

# Single Sign-On 5.0 单点登录

## 目录

一、安装环境.....	1
二、安装步骤.....	1
1、创建 Central Stroe 存储.....	1
2、安装 Single Sign-On 插件.....	5
3、配置 Single Sign-On.....	8
1) 定义应用 (Application Definitons) .....	12
2) 定义用户 (Users Configuration) .....	21
3) 单点登录功能使用和测试.....	28

## 一、 安装环境

主机名	工作组/域	角色	操作系统	镜像
xenapp1	域(test.com)	XenApp6.5 服务器	Windows server 2008 R2 SP1	XA6.5_2008R2_ML.iso

## 二、 安装步骤

### 1、创建 Central Stroe 存储

在 XenApp 服务器上安装镜像后，运行 Autorun.exe 程序：



图 1 选择“手动安装组件”

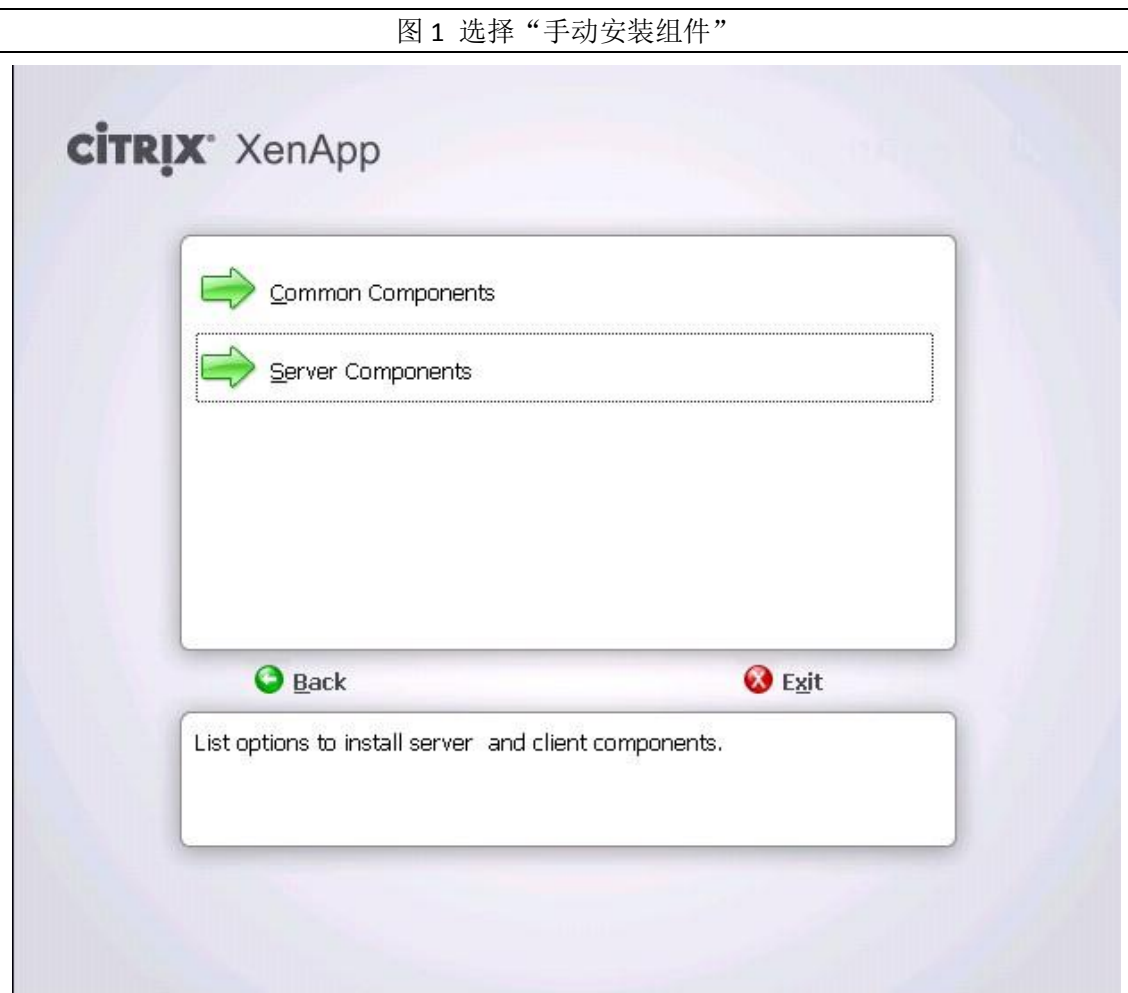


图 2 选择“服务器组件”



图 3 选择“其它”

 Smart Auditor


 Single Sign-On

 Back

 Exit

Single Sign-On components.

图 4 选择“Single Sign-On”组件

 Central Store

 Single Sign-On Service

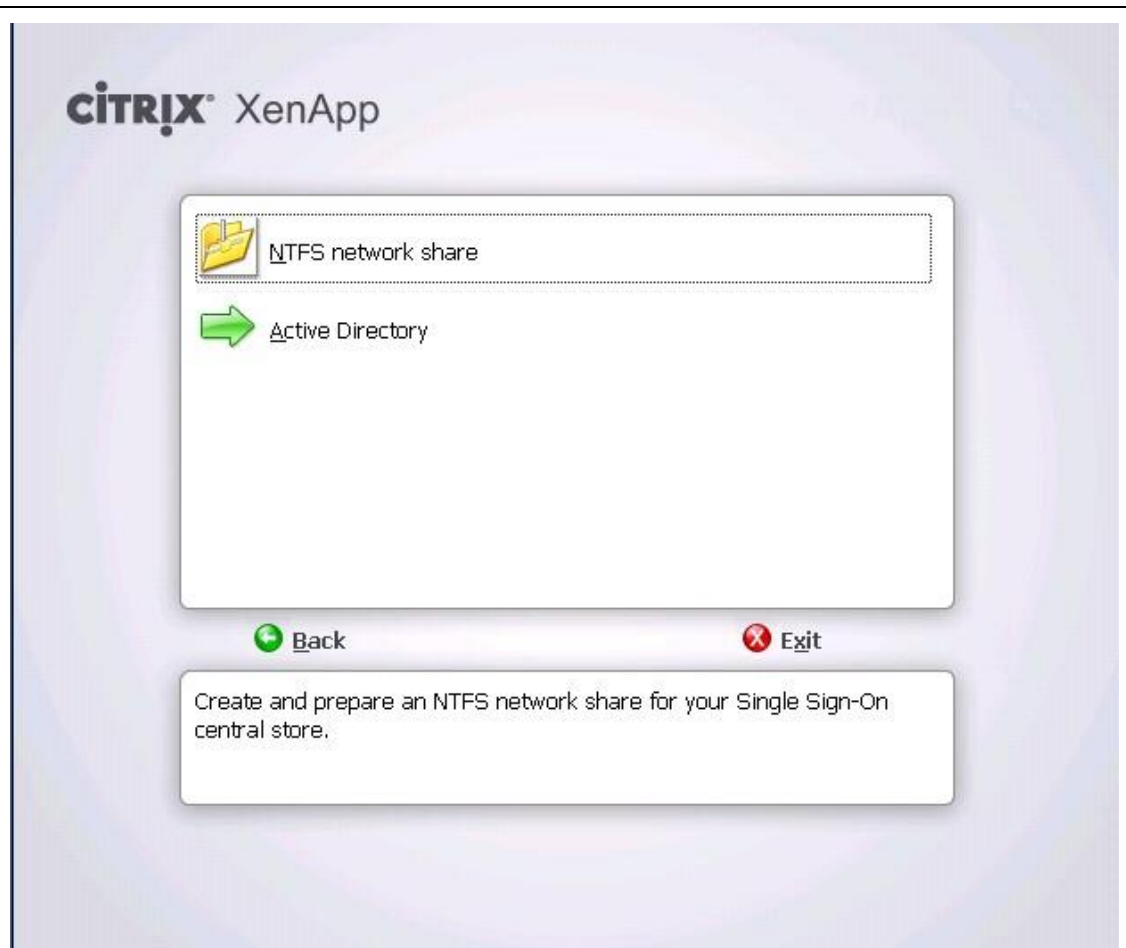
 Single Sign-On Plug-in

 Back

 Exit

List options to create your central stores.

图 5 选择“中央存储库”



- 图 6 选择“NTFS 网络共享”，可以根据需要进行选择，在这里我选择的是 NTFS 方式；
- 1) 点击以后会有一命令行窗口一闪而过，中央存储库即自动创建完成，没有任何提示；
  - 2) 验证是否创建成功，可以切换到 C:\盘目录下查看是否生成“CITRIXSYNC”文件夹（在此放置存储数据，如帐号、密码信息）；
  - 3) 实验环境中，一般会把 XenApp 服务器与中央存储库放在一起，如果在生产环境需要综合考虑中央存储库的放置位置，及账户密码的保存方式等等；
  - 4) 中央存储库可以单独放置，也可以和 XenApp 服务器放在一起。

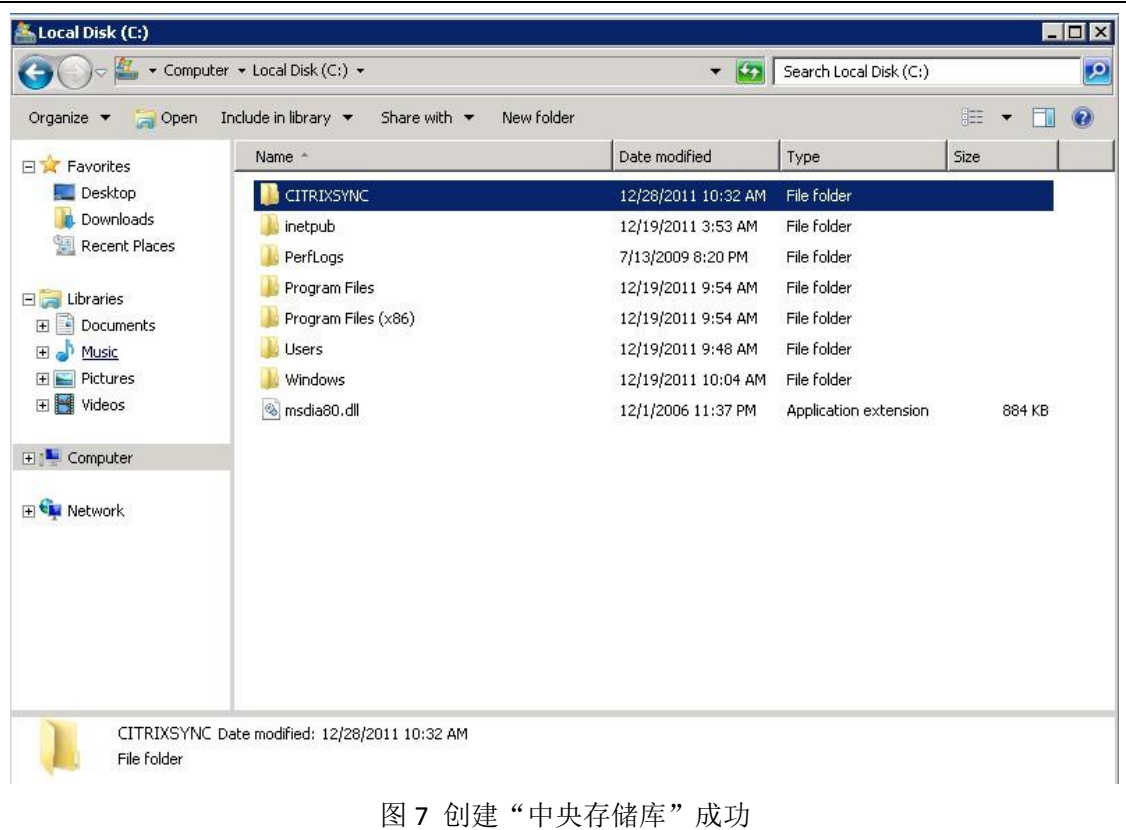
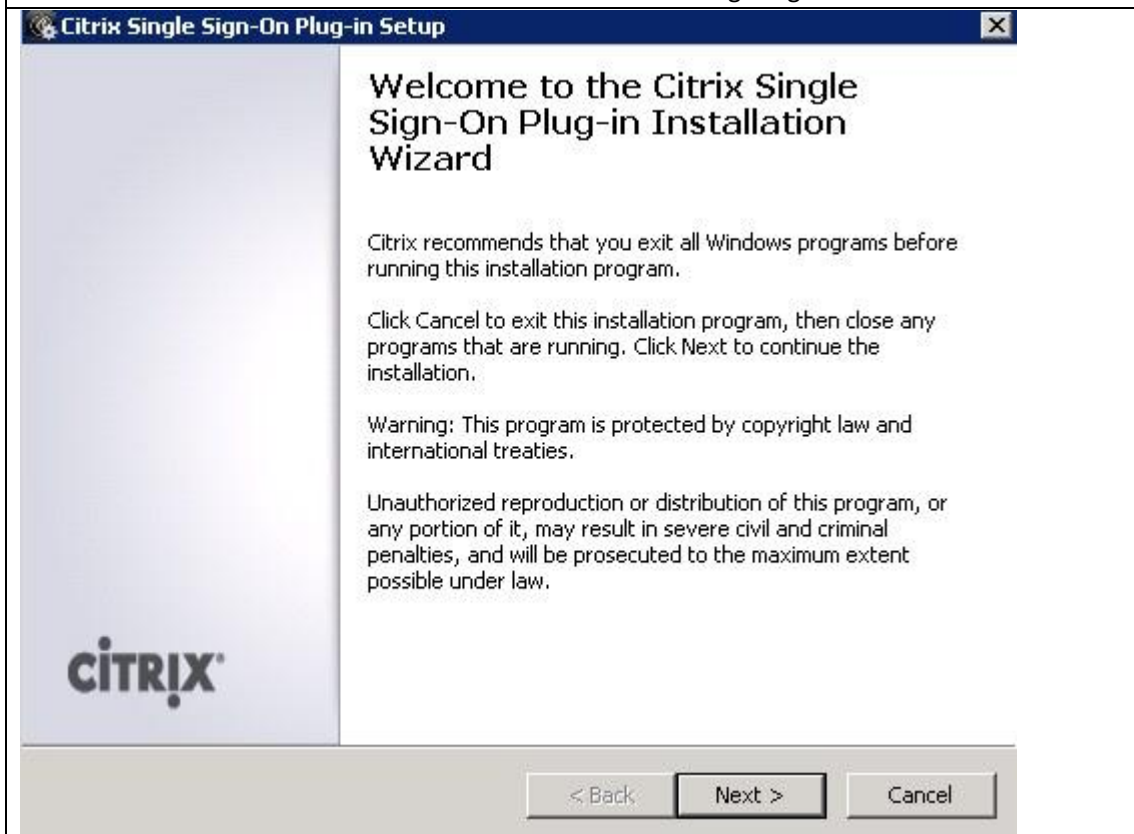


图 7 创建“中央存储库”成功

## 2、安装 Single Sign-On 插件



图 8 在安装中央存储库的界面，选择“Single Sign-O 插件”



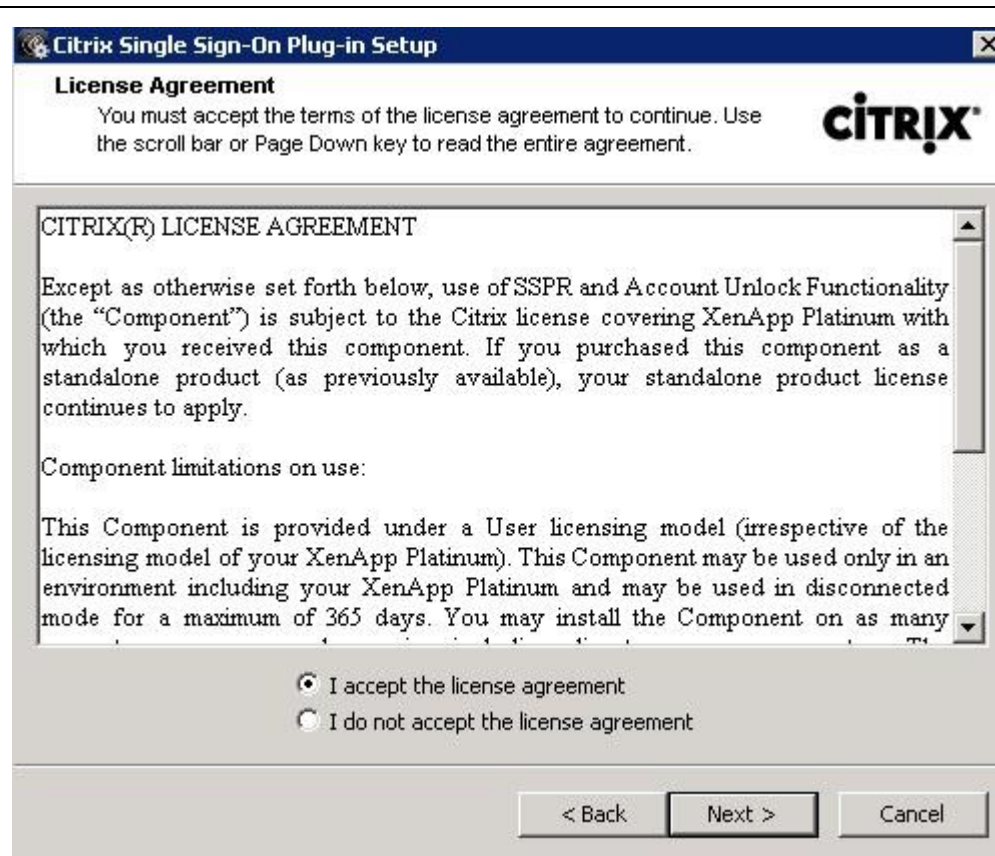


图 9 选择“同意授权”

注意：右边的下拉滚动条拖动到最底，才能进行下一步

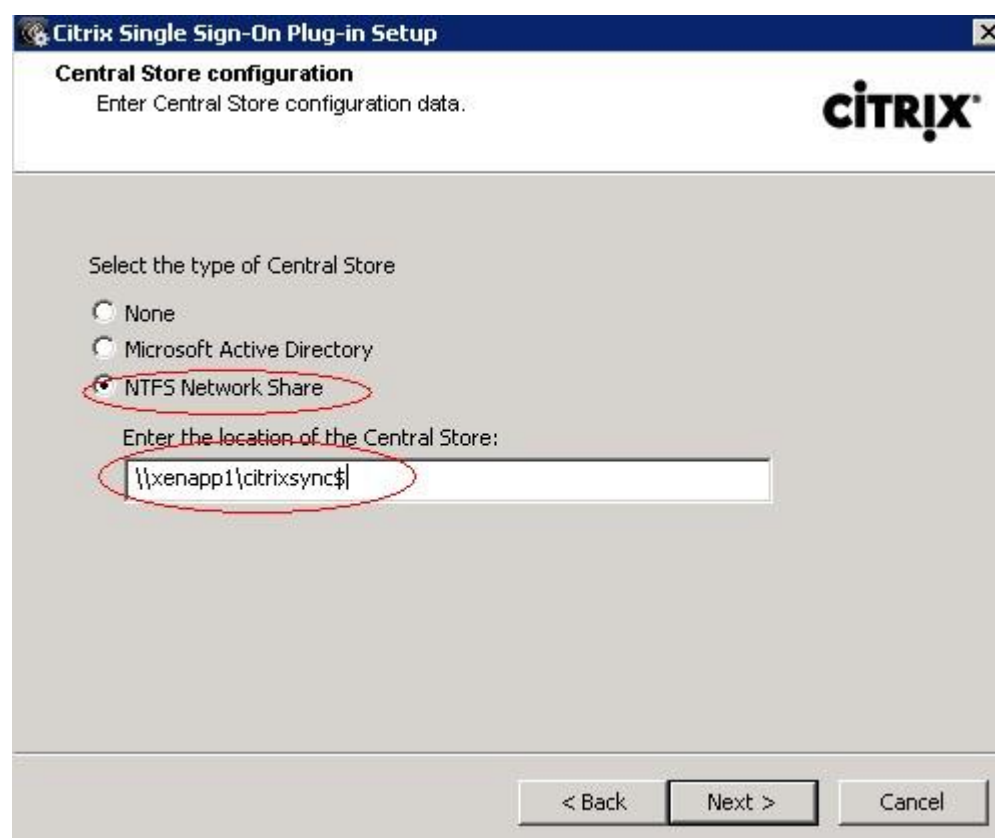


图 10 选择“中央存储库类型”和填写“存储库路径”

- 1) 根据创建的“中央存储库”，选择不同的类型；中央存储库有两种类型：基于域环境下的存储库和基于 NTFS 网络共享的存储库，在这里我选择的是“NTFS 网络共享”；
- 2) 中央存储库路径的输入格式：\\主机名称\citrixsync\$

