

# 资源访问控制系统

## WebVPN

## 安装手册


北京网瑞达科技有限公司

[www.wrdtech.com](http://www.wrdtech.com)

2020-03-03



Copyright © 2010-2020 北京网瑞达科技有限公司及其许可者版权所有，保留一切权利。未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本资料内容的部分或全部，并不得以任何形式传播。

网瑞达、 为北京网瑞达科技有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。网瑞达保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，网瑞达尽全力在本手册中提供准确的信息，但是网瑞达并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。



## 编撰历史

版本	撰写	审核	日期	备注
2.0	杨呈飞		2020-02-07	重新排版
2.0.1	杨滢		2020-03-03	新增 1 安装要求内容

## 目 录

1 安装要求 .....	1
2 典型拓扑 .....	1
3 系统安装 .....	2
3.1 介质准备 .....	2
3.2 安装步骤 .....	3
4 OS 设置 .....	2
4.1 系统账号设置 .....	2
4.2 网络设置 .....	3
4.3 时间配置 .....	5
4.4 更新数据 .....	5
5 系统设置 .....	6
5.1 Web 管理 .....	6
5.1.1 内网网卡设置 .....	6
5.1.2 内网路由设置 .....	7
5.1.3 应用网络和路由配置 .....	8
5.1.4 NTP 设置 .....	8
5.1.5 域名和 HTTPS 设置 .....	9
5.1.6 认证对接 .....	10
5.1.7 门户导航设置 .....	11



5.1.8 申请授权 .....	14
5.2 用户访问 .....	15
6 更多参考 .....	16
7 联系我们 .....	17

## 1 安装要求

建议用于安装 WebVPN 的目标服务器至少满足以下硬件规格要求：

CPU：Intel 或 AMD 64 位 CPU，至少 4 核心 2.2Ghz

内存：16 GB

硬盘：512GB

网络：千兆以太网

注意，若安装在虚拟机上，创建虚拟机时需选择 Linux 操作系统，操作系统版本需选择 Red Hat Enterprise Linux 6（64 位）或 CentOS 6（64 位）。

### 选择客户机操作系统

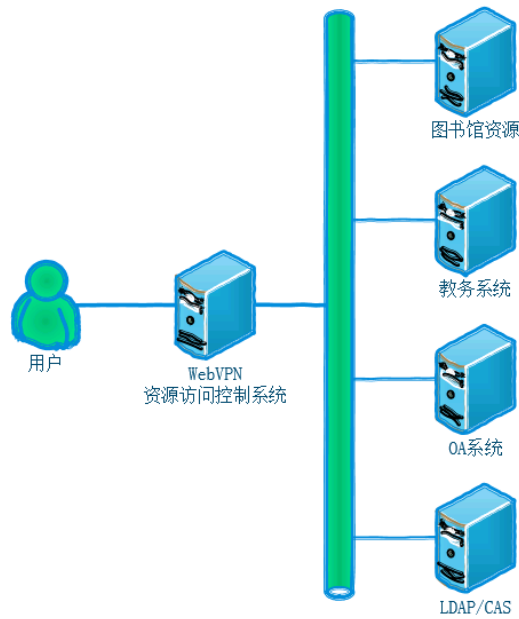
选择将在虚拟机上安装的客户机操作系统

在此处标识客户机操作系统可让向导为操作系统的安装提供适当的默认值。

客户机操作系统系列:	Linux	▼
客户机操作系统版本:	Red Hat Enterprise Linux 6 (64 位)	▼

## 2 典型拓扑

建议 WebVPN 服务器配置两个以太网网卡，一个用于连接内网，一个用于连接外网提供服务；WebVPN 服务器与现有 LDAP 或 CAS 对接。典型部署拓扑结构如下图所示。



### 3 系统安装

网瑞达资源访问控制系统基于自有 WRDOS 操作系统以 ISO 安装光盘为安装介质。使用 ISO 可以为商用服务器硬件、网瑞达专用硬件、工控机、虚拟化客户机、云主机等提供涵盖操作系统、中间组件、产品软件等 WebVPN 所需的一切软件及运行环境。

本手册以借助 KVM 或者服务器带外管理为例进行安装介绍。网瑞达自有 WRDOS 也支持串口等其他安装方式,读者针对本手册提供的信息需要更多更详细说明时,请参考《WRDOS 安装手册》。

