|  |
| --- |
|  |
| **CIAPV7.0**  **.net应用集成接口说明** |
| **版权声明和保密须知**  本文件中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属江苏金智教育信息股份有限公司所有，受到有关产权及版权法保护。任何单位和个人未经江苏金智教育信息股份有限公司的书面授权许可，不得复制或引用本文件的任何片断，无论通过电子形式或非电子形式。  **Copyright © 2015江苏金智教育信息股份有限公司版权所有** |

修改记录表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序 | 修改人 | 修改内容 | 批准人 | 生效日期 | 版本号 |
| 1 | 许继锋 | 创建文档 |  |  | V0.1 |
| 2 | 黄敏 | 完善文档 |  |  | V1.0 |
| 3 | 刘伟锋 | 完善集成内容 |  | 2016-05-25 | V1.1 |
| 4 | 刘伟锋 | 增加.net退出地址 |  | 2016-06-23 | V1.2 |
| 5 | 刘伟锋 | 完善集成demo |  | 2016-11-23 | V1.3 |
| 6 | 刘晓峰 | 更新为适配CIAP7.0版本 |  | 2020-06-16 | V2.0 |

文件信息

|  |  |
| --- | --- |
| **起草人：**刘伟锋 | **审核人：**刘传先 |
| **批准人：**刘传先 | **生效日期：**2015年11月23日 |
| **【文件摘要】**本文件针对CIAP7.0的实施及升级工作进行了纲领性描述，以做为本产品的实施指南。  **【阅读须知】**读者需要熟悉《CIAP7.0术语清单》，并了解项目管理相关要求。  **【发布范围】**产品经理、产品工程部、产品实施人员（含项目经理、合作伙伴等）。  **【发布方式】**小助手平台。 | |

目 录

[1 前言 1](#_Toc467672710)

[1.1 编写目的 1](#_Toc467672711)

[1.2 服务对象 1](#_Toc467672712)

[2 集成方式概述 2](#_Toc467672713)

[3 .net认证接口集成 3](#_Toc467672714)

[3.1 认证接口工作过程 3](#_Toc467672715)

[3.2 拷贝提供的dll文件 3](#_Toc467672716)

[3.3 用户属性获取代码参考 4](#_Toc467672717)

[3.4 修改web.config文件 5](#_Toc467672718)

[3.5 退出地址 10](#_Toc467672719)

[4 demo实例 12](#_Toc467672720)

[4.1 windows下配置IIS搭建程序运行环境 12](#_Toc467672721)

[4.2 部署dotnet的cas\_demo 16](#_Toc467672722)

[4.3 在身份认证管理平台注册集成demo 24](#_Toc467672723)

[4.4 部署demo常遇到的错误 26](#_Toc467672724)

# 前言

## 编写目的

本文档作为CIAP7.0版本中应用系统的认证集成手册，旨在指导校内应用系统实现校内统一身份认证和单点登录集成。

## 服务对象

|  |  |
| --- | --- |
| **读者对象** | **阅读范围** |
| 产品开发项目组人员 | 能熟悉掌握整个产品的流程和实施方法，能做到顺利完成产品项目或指导产品项目的实施。 |
| 产品维护人员 | 阅读全部内容 |
| 工程项目经理 | 阅读全部内容 |
| 产品部署实施人员 | 阅读全部内容 |

# 集成方式概述

将高校的各个业务系统与身份管理平台连接，通过身份管理平台实现用户身份认证和单点登录功能，这个过程即应用系统与身份管理平台的集成。CIAP7.0主要包括以下集成方式：

* 认证接口：这是各个应用系统与身份管理平台集成的最主要的方式。各应用将认证接口的客户端开发包集成在各应用之中，替换自身原有独立的身份认证功能，通过身份管理平台实现身份认证和单点登录过程。该接口目前NET(2.0+)语言和平台的应用程序。
* LDAP接口：对于选课选这样的高并发应用，我们提供LDAP接口，以满足认证的性能需求。该接口直接通过LDAP向应用系统提供认证服务，但是牺牲了单点登录功能。



# .net认证接口集成

代理认证配置完后，均需至统一身份管理平台授权访问。先登录身份认证管理平台，在认证管理的认证应用模板，添加需代理认证的应用；添加完应用后，需给相应的组或者帐号授权，允许其访问该应用。

## 认证接口工作过程



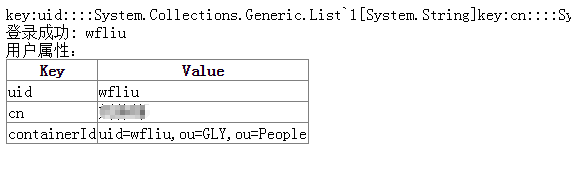
## 拷贝提供的dll文件

将“…/cas\_demo/ExampleWebSite/Bin”下DotNetCasClient.dll文件拷贝到客户端应用所在bin目录下，项目添加该dll的引用。

## 用户属性获取代码参考

代码源文件地址..\cas\_demo\ExampleWebSite\Userinfo.aspx.cs

查看用户信息地址：http://demo访问IP地址/Userinfo.aspx



|  |
| --- |
| public partial class Userinfo : System.Web.UI.Page  {  protected void Page\_Load(object sender, EventArgs e)  {  string userName = User.Identity.Name ;    CasPrincipal p =Page.User as CasPrincipal ;    //获得所有传递过来的用户属性  Dictionary<string, string> userAttrs = new Dictionary<string, string>();  var cnValue=UserAttrHelper.GetUserAttrValueByParamName("cn"); //姓名  var aliasValue=UserAttrHelper.GetUserAttrValueByParamName("alias"); //别名  userAttrs.Add("cn",string.Join(",",cnValue));  userAttrs.Add("alias", string.Join(",", aliasValue));    user.Text = userName.ToString();  attr.DataSource = userAttrs;  attr.DataBind();  }  } |