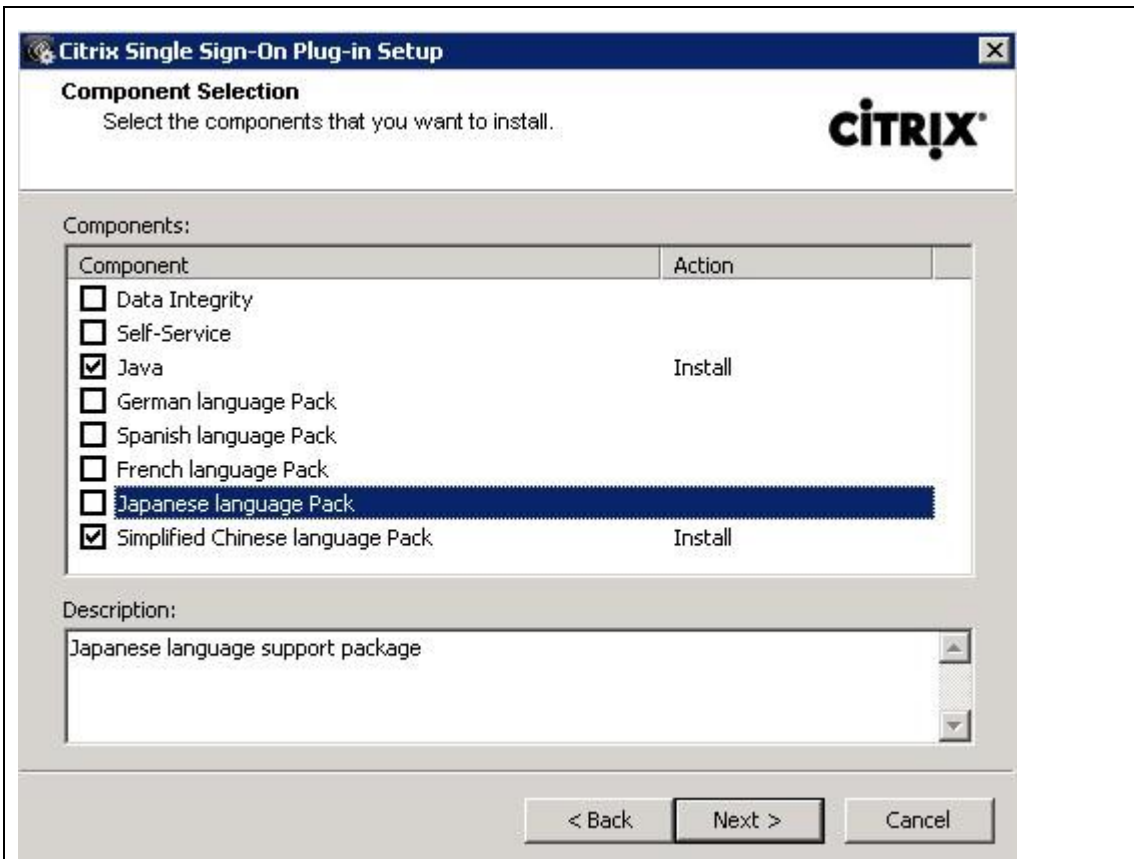
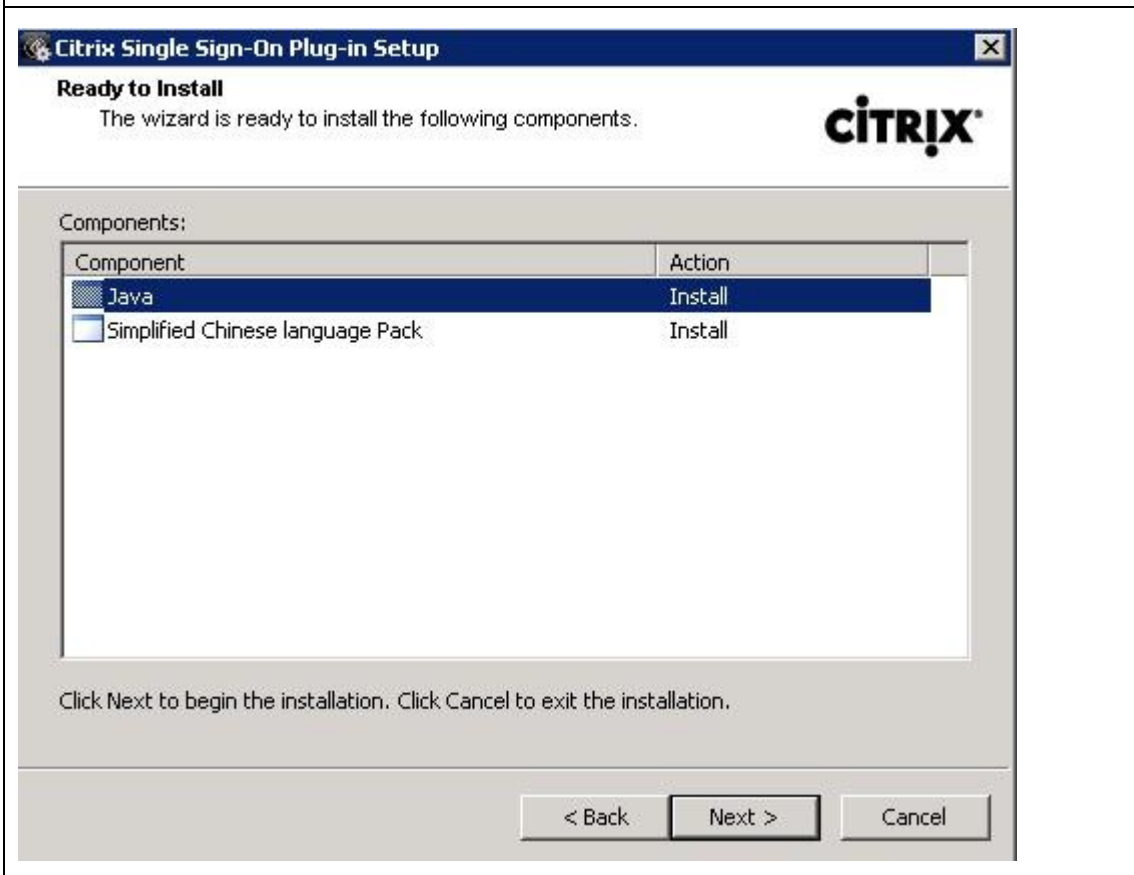


图 11 根据需要选择安装 JAVA 和语言



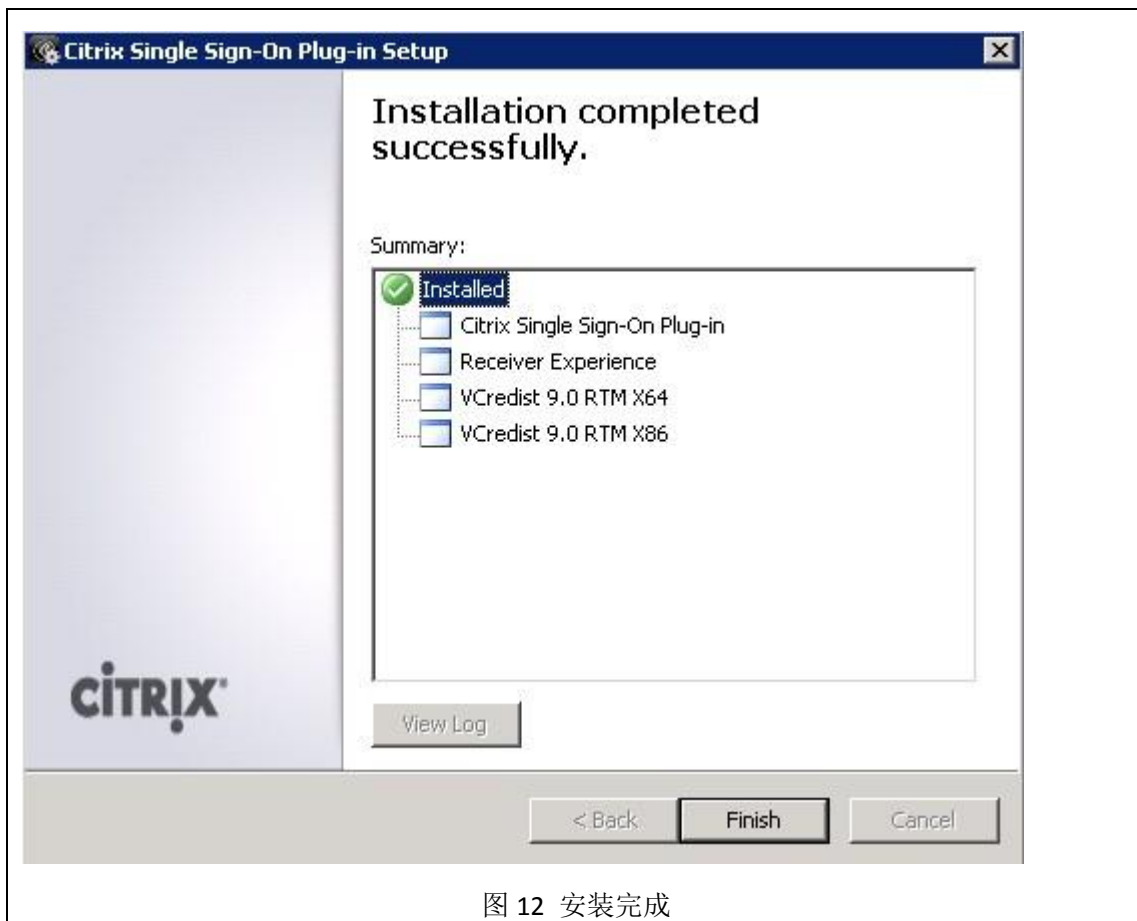


图 12 安装完成

### 3、配置 Single Sign-On



图 13 选择“配置和运行检测”

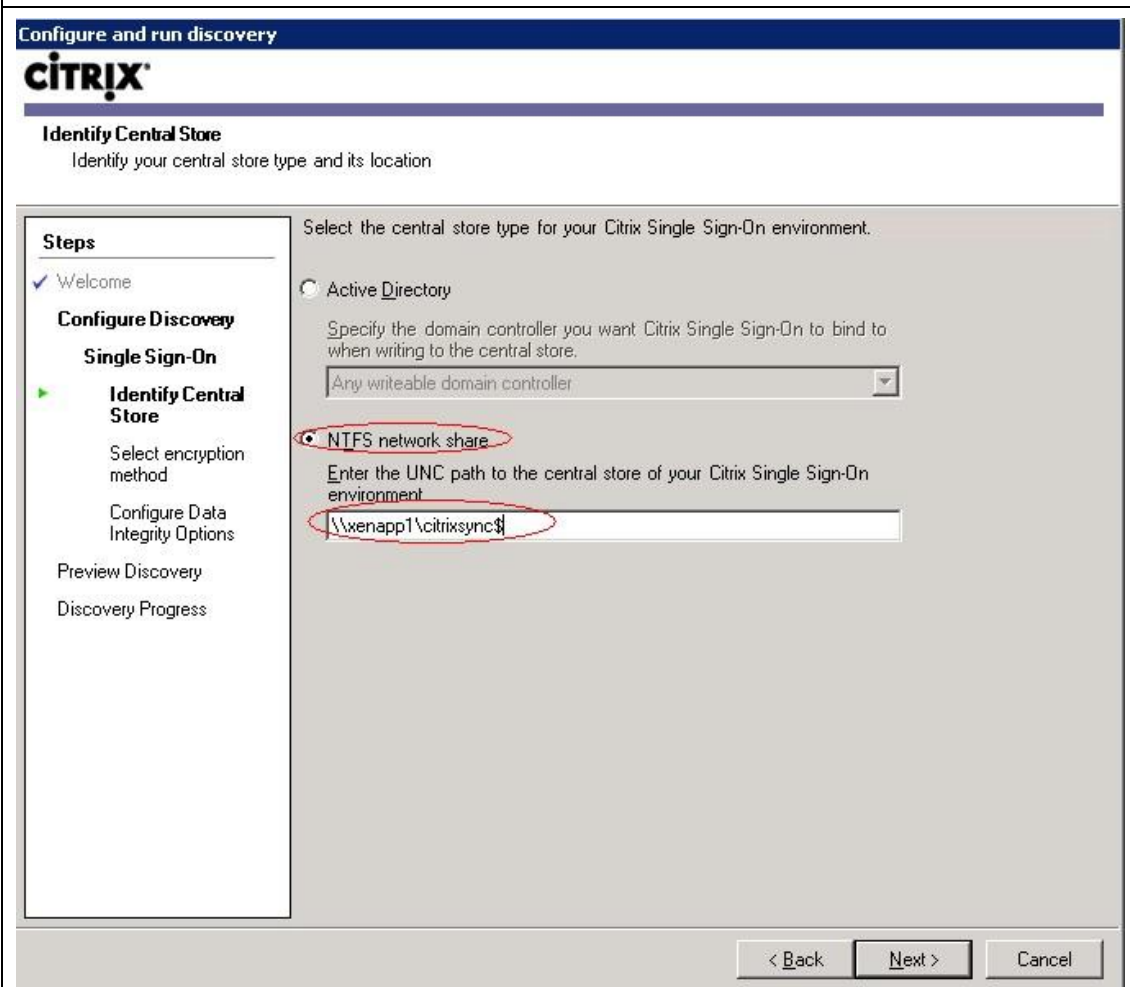
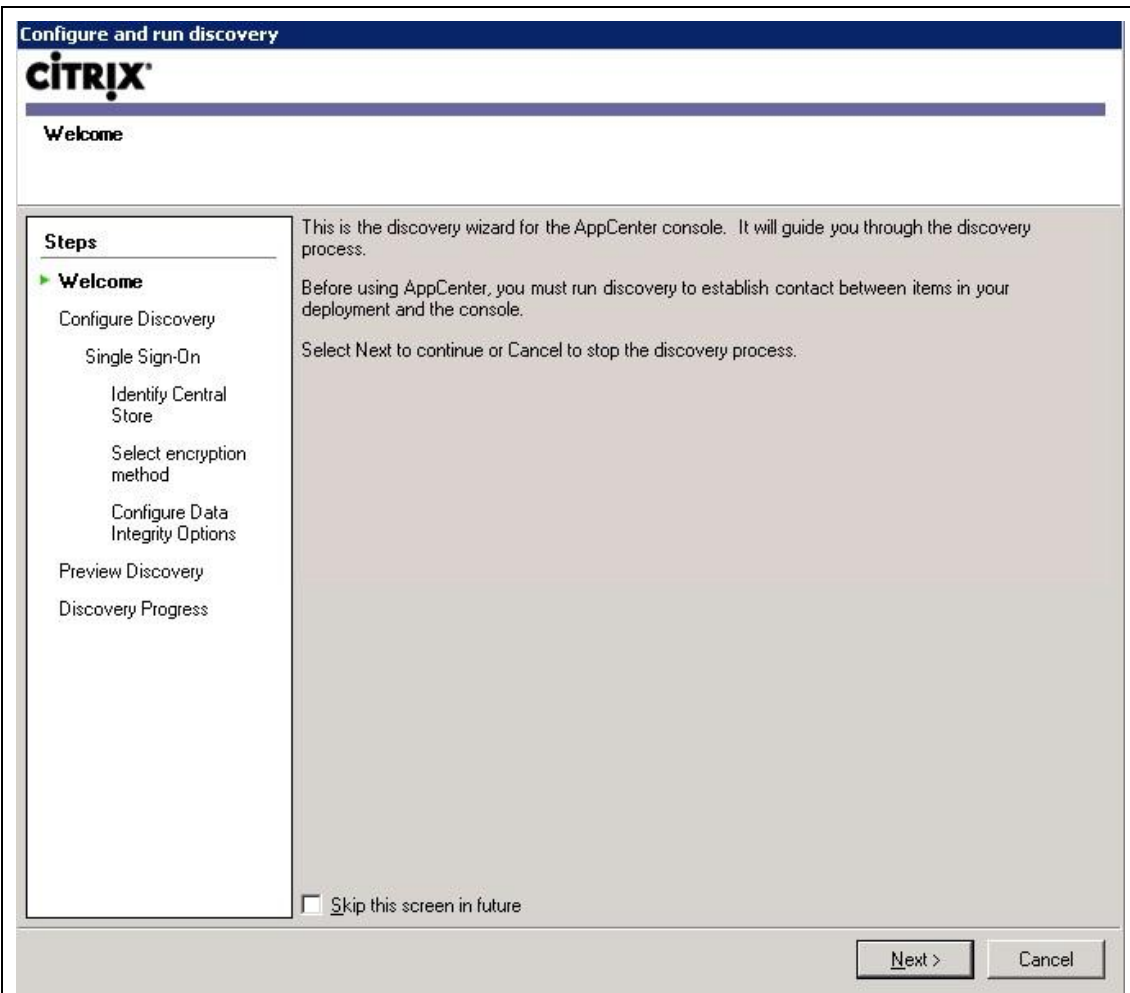


