

数  
字  
远  
程  
IP  
系  
列  
切  
换  
器

操 作 手 册

## 目录

一、设备配置设置.....	3
1.1 通过浏览器进入配置界面.....	3
二、恢复出厂设置.....	5
2.1 重新启动.....	5
2.2 软件升级.....	5
三、系统设置.....	6
3.1 认证设置.....	6
3.2 访问控制列表.....	8
四、网络设置.....	8
4.1 IP 地址设置.....	8
4.2 动态域名设置.....	9
4.3 行为审计设置.....	10
4.4 查看网络信息.....	10
4.5 串口模块设置.....	11
4.6 DDC 设置.....	11
五、用户管理.....	11
5.1 用户组管理：.....	12
5.2 增加用户：.....	12
5.3 用户维护：.....	13
六、通过浏览器进入远程操作界面.....	14
七、远程界面工具栏的设置.....	16
附录 快速查阅.....	20
CAT5 双绞线标准接法.....	20
八、控件下载安装说明.....	20

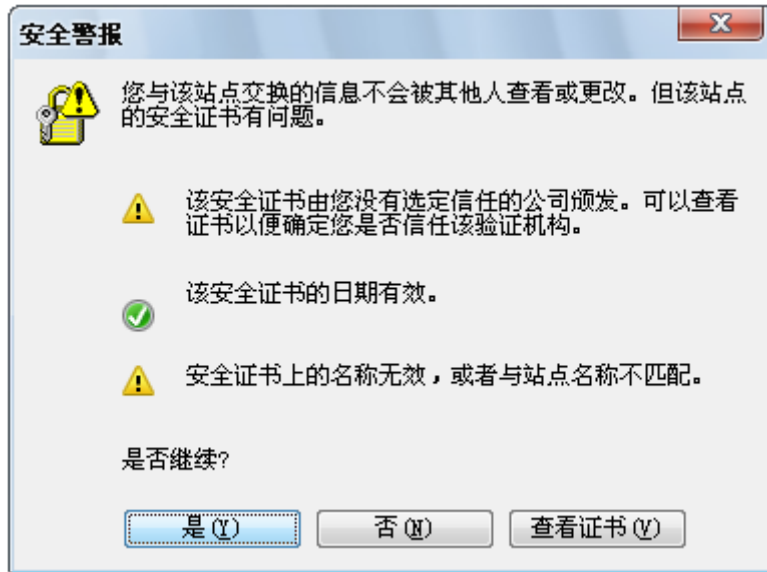
## 一、设备配置设置

### 1.1 通过浏览器进入配置界面

启动网络浏览器，例如 Internet Explorer (IE)、360 安全浏览器等。

输入下列 URL: `https://IP-ADDRESS`，其中 IP-ADDRESS 是管理员给 4 用户数字分配的 IP 地址（如果有 DNS 解析，可以使用域名）。也可以使用 `http`，4 用户数字会将 HTTP 重定向到 HTTPS。

因为是 SSL 连接，浏览器自动从设备下载一个安全证书，浏览器该证书不是信任机构颁发的，会弹出一个安全警报，提问是否要继续操作。



这一步点“是”，让浏览器继续操作。

系统显示登录页面，输入管理员用户名和密码：



输入管理员用户名和密码。单击“登录”。

### 出厂默认设置

出厂默认 IP 地址：192.168.0.100

出厂默认管理员密码： Username: admin Password: 123456

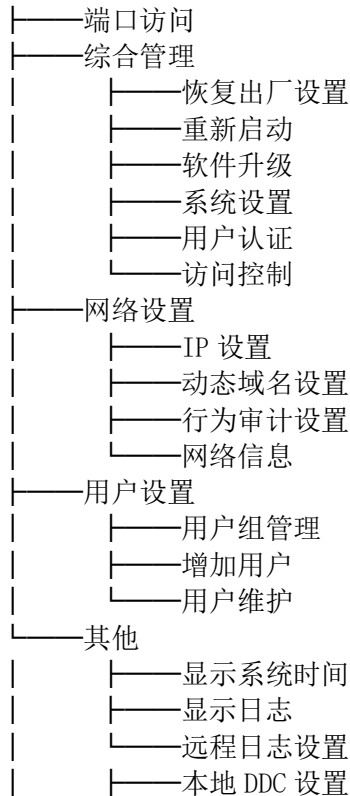
### 恢复出厂默认设置

如遗忘 IP 地址或管理员密码，您可以时用恢复出厂默认设置功能将设置恢复到初始状态。按住 KVM 背面的 RESET 按钮然后开机直到启动完成，即可恢复默认设置。（RESET 按钮隐藏在孔里面，需要用一根较细的针顶进去）

认证通过后，进入 WEB 配置界面：



WEB 配置界面共有 6 个功能项：综合管理、网络设置、用户管理、其他、IPKVM。每个功能项下面还有数量不一的功能子项。以下是功能结构图：





## 二、恢复出厂设置

选择“综合管理” — “恢复出厂设置”，按“确定”即可恢复出厂设置。



### 2.1 重新启动

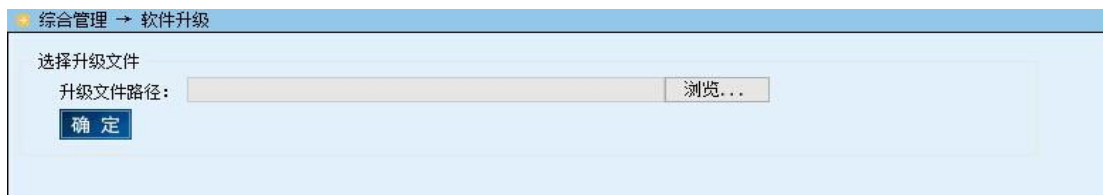
依次选择“综合管理” — “重新启动”。



按上图提示点击“确定”即可重新启动设备。

### 2.2 软件升级

依次选择“综合管理” — “软件升级”。

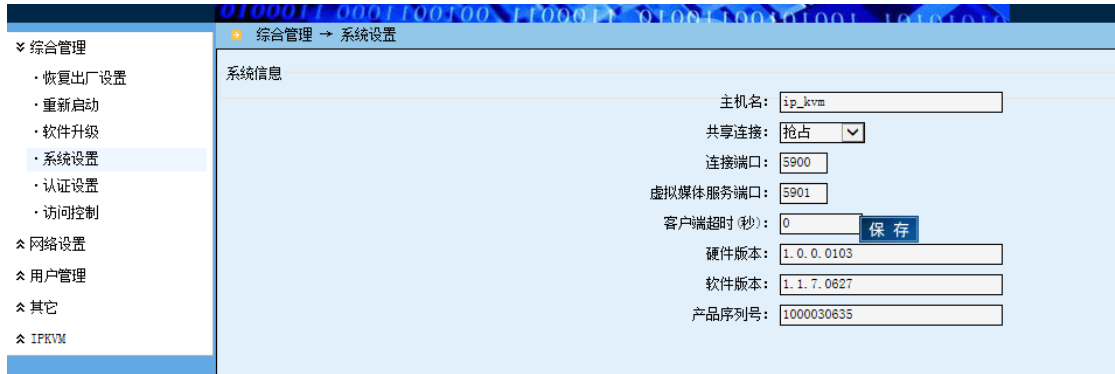


按上图提示点击“浏览”选择升级文件后，点击“确定”即可对设备进行升级。

**注意：**

**软件升级完成后设备会自动重启。在升级过程中务必不要关机或断开电源，否则会造成设备无法正常使用。**

## 三、系统设置



选择“综合管理”—“系统设置”项,修改“共享连接”栏完成共享模式的设置,共有“共享”、“抢占”、“独占”、“被动共享”四种模式可供选择。

共享连接模式:

