Foxit®

Developers Guide

Foxit® RMS PDF Protection Tool

Microsoft® Partner
Gold Independent Software Vendor (ISV)

Prerequisites

Step 1: Install the AD RMS Services Client

To run this SDK, you must have the latest version of the AD RMS client installed. If you have an existing older version of the AD RMS client installed, you will need to uninstall it first and then download and install the latest version of the AD RMS client (http://www.microsoft.com/en-us/download/details.aspx?id=38396).

As for using Windows Azure AD Right Management (AAD RMS), please refer to the Quick Start for Using Windows Azure AD Right Management.

Step 2: Install and configure RMS Server

About how to install and configure an RMS Server, please see AD RMS Step-by-Step Guide .

How to use the SDK

i. Unzip the installation package to a directory, for example, D:\ Foxit RMS PDF Protection Tool(SDK).
ii. Add the file frms.h under the directory "Foxit RMS PDF Protection Tool(SDK)\include" to your project, so that you can check each interface conveniently.
iii. Add the file FPDFRMS.lib to the project, for example, add *#pragma comment(lib,"D:\\ Foxit RMS PDF Protection Tool(SDK)\\library\\FPDFRMS.lib")* to the file stdafx.cpp (pre-compiled file).
iv. Include the header file frms.h in the file which needs to use SDK interfaces, for example, add *include " D:\\ Foxit RMS PDF Protection Tool(SDK)\\library\\frms.h"* to the file stdafx.h (pre-compiled file).
v. Copy the file FPDFRMS.dll under “Foxit RMS PDF Protection Tool(SDK)\library” to the same directory where your application program locates.

Running Your Application

In order to run your RMS application you need to generate a signed application manifest. This guide shows how to generate a manifest

On your development machine:

1. Copy the following files to a single directory:

    - “Foxit RMS PDF Protection Tool(SDK)\tools\Genmanifest.exe”

- “Foxit RMS PDF Protection Tool(SDK)\tools\ isvtier5appsigningprivkey.dat”
- “Foxit RMS PDF Protection Tool(SDK)\tools\ isvtier5appsigningpubkey.dat”
- “Foxit RMS PDF Protection Tool(SDK)\tools\ isvtier5appsignsdk_client.xml”
- “Foxit RMS PDF Protection Tool(SDK)\tools\< YourAppName >.bat”
- “Foxit RMS PDF Protection Tool(SDK)\tools\< YourAppName >.mcf”
- < YourAppName >.exe

Note: If it's the pre-production environment, please copy the files “isvtier5appsigningprivkey.dat”, “isvtier5appsigningpubkey.dat” and “isvtier5appsignsdk_client.xml” under the directory of “FoxitPDF_ADRMS_SDK_10\tools\pre-production”.

2. In this same directory, use notepad.exe to open the file < YourAppName >.mcf. Modify the option **REQ HASH "YourAppName.exe"**, and fill in the name of your application program. The file should have the following contents:

```
AUTO-GUID

"isvtier5appsigningprivkey.dat"

MODULELIST

REQ HASH "YourAppName.exe"

POLICYLIST
    INCLUSION
        PUBLICKEY "isvtier5appsigningpubkey.dat"
    EXCLUSION
```

NOTE: Ensure that “YourAppName.exe” is consistent with the actual < YourAppName >.exe.

3. In this same directory, use notepad.exe to open the file < YourAppName >.bat. Modify the option YourAppName.exe.man, and fill in the name of your application program. The file should have the following contents:

```
cd %~dp0
genmanifest.exe -chain isvtier5appsignsdk_client.xml YourAppName.mcf
YourAppName.exe.man
```

NOTE: Ensure that the file YourAppName.mcf and the file “YourAppName” under YourAppName.exe.man are consistent with the actual ones.

4. You will get a file “YourAppName.exe.man” by double-clicking the file YourAppName.bat.

Note: If the program YourAppName.exe has been modified, you should regenerate the file < YourAppName >.exe.man.