## 修改web.config文件

修改…\cas\_demo\ExampleWebSite\web.config；casClientConfig里设置环境信息，httpmodules为必选，否则不能实现单点登录。

|  |
| --- |
| <?xml version="1.0"?>  <configuration>  <configSections>  <section name="casClientConfig" type="DotNetCasClient.Configuration.CasClientConfiguration, DotNetCasClient"/>  <section name="FilterUrls" type="DotNetCasClient.Configuration.ReWritingConfigurationSetHandler, DotNetCasClient"/>  </configSections>  <appSettings/>  <connectionStrings/>  <casClientConfig casServerLoginUrl="http://authserver.xxx.edu.cn/authserver/login" casServerUrlPrefix="http://authserver.xxx.edu.cn/authserver/" serverName="http://oa.xxx.edu.cn" notAuthorizedUrl="~/NotAuthorized.aspx" cookiesRequiredUrl="~/CookiesRequired.aspx" redirectAfterValidation="true" gateway="false" renew="false" singleSignOut="true" ticketTimeTolerance="5000" ticketValidatorName="Cas20" serviceTicketManager="CacheServiceTicketManager" gatewayStatusCookieName="CasGatewayStatus"/>  <system.web>  <authentication mode="Forms">  <!--身份认证系统地址-->  <forms loginUrl="http://authserver.xxx.edu.cn/authserver/login" timeout="30" defaultUrl="~/Default.aspx" cookieless="UseCookies" slidingExpiration="true" path="/"/>  </authentication>  <authorization>  <allow users="\*"/>  </authorization>  <roleManager enabled="true" defaultProvider="AspNetReadOnlyXmlRoleProvider">  <providers>  <add name="AspNetReadOnlyXmlRoleProvider" type="DotNetCasClient.Security.ReadOnlyXmlRoleProvider" xmlFileName="~/App\_Data/UserRoles.xml"/>  </providers>  </roleManager>  <siteMap enabled="true">  <providers>  <clear/>  <add siteMapFile="Web.sitemap" name="AspNetXmlSiteMapProvider" type="System.Web.XmlSiteMapProvider"/>  </providers>  </siteMap>  <compilation debug="true" targetFramework="4.0">  </compilation>  <pages controlRenderingCompatibilityVersion="3.5" clientIDMode="AutoID">  <controls>  <add tagPrefix="cas" tagName="CookieViewer" src="~/Controls/CookieViewer.ascx"/>  <add tagPrefix="cas" tagName="TicketManager" src="~/Controls/TicketManager.ascx"/>  </controls>  </pages>  <httpModules>  <add name="DotNetCasClient" type="DotNetCasClient.CasAuthenticationModule,DotNetCasClient"/>  </httpModules>  </system.web>  <!--编写自定义的url过滤器，符合此过滤器的页面 地址不需要登录，也能访问-->  <FilterUrls>  <Rules>  <Url>  <ServletName>Test</ServletName>  <Url-Mapping>^/cas/test\_(/S\*)(.aspx)</Url-Mapping>  </Url>  </Rules>  </FilterUrls>  <system.diagnostics>  <trace autoflush="true" useGlobalLock="false"/>  <sharedListeners>  <add name="TraceFile" type="System.Diagnostics.TextWriterTraceListener" initializeData="C:\inetpub\DotNetCasClient.Log" traceOutputOptions="DateTime"/>  </sharedListeners>  <sources>  <source name="DotNetCasClient.Config" switchName="Config" switchType="System.Diagnostics.SourceSwitch">  <listeners>  <add name="TraceFile"/>  </listeners>  </source>  <source name="DotNetCasClient.HttpModule" switchName="HttpModule" switchType="System.Diagnostics.SourceSwitch">  <listeners>  <add name="TraceFile"/>  </listeners>  </source>  <source name="DotNetCasClient.Protocol" switchName="Protocol" switchType="System.Diagnostics.SourceSwitch">  <listeners>  <add name="TraceFile"/>  </listeners>  </source>  <source name="DotNetCasClient.Security" switchName="Security" switchType="System.Diagnostics.SourceSwitch">  <listeners>  <add name="TraceFile"/>  </listeners>  </source>  </sources>  <switches>  <add name="Config" value="Information"/>  <add name="HttpModule" value="Verbose"/>  <add name="Protocol" value="Information"/>  <add name="Security" value="Information"/>  </switches>  </system.diagnostics>  </configuration> |