图 14 指定中央存储库类型、并输入存储位置

- 1) 在这里选择的是“NTFS 网络共享”
- 2) 填写路径如图 10

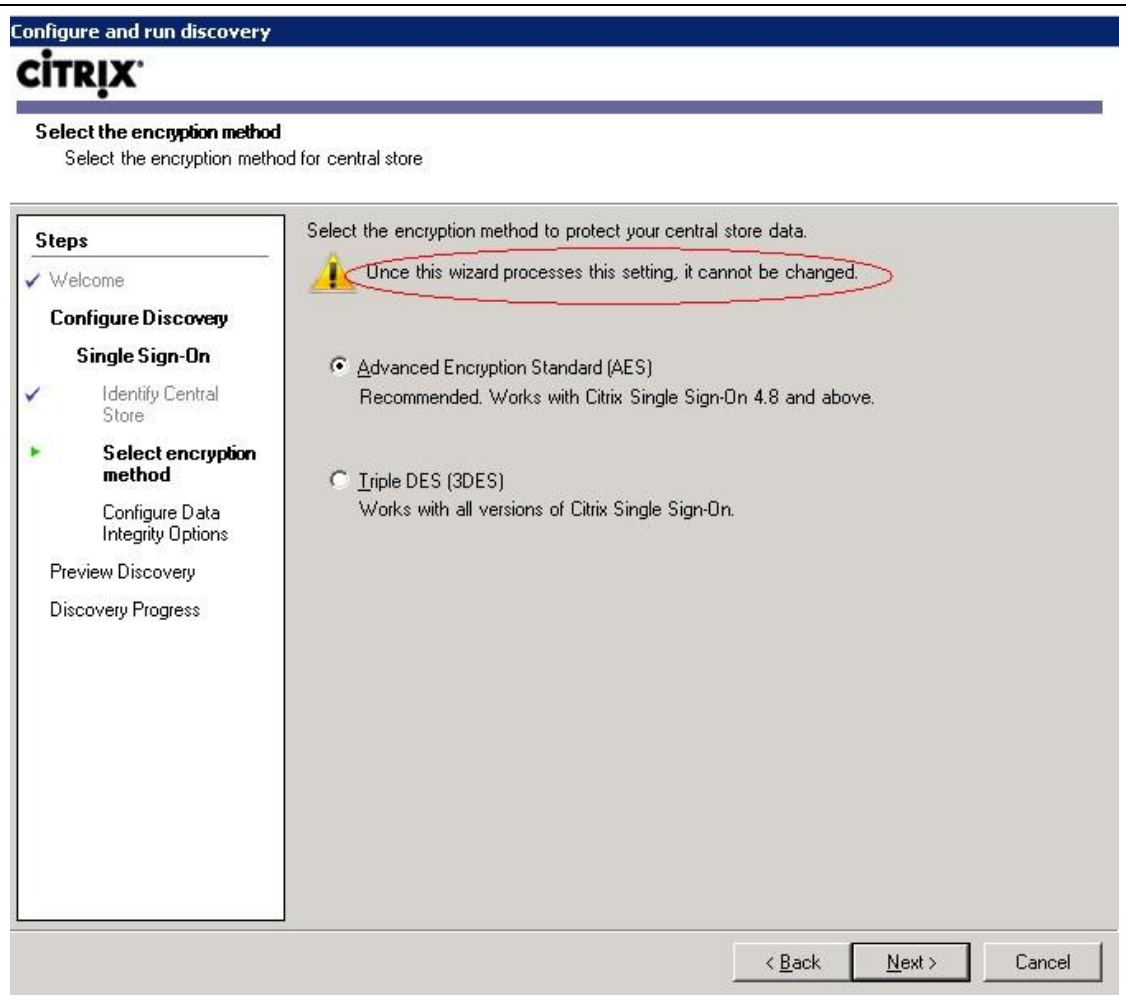


图 15 选择中央存储数据的加密方式  
注意：在这里选择之后，将不能在修改

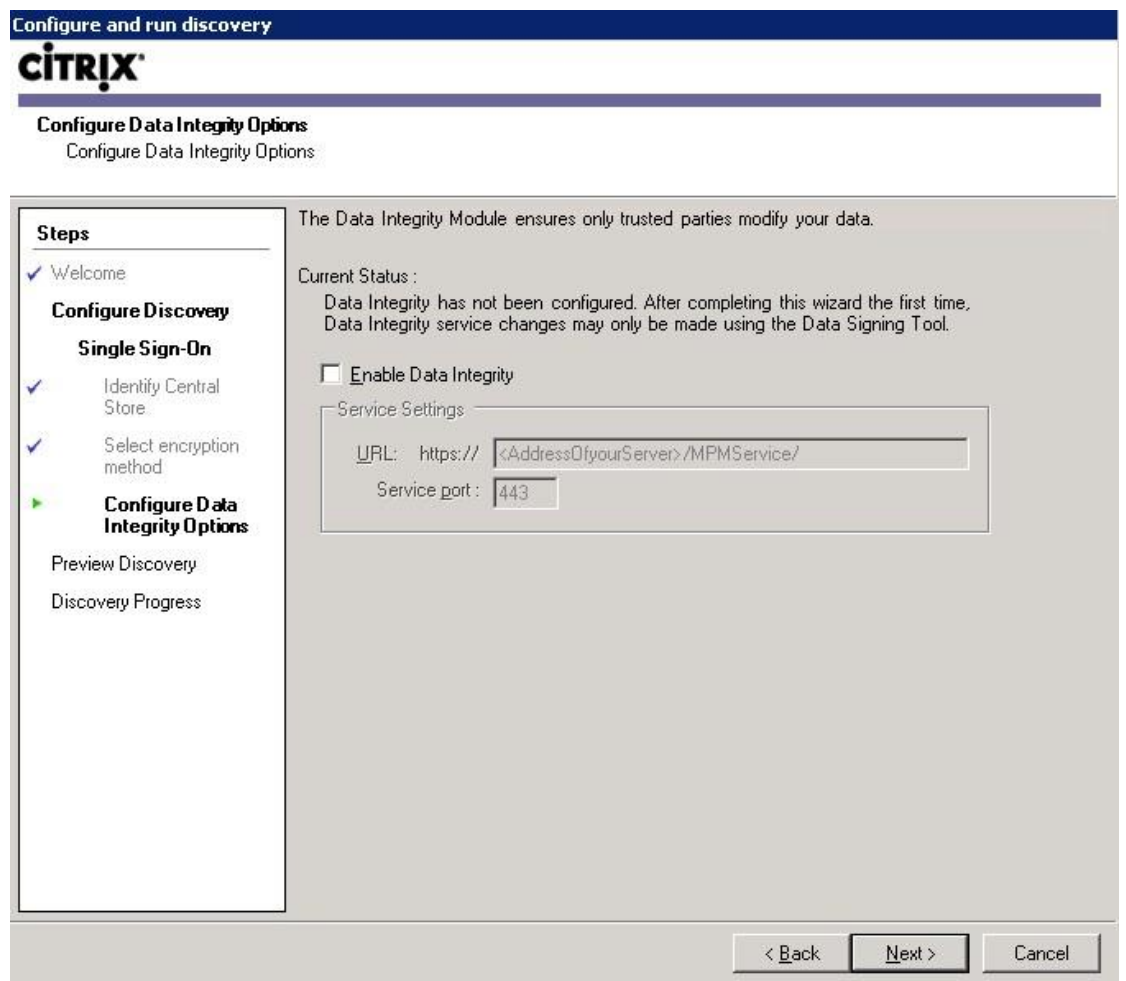


图 16 没有安装 Date Integrity 插件，在这里默认即可

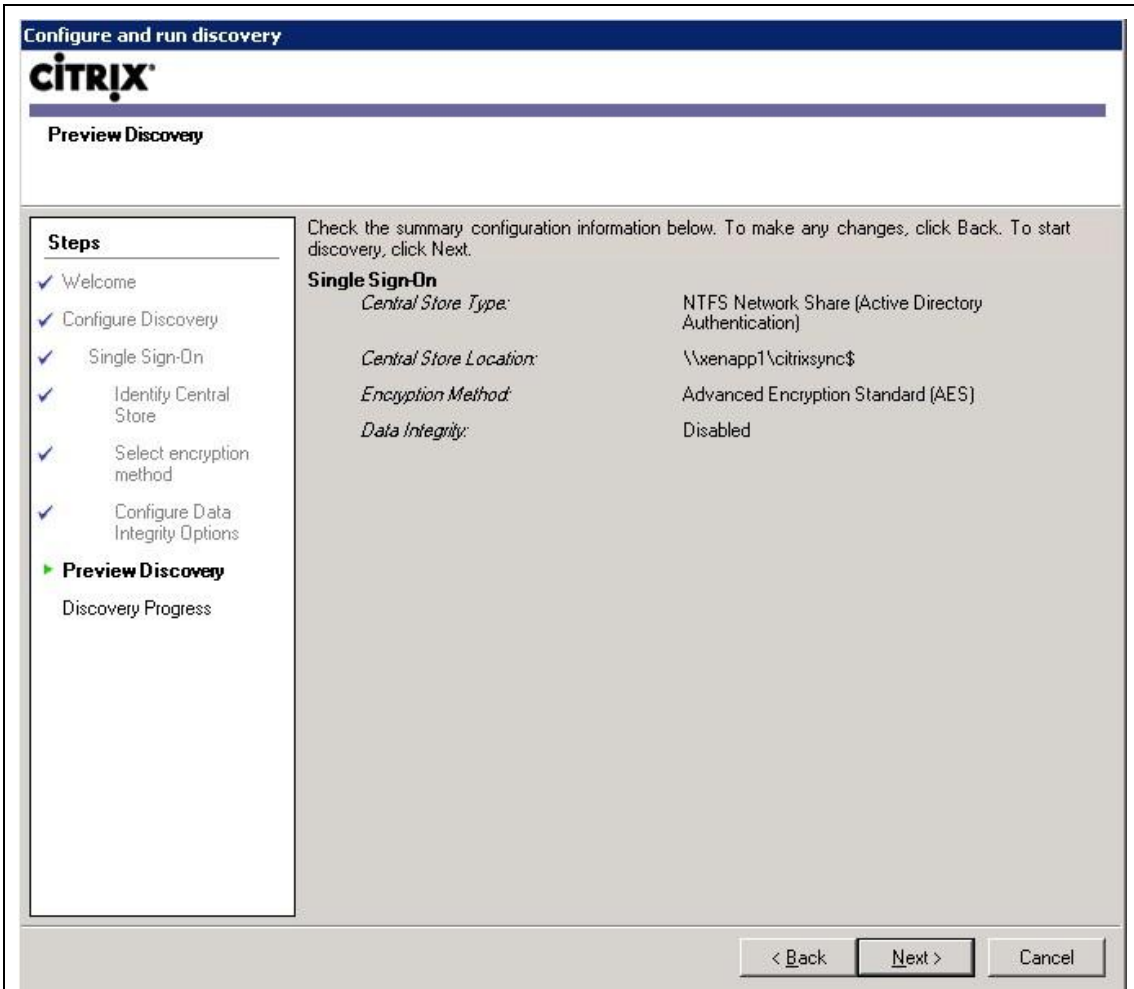


图 17 直接下一步

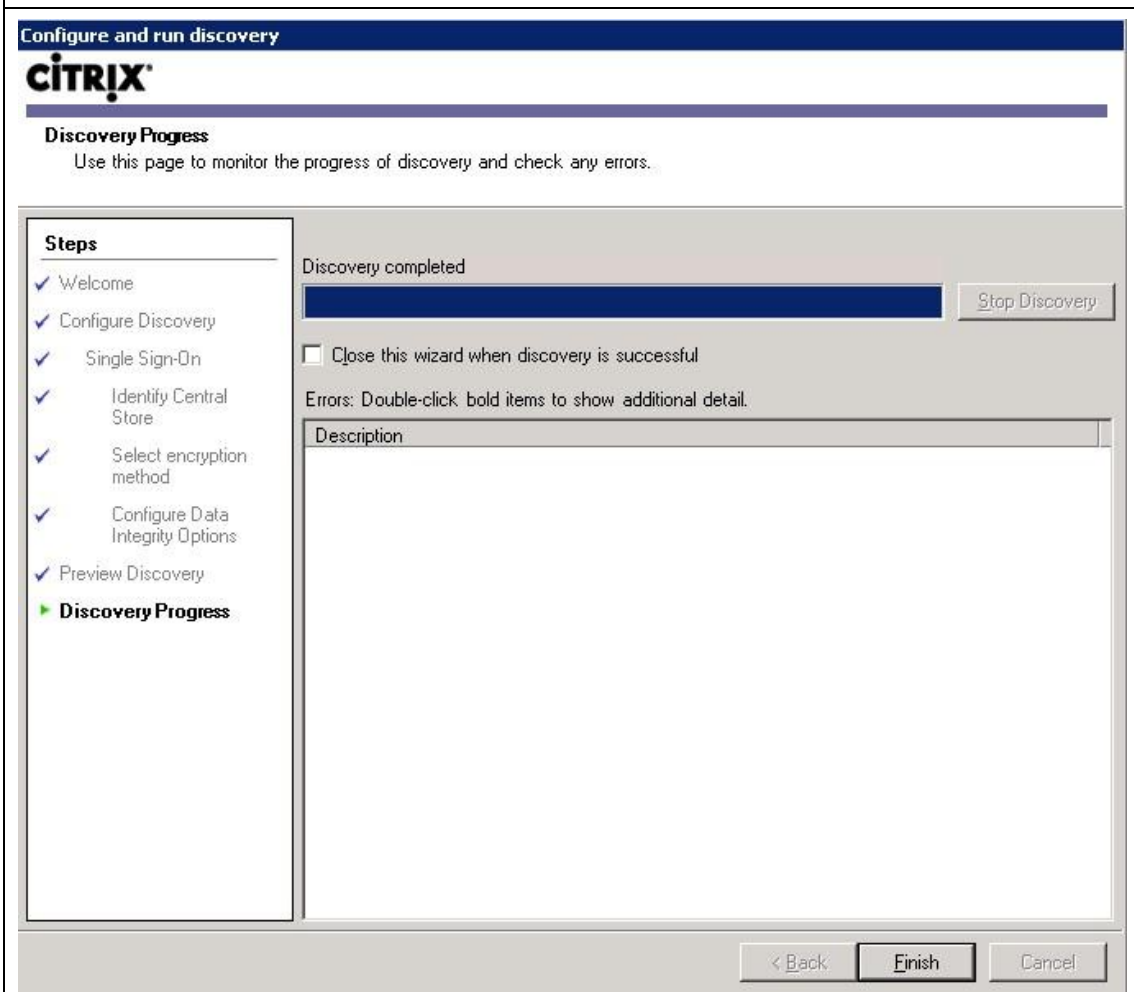


图 18 检测完成

## 1) 定义应用 (Application Definitions)

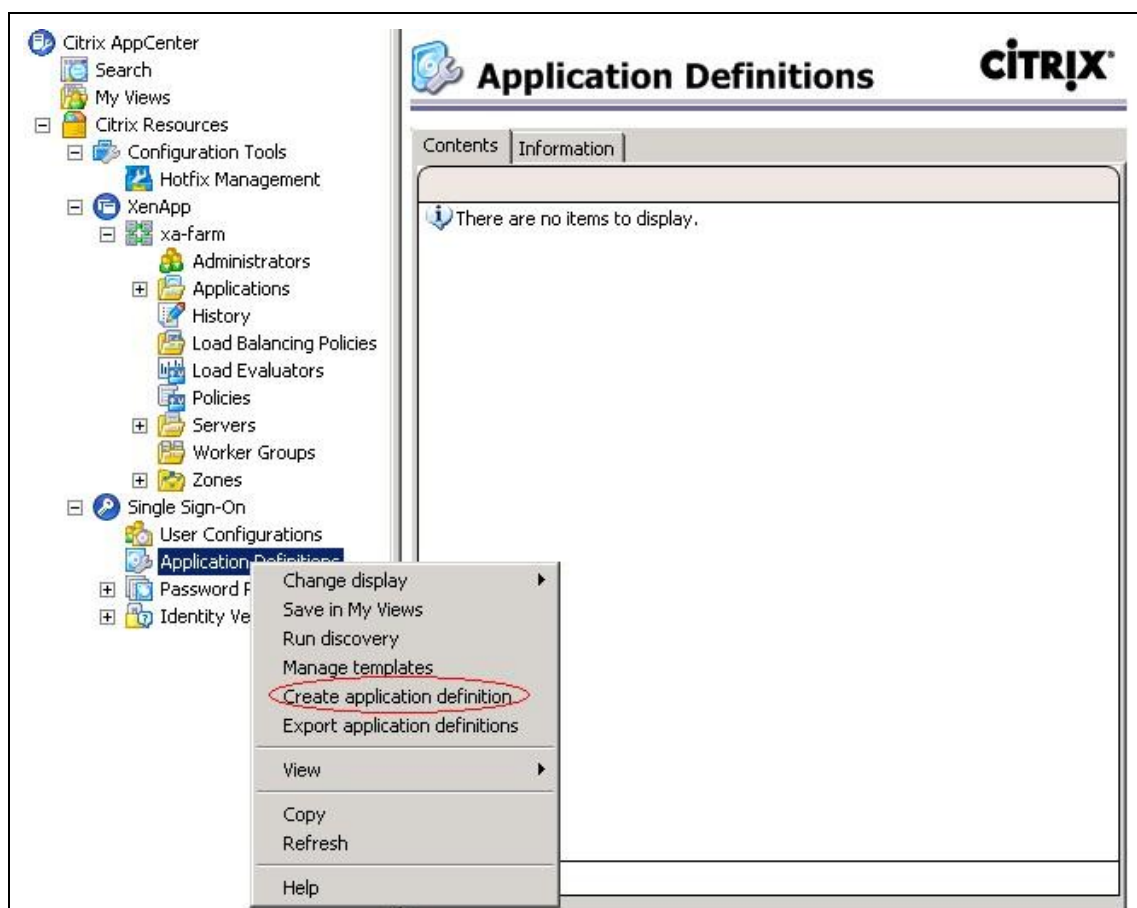
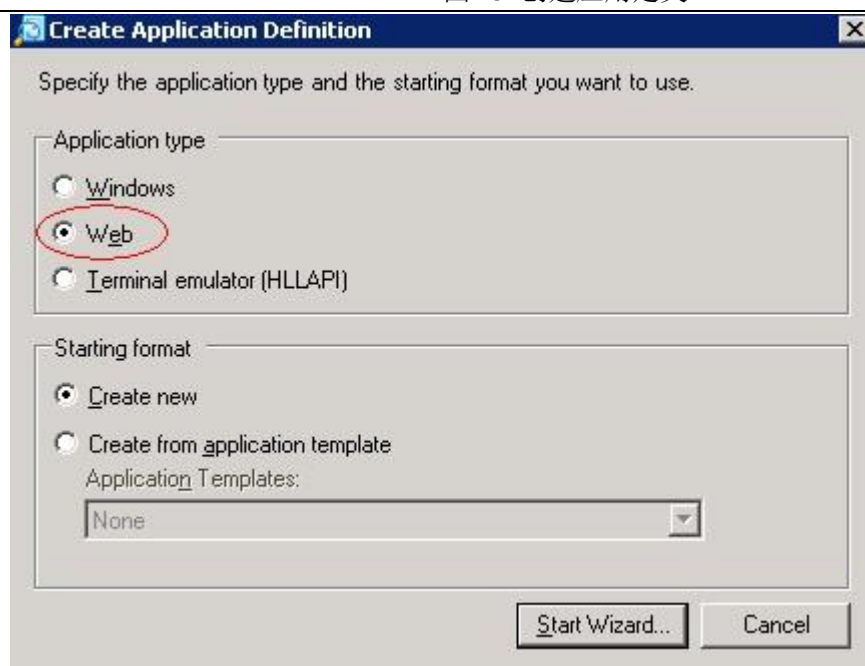


图 19 创建应用定义



- 1、图 20 选择“应用类型”在这里有 3 种，Windows、Web、终端模拟器；
- 2、根据应用类型进行选择，实验环境使用的是 Web 类型。
- 3、可以创建一个新的形式，也可以基于应用程序模版创建。

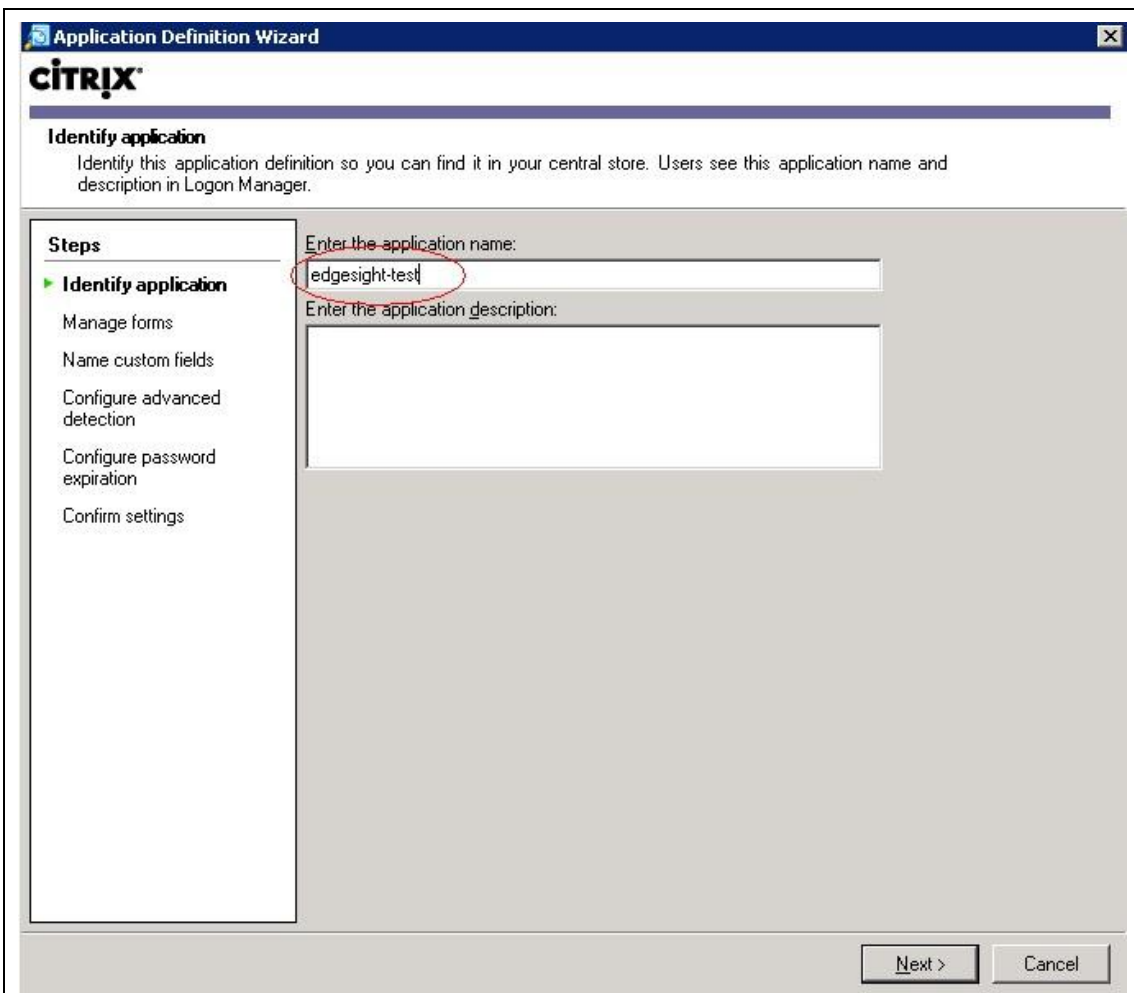


图 21 输入应用程序的名称  
注意：不需要和所发布的应用名称对应

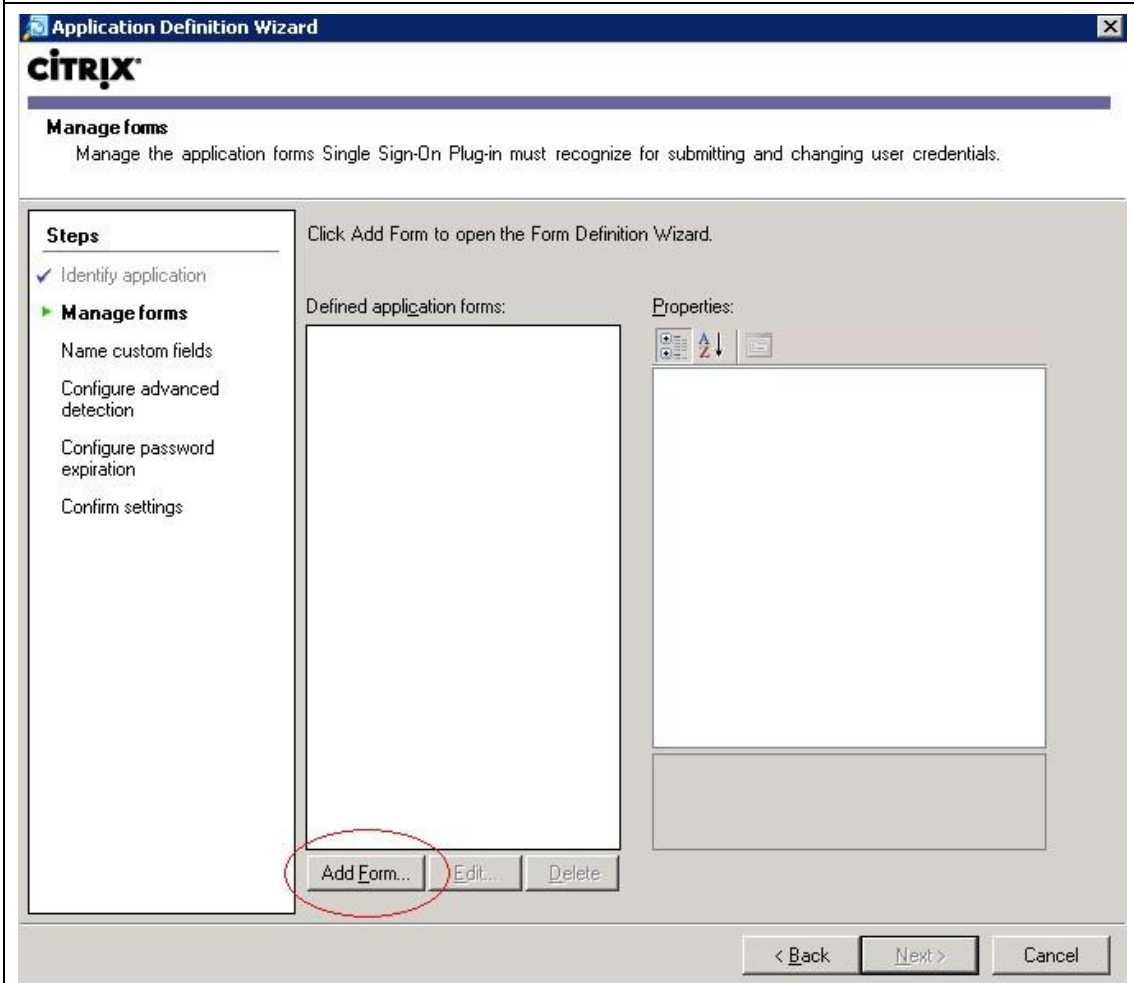


图 22 定义应用的 form

1、点击“添加 Form”；

## 2、在这里可以添加依次多个应用。

**Form Definition Wizard**

**CITRIX**

**Name form**  
Provide a name for this form and select a type of form to detect. Optionally select redirection and form detection options.

