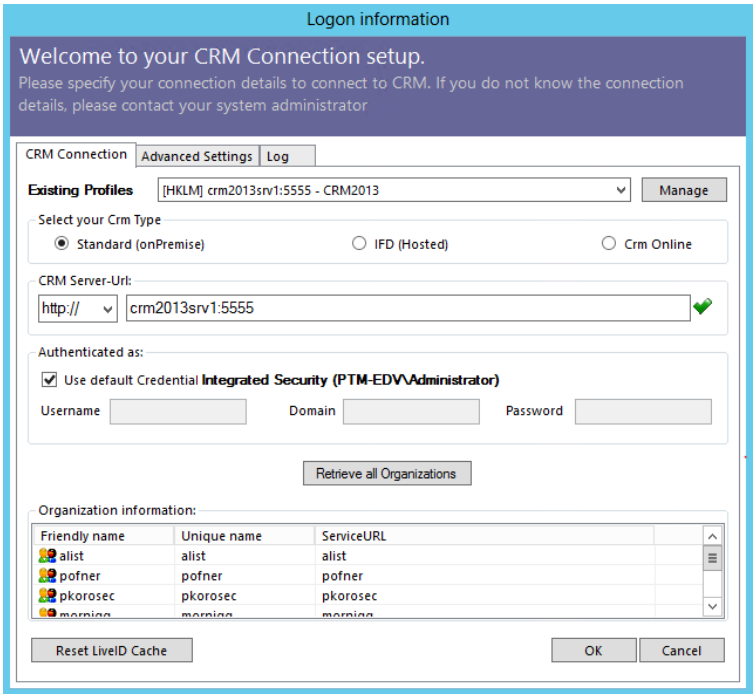
AD FS Server:
https://win2008domain.ptm-edv.at

The Addon itself also requires a dns name:
https://activitytoolsserver.rc1ifd.ptm-edv.at

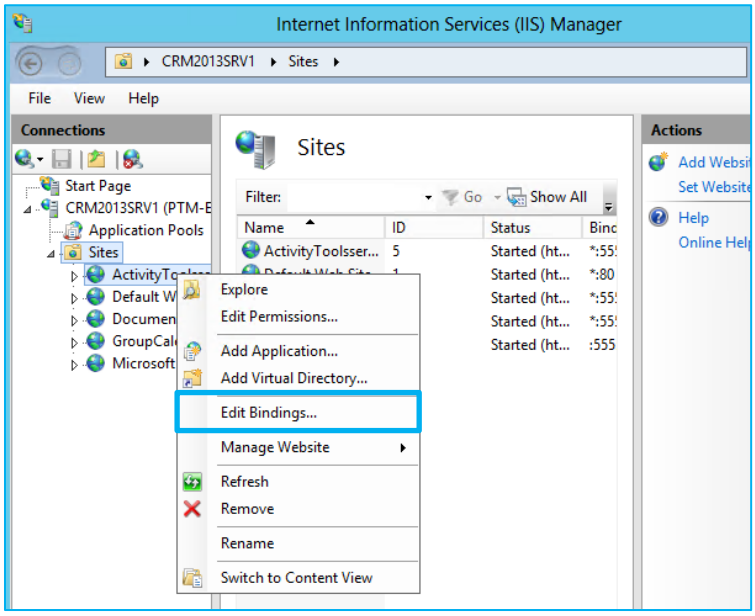
Basic installation/configuration of our Add-On:

1. Install the Addon on the CRM Server.

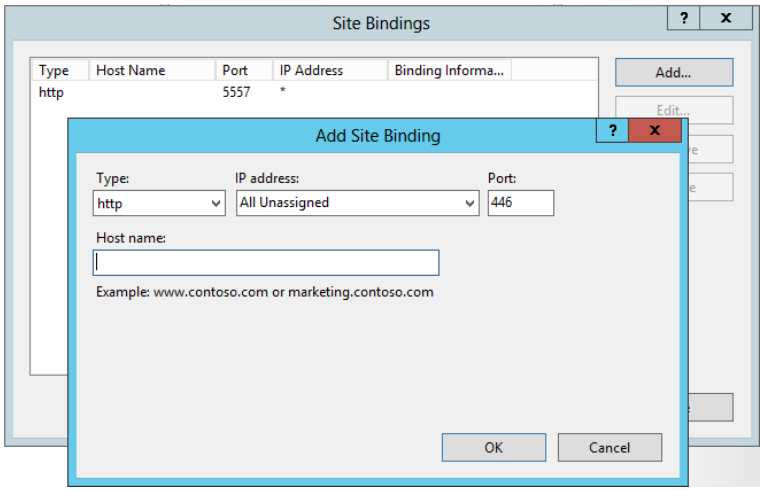
2. You will be asked for the Logon Information. Fill in the internal IFD name of your CRM. In our case, it is internalcrm.rc1ifd.ptm-edv.at. Select the organization on which you want to install the Addon and click on OK. See next screenshot:



3. After the installation is finished, you have to open the IIS (inetmgr.exe) and to go to Sites-> the Addon web site. Right click the ActivityToolsserver – web site and select "Edit Bindings..."



On the Bindings click on "Add..."and select in the "Add Site Binding" the type "https".
You also have to specify the port in our example we use 4446

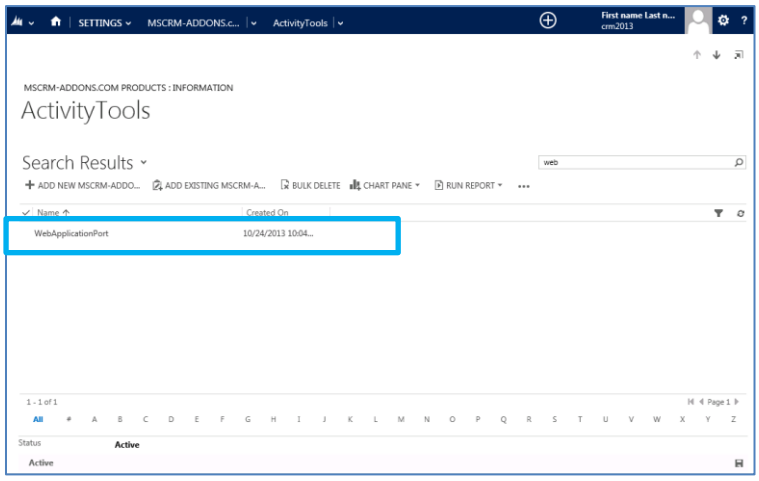


4. Reselect the Addon website and double click on the "Authentication" item in the right side details pane. Verify that the options "Anonymous" and "ASP.Net Impersonation" settings are enabled.

5. The Addon url needs to be added to your DNS Server. Your DNS-Servers have to resolve the activitytoolsserver.[your-domain] names correctly. This means that they should resolve it with the same ip address as your CRM Server has. IF you are also using an external DNS, make sure that both external and internal DNS are able to resolve the URL.

6. Extract the IFD-Tool (zip-File) that you downloaded before and execute the IFDSetupWizard.exe. Follow the steps in the IFD Setup carefully.

7. Open your CRM in Internet Explorer and go to "Settings" -> "MSCRM-ADDONS.com Products" -> Open ActivityTools -> within the MSCRM-ADDONS.com Products form, select the MSCRM-ADDONS.com Settingskeys and search for the "WebApplicationPort" entry.



8. Open the WebApplicationPort and replace the existing KeyValue with the following: [httpsPort]|[httpPort]|[claimsbased]|[addonname]|[debugging], e.g.: 4446|5557|true|activitytoolsserver|false

You have finished the configuration of the CRM part and now need to **configure the AD FS.**

NOTE: If you use AD FS you have to perform the IFD wizard again, if the https certificate and/or the TokenSignal certificate expire on AD FS.