## 退出地址

代码源文件地址..\cas\_demo\ExampleWebSite\Logout.aspx.cs

红色部分为学校身份认证地址，service填写登出回跳地址。

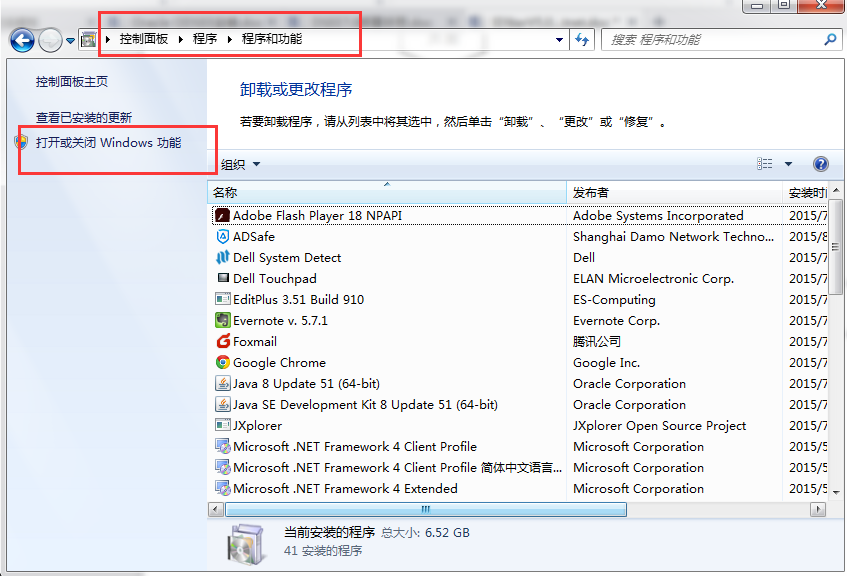
退出访问地址：http://demo访问IP地址/Logout.aspx

|  |
| --- |
| if (CasAuthentication.ServiceTicketManager != null)  {  //清除认证cookie  CasAuthentication.ClearAuthCookie();  //清除会话  Session.Clear();  //退出调用地址，红色部分为学校身份认证地址，service后面的地址登出回跳地址  string singleSignOutRedirectUrl = "http://authserver.xxx.edu.cn/authserver/logout?service=http://172.16.40.23/default.aspx";  Response.Redirect(singleSignOutRedirectUrl, true);  } |

# demo实例

## windows下配置IIS搭建程序运行环境

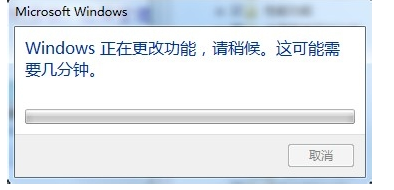
1. 我使用的环境是win7，其他操作系统请自行百度安装环境，大体上都差不多。进入Win7的控制面板，选择“程序”然后在点击“程序和功能”，在左侧选择的“打开或关闭Windows功能”在出现的列表中选择IIS7然后确定