5. Copy the following files to your RMS server:

   - < YourAppName >.exe
   - < YourAppName >.exe.man
   - FPDFRMS.dll

6. Run your application. You can run the application from any directory, but your generated manifest (<YourAppName >.exe.man and FPDFRMS.dll) must be in the same directory as < YourAppName >.exe

How to build your application

1. Before you can call any functions, you need to first call FRMS_UnlockLibrary function to unlock the library. If you are in free 30-day trial, don't pass any parameter to the function FRMS_UnlockLibrary, for example, FRMSAPI FRMS_HRESULT FRMS_UnlockLibrary().

Example:

```
// Use the Key information to unlock the library
FRMS_HRESULT hr =
FRMS_UnlockLibrary("XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX");
if (FRMS_HRESULT_OK != hr)
{
    DisplayFRMSError(hr);
    goto Exit;
}
```

2. Initialize the SDK with FRMS_Initialize. Before the application exits, destroy the library to release resources.

Example:

```
//Initalize the SDK with library
hr = FRMS_Initialize(FRMS_API_MODE_CLIENT);
if (FRMS_HRESULT_OK != hr)
{
    DisplayFRMSError(hr);
    goto Exit;
}

//Release all resources allocated by the SDK library
if(Null != hProtector)
```

```
{
    FRMSProtector_Release(hProtector);
}
.
```

NOTE: If failing to call the function, 1. ensure you have called the function FRMS_UnlockLibrary successfully. 2. check whether the AD RMS environment has been set up correctly if the function FRMS_UnlockLibrary is returned successfully.

3. Sets the source to be protected. It can be a folder containing PDF files or can be a PDF file path.

Example:

```
//Set the PDF file path
wchar_t wsSource[20] = L"C:\\test.pdf";
FRMS_HPROTECTOR hProtector = NULL;
Hr = FRMSProtector_Create(&hProtector);
if (NULL != hProtector)
{
    hr = FRMSProtector_SetSource(hProtector,wsSource);
    if(hr != FRMS_HRESULT_OK)
    {
        DisplayFRMSError(hr);
        goto Exit;
    }
}
```

4. Get all Issuers.

Example:

```
int nCount = 0;
// Gets the count of issuers
hr = FRMSProtector_GetIssuerCount(hProtector, this->GetSafeHwnd(), &nCount);
if(hr != FRMS_HRESULT_OK)
{
    DisplayFRMSError(hr);
    goto Exit;
}
for(int i=0; i<nCount; i++)
{
    LPWSTR lpwsIssuer = NULL;
    int nLen = 0;
    // Gets the length of the issuer name
    hr = FRMSProtector_GetIssuer(hProtector, i, this->GetSafeHwnd(), lpwsIssuer, &nLen);
    if(hr != FRMS_HRESULT_OK)
```

```
    {
        DisplayFRMSError(hr);
        goto Exit;
    }
    lpwsIssuer = new wchar_t[nLen];
    memset(lpwsIssuer, 0, sizeof(wchar_t)*nLen);
    //Gets the issuer name by index
    hr = FRMSProtector_GetIssuer(hProtector, i, this->GetSafeHwnd(), lpwsIssuer, &nLen);
    if(hr != FRMS_HRESULT_OK)
    {
        DisplayFRMSError(hr);
        delete [] lpwsIssuer;
        goto Exit;
    }
}
```

5. Get the number of Rights Poilcy Template.

Example:

```
int nTemplateCount = 0;
//Gets the count of RMS rights policy templates of the specified issuer.
hr = FRMSProtector_GetTemplateCount(hProtector, lpwsIssuer, TRUE, this->GetSafeHwnd(),
&nTemplateCount);
if (hr != FRMS_HRESULT_OK)
{
    DisplayFRMSError(hr);
    delete [] lpwsIssuer;
    goto Exit;
}
```