- 最多四个通道共享,每个通道最多共享四个用户(包括主用户)
- 当四个通道都存在访问用户时,其他用户则禁止访问其他通道
- 先进入通道的第一个用户为主用户,其他三个为共享用户
- 主用户根据用户权限设置具有鼠标键盘操作权限,其他三个共享用户有键鼠权限
- 当主用户关闭时,其他三个用户强制关闭。

被动共享模式: 共享用户鼠标键盘不能使用

抢占模式: 根据不同的用户权限,低权限不可以抢占高权限用户访问通道,同等级权限或高等级权限可以抢占

独占模式: 不论用户权限高低,某一用户在访问时不可被抢占

客户端超时: 本地与远程用户登录后一段时间内不操作的自动退出时间

### 3.1 认证设置

提供多种用户认证方式:

- 本地认证方式:



- 认证模式 None：  
不需要认证直接连接 KVM 设备。
- 认证模式 HikAuth：  
要在 KVM 设备中增加用户通过用户名和密码认证连接 KVM 设备。
- 认证模式 LDAP：  
客户端连接 KVM 设备需要通过 LDAP 服务器的认证。LDAP 服务器要有认证用户的信息，进入 LDAP 详细设置，设置 LDAP 服务器信息。
- 认证模式 RADIUS：  
连接 KVM 设备需要通过 RADIUS 服务器的认证。RADIUS 服务器要有认证用户的信息。进入 RADIUS 详细设置，设置 RADIUS 服务器信息。
- 认证模式 TACACS：  
连接 KVM 设备需要通过 TACACS 服务器的认证。TACACS 服务器要有认证用户的信息。进入 TACACS 详细设置，设置 TACACS 服务器信息。

**注意：**

选择用户认证方式必须在创建用户之前设置。如果用户认证方式改变，以前创建的用户也必须删除重建。

2、集中认证方式：



**注意：**

集中认证方式继续配合 IV3 集中管理平台使用，将 IV3 管理平台的认证服务器地址及端口号填上后保存并重新启动，即可在管理平台中查看到设备上报信息。

## 3.2 访问控制列表

访问控制是通过控制用户的 IP 地址和子网掩码，来设置该用户的访问权限。

“允许列表”是允许访问的网段和主机。“禁止列表”是禁止访问的网段和主机。  
例如设置允许访问主机列表：

允许主机列表	ip 地址	掩码
主机 192.168.1.120	192.168.1.120	255.255.255.255
网段 192.168.1.1-192.168.1.254	192.168.1.0	255.255.255.0

同理设置禁止访问列表。

访问控制列表				
序号	允许列表		禁止列表	
	IP地址	子网掩码	IP地址	子网掩码
01	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
02	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
03	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
04	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
05	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
06	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
07	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
08	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
09	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

## 四、网络设置

### 4.1 IP 地址设置

IP 地址有三种模式：

- StaticIP--设置静态 IP 地址、子网掩码、缺省网关。
- DHCP--通过网络中的 DHCP 服务器，自动分配 IP 地址。
- PPPOE--通过 PPPoE 方式接入到宽带网中。

选择 StaticIP 模式，依次填写“静态 IP 地址”、“子网掩码”、“缺省网关”。MAC 地址是网卡的设备物理地址，不能修改。

PPPoE 模式下，需要填写的用户名和密码请联系电信运营商取得。



依次选择“网络设置” — “IP 设置”， 然后进行相应的设置。

网络设置 → IP设置

网络模式

StaticIP

MAC地址: 00:25:e6:00:0b:2b

静态IP地址: 192.168.0.86

子网掩码: 255.255.255.0

缺省网关: 192.168.0.1

DHCP

PPPoE

PPPoE用户名:

PPPoE密码:

保存

## 4.2 动态域名设置

动态域名解析（DDNS）主要是为那些 IP 地址不固定的应用提供域名解析服务。如通过 PPPOE 或 DHCP 获得 IP 地址，每次启动得到的 IP 地址是不固定的，客户端无法获知设备当前使用的 IP 地址，当然也无法通过 IP 地址去访问该设备。这种情况下 DDNS 就可以发挥作用。

要使用动态域名解析，首先要到动态域名解析服务提供商处申请一个域名。Internet 上有一些免费的动态域名解析服务，如 dyndns。域名申请成功后，服务商會提供你如下信息：DDNS 服务器地址、端口号、用户名、密码、域名。你要把这些信息设置在 KVM 里。启用 DDNS 服务后，KVM 网络连接成功后，会自动到指定的 DDNS 服务器上更新 IP 地址。客户端访问域名，就对应到最新的 IP 地址。

依次选择“网络设置” — “动态域名设置”， 然后进行相应的设置。

DDNS服务设置

启用DDNS服务: No

DDNS服务器地址:

端口:

用户名:

密码:

域名:

保存

## 4.3 行为审计设置

行为审计功能可以将用户开启会话后的图像进行录像并保存在行为审计服务器中供审查员进行事后的回放功能。

将“启动行为审计服务”选择为 YES，填上正确的审计服务器地址与端口号，保存并重启 KVM，此功能就可以正常运行。

### 注意：

集中认证方式继续配合集中管理平台使用，将管理平台的认证服务器地址及端口号填上后保存并重新启动，即可在管理平台中通过审查员账号登录即可查看到所有用户开启会话后的视频。

## 4.4 查看网络信息

通过查看网络信息可以观察 KVM 网络接口、路由等配置是否正确。

依次选择“网络设置” — “网络信息”，查看网络信息。

```
网络信息

lo: ip 127.0.0.1 mask 255.0.0.0
eth0: ip 192.168.0.85 mask 255.255.255.0
eth1: ip 192.168.0.85 mask 255.255.255.0

Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.0.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
192.168.0.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
0.0.0.0 192.168.0.1 0.0.0.0 UG 0 0 0 eth0
```

## 4.5 串口模块设置

串口模块设置							
端口号	波特率	数据位	停止位	校验	流控	服务端口	启用
1	9600	8	1	无	无	8000	禁用
2	9600	8	1	无	无	8001	禁用
3	9600	8	1	无	无	8002	禁用
4	9600	8	1	无	无	8003	禁用
5	9600	8	1	无	无	8004	禁用
6	9600	8	1	无	无	8005	禁用
7	9600	8	1	无	无	8006	禁用
8	9600	8	1	无	无	8007	禁用

选择通道对应的串口设备修改相应信息，并将禁用改为启用，保存后重启 KVM 设备。

## 4.6 DDC 设置

DDC 选项

- 1) High: 227ELH 20 寸及以上显示器 推荐默认分辨率 1920×1080
- 2) Standard: DELL E178FP 17 寸到 19 寸显示器 推荐默认分辨率 1280×1024
- 3) Low: FLATRON LCD 5 15 寸显示器 推荐默认分辨率 1024×768
- 4) None 没有 DDC
- 5) Ultra: LA2405 24 寸及以上显示器 推荐默认分辨率 1920×1200
- 6) Middle 推荐默认分辨率 1680x1050 60Hz

## 五、用户管理

用户管理包括管理用户的认证信息（用户名、密码、RSA 私钥）、操作权限、优先级。

用户认证信息与“用户认证方式”有关，所以必须先修改认证方式，再添加用户。

用户操作权限可以管理到服务器端口，即可以指定用户对某个服务器端口有没有操作权限。

优先级是指用户获取 KVM 控制权的优先权高低，数字越大优先级越高，4 为最高优先级，0 为最低优先级。有多个用户同时访问 KVM 时，优先级高的用户获得 KVM 控制权，优先级低的用户失去 KVM 控制权。相同优先级的用户后登录的用户可以抢占先登录的用户。

操作权限和优先级都是通过用户组来管理的。先创建用户组，给用户组定义相应的优先级，指定对每个端口的访问权限。创建用户时给用户指定用户组，用户即拥有这个用户组的操作权限和优先级。