1. 进入Windows功能窗口，然后看到internet信息服务选项，选择配置即可，Ps：打√的选项下面为全选，方圈的下面按照图中打√的选择即可。



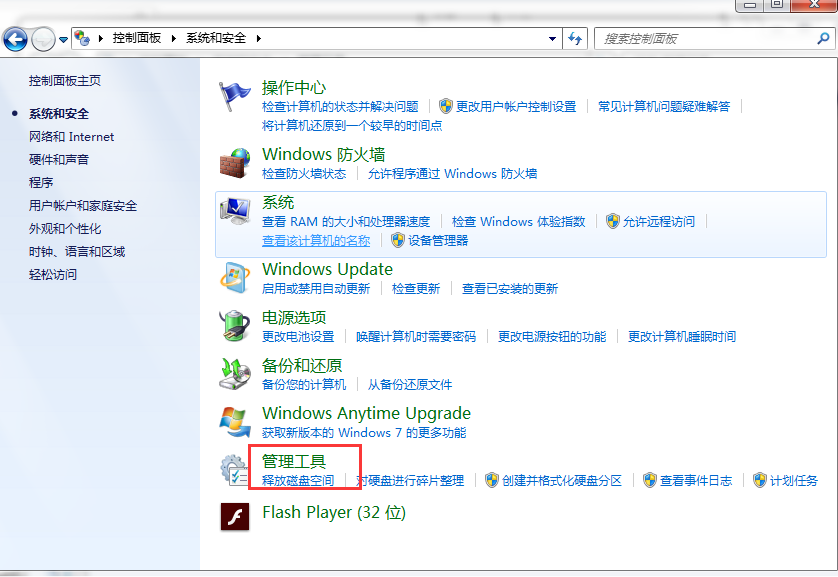
1. 点击确定，会进入系统安装设置，此时可能需要等待两三分钟的样子。



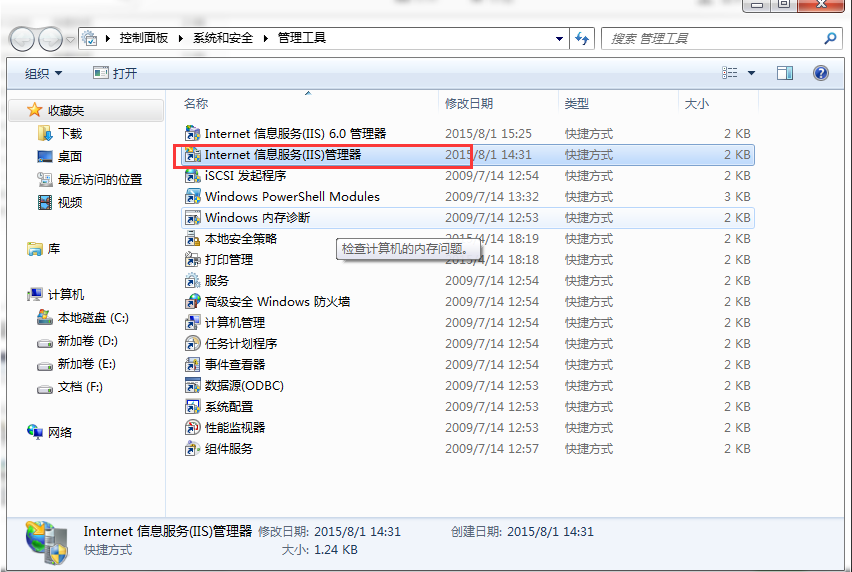
1. 安装成功后，窗口会消失，然后回到控制面板，选择系统和安全。



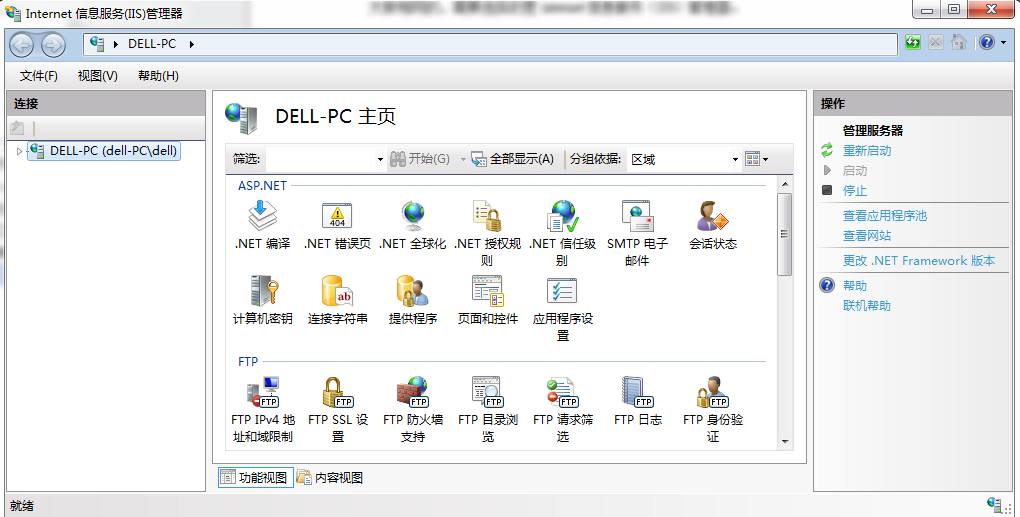
1. 进入系统和安全窗口，然后选择左下角的管理工具。



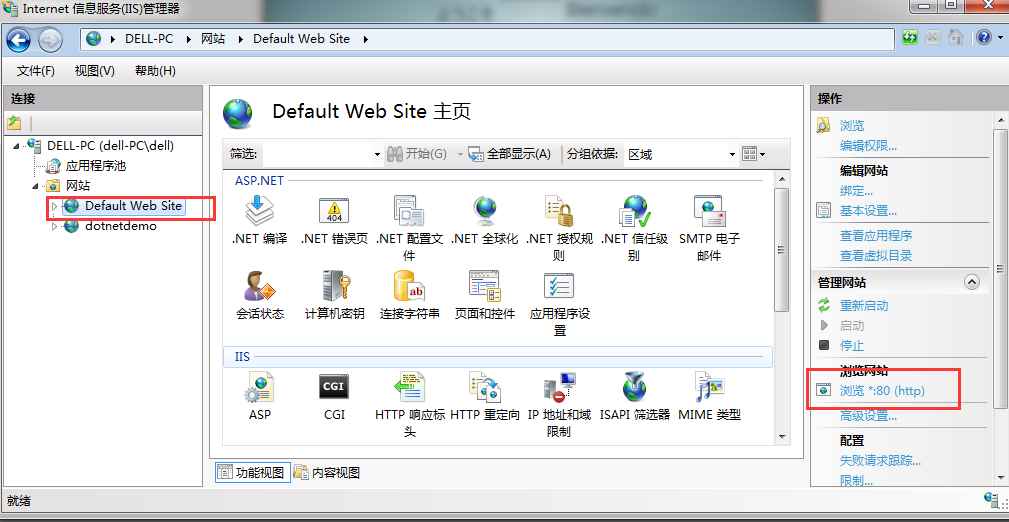
6、进入管理工具窗口，此时就可以看到internet信息服务了，不过此时需注意，因为有两个大致相同的，需要选择的是internet信息服务（IIS）管理器。