6. Get the names of all templates.

Example:

```
for(int j=0; j<nTemplateCount; j++)
{
    LPWSTR lpwsName = NULL;
    int nLen = 0;
    // Gets the length of the template name
    hr = FRMSProtector_GetTemplateName(hProtector, j, lpwsIssuer, this->GetSafeHwnd(),
lpwsName, &nLen);
    if(hr != FRMS_HRESULT_OK)
    {
        DisplayFRMSError(hr);
        delete [] lpwsIssuer;
```

```
            goto Exit;
        }
        lpwsName = new wchar_t[nLen];
        memset(lpwsName, 0, sizeof(wchar_t)*nLen);
        // Gets the name of RMS rights policy template by specified index.
        hr = FRMSProtector_GetTemplateName(hProtector, j, lpwsIssuer, this->GetSafeHwnd(),
lpwsName, &nLen);
        if(hr != FRMS_HRESULT_OK)
        {
            DisplayFRMSError(hr);
            delete [] lpwsName;
            delete [] lpwsIssuer;
            goto Exit;
}
}
```

7. Set the template which is used to encrypt documents, and ensure this template can be retrieved on the AD RMS server.

Example:

```
LPCWSTR lpwsIssuerName = L"IssuerName";
LPCWSTR lpwsTemplateName = L"TemplateName";
//Sets the current RMS rights policy template name used to protect the source.
hr = FRMSProtector_SetTemplate(hProtector, lpwsIssuerName, lpwsTemplateName,NULL);
if (hr != FRMS_HRESULT_OK)
{
    DisplayFRMSError(hr);
    goto Exit;
}
```

8. Finally, you can do the actual encryption.

Example:

```
hr = FRMSProtector_Protect(hProtector, 0 , NULL);
if (hr != FRMS_HRESULT_OK)
{
    DisplayFRMSError(hr);
    goto Exit;
}
```

9. Throughout this example application the DisplayFRMSError function is being used to handle errors.

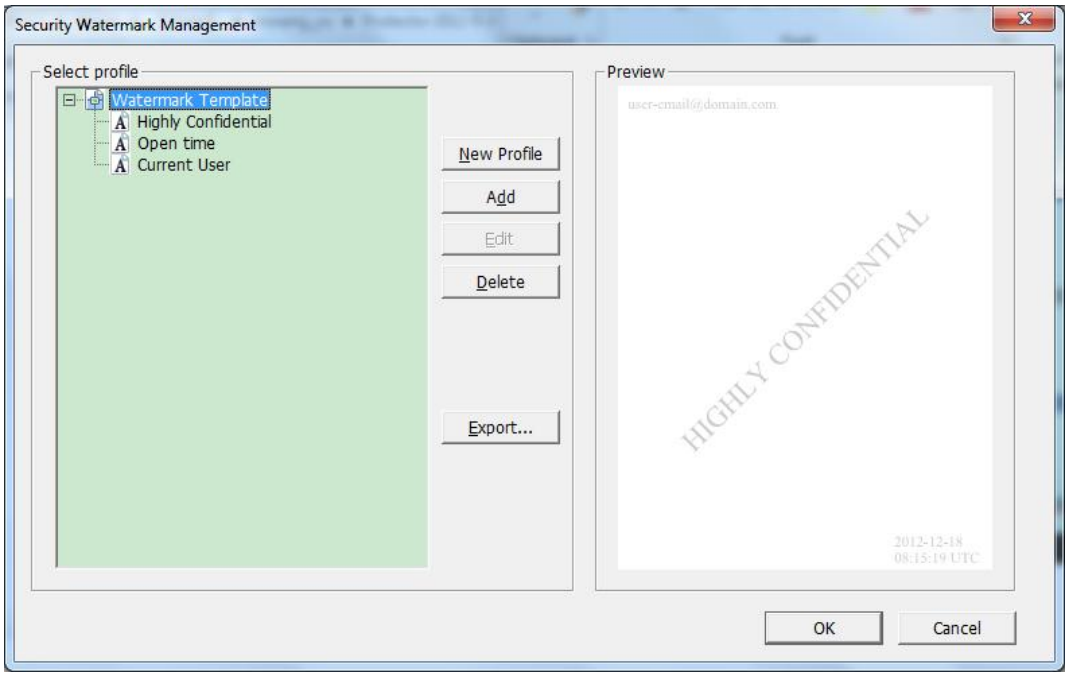
Example:

```
void DisplayFRMSError(HRESULT hr)
```

```
{
    LPWSTR lpwsText = NULL;
    int nLen = 0;
    FRMS_HRESULT hrGet = FRMS_GetErrorMessage(hr, 1033, lpwsText, &nLen);
    if(hrGet == FRMS_HRESULT_OK)
    {
        lpwsText = new wchar_t[nLen];
        memset(lpwsText, 0, sizeof(wchar_t)*nLen);
        hrGet = FRMS_GetErrorMessage(hr, 1033, lpwsText, &nLen);
        wprintf(L"%s\r\n", lpwsText);
        delete [] lpwsText;
    }
}
```