### 注意：

选择用户认证方式必须在创建用户之前做。如果用户认证方式改变，以前创建的用户也必须删除重建。

## 5.1 用户组管理：

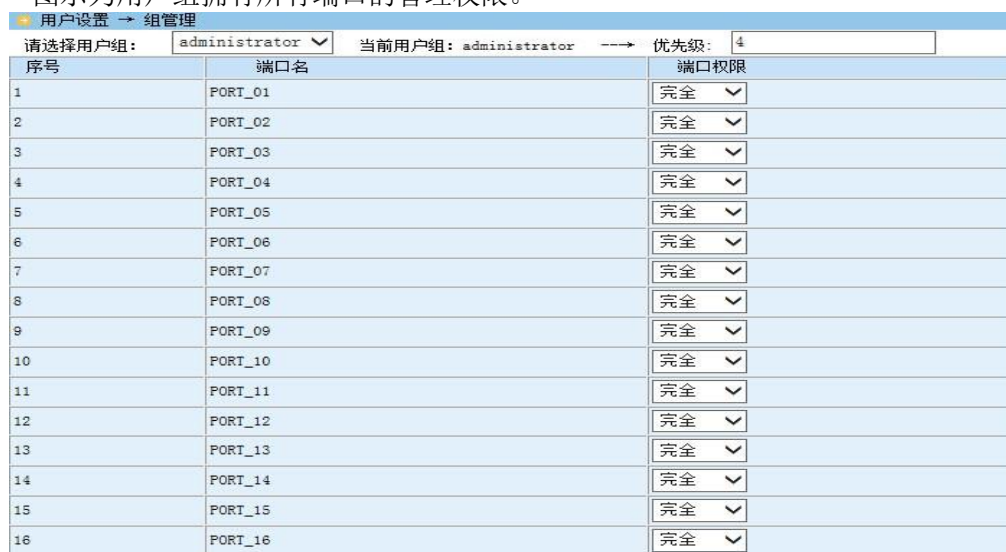
管理员可以建立 5 个用户组，并设置各自的优先级别及端口权限。

可以自行指定用户组名，只需删除原有的用户组名，输入新的即可。

组优先级最高是 4，最低是 0，可点选下拉菜单进行选择。

要赋予一用户组对某端口的访问权限，需要将相应的端口选择权限。权限分为完全、执行、浏览、无权限四种，分别对应完全操作权限、视频及键鼠控制权限、视频权限、无权限。

图示为用户组拥有所有端口的管理权限。



The screenshot shows the 'Group Management' interface. At the top, there is a breadcrumb '用户设置 -> 组管理'. Below it, there are fields for '请选择用户组:' (Please select user group) with a dropdown menu showing 'administrator', '当前用户组:' (Current user group) showing 'administrator', and '优先级:' (Priority) with a dropdown menu showing '4'. The main part of the interface is a table with three columns: '序号' (Serial Number), '端口名' (Port Name), and '端口权限' (Port Permission). The table lists 16 ports, each with a '完全' (Full) permission.

序号	端口名	端口权限
1	PORT_01	完全
2	PORT_02	完全
3	PORT_03	完全
4	PORT_04	完全
5	PORT_05	完全
6	PORT_06	完全
7	PORT_07	完全
8	PORT_08	完全
9	PORT_09	完全
10	PORT_10	完全
11	PORT_11	完全
12	PORT_12	完全
13	PORT_13	完全
14	PORT_14	完全
15	PORT_15	完全
16	PORT_16	完全

## 5.2 增加用户：

建立新用户并指定其所在的用户组。



The screenshot shows the 'Add User' interface. At the top, there is a breadcrumb '用户设置 -> 增加用户'. Below it, there is a section titled '用户信息' (User Information). The form contains four fields: '用户名:' (Username) with an empty text input, '输入密码:' (Enter password) with an empty text input, '确认密码:' (Confirm password) with an empty text input, and '用户组:' (User group) with a dropdown menu showing 'administrator'. At the bottom right, there is a blue button labeled '保存' (Save).

## 5.3 用户维护：

在此项界面中可以显示、更新用户及其所在的用户组，修改已建立的用户密码，删除用户。

用户管理 → 用户维护

注意事项  
注： 密码修改是修改当前选中用户的设备登录密码！

用户名:

用户组: administrator

新密码:

确认新密码:

序号	用户名	用户组	是否选择		
1	admin	administrator	<input type="radio"/> 是否选中		

首先需要选中用户，选择用户组后点击“用户更新”可以修改用户所属用户组，点击“修改密码”可以修改用户密码，点击“删除”可以删除选中用户。

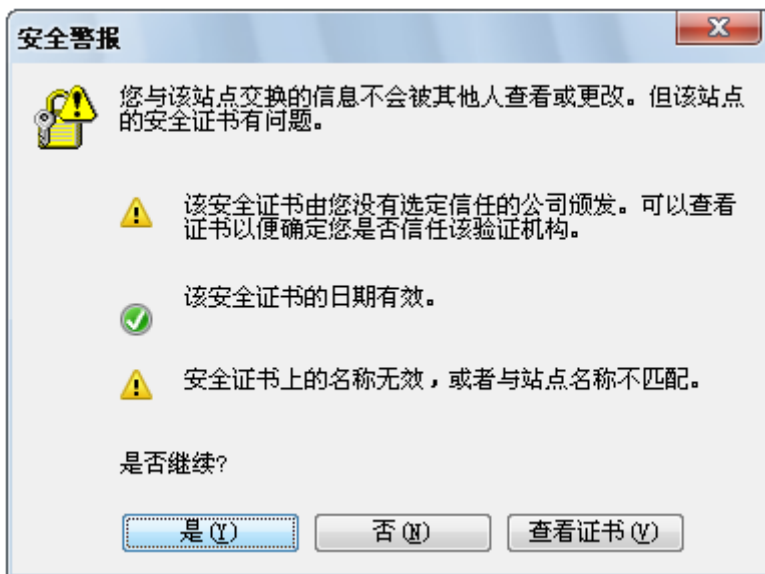
(此页刻意留白)

## 六、 通过浏览器进入远程操作界面

启动网络浏览器，例如 Internet Explorer (IE)、360 安全浏览器。

输入下列 URL: https://IP-ADDRESS, 其中 IP-ADDRESS 是管理员给 4 用户数字分配的 IP 地址 (如果有 DNS 解析, 可以使用域名)。也可以使用 http, 4 用户数字会将 HTTP 重新定向到 HTTPS。

因为使用 SSL 连接, 浏览器自动从设备下载一个安全证书。当浏览器认为该证书不是信任机构颁发的, 会弹出一个安全警报, 提问是否要继续操作。



这一步点“是”，让浏览器继续操作。

系统显示登录页面，输入用户名和密码：



输入用户名和密码。单击“确定”。

出厂默认 IP 地址：192.168.0.100

出厂默认管理员密码： Username: admin Password: 123456

#### 恢复出厂默认设置

如遗忘 IP 地址或管理员密码，您可以时恢复出厂默认设置功能将设置恢复到初始状态。按住 KVM 背面的 RESET 按钮然后开机直到启动完成，即可恢复默认设置。（RESET 按钮隐藏在孔里面，需要用一根较细的针顶进去）

认证通过后，进入远程用户操作界面：



在主界面中，鼠标移动到 IPKVM---通道，点击“连接”选择目标服务器。

#### 注意：

如点击“连接”后未出现服务器端口界面，请查看[控件下载安装说明](#)。

## 七、 远程界面工具栏的设置

窗口正上方中间位置显示的是设置工具栏，如下图所示：



下面介绍下工具栏的各项功能。



显示/隐藏工具栏：

此项用来切换工具栏的显示方式。工具栏默认为隐藏状态，将鼠标移至窗口上方位置显示工具栏，移开鼠标则隐藏。点击此按钮，工具栏将变为显示状态，不自动隐藏。两种状态可以互相切换。