#### 3.1 介质准备

网瑞达资源访问控制系统以可引导 ISO 文件作为标准发布形式,读者可以使用 ISO 文件引导虚拟机或者通过挂载 ISO 文件引导具备带外管理的服务器、

刻录为 DVD 光盘，还可以制作为可引导 U 盘。启动 U 盘的制作建议使用『Win32 Disk Imager』工具，下载地址：

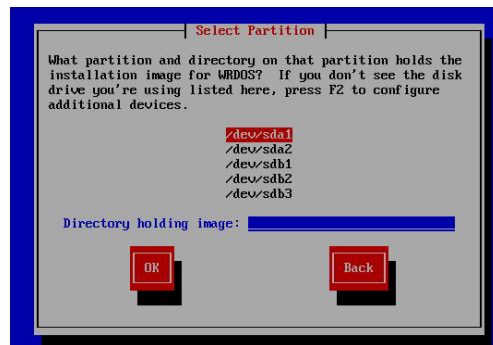
<https://sourceforge.net/projects/win32diskimager/>

### 3.2 安装步骤

1. 挂载镜像后进入引导系统，出现系统首界面如下图。选择安装选项，请选择『All-in-One』安装。

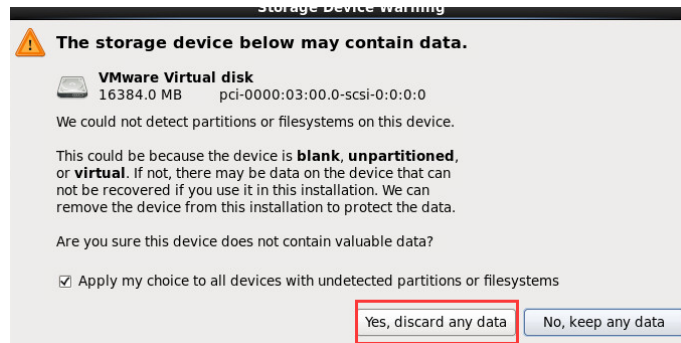


2. 若是使用 U 盘引导安装，则会出现引导介质设备类型选择界面如图 3-1 所示。选择『Hard drive』并按『OK』按钮进入引导介质设备名称选择界面如图 3-2 所示。选择引导类型和对应磁盘设备名称（一般为 /dev/sda1，因机型和硬件配置而异，可做多次选择加以尝试）。

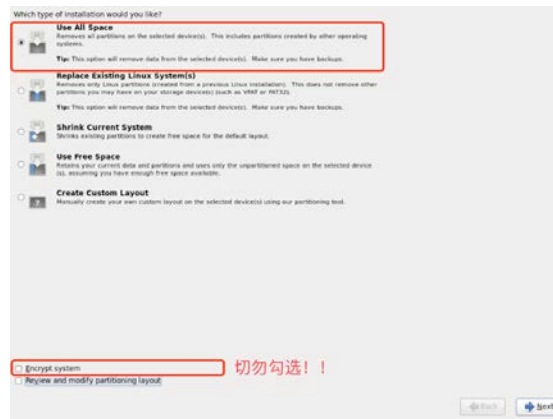




3. 是全新磁盘或者新建 RAID,可能会出现提示如下图。选择『Yes, discard any data』 建立分区表。



4. 选择磁盘分区方法如下图所示。选择『Use All Space』 使用所有磁盘空间,这将删除磁盘上所有数据,并创建默认分区结构。需要注意的是,不要勾选『Encrypt system』 选框,避免降低磁盘性能。



5. 点击 『Reboot』 重新启动系统。



## 4 OS 设置

### 4.1 系统账号设置

1. 登录系统控制台，使用用户名: 『root』, 密码: 『@dm1n\$』 登录命令行。

```
WRDOS release 6.10 (camellia)
Kernel 2.6.32-754.23.1.el6.x86_64 on an x86_64

WRDUPN login: root
Password: _
```

特别地，强烈建议用户修改默认 root 密码，以提高系统安全性。修改密码需输入命令 『passwd root』，然后输入新密码即可。

2. 系统 root 用户因安全加固已禁止远程登录访问，远程访问需要创建新用户。远程 SSH 登录端口为 『13911』。输入命令 『useradd wrd』新建用户（"wrd"即为新用户名，请根据实际情况自行更改）。

```
WRDOS release 6.10 (camellia)
Kernel 2.6.32-754.23.1.el6.x86_64 on an x86_64

WRDUPN login: root
Password:
Last login: Sat Feb  8 11:13:45 on tty1
[root@WRDUPN ~]# useradd wrd
[root@WRDUPN ~]#
```