Add Security Dynamic Watermark to the File Encrypted by RMS

1. Unzip the installation package on RMS server.
2. Run the file “Foxit Security Watermark Configuration Tool.exe” in “tool” folder to open Security Watermark Management.
3. Create a required watermark and export it.



a. Add a Watermark
   i. Click New Profile to create a profile and name it.
   ii. Select a profile you created and click Add to add watermarks in the profile.
   iii. Type the watermark’s name.
   iv. Type the watermark’s content in the text box and set the font, size, color, underline, and

alignment.

Note: you can only set text as watermark.

v. Choose the Dynamic Text. When any PDF reader opens the file, the watermark will show the current document information dynamically and you can use multiple text at the same time.

Document Title: shows the current document title.
Author: shows the author of current document.
Current User: shows the current user who is reading the document.
Date: shows the current system date when opening the document.
Day: shows the current system day when opening the document.
Month: shows the current system month when opening the document.
Year: shows the current system year when opening the document.
Time: shows the current system time when opening the document.
Hour: shows the current system hours when opening the document.
Minute: shows the current system minutes when opening the document.
Second: shows the current system seconds when opening the document.

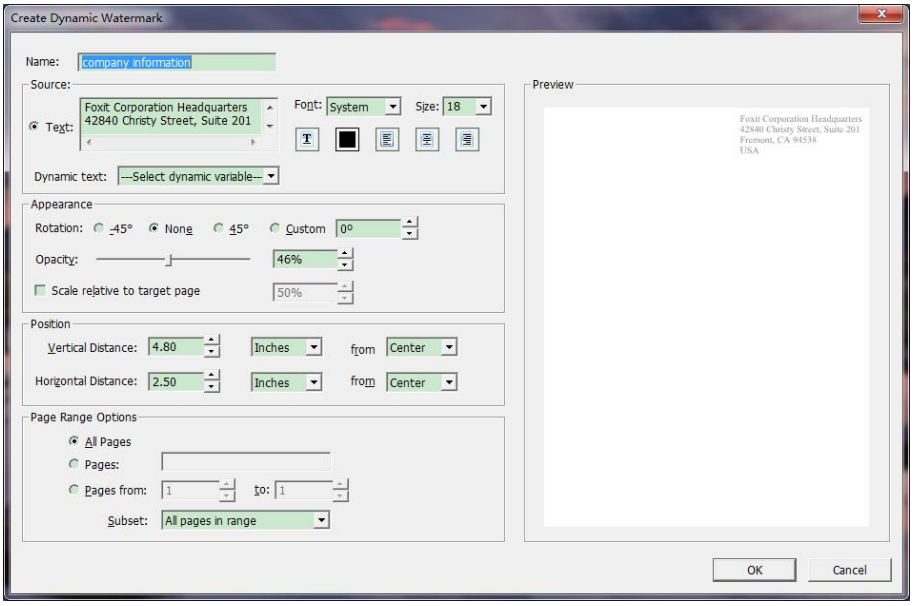
vi. Set the appearance by choosing the rotation degree and the opacity. You also have the option to make the scale relative to target page.