1. 双击internet信息服务（IIS）管理器，进入到管理窗口，看上去很复杂，有三大主要功能:FTP,IIS,管理，现在需要设置都在IIS这个里面。



8、选中默认网站，点击右侧的浏览

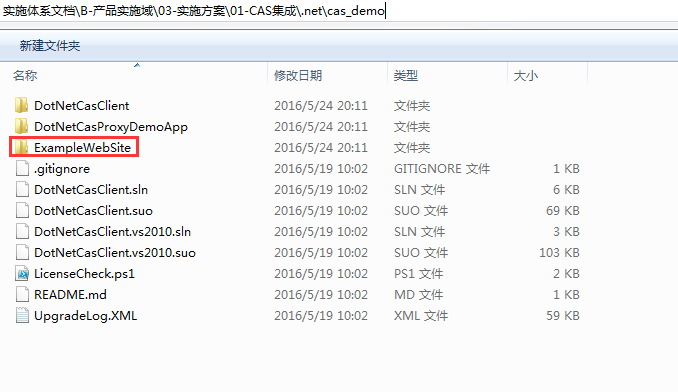


1. 浏览，出现该界面，IIS配置成功

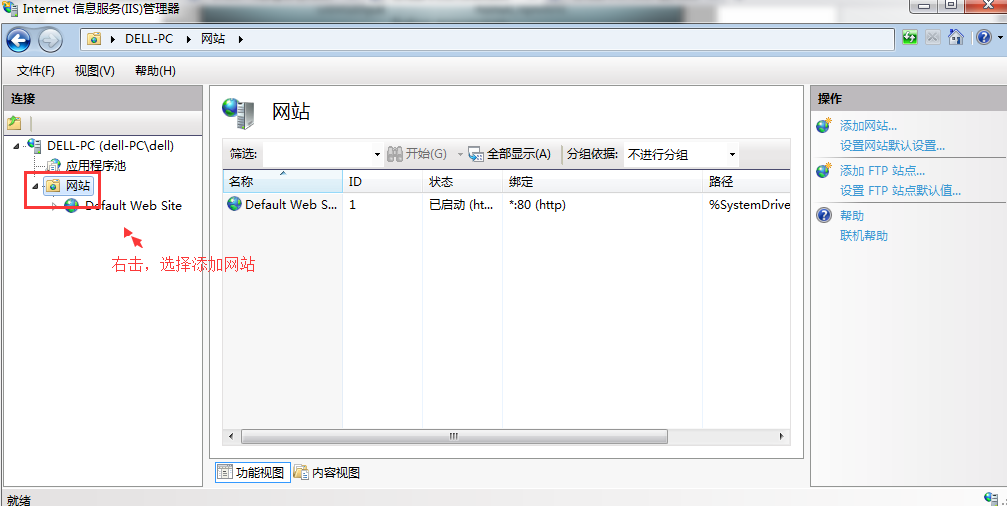


## 部署dotnet的cas\_demo

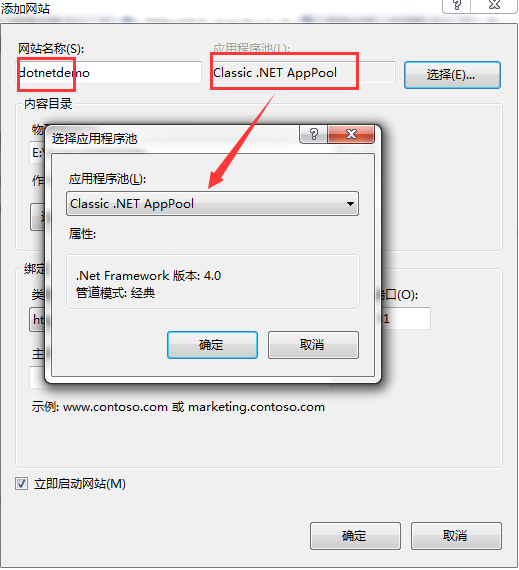
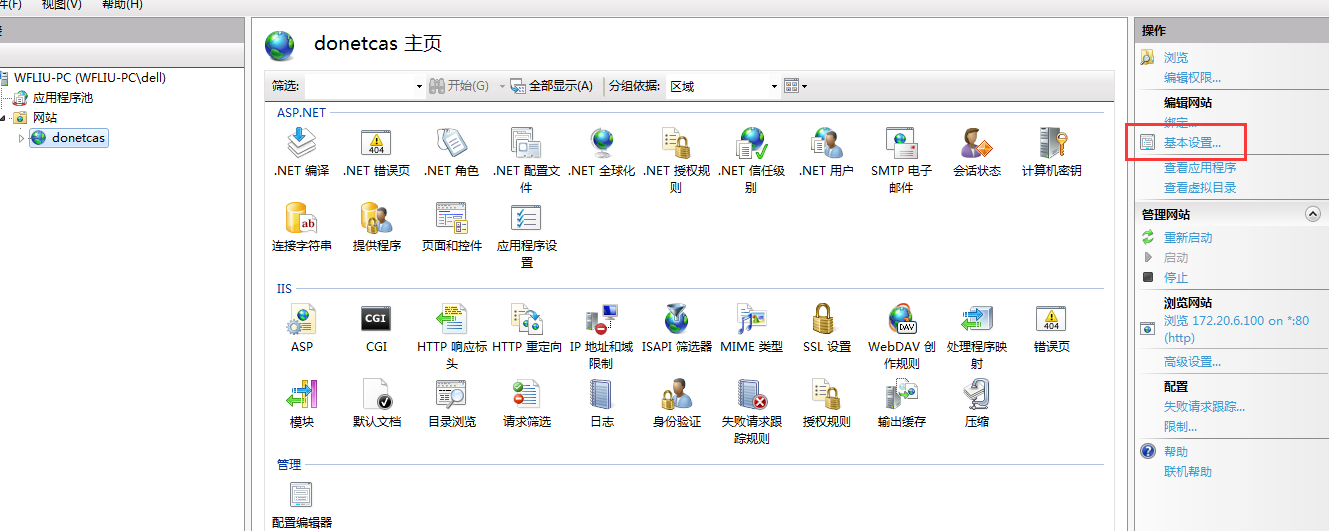
**备注：**集成demo程序是…/cas\_demo/ExampleWebSite