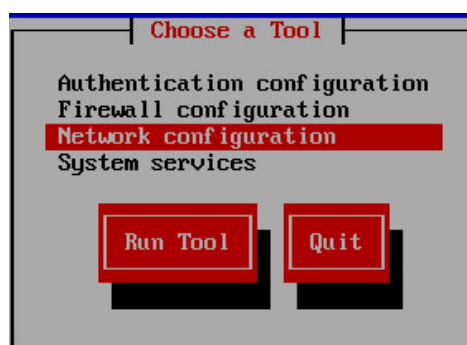
3. 为新用户设置密码。输入命令 『passwd wrd』，按 『回车』 键后输入密码两次确认。

```
WRDOS release 6.10 (camellia)
Kernel 2.6.32-754.23.1.el6.x86_64 on an x86_64

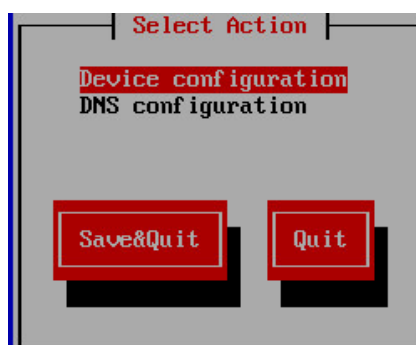
WRDUPN login: root
Password:
Last login: Sat Feb  8 11:13:45 on tty1
[root@WRDUPN ~]# useradd wrd
[root@WRDUPN ~]# passwd wrd
Changing password for user wrd.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@WRDUPN ~]# _
```

## 4.2 网络设置

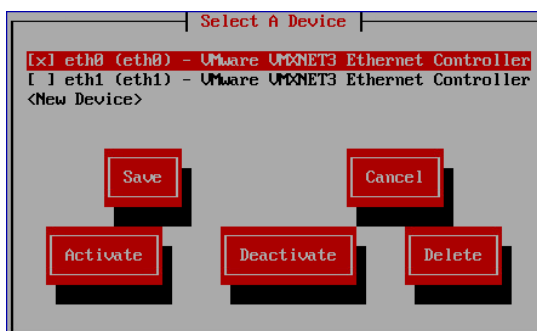
1. 在系统控制台以 root 用户登录后, 输入 『setup』 命令进入配置界面 (如下图), 选择 『Network configuration』 (网络配置项)。



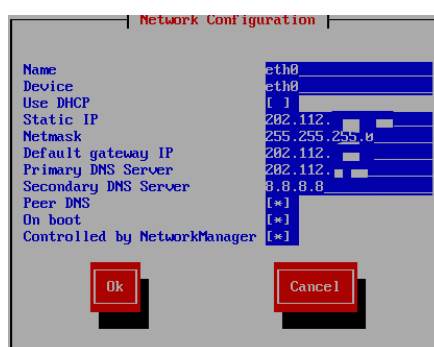
2. 选择 『Device configuration』 (设备配置项)。



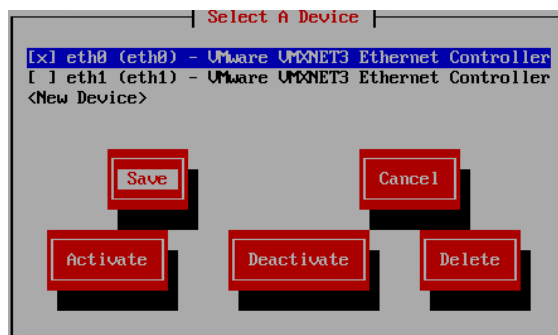
3. 在设备配置项页面中选择要使用的第一块网卡, 作为外网网卡使用。



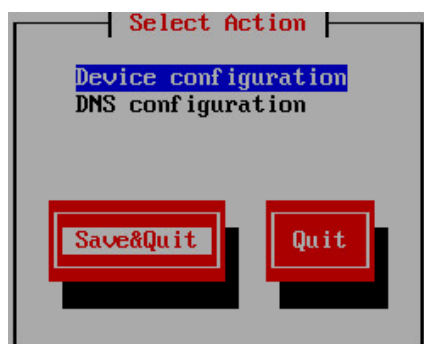
4. 配置 IP 地址 (此 IP 在网卡的网段中)、子网掩码、网关、DNS 信息, 最后按『OK』确认。