选项：

点击此项会弹出选项对话框。



- 键盘鼠标发送设置

发送键盘事件：支持远程键盘的使用，取消该选项将使远程键盘不可使用，该选项默认为选择。

发送鼠标事件：支持远程鼠标的的使用，取消该选项将使远程鼠标不可使用，该选项默认为选择。



- 键盘设置

传递特殊功能键到键盘：选择此功能时 Win 键只能在被控端使用；未选择此功能时，Win 键只能在控制端使用。

- 鼠标设置

单鼠标光标：选择此功能，则隐藏本地鼠标光标。

鼠标事件采样率：提高视频中被控电脑的鼠标刷新速度，采样率越高，鼠标刷新速度越快，鼠标效果越好，该选项默认为快。

光标类型：设置光标类型：可选择圆点，箭头，十字，默认为箭头。

- 全屏设置

全屏时画面缩放：全屏时画面是否缩放，默认为缩放模式。



视频设置：

此项为视频设置对话框。



选中自定义参数，用户可以对参数进行调节，功能如下表所示：

亮度	调节视频亮度
对比度	调节视频对比度
垂直偏移	调节视频上下幅度
水平偏移	调节视频左右幅度
相位	图像质量，当出现图像出现扭动时，调节此功能修正。 选择范围为 0-31
视频质量	数值越大，图像更新速度越快，图像质量越差。
音频设置	勾选静音为不传输服务器音频到控制端
鼠标模式设置	普通模式需要调整服务器鼠标选项
CAT5 线缆距离设置	根据服务器与 KVM 之间所连接线材的距离调整视频质量

如果远程客户端视频出现异常抖动，用户可以勾选自动校准选项  自动校准，再按确定，系统将根据实际情况进行视频调整。

#### 注意：

灰色不可调整项为此设备不支持此功能。



#### 鼠标同步：

鼠标同步是指校对鼠标位置，使被控制服务器的鼠标与远程客户端鼠标保持同步。当客户端鼠标与被控服务器鼠标不重合时，可使用该功能实现同步。



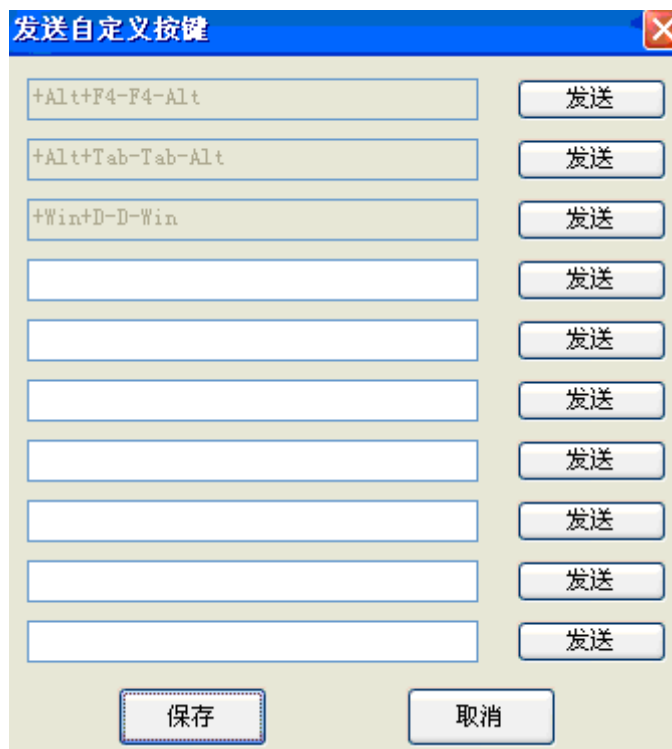
#### 服务器锁机：

此功能是发送锁机键“Ctrl-Alt-Del”命令。当被控服务器系统设置“Ctrl-Alt-Del”为锁机命令时，可实现锁机功能。

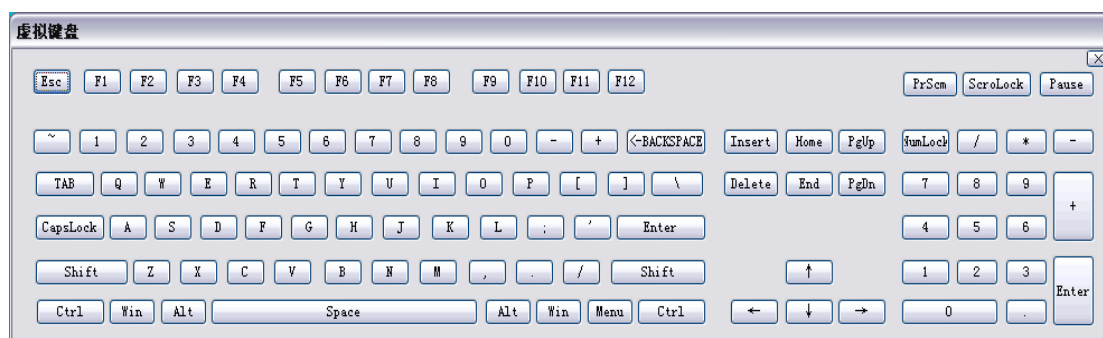


#### 发送自定义按键：

此功能是用来发送用户自定义的组合键。  
点击弹出对话框。




如要添加新自定义按键，将光标移至空白栏点击左键出现如下按键框，选择相应的按键先保存后释放即可。



 缩放：100% 窗口缩放：

此项功能可以调整窗口的大小。默认为 100%，用户可以调整窗口大小为 50%，75%。

 全屏/窗口切换：

此功能将窗口扩展为全屏。如要退出全屏，可再次点击此按键退出全屏。

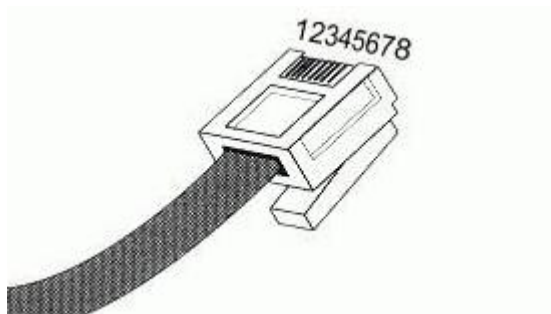
## 附录 快速查阅

---

### CAT5 双绞线标准接法

为了避免信号在 CAT5 双绞线传输时受外界干扰影响，在制作线缆时应该严格按照标准压接 RJ45 水晶头。CAT5 双绞线有两种标准，分别为 TIA/EIA 568B 和 TIA/EIA 568A。建议采用 TIA/EIA 568B 标准。