vii. Set the vertical and horizontal distance between the target page and the watermark.

viii. Choose the page range to play the watermark. You can select the different page range options via clicking the right items in the subset list.

ix. Preview the watermark in the right pane.

x. Click OK to finish it.



b. Editing or Deleting Watermark

Editing a Watermark

i. Open the Security Watermark Management and select a watermark you want to edit.
ii. Click **Edit** to open the Create Security Watermark dialog box.
iii. Begin editing the watermark, please refer to "Adding Watermark".
iv. Click **OK** to finish the operation.

Deleting a Watermark
Open the Security Watermark Management and select a watermark you want to delete.
Click **Delete** to remove the selected watermark.

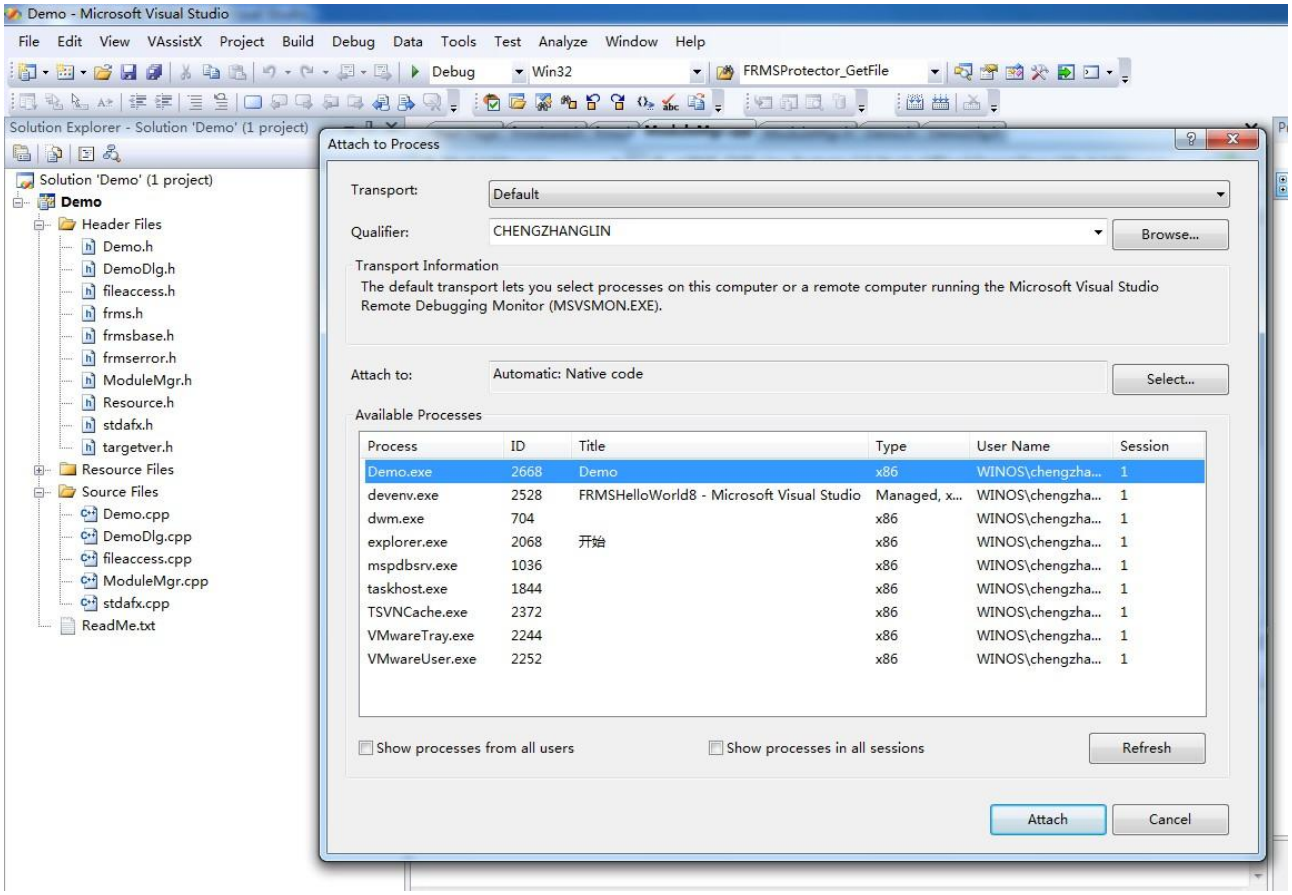
Exporting a Watermark
xi. Open the Security Watermark Management and select a watermark you want to export.
xii. Click Export and choose a file type and location to save.
xiii. The watermark will be exported as an encoded file (.txt format).