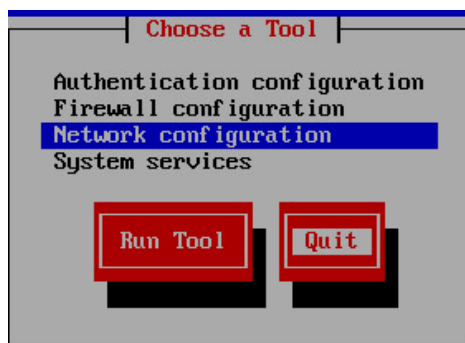
5. 选择『Save』(保存)。



6. 选择『Save&Quit』 (保存并退出)。



7. 选择『Quit』 退出配置界面。



8. 执行『service network restart』命令重启网络服务，以生效配置。

```
[root@WRDUPN ~]# service network restart
Shutting down interface eth0:          [ OK ]
Shutting down loopback interface:      [ OK ]
Bringing up loopback interface:        [ OK ]
Bringing up interface eth0: Determining if ip address [REDACTED] is already in use for device e
th0...                                  [ OK ]
[root@WRDUPN ~]# _
```

### 4.3 时间配置

输入『date』命令检查系统时间是否正确，若不正确，则使用『date』命令来校正系统时间位当前准确时间，如下图所示。

```
[root@WRDUPN ~]# date
Sat Feb  8 11:39:24 CST 2020
[root@WRDUPN ~]# date -s "2020-02-08 11:40:00"
Sat Feb  8 11:40:00 CST 2020
[root@WRDUPN ~]# _
```

### 4.4 更新数据

在 WebVPN 服务器可以访问外网后，建议手工同步一次 VPN 的德尔塔数据，使用『vpndelta』命令，如下图所示。

```
[root@WRDUPN ~]# vpndelta
[JS UPDATE] fetching new js...
[JS UPDATE] fetching new js success!
[root@WRDUPN ~]# _
```

在第一次手工同步之后，无需再次手工操作。

## 5 系统设置

### 5.1 Web 管理

完成 OS 基本设置后，资源访问与控制系统的管理端默认使用 HTTP 协议访问，进入管理端口也可以设置管理端使用 HTTPS 协议访问。

管理端工作在 TCP 『9080』端口，可用 Chrome、Firefox、Safari 等现代浏览器访问 URL：http://<ip>:9080 。

默认管理端用户名『admin』 密码为『Wrd123!@#』。

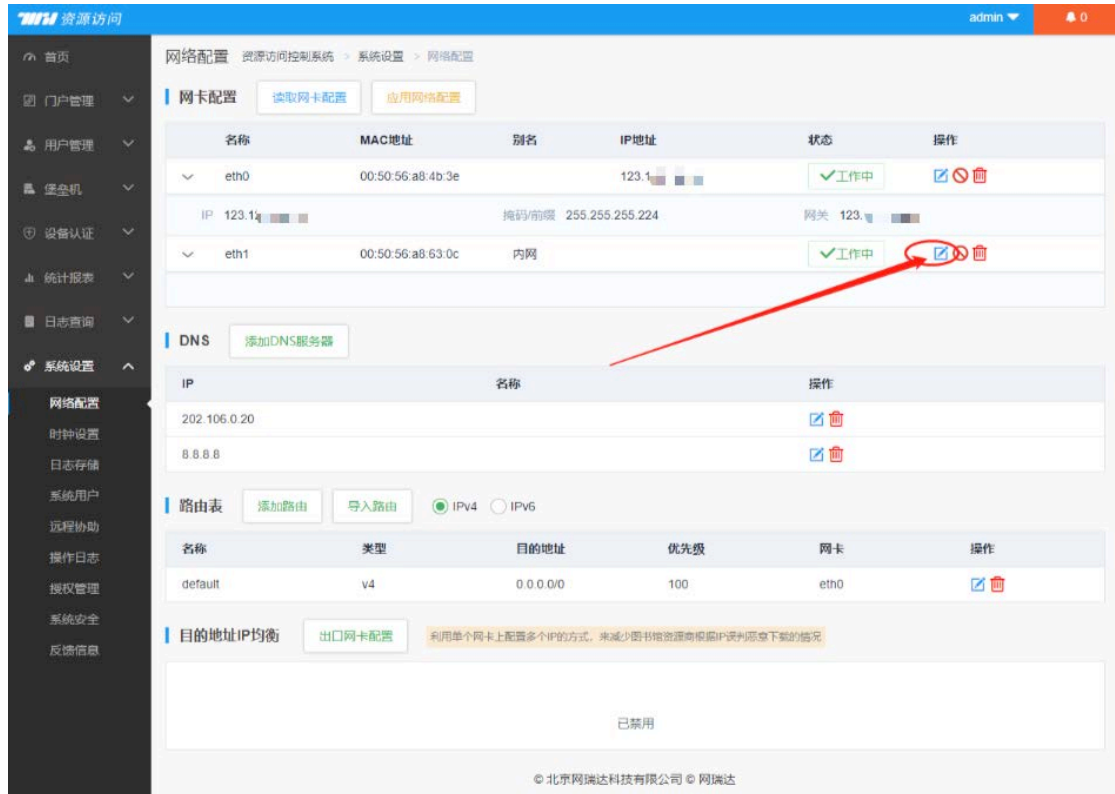
特别地，强烈建议用户修改默认账户密码，以提高系统安全性。  
密码修改入口为：管理端『系统设置』/『系统用户』菜单。