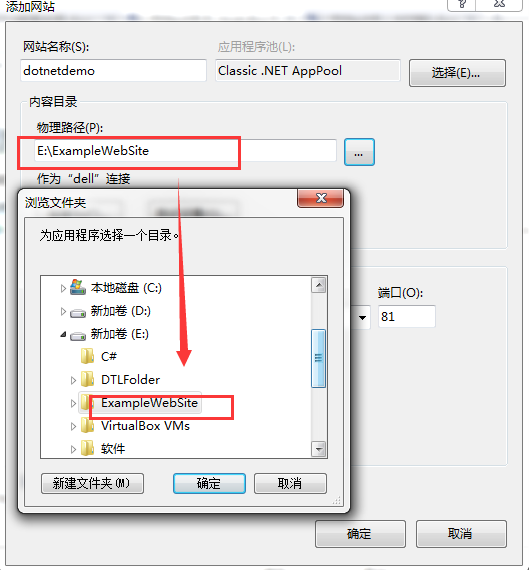
1、右击网站，选择添加网站



1. 配置网站



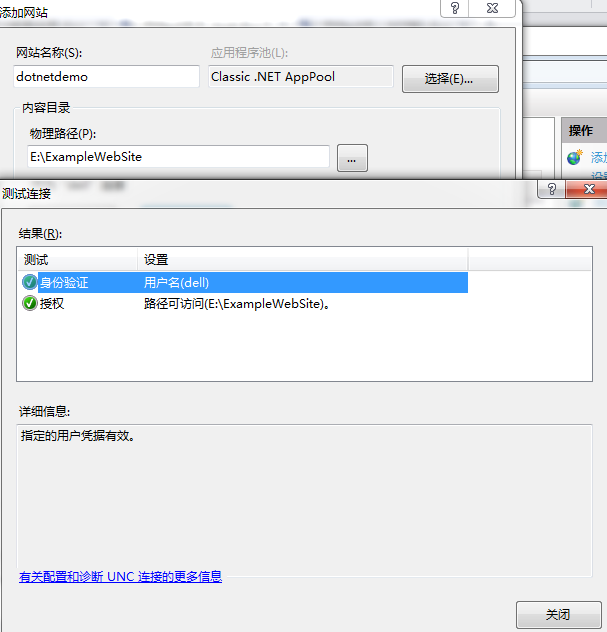
1. 配置物理路径



4、点击“连接为”，选择“特定用户”，点击设置，输入系统用户名密码。这里必须用操作系统的登录名和密码，不然无权访问硬盘分区。我这里设置



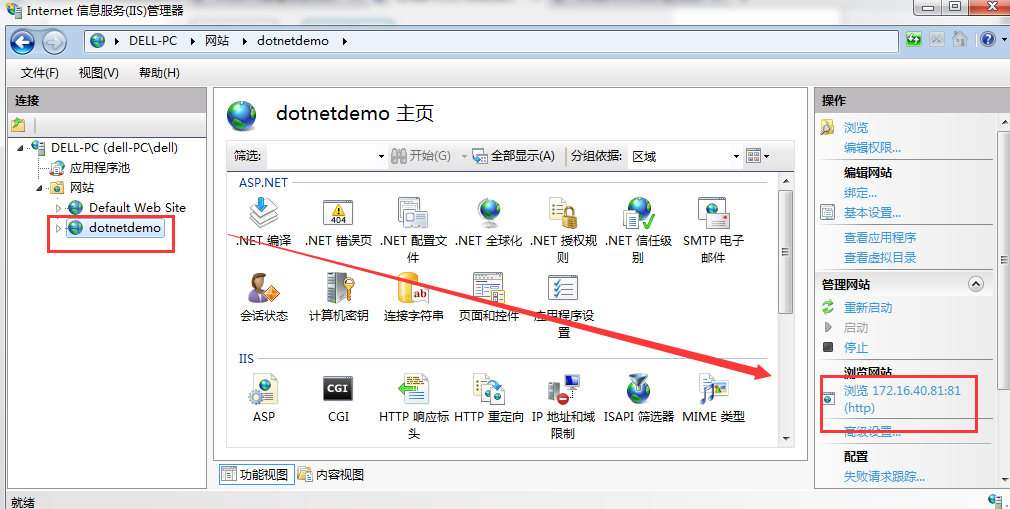
5、然后，测试连接