4. Open the file "Add Security Watermark.vbs" in "tool" folder with Notepad.exe.
5. Find the text (templateName = "") and type in the name of the template which needs to be added to the exported watermark.
6. Fill in the following content according to the exported watermark:
appDataName = ""
appDataValue = ""
7. Run "Add Secrity Watermark.vbs" and the watermark will be added to the target template.

How to debug applications that use RMS PDF Protection Tool

If the parameter you passed is FRMS_API_MODE_SERVER when calling the function "FRMS_Initialize", you can toggle breakpoint and debug the program directly.
If the parameter you passed is FRMS_API_MODE_CLIENT when calling the function FRMS_Initialize, the anti-debugging checks in the developer version of our runtime are disabled.

For Visual Studio 2005 or later：
You can turn on debug tracing by using the following steps:
1. Call the function afxmessageBox when you need to debug.
2. Run your program.
3. When the dialog box afxmessageBox pops up, choose the option *Attach to Process…* under the menu Debug of the Visual Studio. In the dialog box, choose your application program and click *Attach*
but



4. Set the debugging breakpoint behind AfxMessageBox. When you close the dialog box AfxMessageBox, the breakpoint will be activated.

For VC6.0:

1. Open regedit.exe and navigate to HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/WindowsNT/CurrentVersion/AeDebug
2. Change the following key values:

Key :Auto
Value: 0

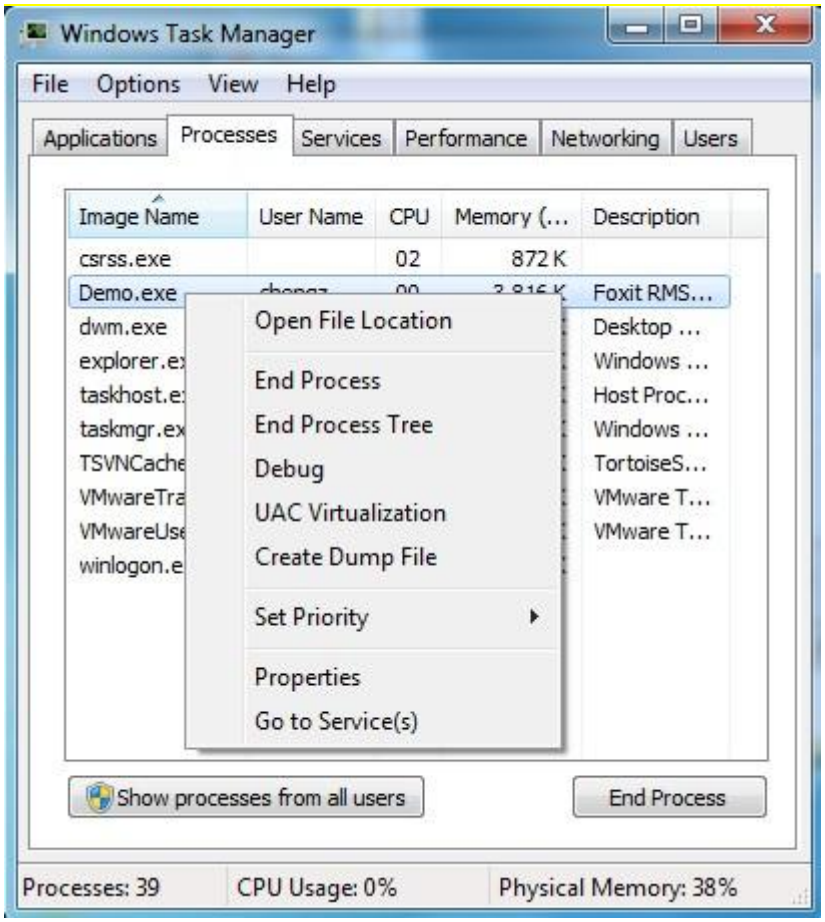
Key: Debugger
Value: C:\Program Files\Microsoft Visual Studio\Common\MSDev98\Bin\msdev.exe" -p %ld -e %ld
NOTE: Ensure that “YourAppName.exe” is consistent with the actual msdev.exe.