WebVPN 管理端登录页如下图所示。



#### 5.1.1 内网网卡设置

WebVPN 管理端进入『系统配置』/『网络配置』菜单，可调整网卡 IP 地址、DNS 解析服务器、IP 路由表 等设置，如下图所示。用户可根据需要调整。点击要作为内网网卡的『编辑』图标按钮，如下图所示。



在弹出对话框中填写别名、IP、掩码、网关等信息，如下图所示。

编辑网卡
✕

名称 eth1

MAC地址 00:50:56:a8:63:0c

别名

IPv4    ✕

+ 新增

启用IPv6  OFF

取消
确定

### 5.1.2 内网路由设置

内网路由可以逐条添加，在上述网络配置页面中点击『路由表』分项下『添加路由』按钮，注意选择对应的内网网卡，如下图所示。

添加路由

名称 10段

类型  IPv4  IPv6

目的地址 10.0.0.0/8

优先级 100

网卡名称 eth1

取消 确定

若有较多路由条目需要添加，可以点击『导入路由』按钮，以批量导入方式进行。

### 5.1.3 应用网络和路由配置

检查网卡配置和路由配置正确后点击页面上方的『应用网络配置』按钮再次检查后，点击『确认』按钮，如下图所示。

提示

请检查网络信息是否正确，确认会重启网卡，需要等待一段时间。

名称	IP地址	掩码/前缀	网关
eth0		255.255.255.224	
eth1	10.3.9.100	255.255.255.0	10.3.9.1

名称	类型	目的地址	网卡
default	v4	0.0.0.0/0	eth0
10段	v4	10.0.0.0/8	eth1

取消 确定

### 5.1.4 NTP 设置

为了确保 WebVPN 记录信息的时间准确性，建议用户设置 NTP 服务以同



步准确时间。WebVPN 管理端进入『系统设置』/『时钟设置』菜单，界面如下图所示。



### 5.1.5 域名和 HTTPS 设置

#### 域名

为了便于对外发布服务，建议分配 WebVPN 专用域名指向服务 IP 地址，如用 webvpn.xxx.edu.cn 形式域名发布 WebVPN 服务。在权威 DNS 解析服务器上设置 webvpn.xxx.edu.cn 解析指向 WebVPN 服务器的外网网卡 IP 地址。

#### HTTPS 设置

WebVPN 管理端进入『门户管理』/『安全配置』菜单，在页面中『HTTPS 和证书配置』分项点击『HTTPS』开关设为『ON』状态，设定 WebVPN 服务要使用的域名、HTTPS 模式、上传方式（证书来源），并点击『确定』按钮，如下图所示。