**Steps**

- Name form
- Identify form
- Define form actions
- Configure other settings
- Confirm settings

Enter form name:  
form01

Select form type:  
Logon form

Special actions

- No special action
- Redirect to Windows application
- Ignore this form when it is detected by Single Sign-On Plug-in

Next > Cancel

图 23 输入 Form 名称和选择 Form 类型

### 1、选择 form 类型

- 1) Logon form
- 2) Password change form
- 3) Successful password change form
- 4) Failed password change form

### 2、指定行为

- 1) 不指定
- 2) 重定向到 Windows 下应用
- 3) 被检测到有 SSO 时忽略这种 form

### 3、根据测试应用要求选择不同类型和行为，在这里选择的是“logon form”和“不指定”

注意：在进行下一步之前，打开实验环境中测试单点登录功能的应用程序

**Form Definition Wizard**

**CITRIX**

**Identify form**  
Identify the detection criteria for this form.

**Steps**

- ✓ Name form
- Identify form
- Define form actions
- Configure other settings
- Confirm settings

Add one or more URLs and fields to identify this form. Select strict URL matching to force the Single Sign-On Plug-in software to respond only to the exact URLs defined below

Form identifiers

URLs:

Select...

Strict URL matching

Case-sensitive URL

Add... Edit... Delete

Advanced Matching

Configure advanced matching to detect applications that contain dynamic URLs

Advanced Matching...

< Back Next > Cancel

图 24 指定 Form，点击“Select”

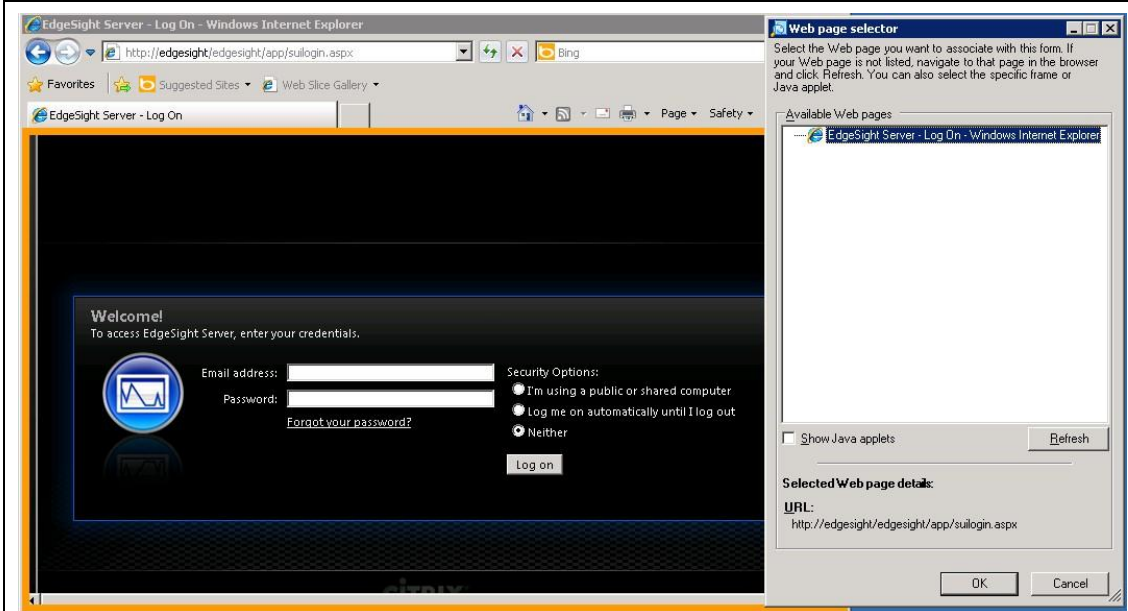


图 25 在右边窗口选择要定义的应用程序，选中之后会显现高亮

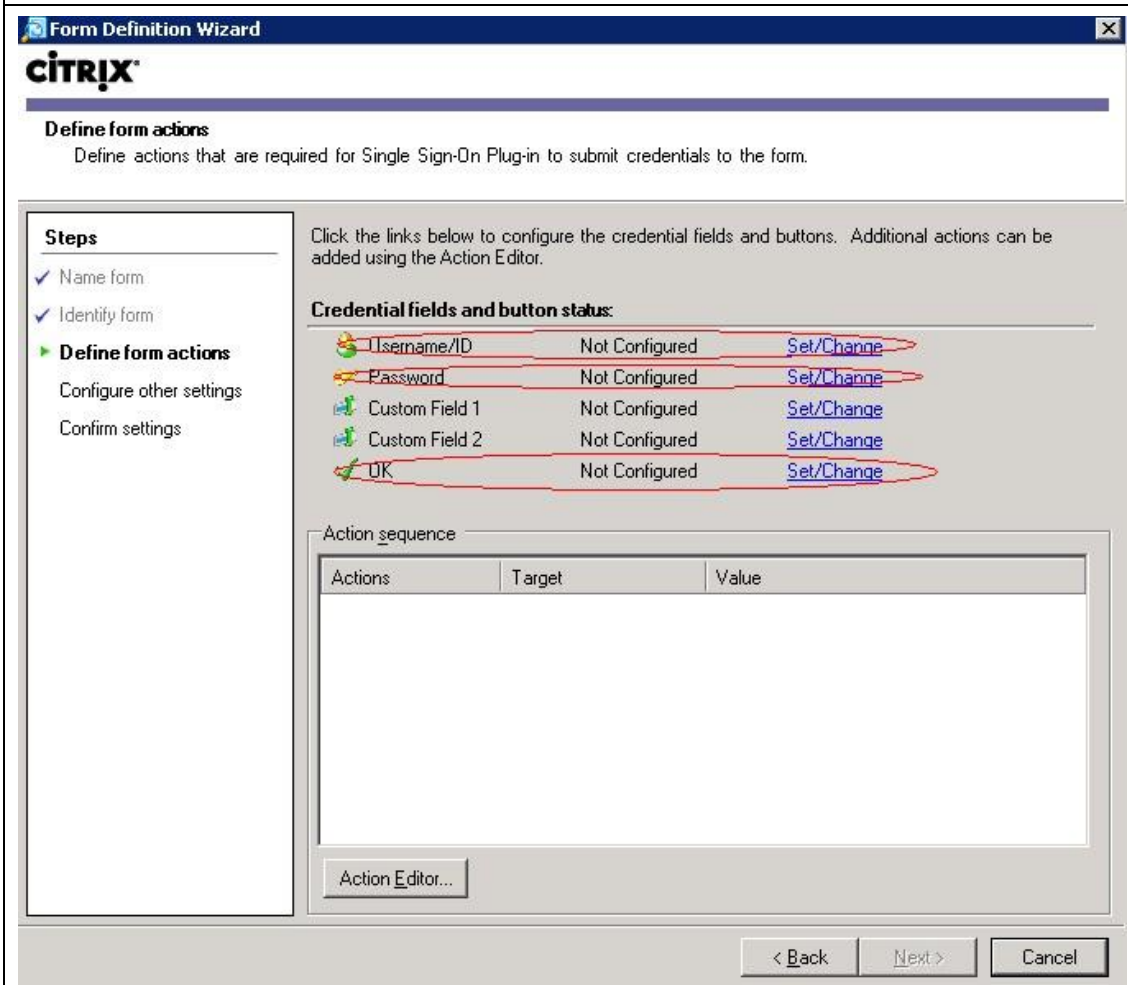


图 26 定义 form 的行为

结合我们的测试应用，在这里选择定义“Username、Password、OK”3个控件，点击各自后面的“Set/Change”进行定义（注意，测试应用不能关闭，如果关闭请重新打开）；选中相应的控件后，应用上会相应的显现出高亮。