Key: UserDebuggerHotKey
Value: 0

3. Restart your computer.
4. Call the function afxmessageBox when you need to debug.
5. Run your program. Then the dialog box afxmessageBox pops up.

6. Open Windows Task Manager.

7. Right-click on your application and choose Debug. VC6.0 will be started automatically.



i. Open the debug file and set the debugging breakpoint behind AfxMessageBox. When you close the dialog box AfxMessageBox, the breakpoint will be activated.

How to understand common error conditions and solutions

1. When running your application, the error prompt may appear as below:

This application is not trusted to consume rights managed content. The application's rights management manifest is missing or is not valid. Contact your application support for further investigation.

Action required to fix the error:

Make sure you regenerate your application manifest every time you rebuild your application.

2. When running your application, the error prompt may appear as below:

This operation could not be completed because a debugger was detected.

Action required to fix the error：

Please choose the option **Start without debugging** under the menu Debug of the Visual Studio to debug and run your program.

Quick Start for Using Windows Azure AD Right Management

Enable Windows Azure AD Rights Management for your organization:

- Download the Windows Azure AD Rights Management administration module (WindowsAzureADRightsManagementAdministration.exe) for Windows PowerShell from here.
- In the local folder where you downloaded and saved the Rights Management installer file, double-click the file WindowsAzureADRightsManagementAdministration.exe to launch installation of the Rights Management administration module.
- Open Windows PowerShell.
- Type the following commands:

  ✓ Import-Module AADRM
  ✓ Connect-AadrmService -Verbose

- Enter your Office 365 credentials when prompted, for example“user@company.onmicrosoft.com”.
- Type the following commands:

  ✓ Enable-Aadrm
  ✓ Disconnect-AadrmService

Contact Us

Feel free to contact Foxit should you need any information or have any problems with our products. We are always here, ready to serve you better.

- ***Office Address:***
  Foxit Corporation
  42840 Christy Street. Suite 201
  Fremont CA 94538
  USA
- ***Mailing Address:***
  Foxit Corporation
  42840 Christy Street. Suite 201
  Fremont CA 94538
  USA
- ***Sales:***
  1-866-680-3668 (24/7)
- ***Support:***
  1-866-MYFOXIT or 1-866-693-6948 (24/7)
- ***Fax:***
  530-535-9288
- ***Website:***
  www.foxitsoftware.com
- ***E-mail:***
  Sales and Information - sales@foxitsoftware.com
  Technical Support - support@foxitsoftware.com
  Marketing Service - marketing@foxitsoftware.com