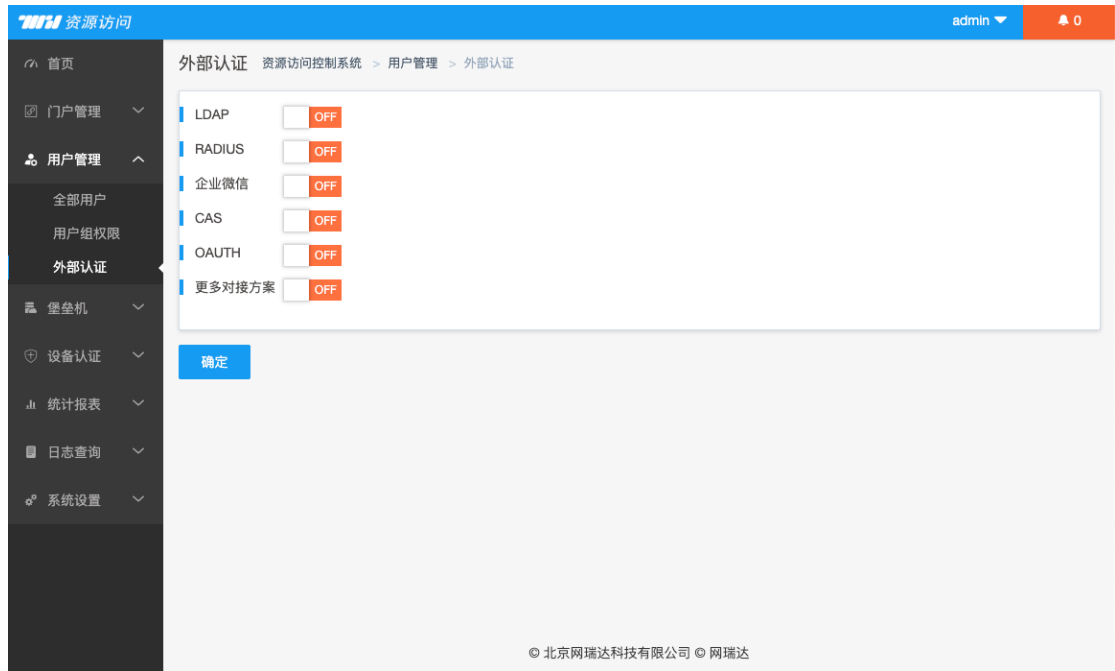


其中,『自动签发』使用 Let' s Encrypt 作为 SSL 证书提供者, 确保可信可验证。

特别地, 建议使用 HTTPS 协议以提升安全性。

### 5.1.6 认证对接

WebVPN 支持与现有各类认证系统对接, 以便使用 WebVPN 的用户使用在认证系统中已有的账户。对接后, 使用外部认证源登陆的用户继承默认用户组权限。WebVPN 管理端进入『用户管理』/『外部认证』菜单进行设置, 如下图所示。