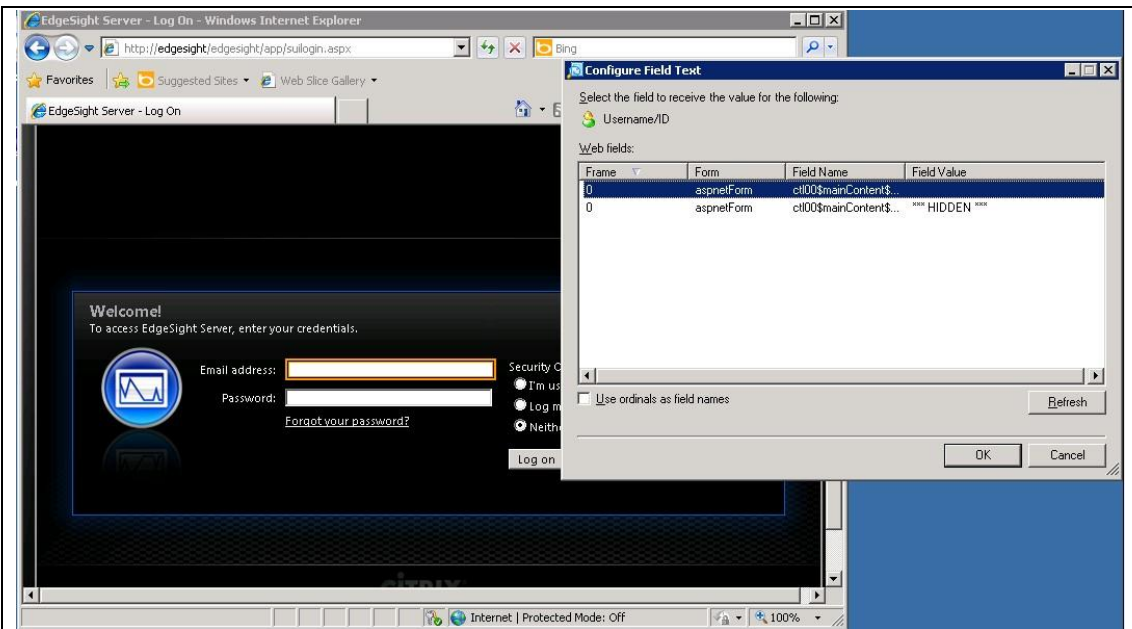


图 27 定义“Username”控件

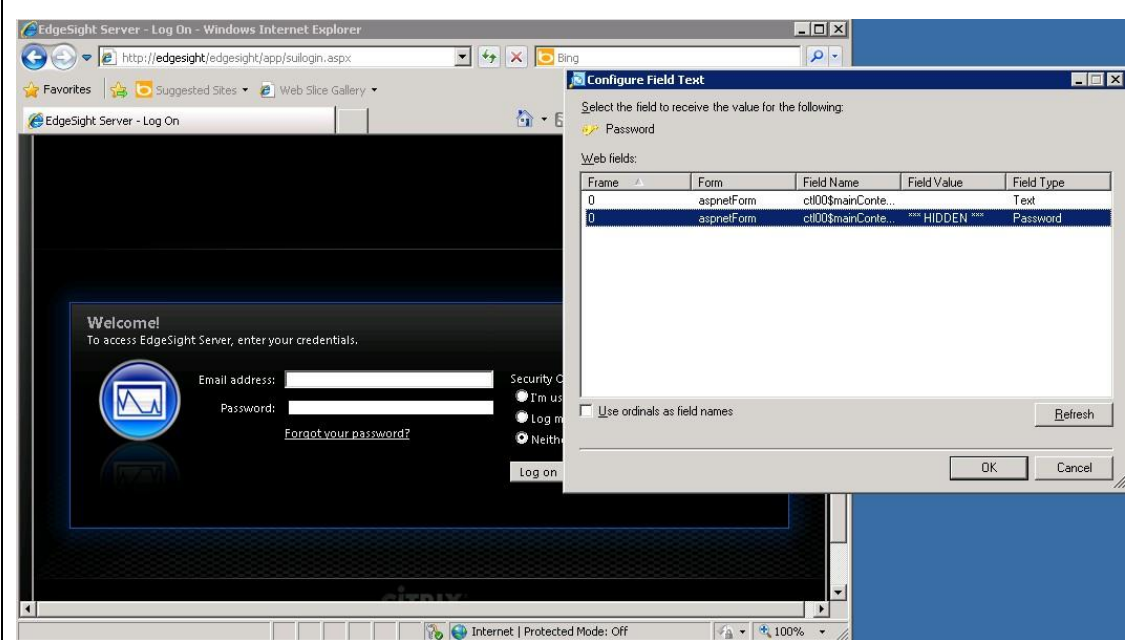


图 28 定义“Password”控件

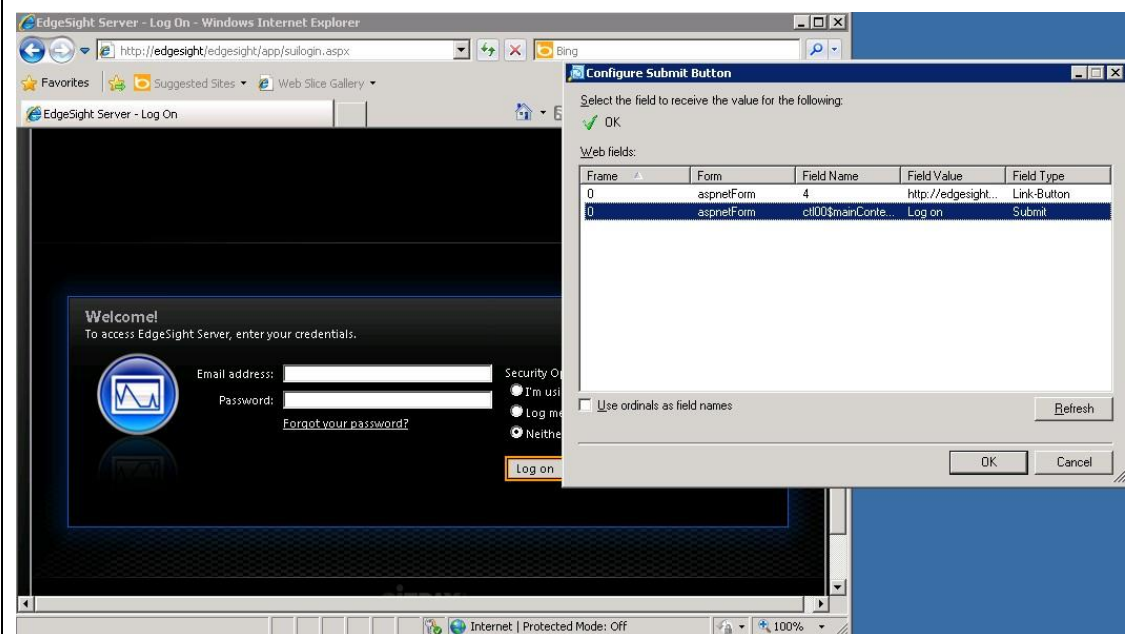


图 29 定义“OK”控件

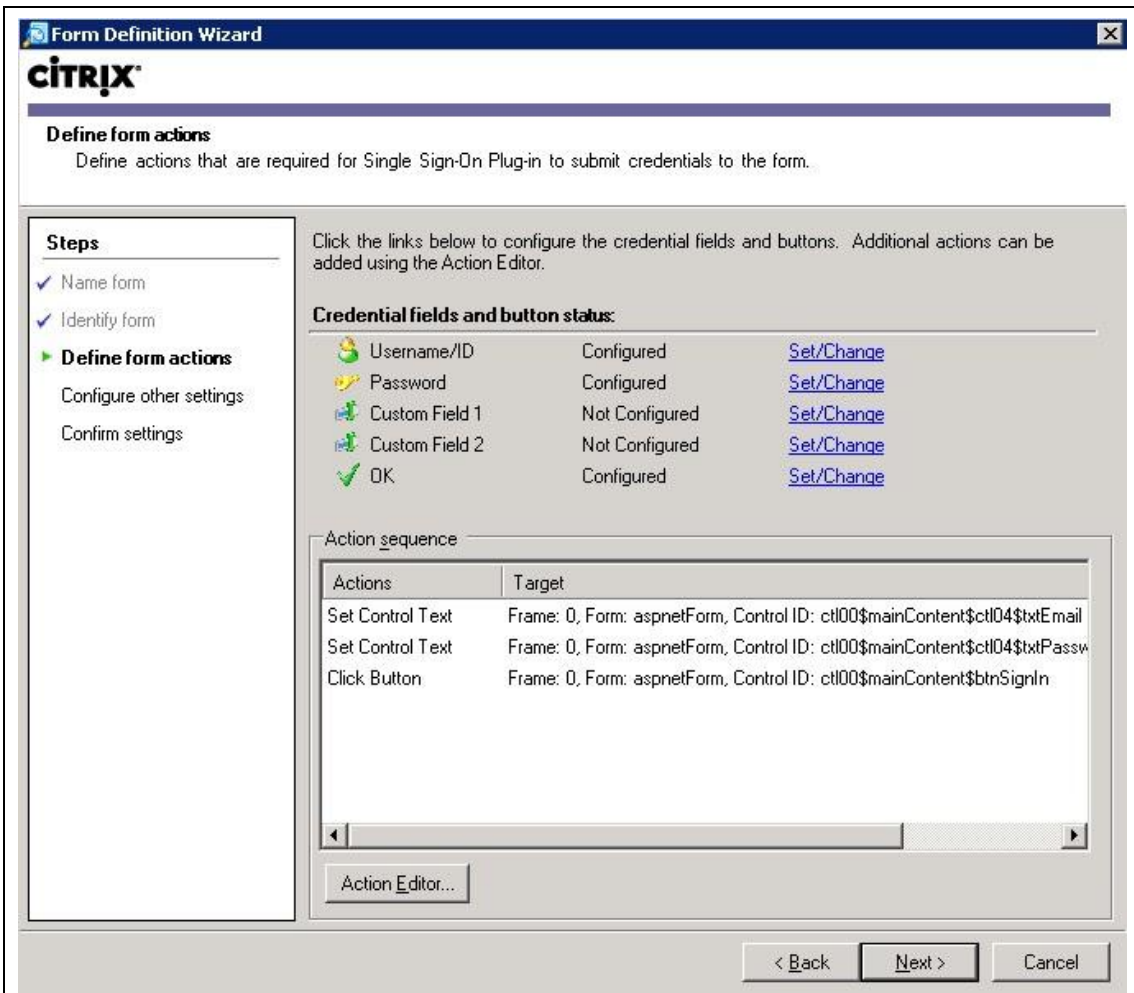


图 30 定义完 3 个控件后状态

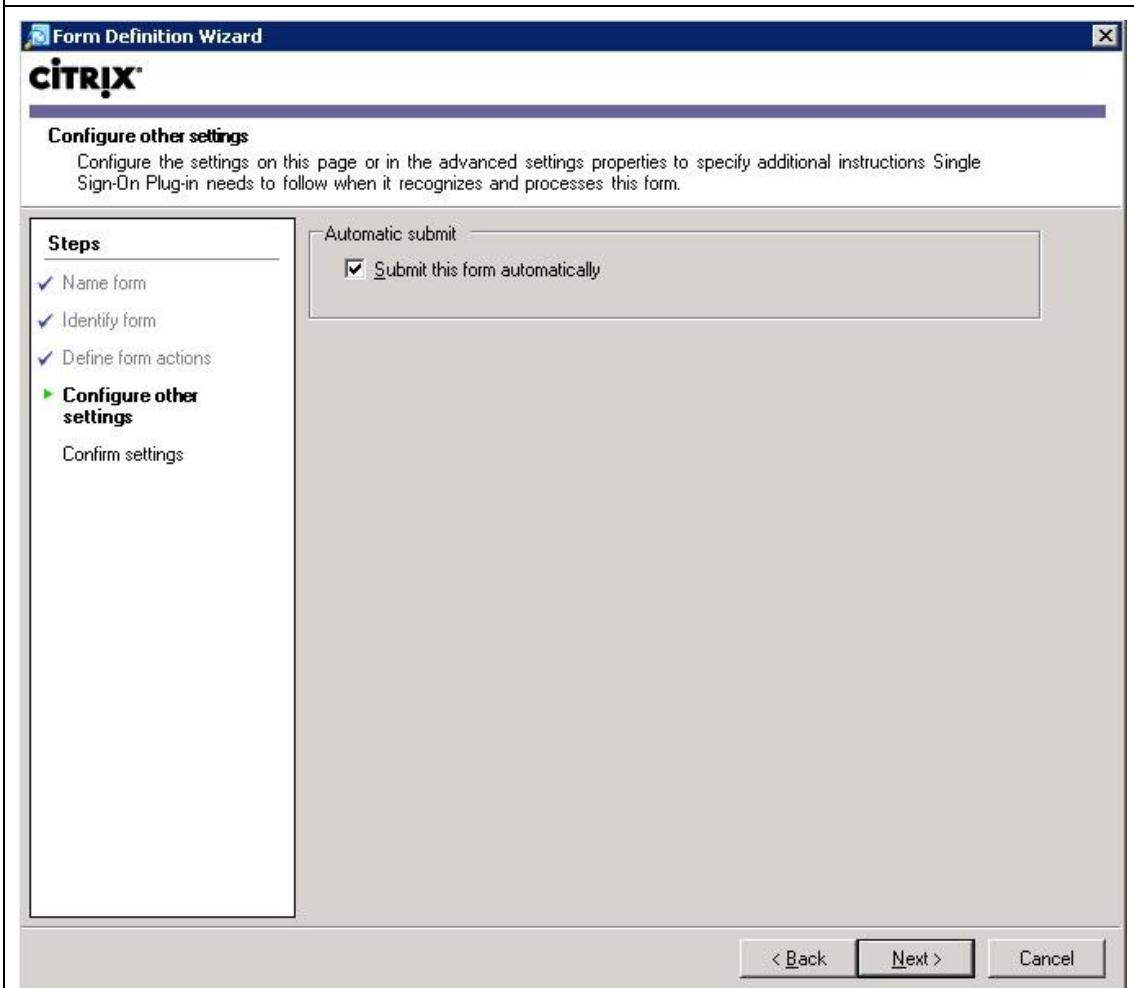


图 31 默认即可（自动提交）

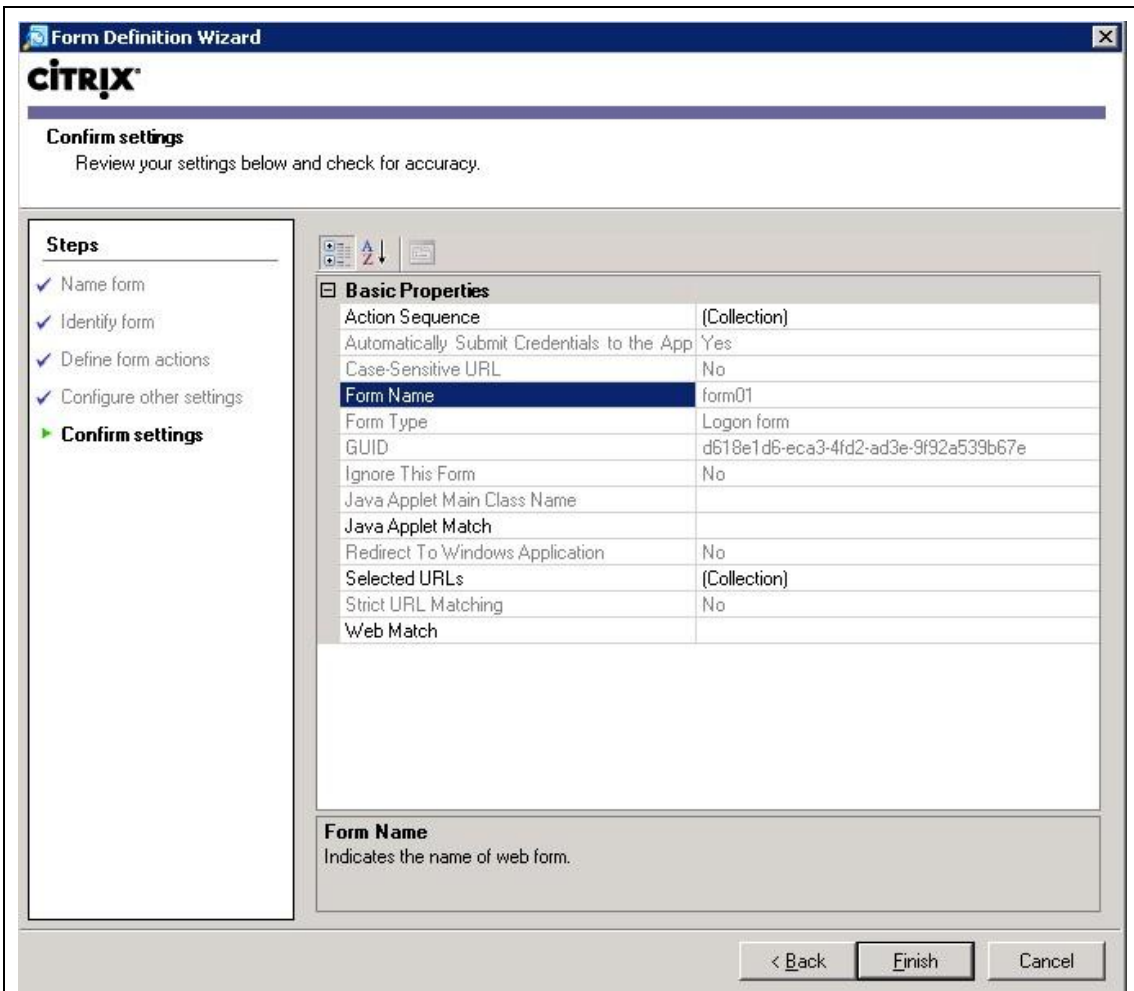


图 32 确认正确配置后，点击完成

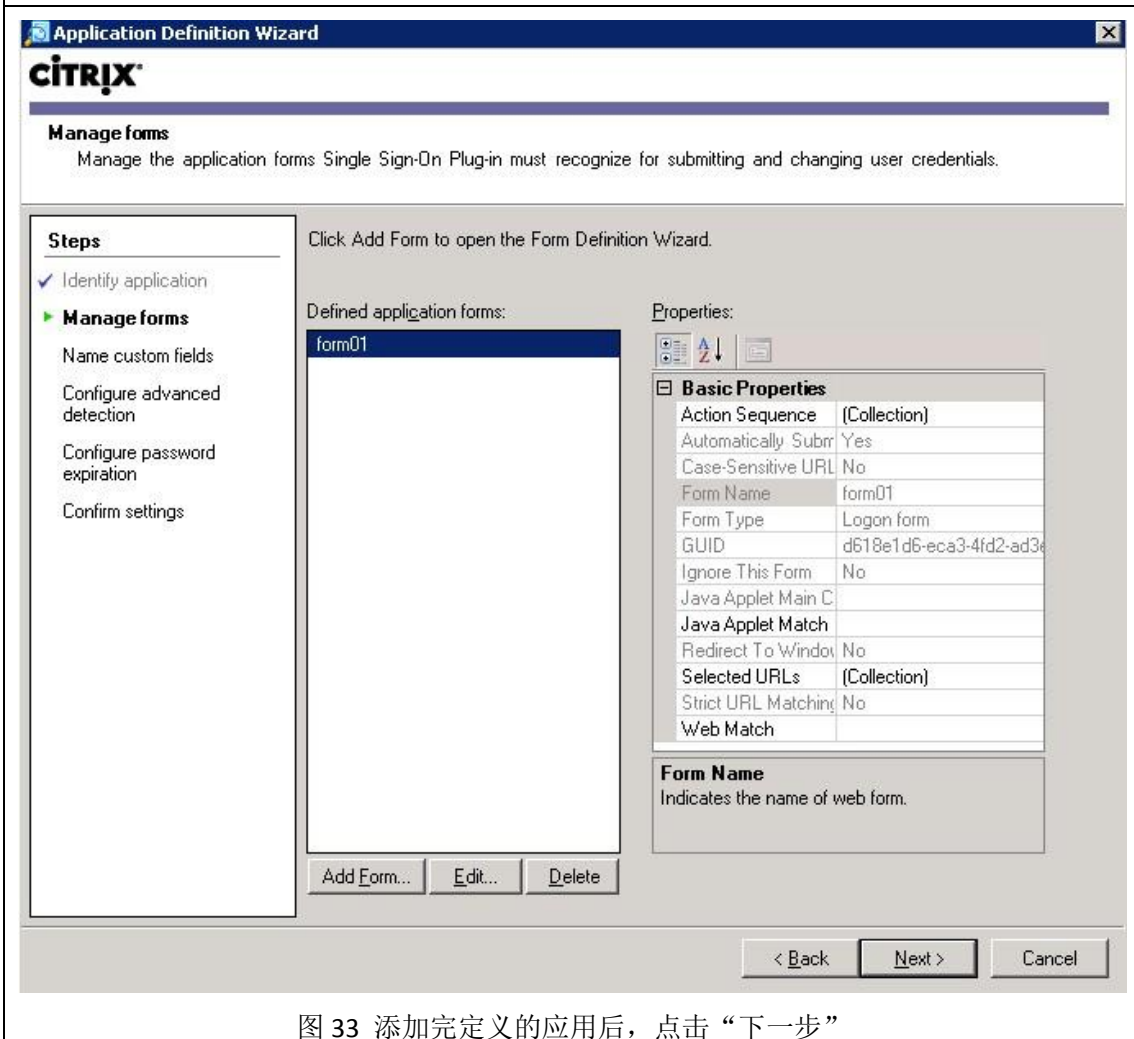


图 33 添加完定义的应用后，点击“下一步”