水晶头有铜片的一面朝上，有开口的一方朝向自己身体，从左向右排序为 12345678，如下图。



TIA/EIA 568B 线序：

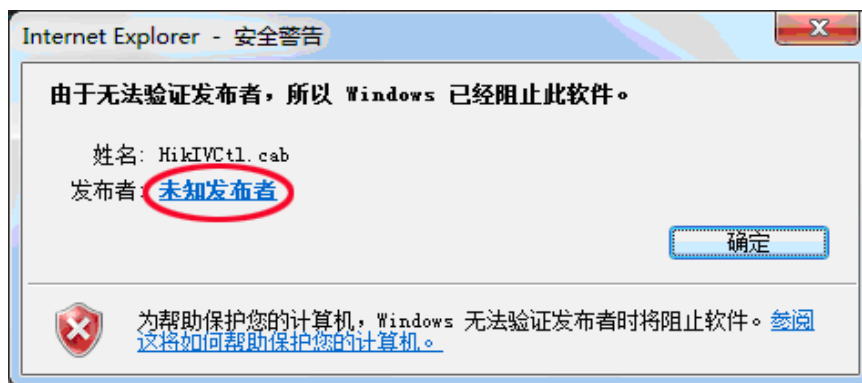
1、白橙，2、橙，3、白绿，4、蓝，5、白蓝，6、绿，7、白棕，8、棕。

## 八、 控件下载安装说明

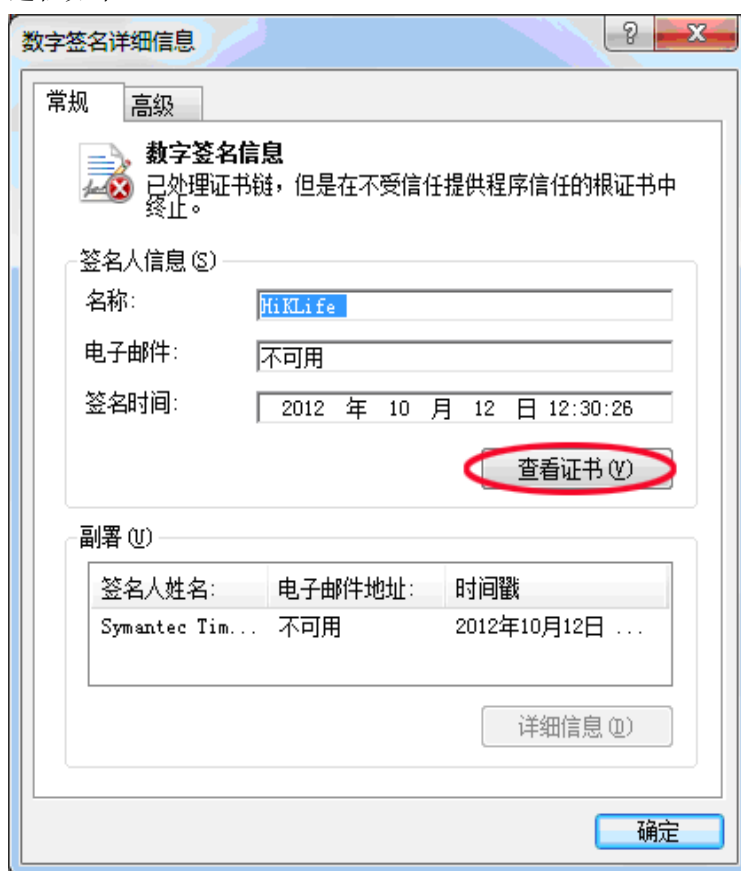
IE9 下如图所示



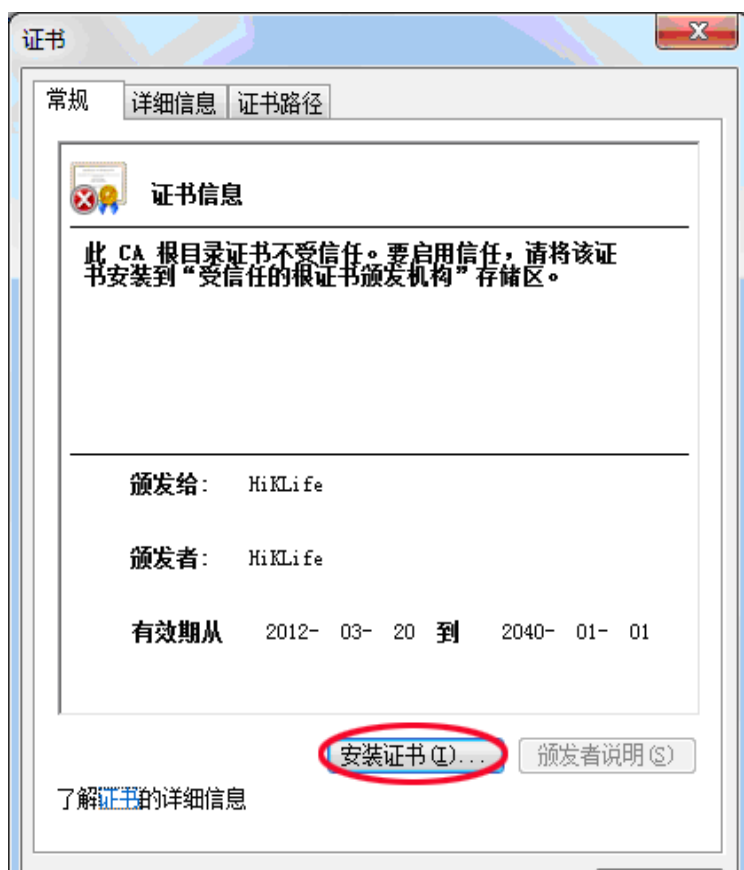
因为浏览器需要安装一个控件，点击安装



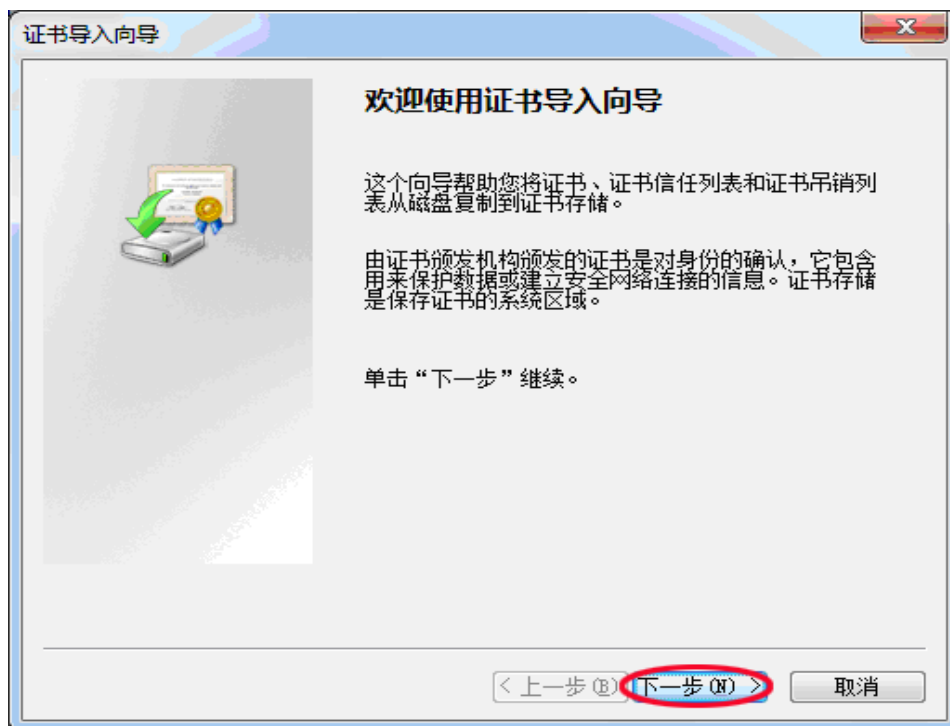
请首先点击【未知发布者】以安装证书  
过程如下：