1. Please logon your AD FS Server and start AD FS 2.0 Management.

2. On the Actions menu located in the right column, click Add Relying Party Trust.

3. In the Add Relying Party Trust Wizard, click Start.

4. On the Select Data Source page, click Import data about the relying party published online or on a local network, and then type the URL to locate the federationmetadata.xml file.

   This federation metadata is created with the IFD-Tool on the CRM Server.
   For example, https://activitytoolsserver.rc1ifd.ptm-edv.at:4446/FederationMetadata/2007-06/FederationMetadata.xml

   Type this URL in your browser and verify that no certificate-related warnings appear.

5. Click Next.

6. On the Specify Display Name page, type in a display name, such as ActivityTools IFD, and click on Next.

7. On the Choose Issuance Authorization Rules page, leave the "Permit all users to access this relying party"-option selected, and then click Next.

8. On the Ready to Add Trust page, click Next, and then click Close.

9. If the Rules Editor appears, click Add Rule. Otherwise, in the Relying Party Trusts list, right-click the relying party object that you created, click Edit Claims Rules, and then click Add Rule. Important: Be sure the Issuance Transform Rules tab is selected.

10. In the Claim rule template list, select the Pass Through or Filter an Incoming Claim template, and then click Next.

11. Create the following rule:
    • Claim rule name: Pass Through UPN (or something descriptive)
    • Add the following mapping:
    i. Incoming claim type: UPN
    ii. Pass through all claim values

12. Click Finish.

13. In the Rules Editor, click Add Rule, and in the Claim rule template list, select the Pass Through or Filter an Incoming Claim template, and then click Next:
    • Claim rule name: Pass Through Primary SID (or something descriptive)
    • Add the following mapping:
    i. Incoming claim type: Primary SID
    ii. Pass through all claim values

14. Click Finish.

15. In the Rules Editor, click Add Rule.

16. In the Claim rule template list, select the Transform an Incoming Claim template, and then click Next.

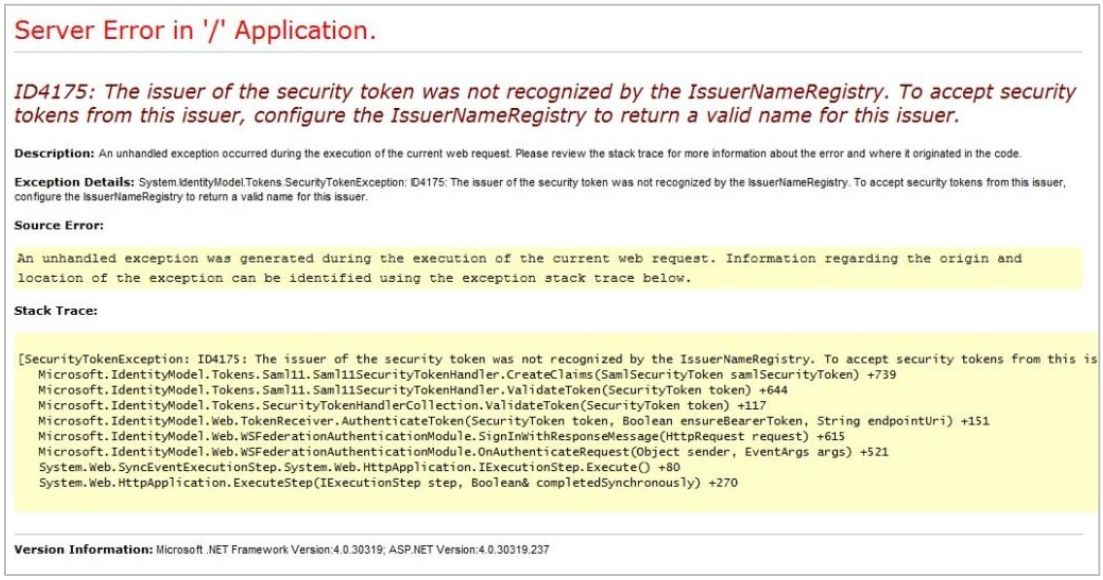
17. Create the following rule:
    • Claim rule name: Transform Windows Account Name to Name
    (or something descriptive)
    • Add the following mapping:
    i. Incoming claim type: Windows account name
    ii. Outgoing claim type: Name
    iii. Pass through all claim values