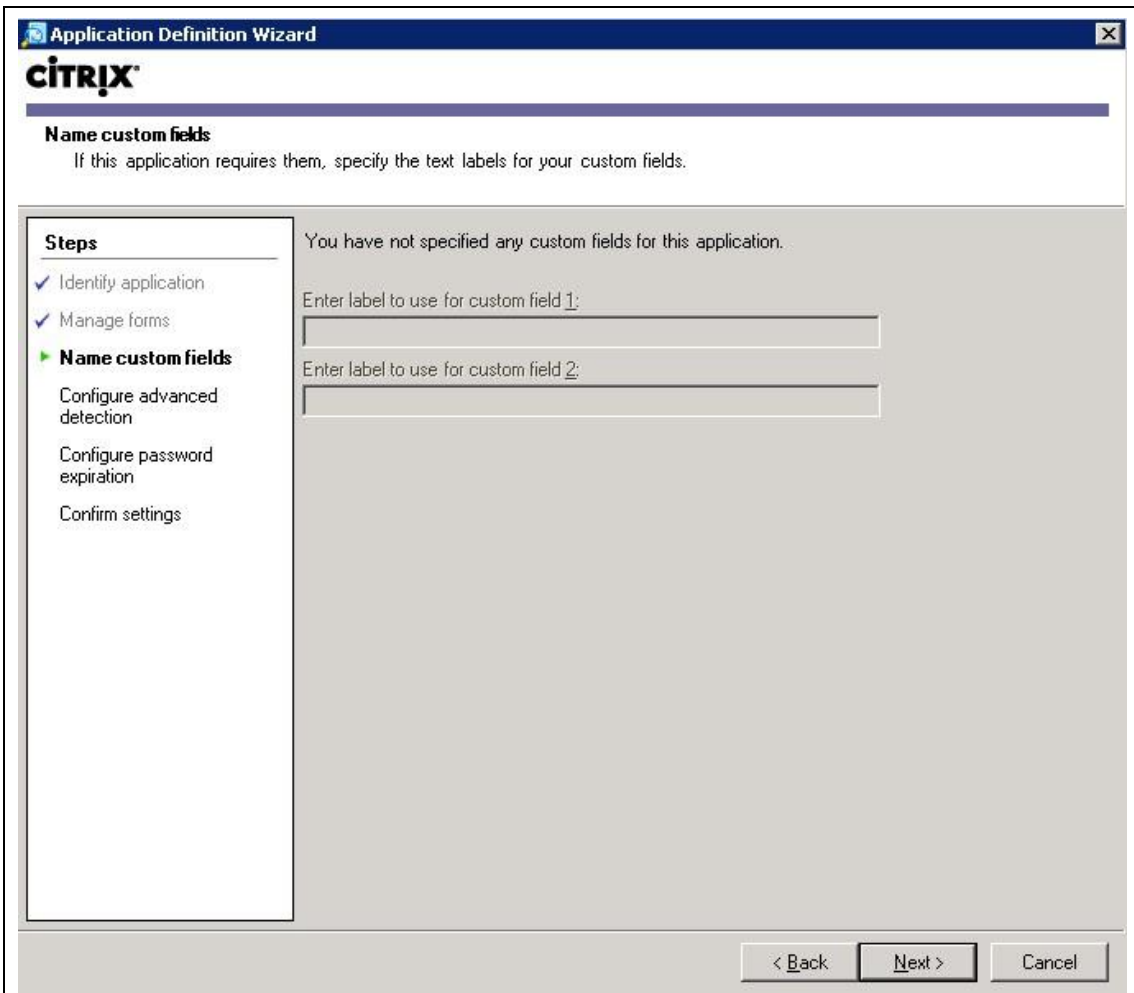


图 34 在图 30 中没有定义此控件，直接下一步

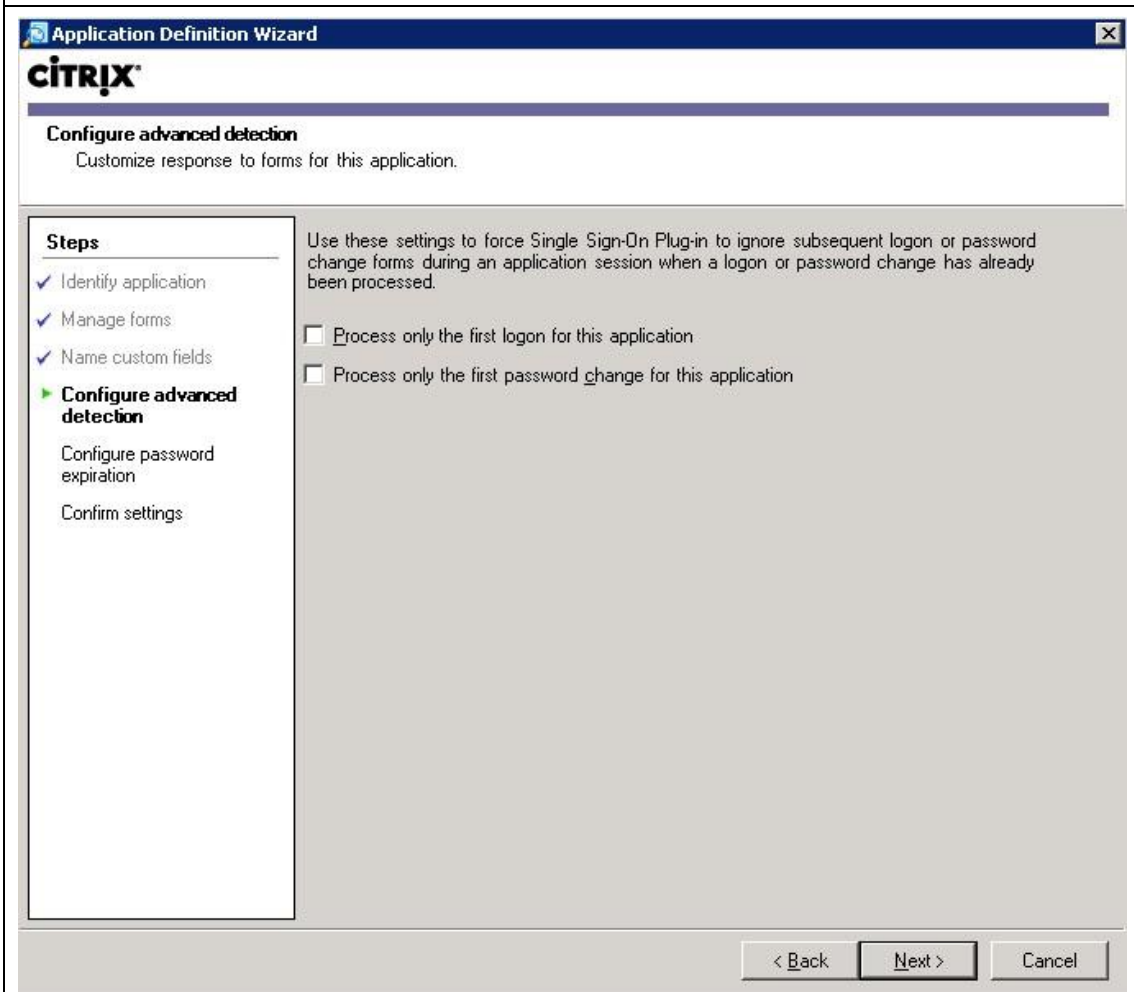


图 35 单点登录的处理机制（在一次登录中，是否多次自动提交）默认即可

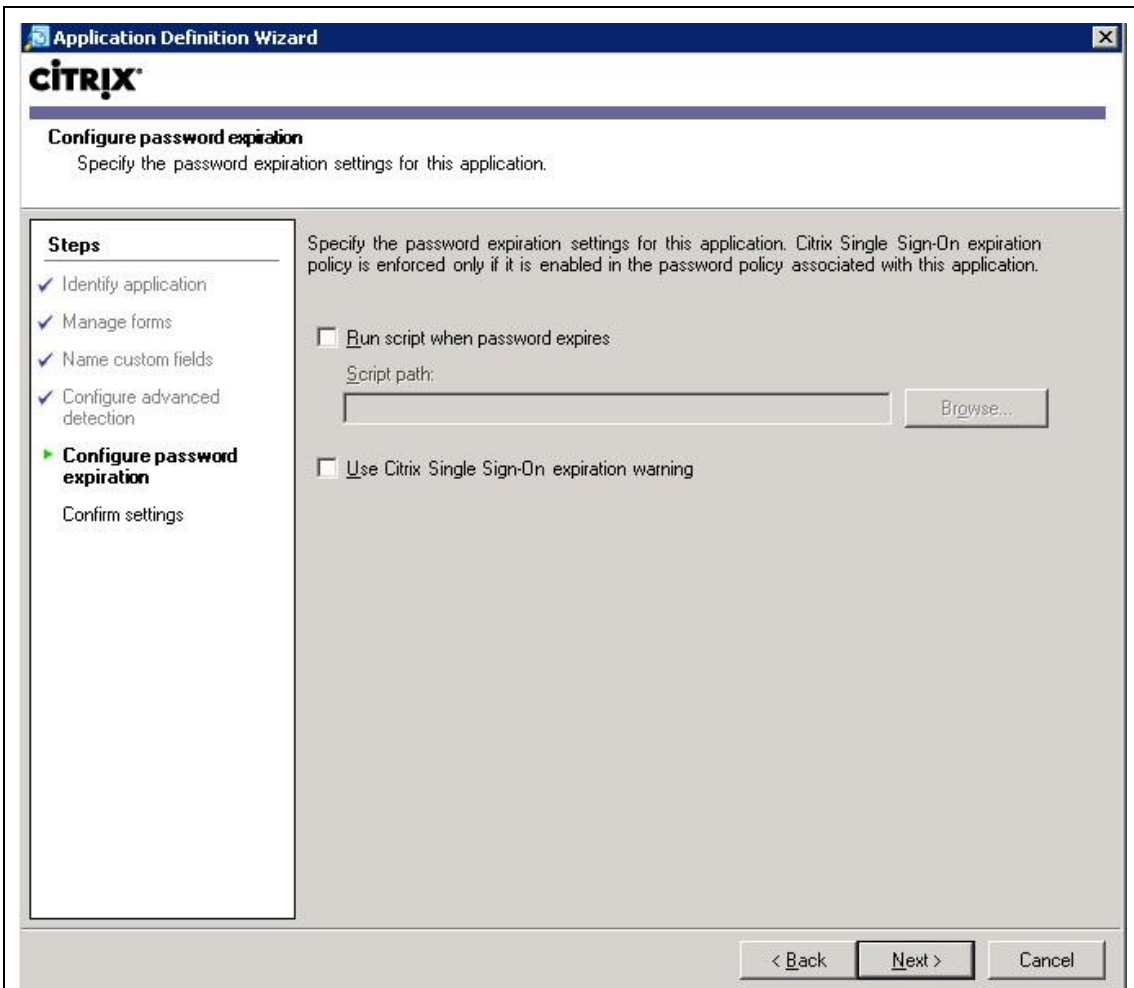


图 36 配置 password 失效，

- 1) 密码失效后可以运行自定义脚本文件
- 2) 打开 Single Sign-On 失效警告

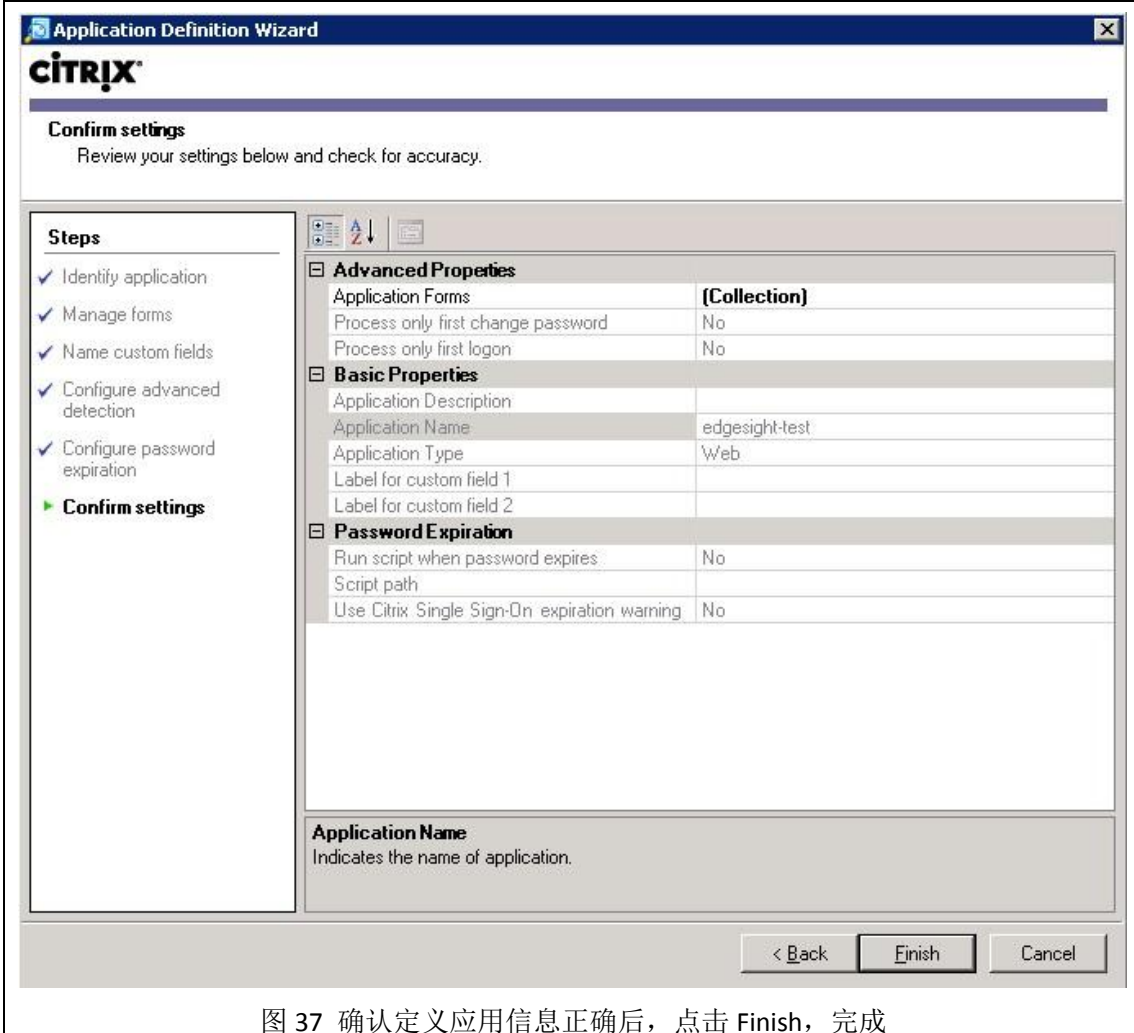


图 37 确认定义应用信息正确后，点击 Finish，完成

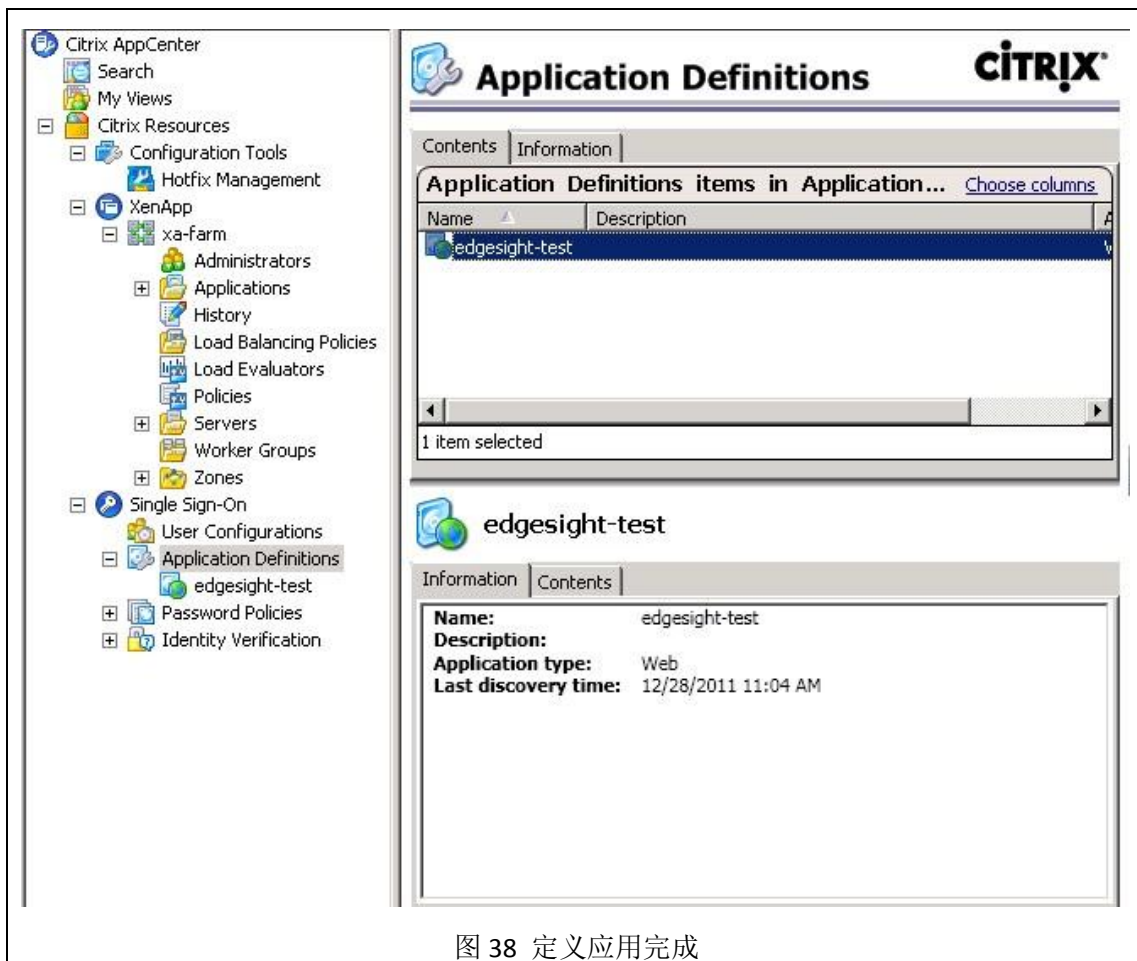


图 38 定义应用完成

## 2) 定义用户 (Users Configuration)

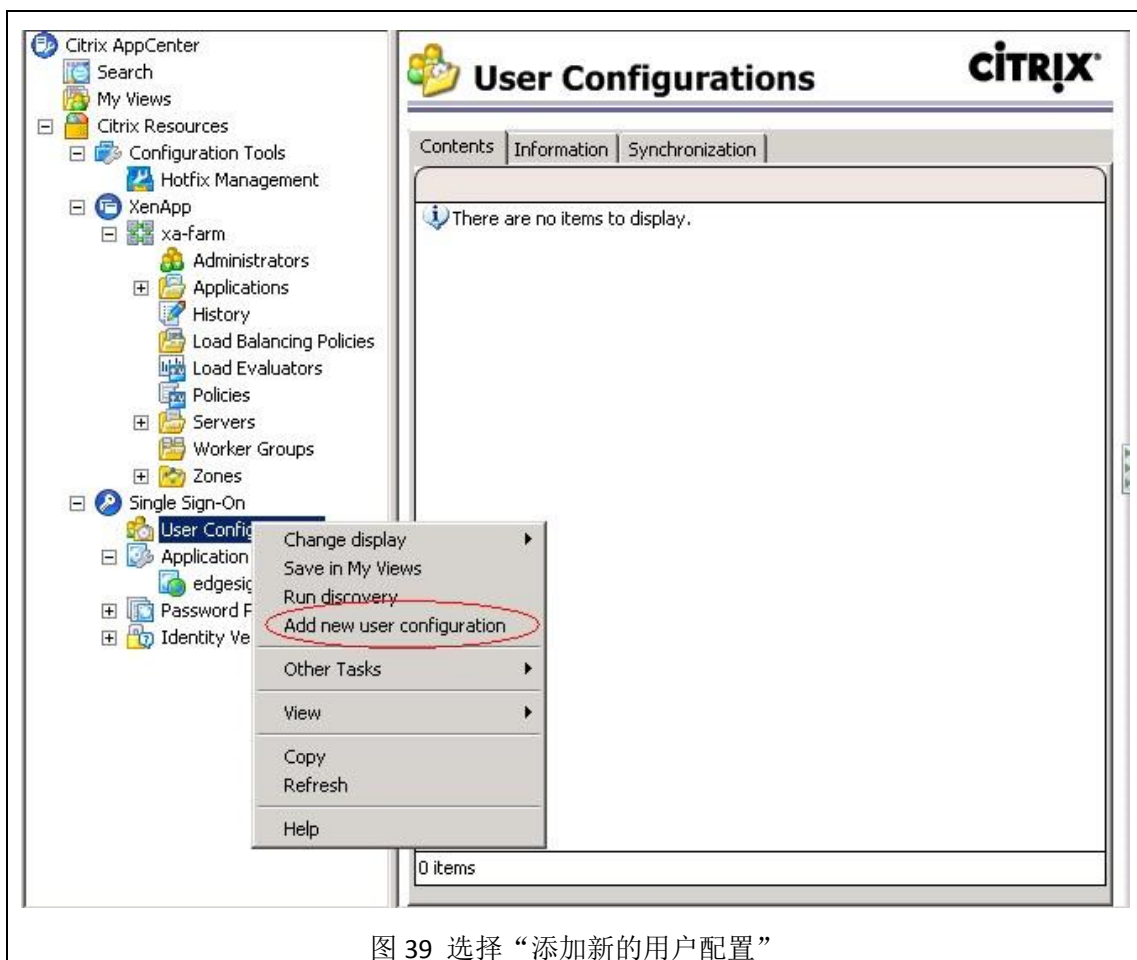


图 39 选择“添加新的用户配置”

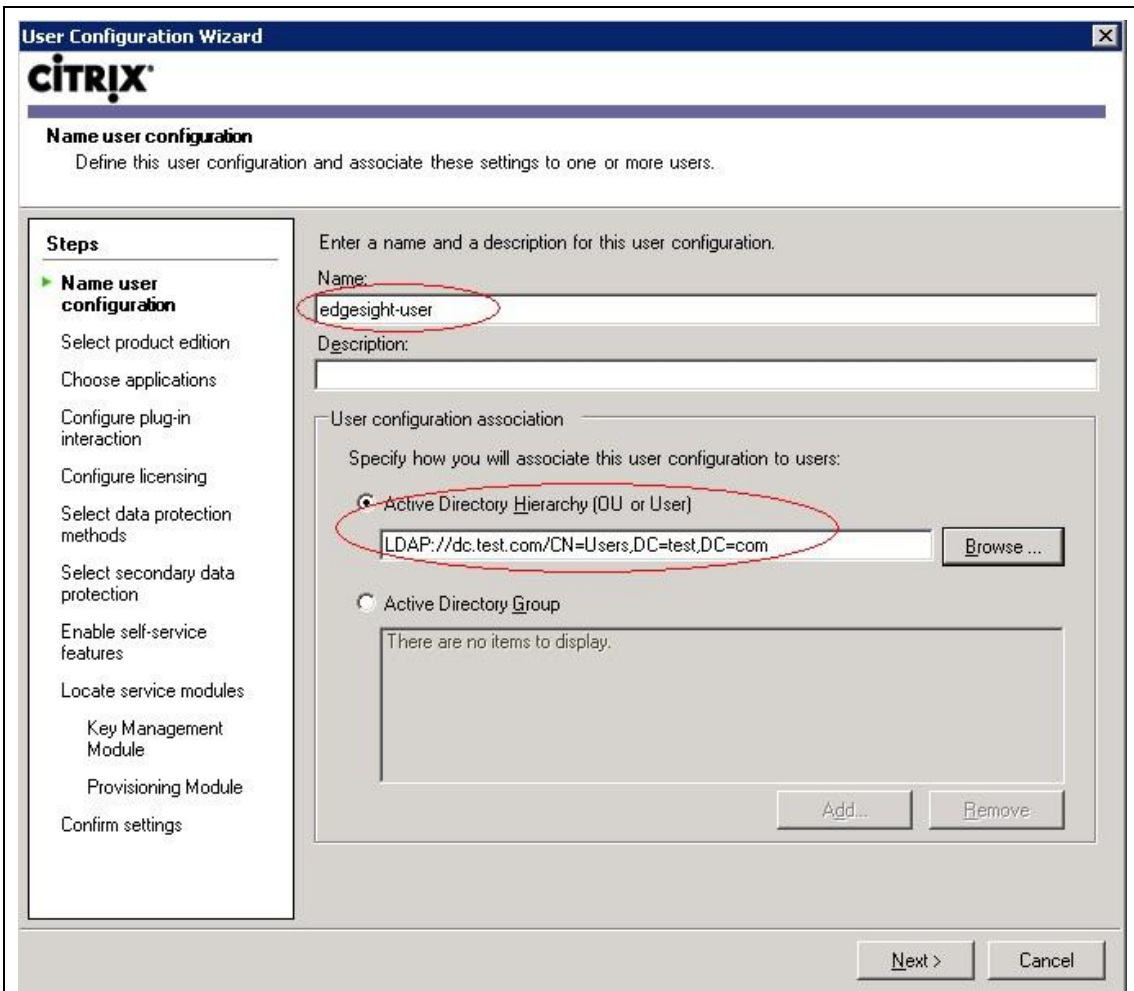


图 40 填写“用户名称和描述”、用户的关联方式（OU 或者组的方式）

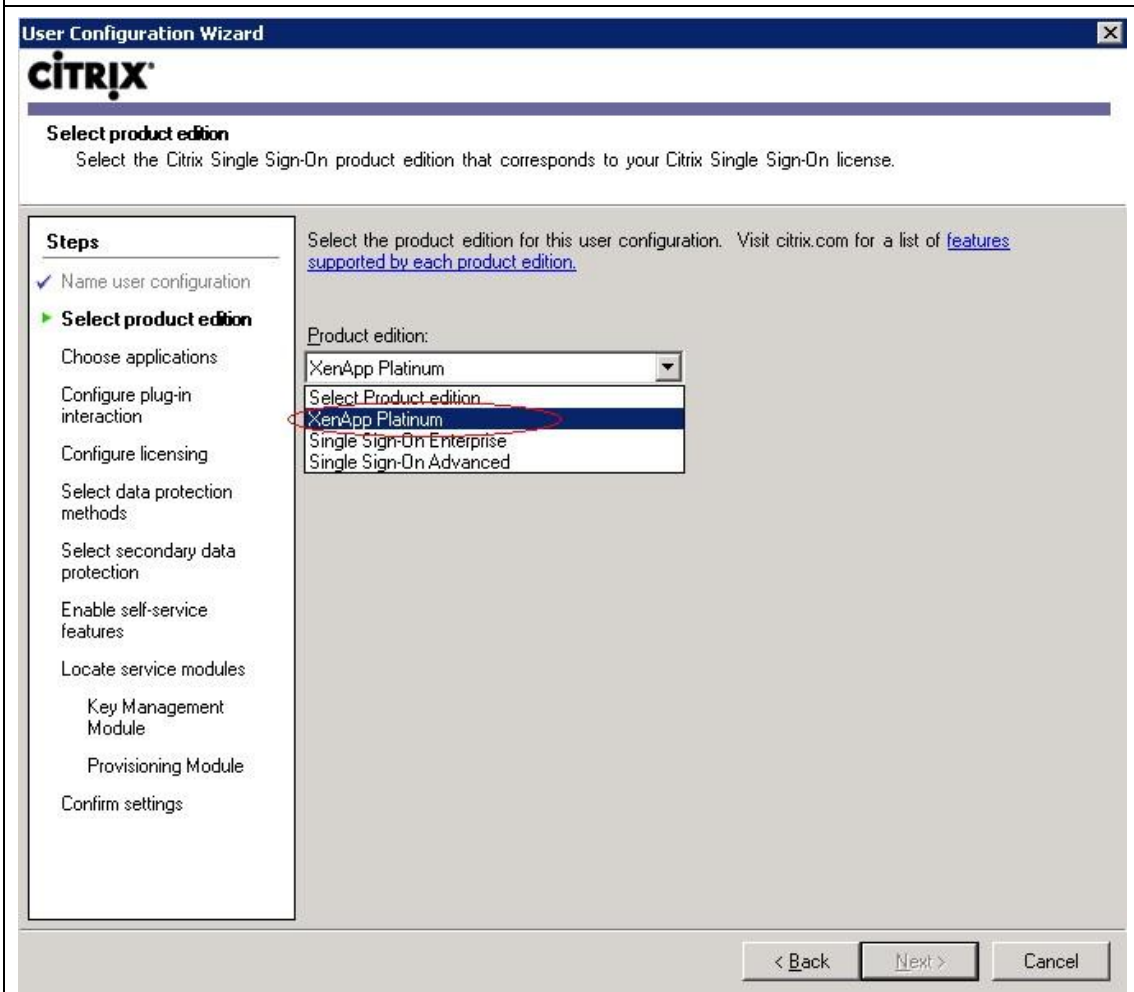


图 41 选择 SSO 产品版本（对 License 版本有一定的要求）

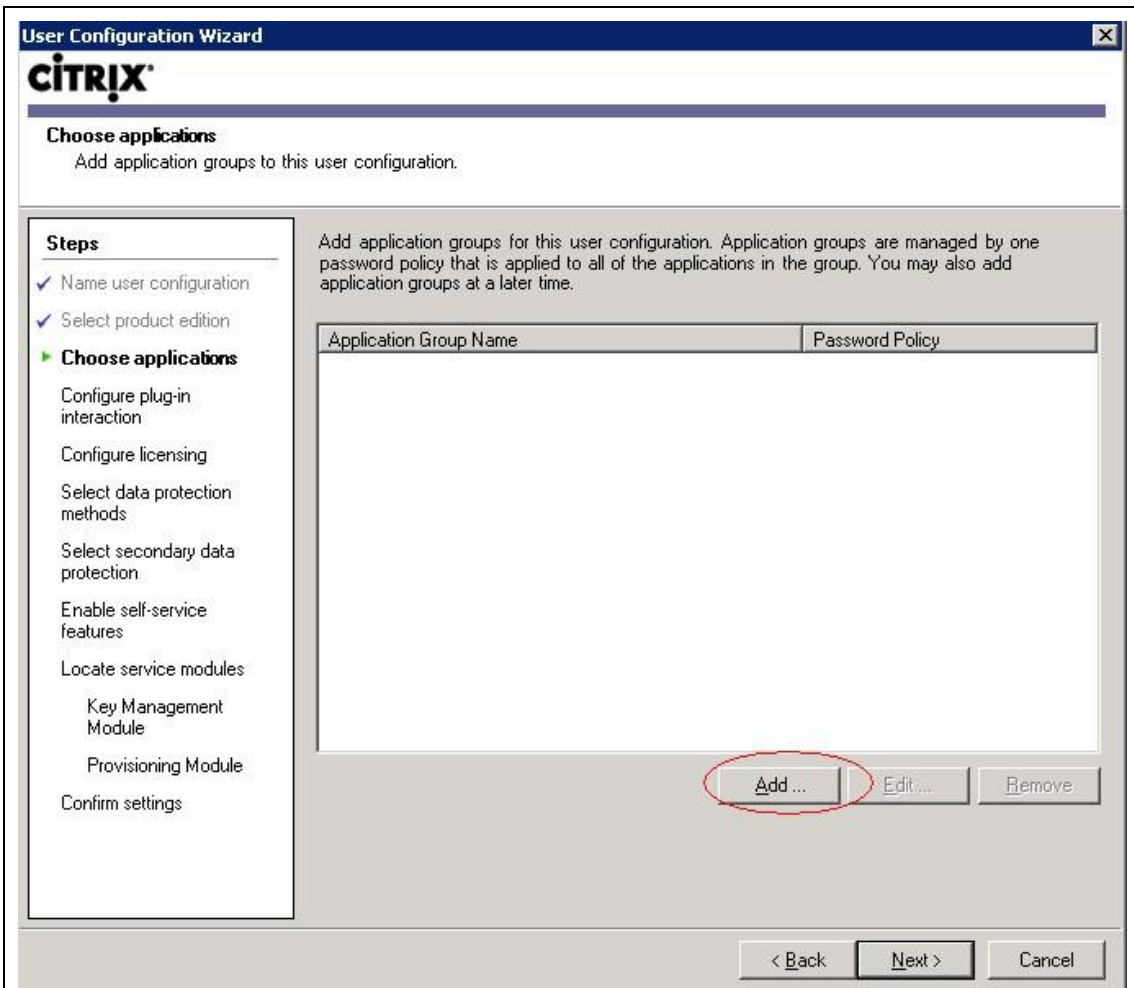


图 42 添加这一组用户针对哪一组的应用程序有效，点击“添加”