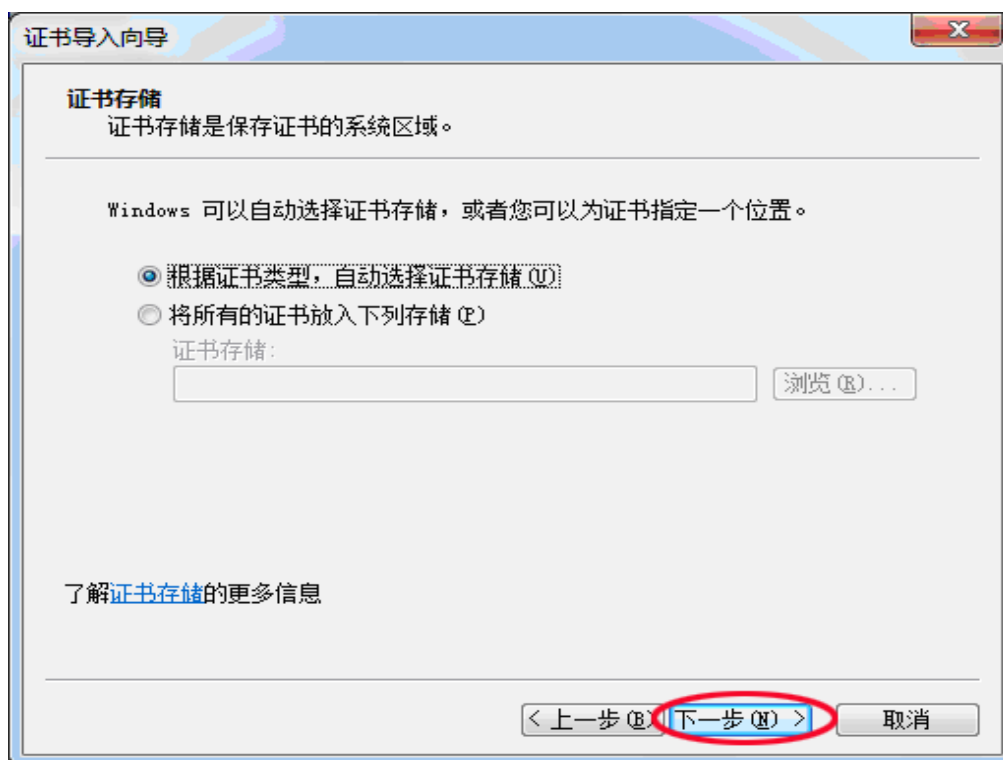
点击查看证书



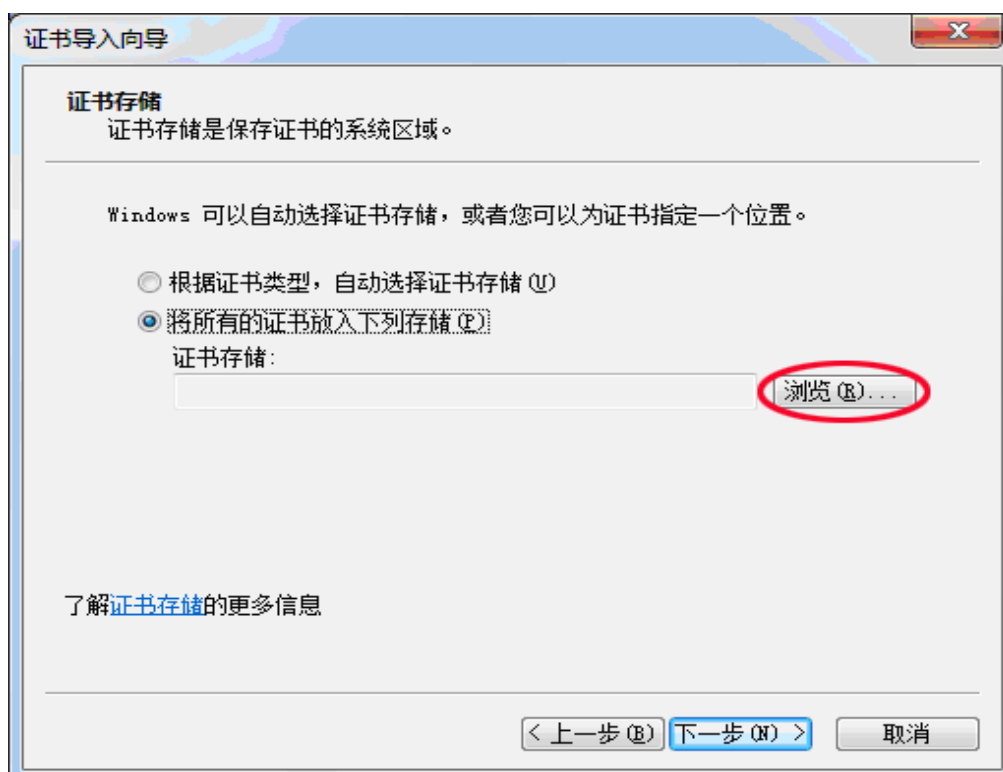
点击安装证书



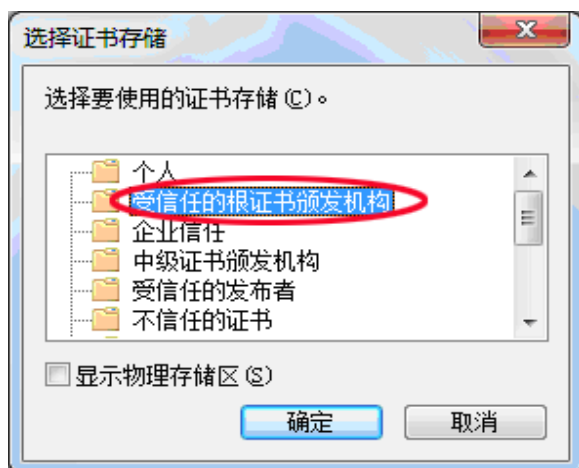
点击下一步



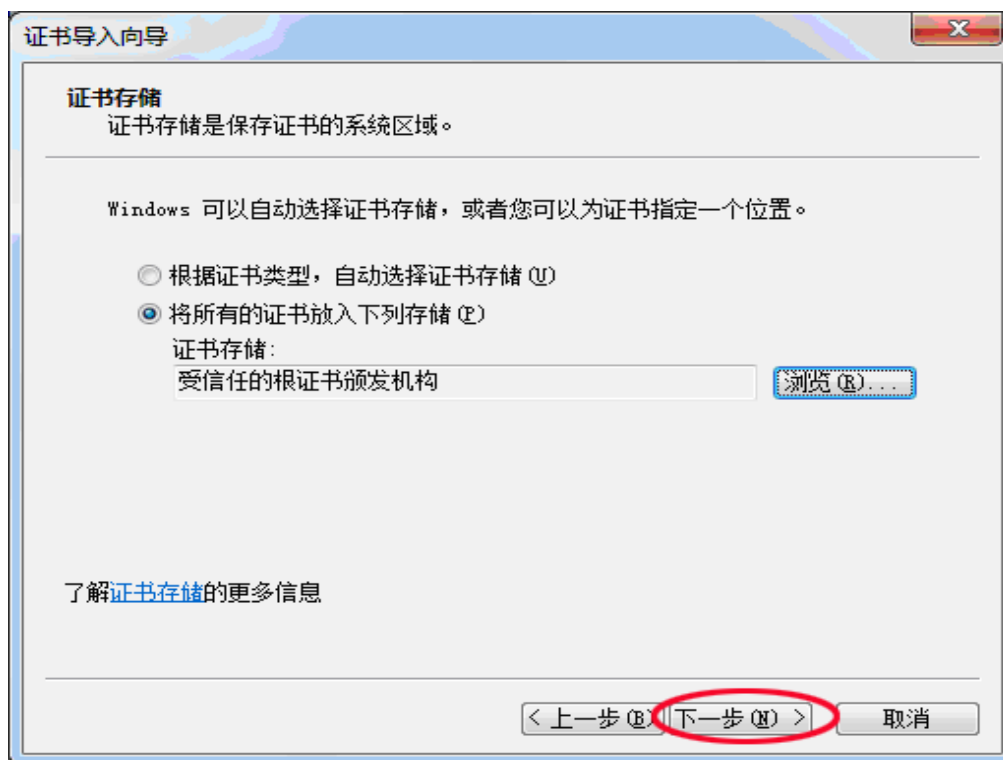
这里可以点击下一步，但建议选择将所有证书放入下列存储



点击浏览，选择受信任的根证书颁发机构



点击确定

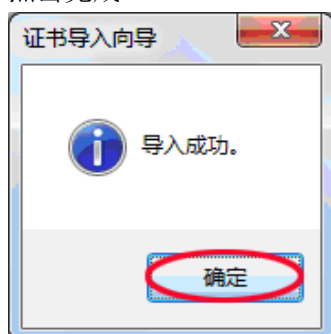


点击下一步

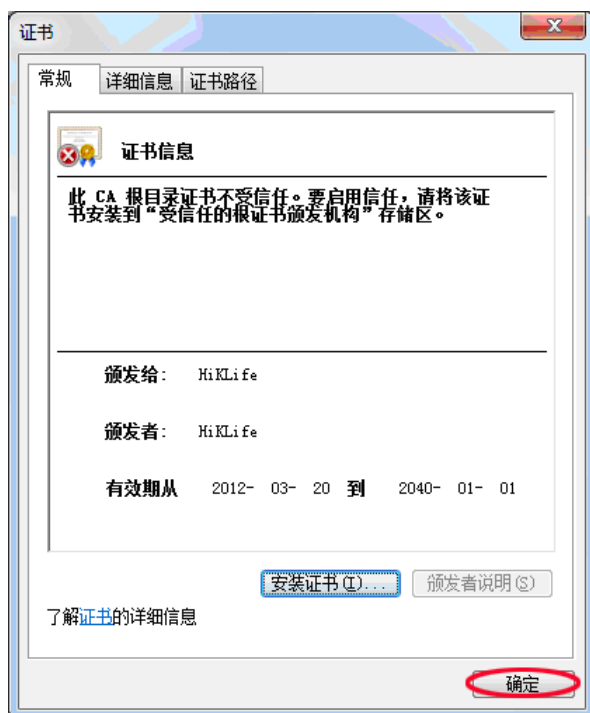




点击完成



点击确定，关闭提示框