18. Click Finish, and when you have created all three rules, click OK to close the Rules Editor.

You have finished the configuration and you should be able to use the Addon in your IFD/Claims Environment now.

9 Troubleshooting

If you see the following error, there may be two reasons for this:



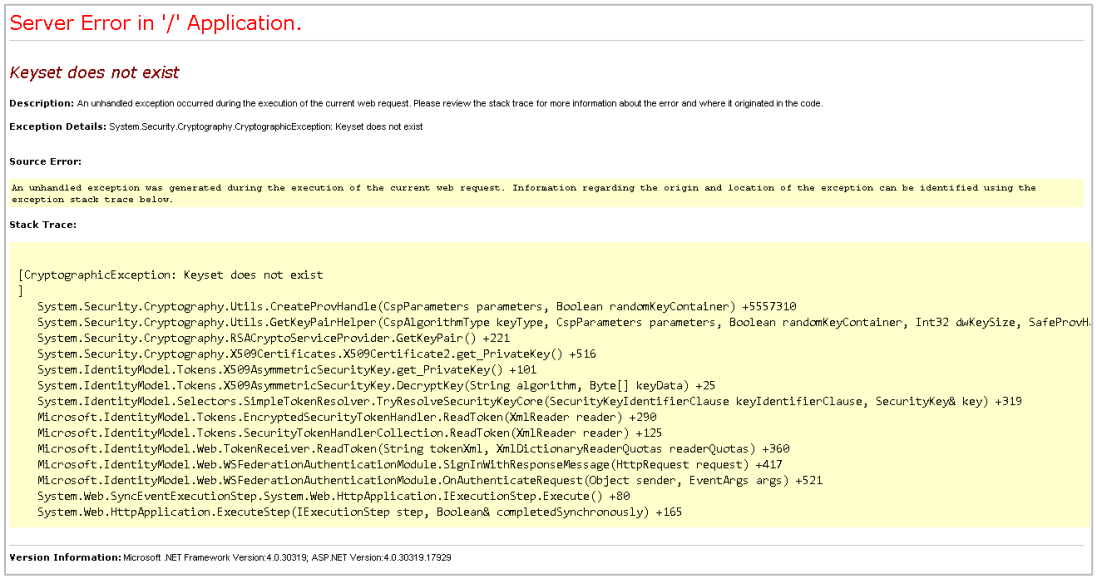
Reason 1:

This indicates that you are using a wrong certificate for the ADFS signing. Make sure the thumbprint in the web.config matches the one in the token signing certificate in ADFS.

```
<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>
```

If you see the following error:



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

Reason 2:
This error could also indicate access rights problems with the certificates private key (Mainly an issue for self-signed certificates).

Open your certificate store on the server (MMC, add certificate snap-in for local computer) and find your HTTPS certificate. In the context menu, under all tasks, select the "manage private keys" option and grant access to everyone.

Checklist for general troubleshooting:

- Is the Setting WebApplicationPort still intact?
- Are there any not http/https bindings in CRM?
- Are there any not http/https bindings in the products website?
- Is the DNS correctly resolving the products link?
- Has the ConnectionProfile been created with IFD as connection type?
- Is the firewall allowing the required ports both internally and externally?

10 Contact

If you have questions to the product send an Email to
support@mscrm-addons.com
or visit our 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