6、设置ip和端口



7、选中程序，点击浏览



1. 出现该界面，demo程序运行成功

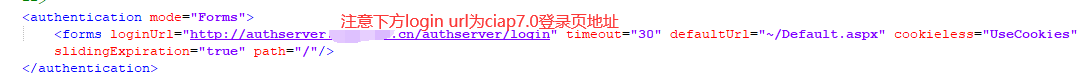


## 在身份认证管理平台注册集成demo

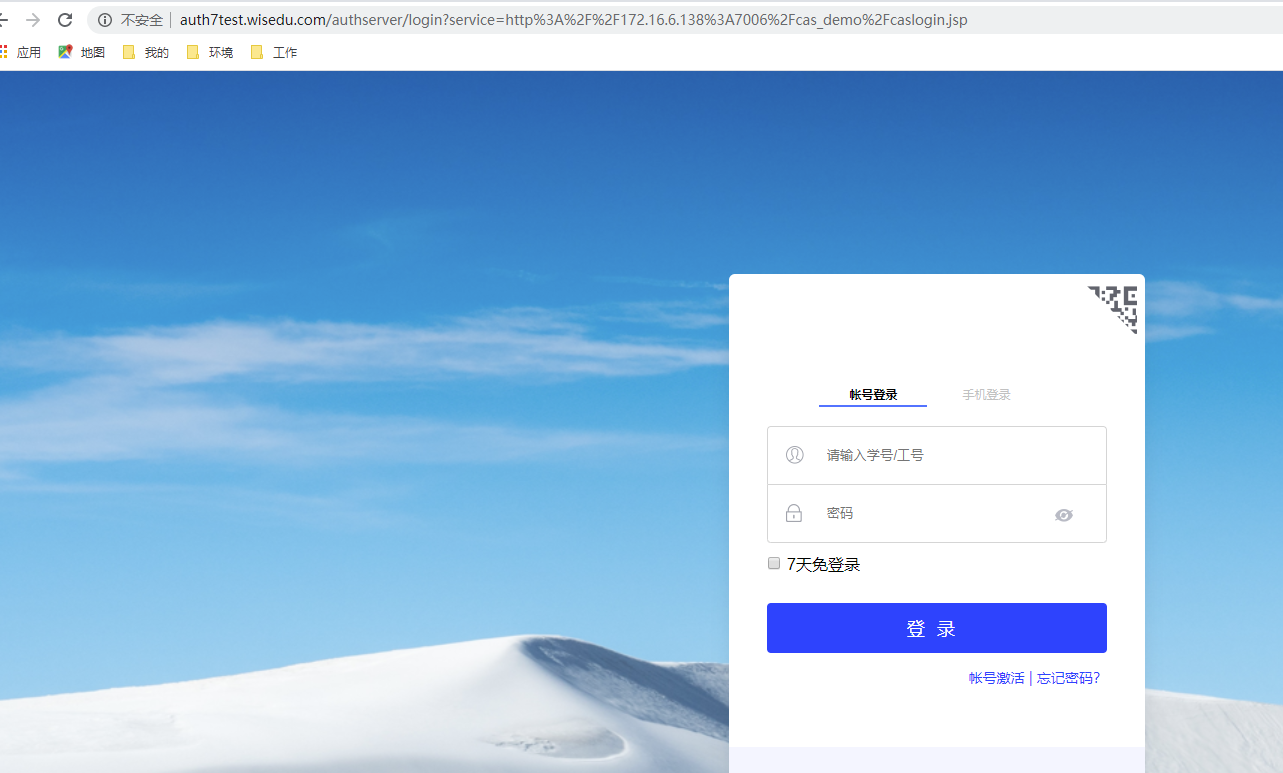
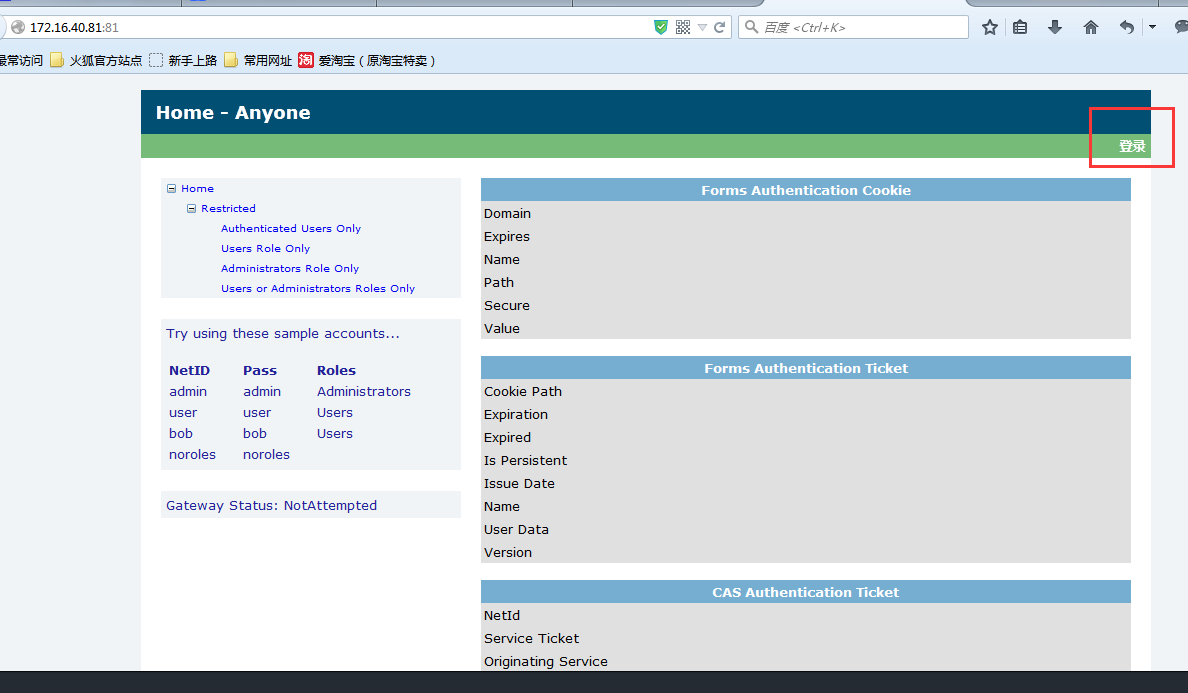
1. 登录Mions Console身份管理平台
2. 注册应用，用户授权