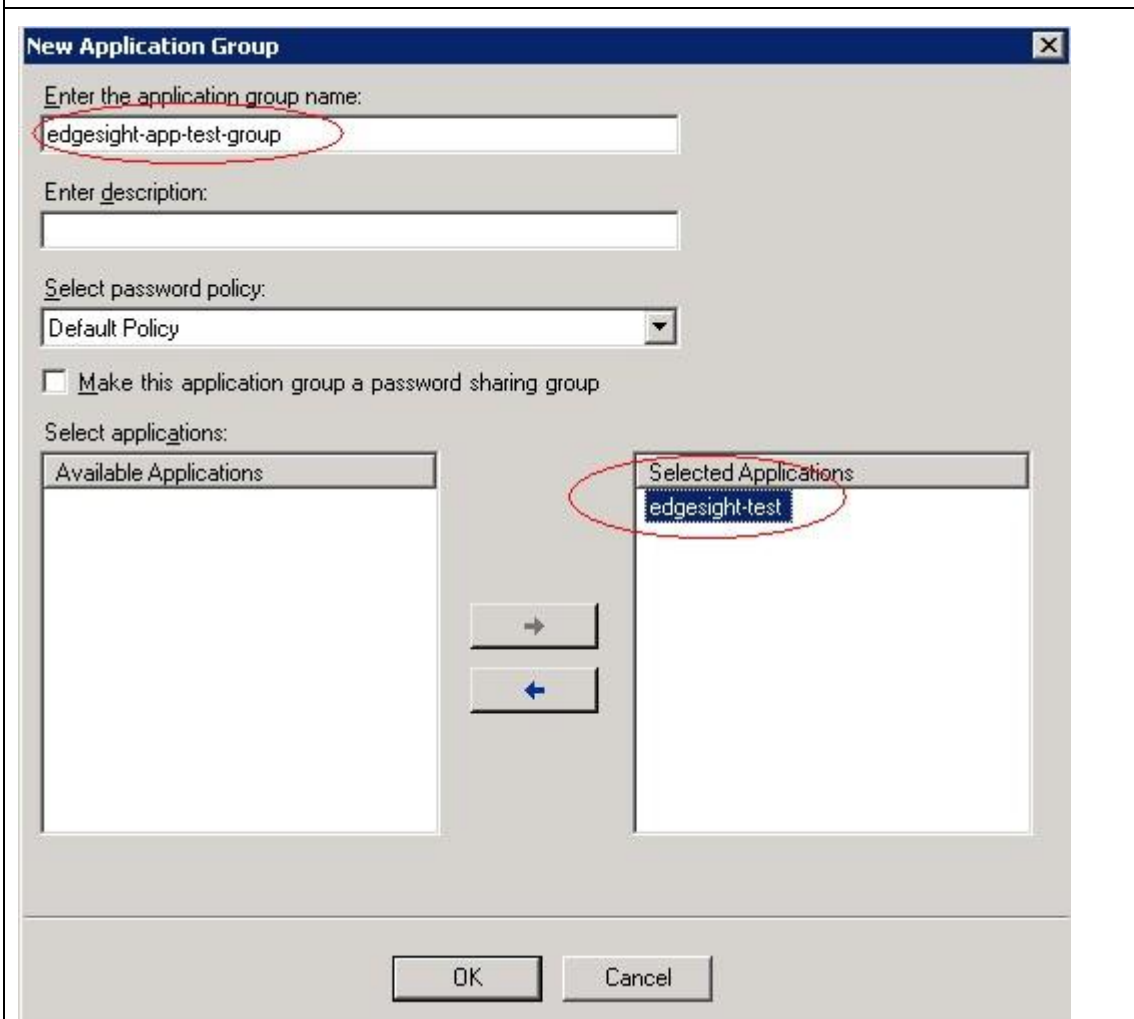


图 43 创建应用程序组，组中包含哪些应用程序；  
填写“应用程序组名称”、默认密码策略、选择左边窗口的应用程序

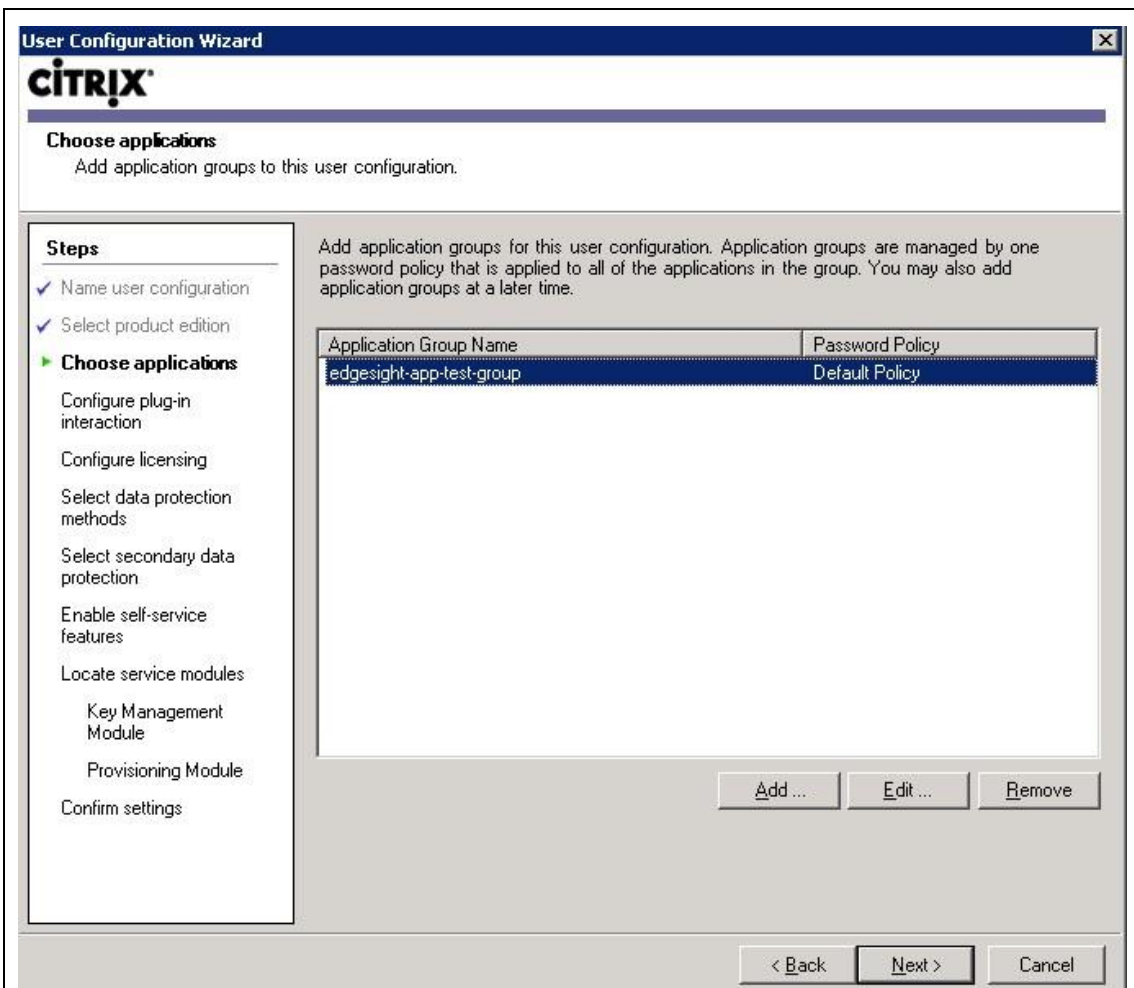


图 44 添加完应用程序组后，下一步

1) 在此可以添加过个应用程序组；

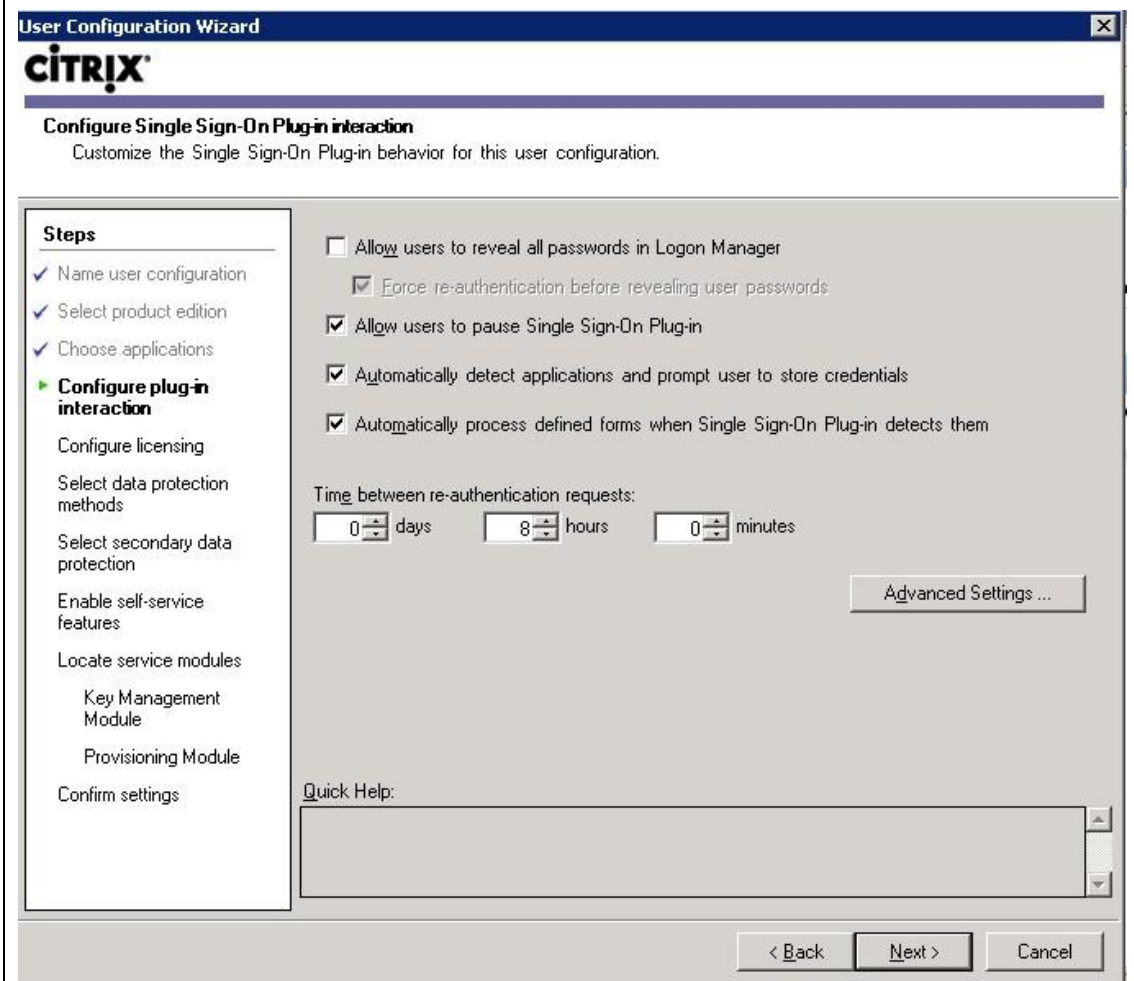


图 45 定义 SSO 插件的一些行为与功能

1) 允许用户查看所有密码

- 2) 允许用户暂停 SSO
  - 3) 自动检测应用和提示用户保存证书
  - 4) 在 SSO 检测到应用时，自动进行定义 forms
- 一般默认即可

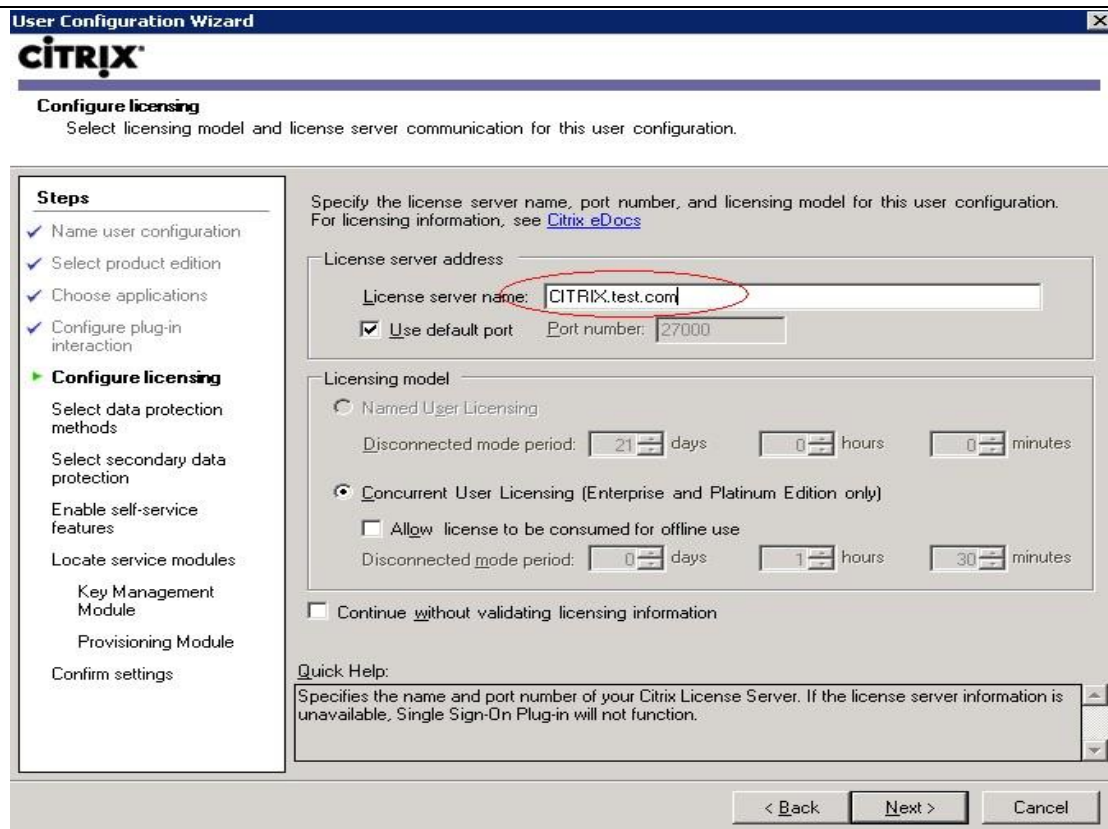


图 46 SSO 需要 License 授权，在此输入 License 服务器地址

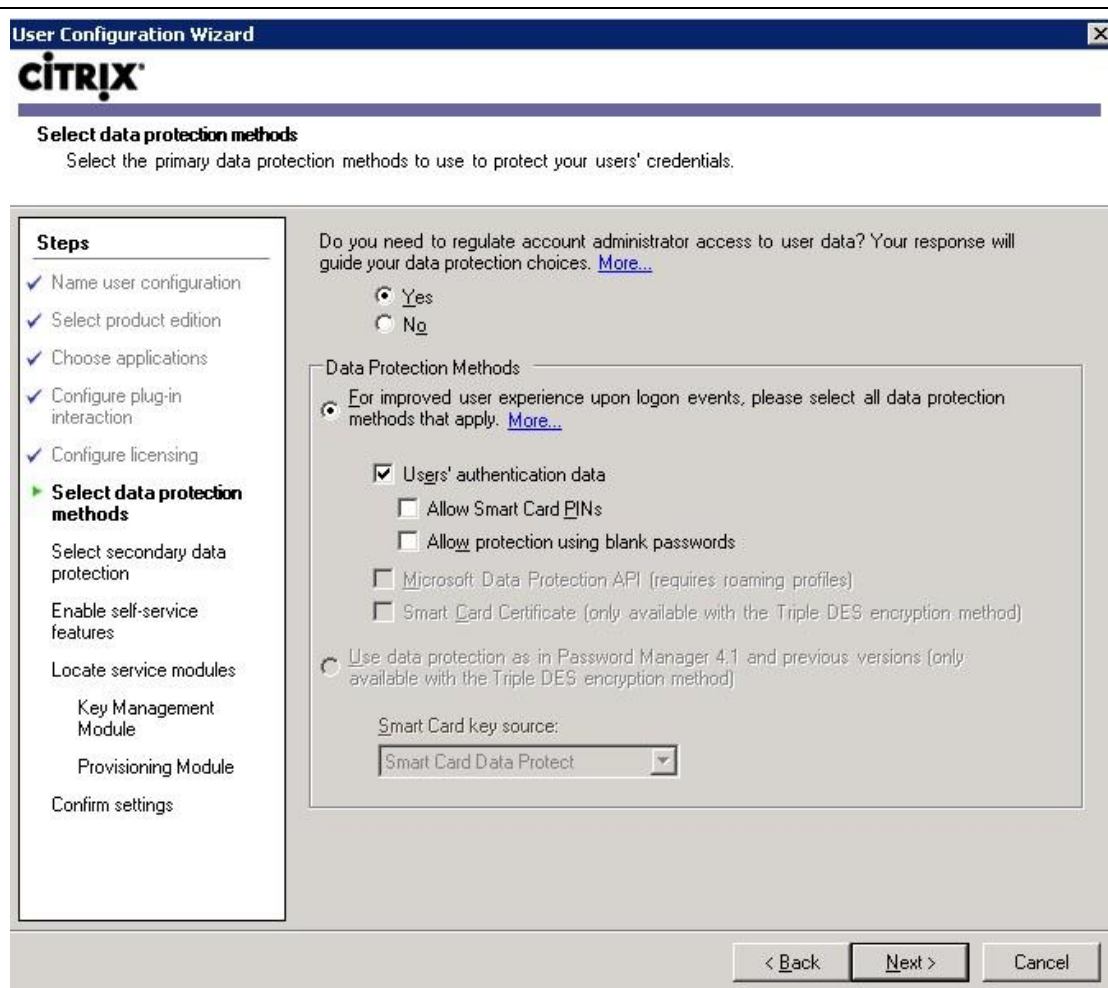


图 47 定义一些 SSO 的帐号数据安全设置（默认即可）

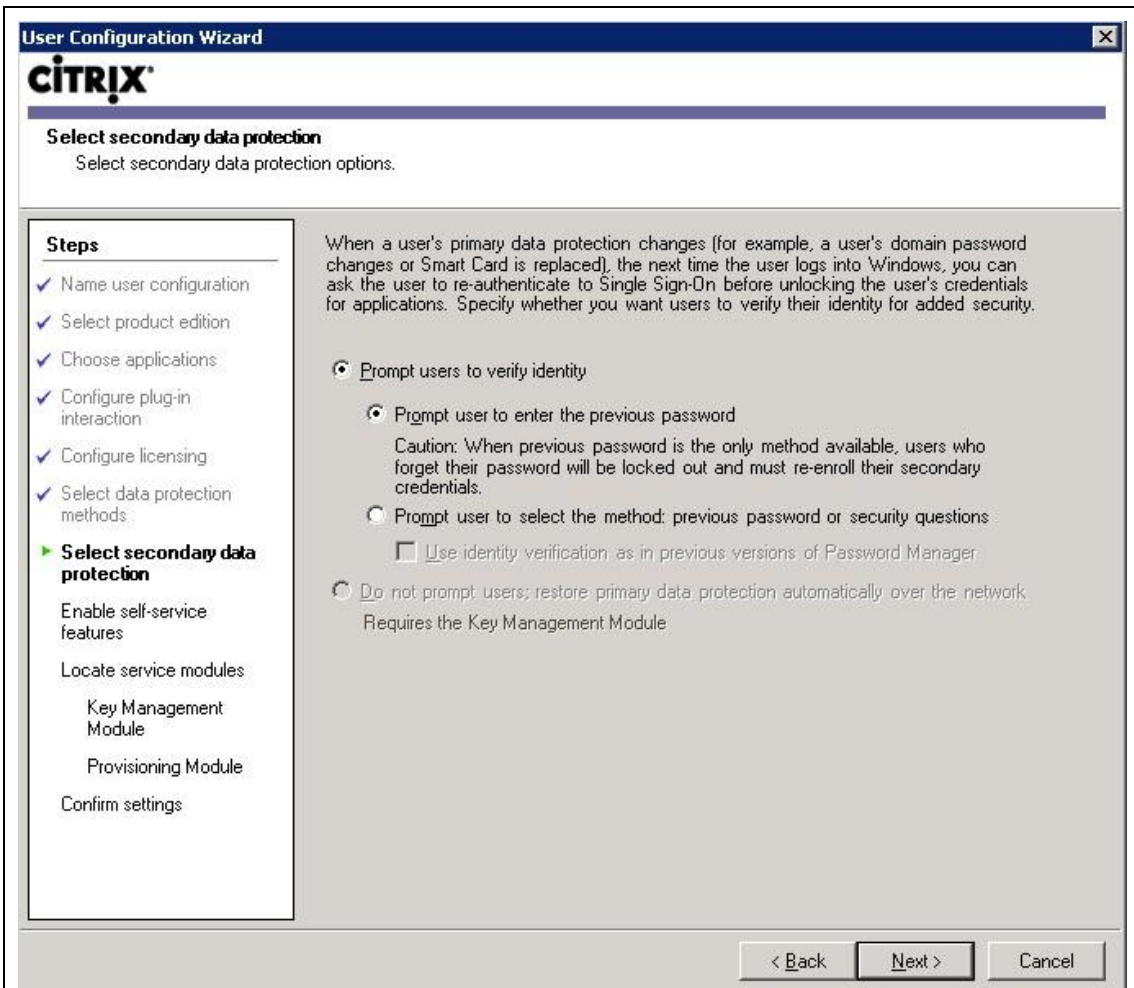


图 48 提示用户身份安全验证和方式，一般默认即可，直接下一步

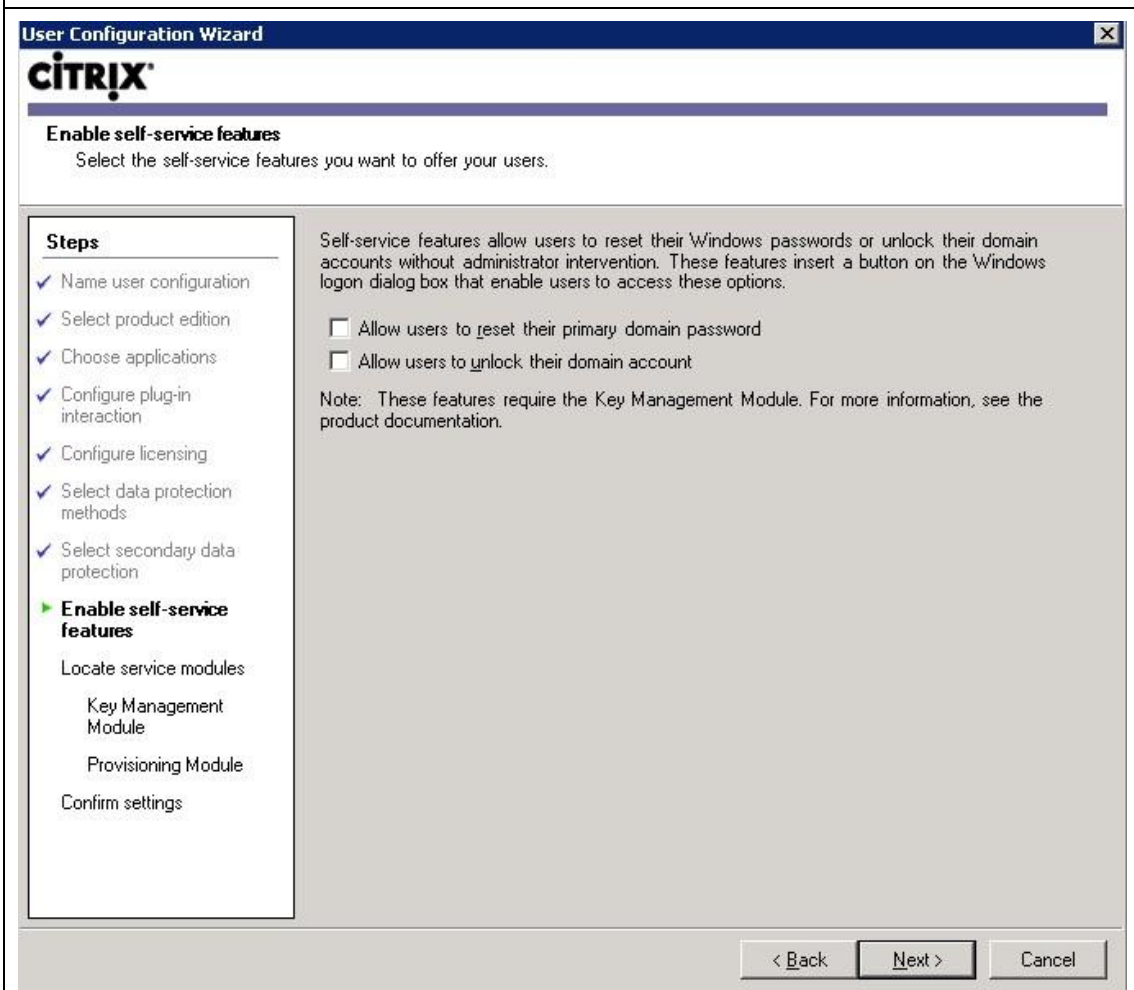


图 49 开启自助服务功能，因为没有安装自助服务插件，默认即可

- 1、允许用户重置域密码
- 2、允许用户解锁域账户

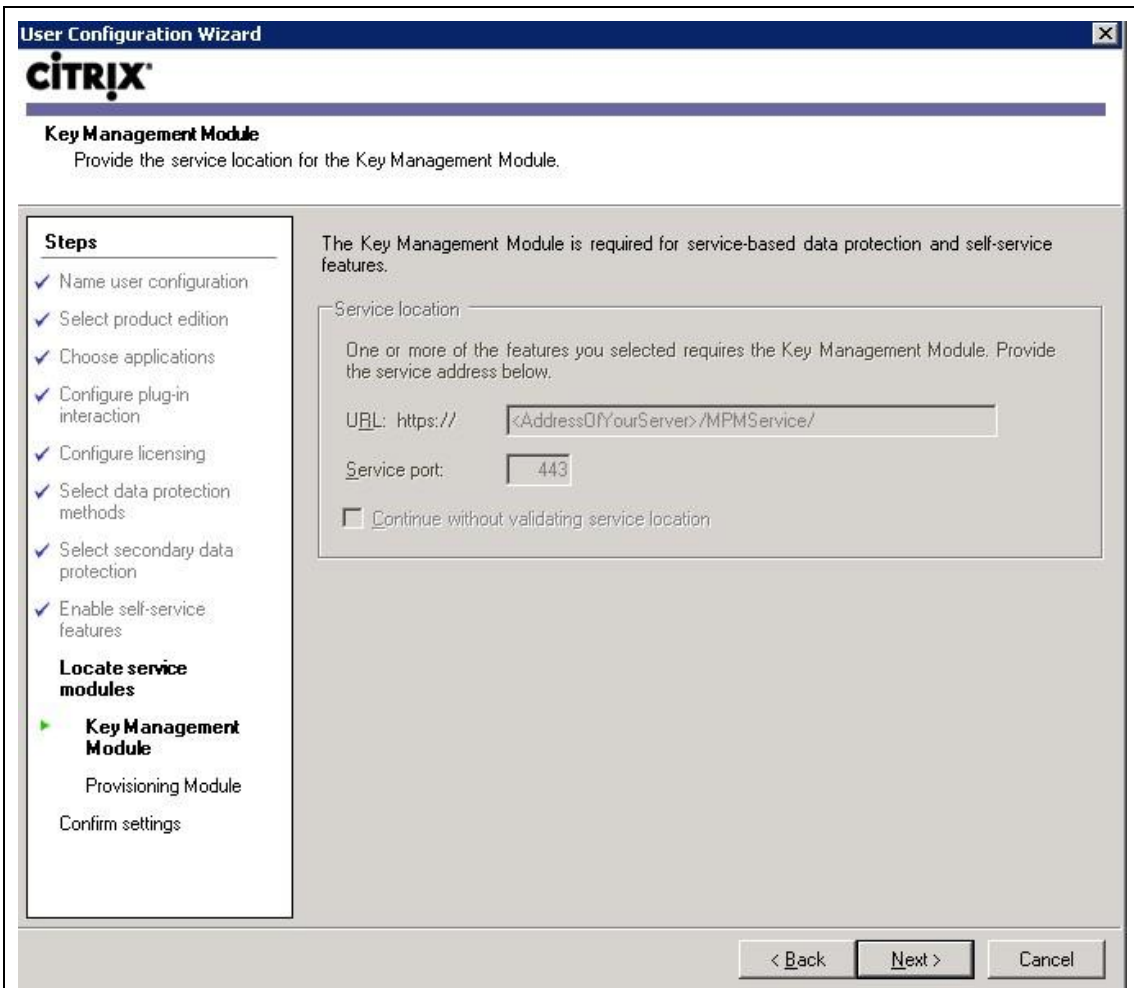


图 50 默认，直接一下