常见的认证系统支持包括：LDAP、RADIUS、CAS、OAuth 等。根据认证系统的类型，选择并打开对应选项开关，填入相关参数。

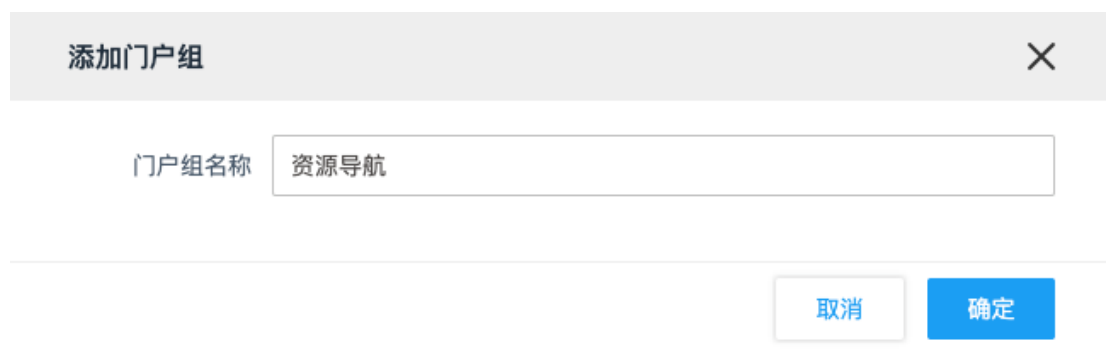
### 5.1.7 门户导航设置

#### 使用内置门户导航

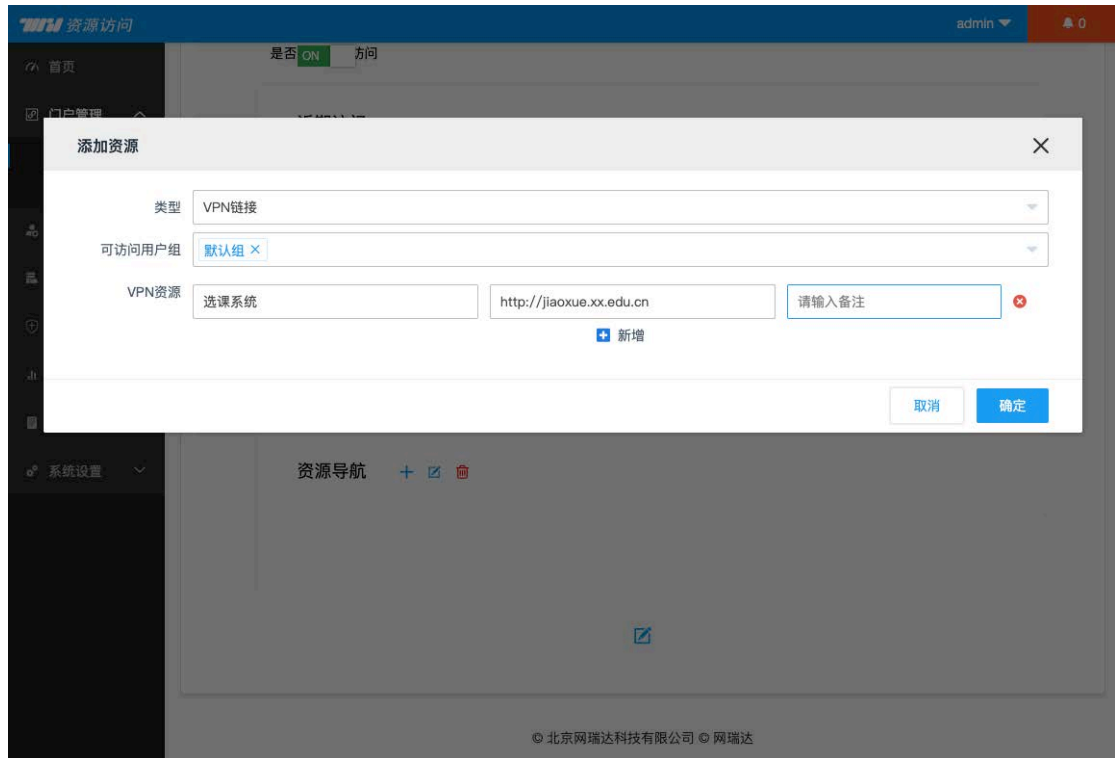
WebVPN 默认提供内置的导航门户，用户登录 WebVPN 后默认限制内置导航门户定义的内容。导航门户显示内容通过 WebVPN 管理端『门户管理』/『内容配置』菜单，在『门户页』标签页页面中点击『添加分组』创建导航资源分组，如下图所示。



在弹出的对话框中输入资源分组名称，如『资源导航』；如下图所示。



在新建的资源导航分组右侧点击『+』符号按钮，创建用户可通过门户导航页直接点击访问的 VPN 资源。如下图所示。



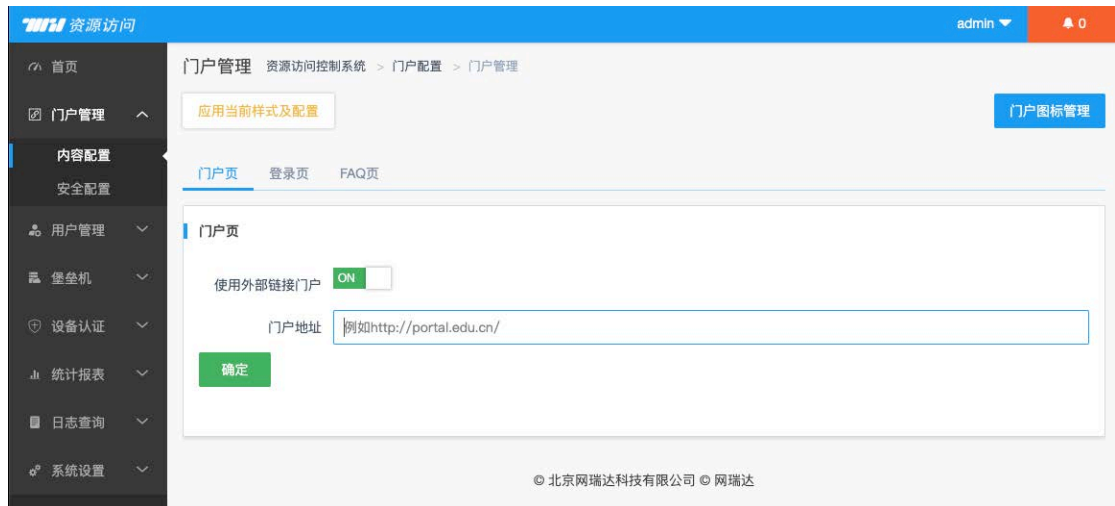
多个资源或分组，可以重复上述步骤添加更多。

最后，点击页面上部的『确定』按钮保存修改；点击『应用当前样式及配置』按钮以使配置生效。

### 使用校内门户导航

也可以设置校内门户作为 WebVPN 登录后导航门户，用户登录 WebVPN 之后默认显示校内门户导航页面，保持原有用户使用习惯。

WebVPN 管理端进入『门户管理』/『内容配置』菜单，在『门户页』标签页页面中点击『使用外部连接门户』开关，在『门户地址』输入框种输入校内门户页面地址，最后点击『确定』保存。参见下图。