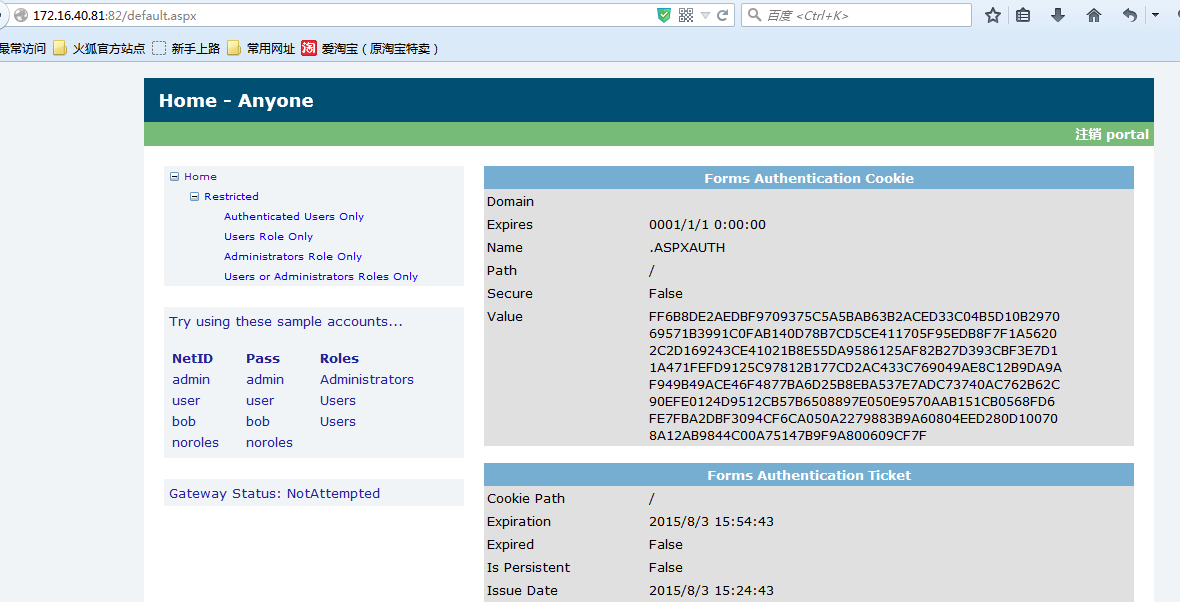
1. 修改程序的web.conifg配置文件



1. 访问程序，点击登录，跳转到CIAP的登录界面



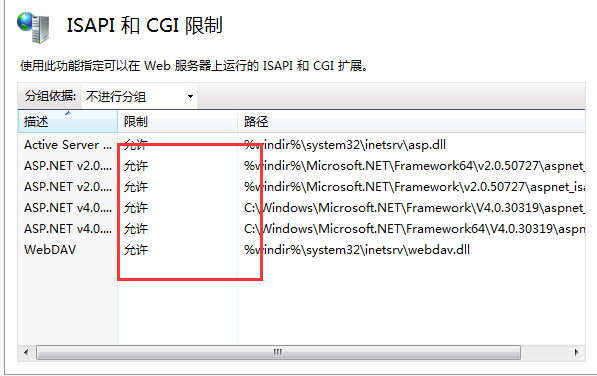
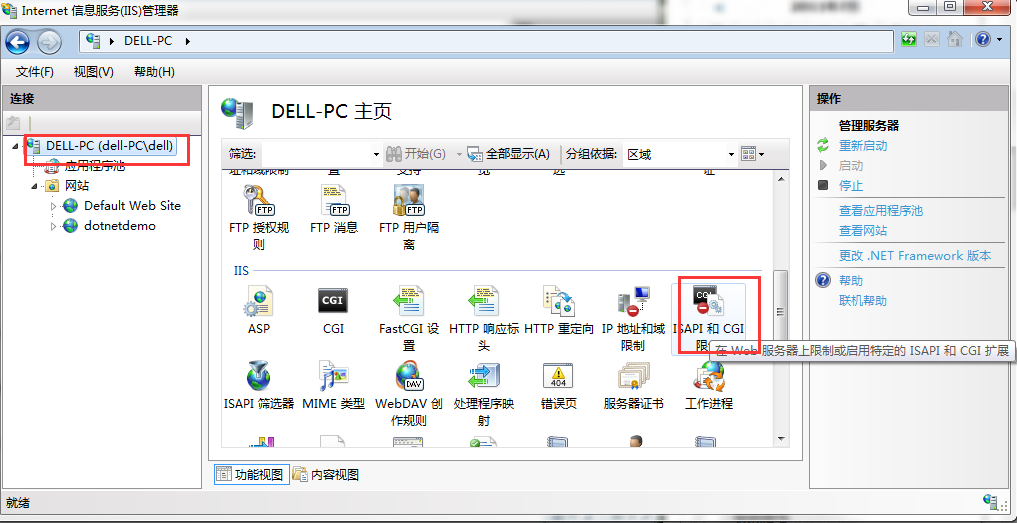
1. 实现单点登录，用户信息校验后，返回应用



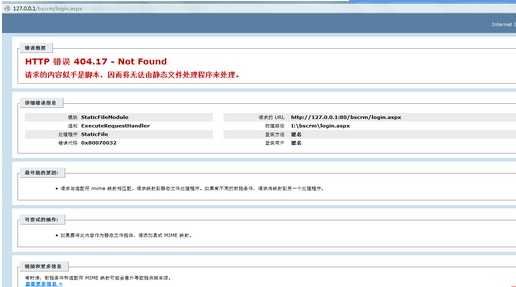
## 部署demo常遇到的错误

1. HTTP 错误 404.2 - Not Found

**解决方案：**选中到iis根目录，把.net4中的ISAPI和CGI限制 把设置为允许  ASP.NET V4.0的两个设置为允许。见下图



2. [ASP.Net .Net4.0 HTTP 错误 404.17 - Not Found](http://tankywang.iteye.com/blog/1409407)



**解决方案：**

以管理员身份运行cmd

cmd:C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\aspnet\_regiis.exe -i

1. HTTP 错误 500.22 - Internal Server Error （Win7 IIS 配置错误）

解决方案：把iis配置右边 [浏览网站] 里的 [高级设置] 里面的 [应用程序池]  选择为  [Classic .net AppPool ]   经典模式就可以了。默认是 DefaultAppPool 。