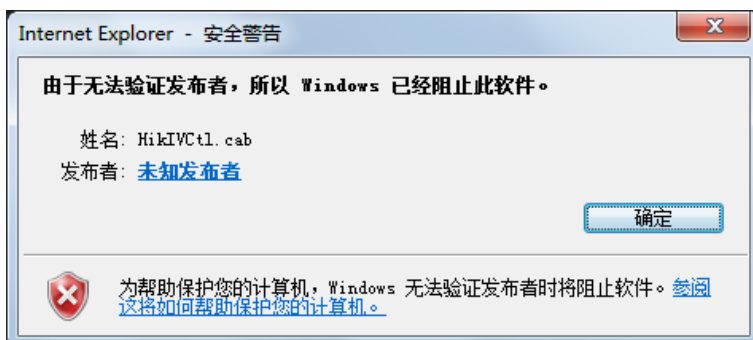


点击确定，关闭提示框

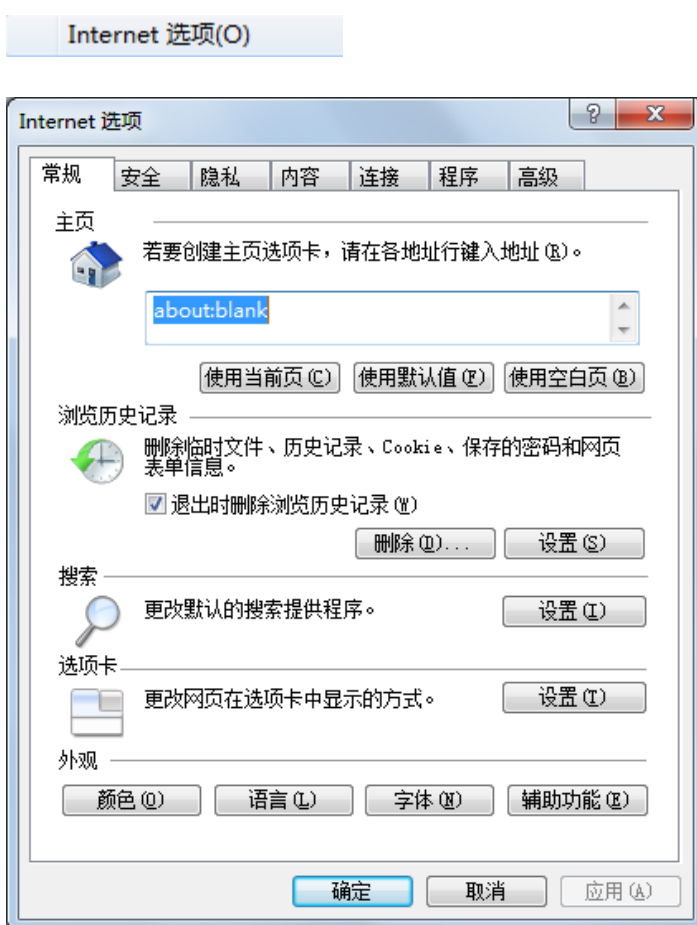


点击确定，关闭提示框

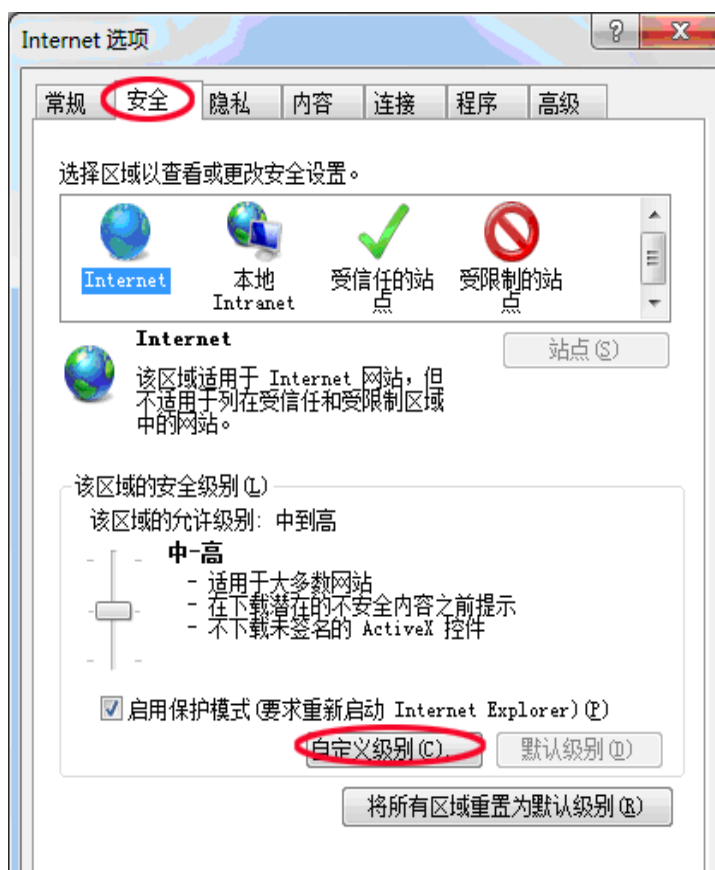
刷新浏览器，如果弹出窗仍是如下图所示



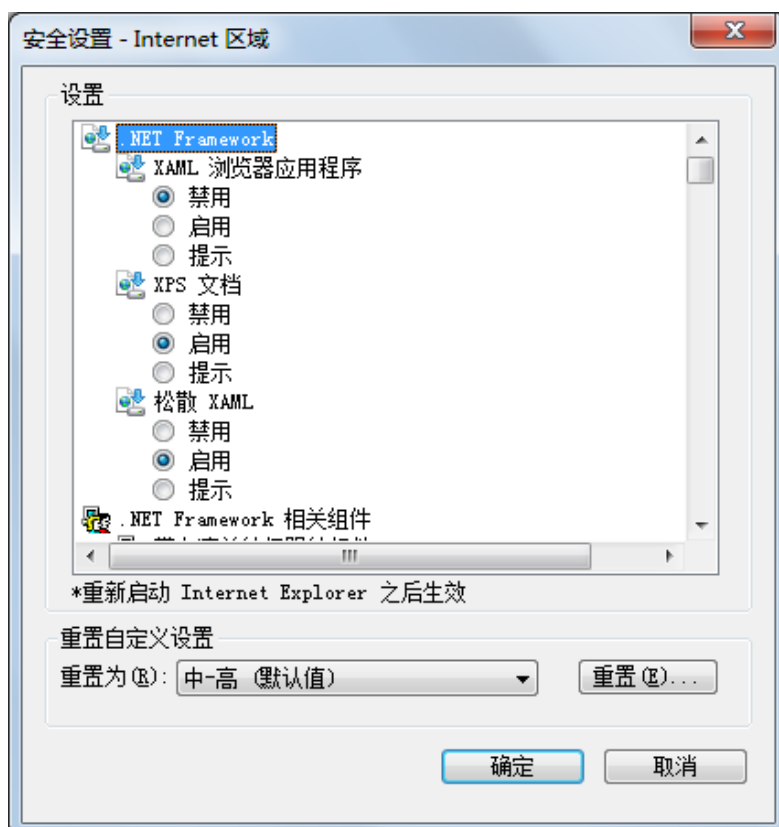
说明浏览器不允许安装第三方控件，请关闭该对话框，再打开 Internet 选项。

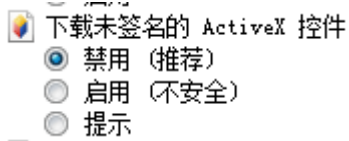


选择安全

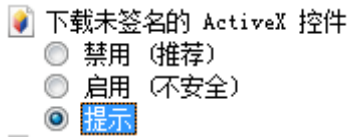


选择自定义级别

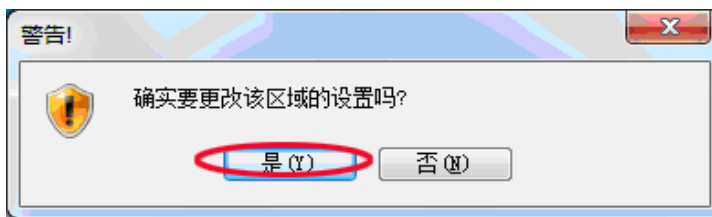