### 5.1.8 申请授权

WebVPN 管理端进入『系统设置』/『授权管理』菜单，在页面中填写必要信息后点击『确定』按钮以下载授权申请文件，如下图所示。将授权申请文件发送给我司技术人员以申请 License 授权文件，之后在『更新授权』处上传获得的 License 授权文件即可。我司各区销售服务人员为您提供授权服务，请参阅后文联系我们。



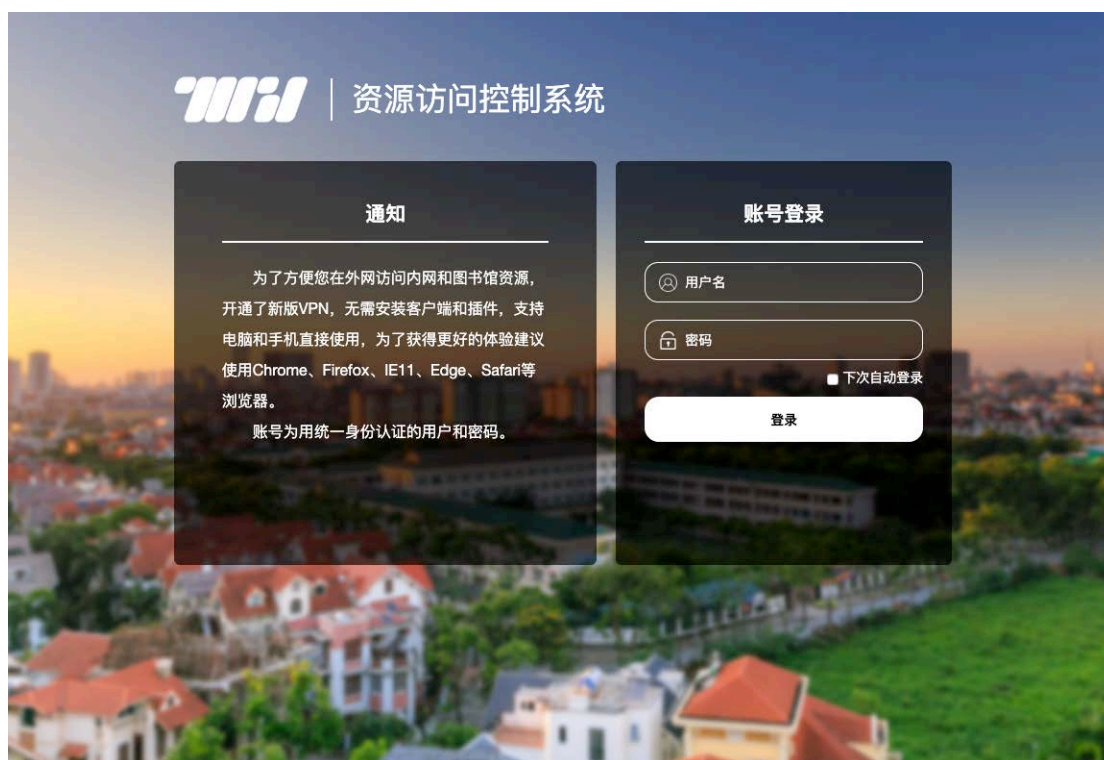
## 5.2 用户访问

用户端工作在 TCP 『80』 端口, 可用 Chrome、Firefox、Safari 等 现代浏览器访问 URL: `http://<ip>` 。

默认用户端内置普通用户 『test』 密码为 『1111』。

特别地, 强烈建议用户修改默认账户密码, 以提高系统安全性。  
密码修改入口为: 管理端 『用户管理』 / 『全部用户』 菜单。也可删除内置用户。

用户访问 WebVPN 服务登录页面如下图所示。



用户登录后门户导航页面如下图所示。



## 6 更多参考

更多资源访问控制系统的管理与使用参见下列手册。

- 《资源访问控制系统系统管理手册》
- 《资源访问控制系统用户手册》



## 7 联系我们

微信扫下方二维码或搜索『网瑞达科技』关注我们，获取更多服务信息；全国各区销售服务人员联系方式可在微信公众号『关于我们』→『联系我们』中查询。