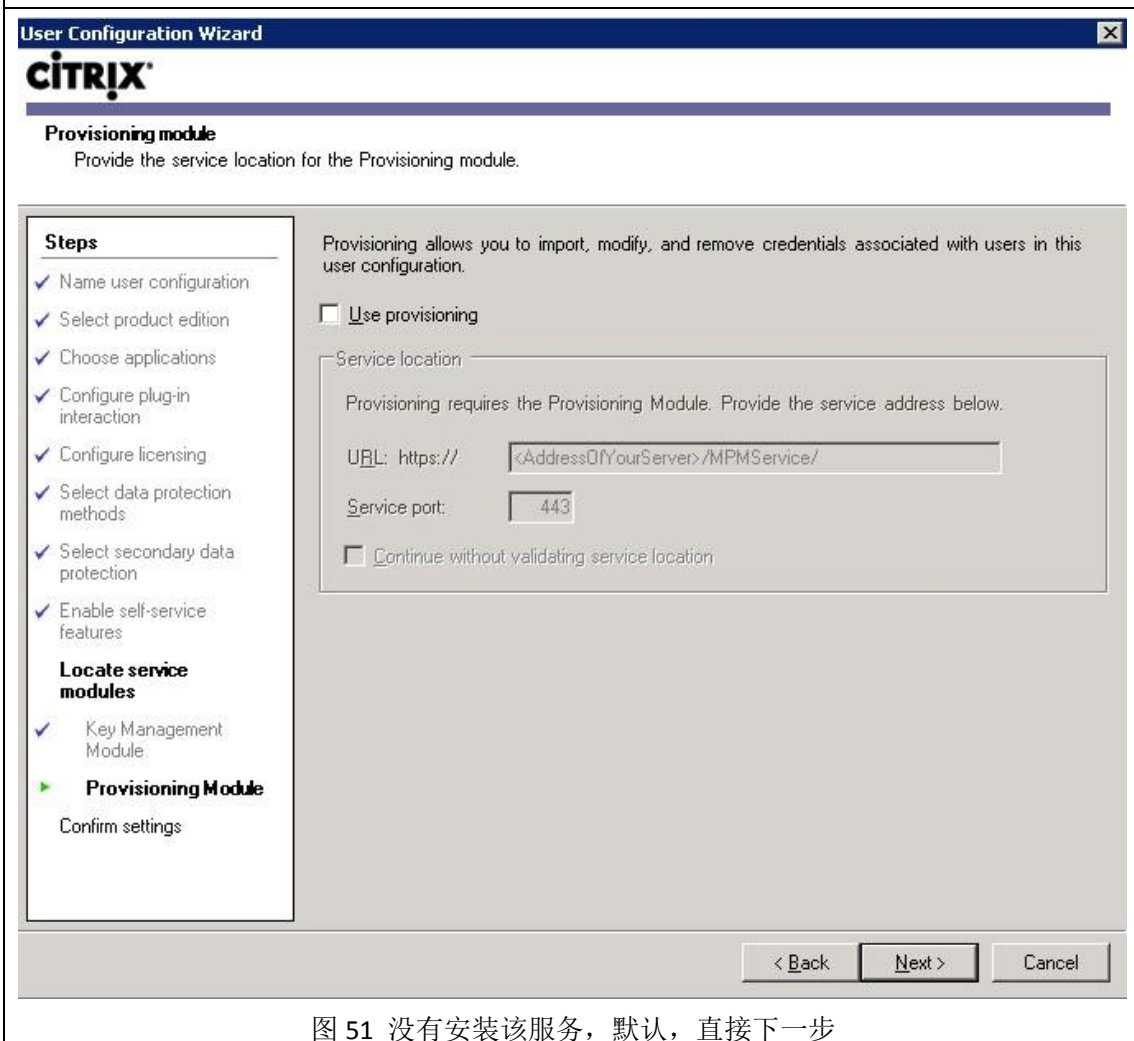


图 51 没有安装该服务，默认，直接下一步

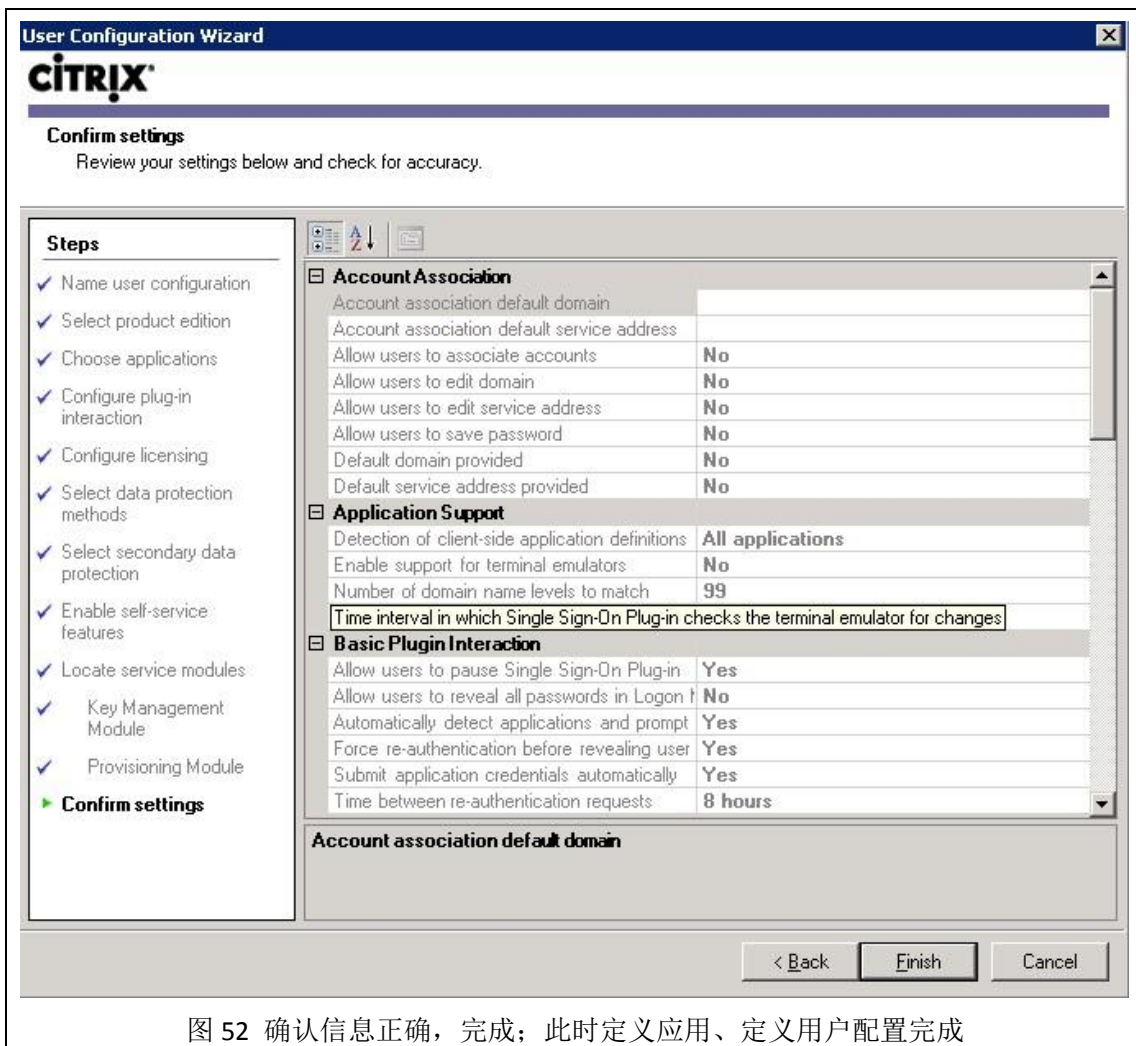


图 52 确认信息正确，完成；此时定义应用、定义用户配置完成

### 3) 单点登录功能使用和测试

登录 Web Interface，并启动 XenApp 已经发布的 Edgesight。

发布 Edgesight 应用：

格式：“c:\program files\internet explorer\iexplorer.exe” “%\*” <http://xenapp2/edgesight>(类似 OA 应用的地址)

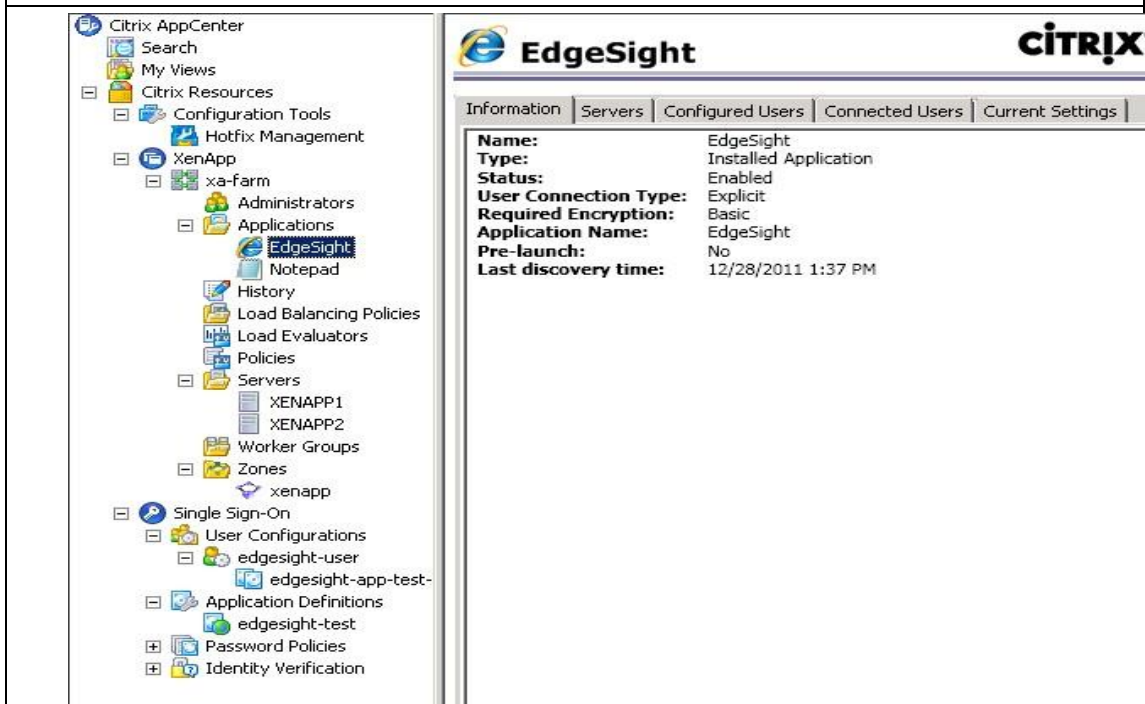




图 53 点击应用程序后，弹出“Remember this password”对话框，选择“Remember”



图 54 选择“Yes”

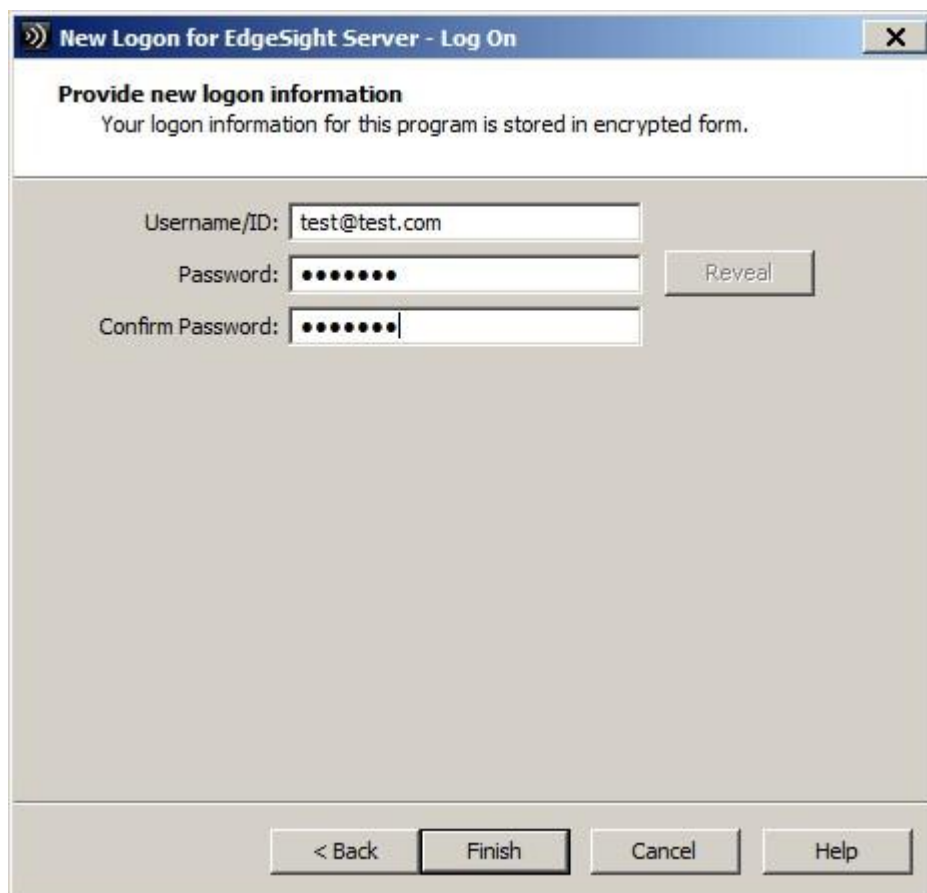


图 56 弹出对话框，配置单点登录信息

输入“Username/ID、Password、Confirm Password”，点击“Finish”

此时发布的应用将使用我们配置的单点登录信息进行验证登录

以后，只要我们在启动 Edgesight 应用时，单点登录组件就会自动输入 Edgesight 的帐号、密码并自动登录打开应用。

搜索



登录身份: anmingyang

主页



EdgeSight



Notepad

提示: 是否找不到所需的资源? 请使用“搜索”进行查找。

实验测试完成。

作者: 安明洋

日期: 2012-02-10