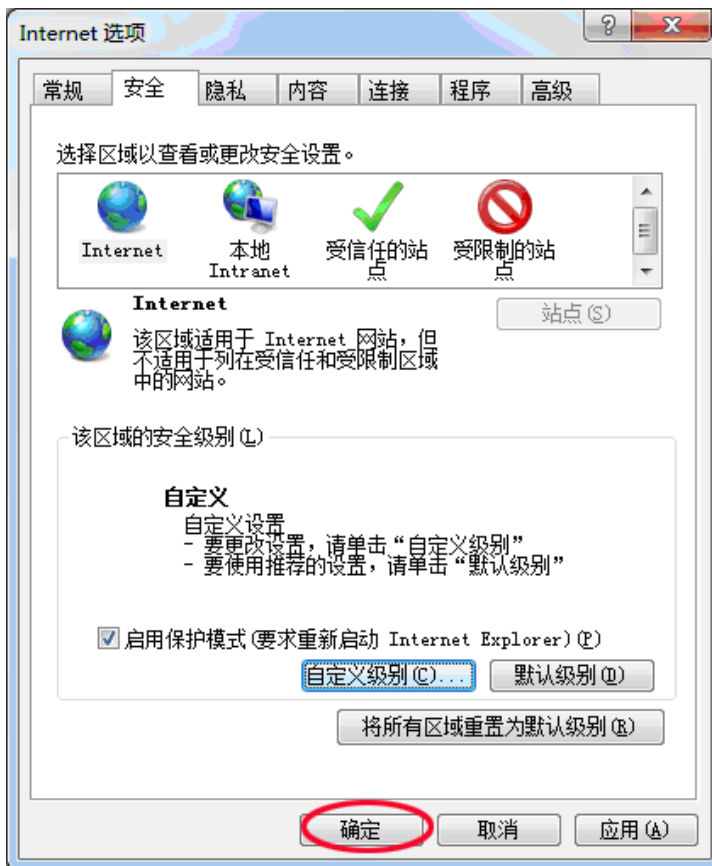
将下载未签名的 ActiveX 控件选为提示或启用



点击确定

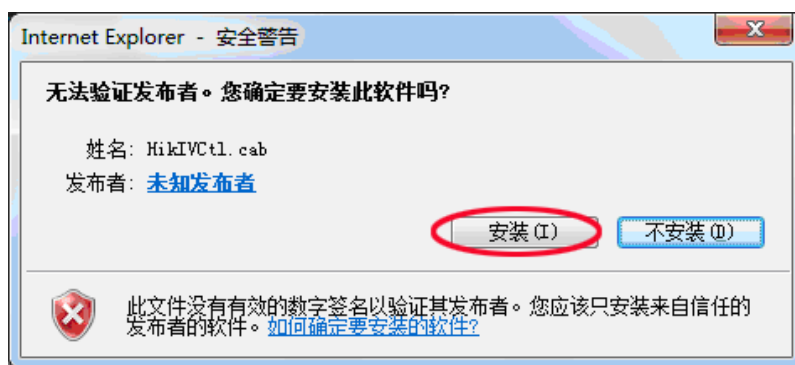


点击是



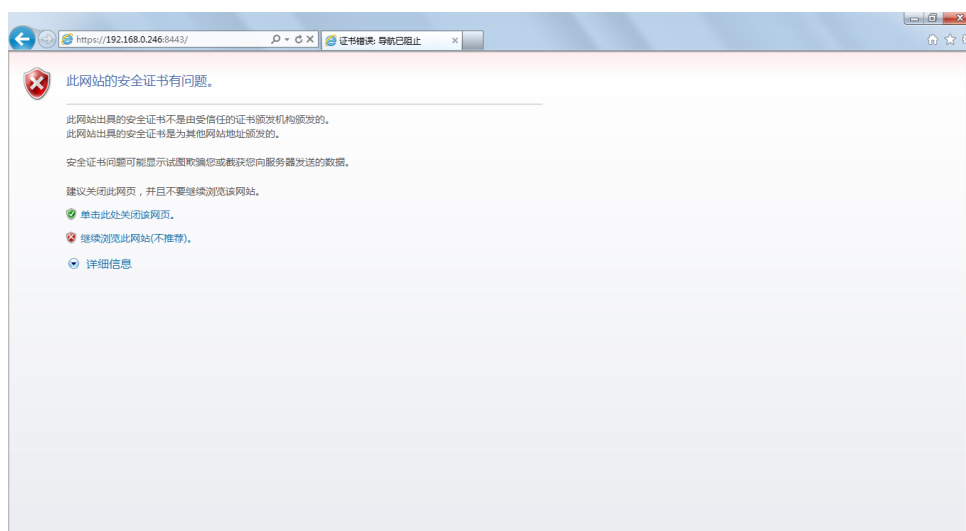
点击确定,这个时候安全级别变为了自定义。

刷新浏览器,这个时候的弹出窗就变为了下图这个样子



点击安装即可完成。

https 方式基本类似，请在浏览器内输入 https://192.168.0.246:8443 会打开如下页面



请点击继续浏览此网站，如果不想显示该提示框，请选择【Internet 选项】，【高级】，去掉【对证书地址不匹配发出警告】的勾选。

