Array SSL VPN 操作手册

目录

一. Array SSL VPN 创建与访问 1
1.1 部署 Array SSL VPN 1
1.2 管理 Array SSL VPN 1
1.2.1 登录指导、管理员账号密码修改 1
二. Array SSL VPN 常用配置维护 4
2.1 License 申请与导入 4
2.2 SSL VPN 虚拟站点建立 6
2.3 本地数据库认证建立 7
2.4 SSL VPN 建立 8
2.5 角色的建立 10
2.6 添加本地用户账号 12
2.7 登录 VPN 系统 13
2.8 VPN 账号权限配置 13
2.9 登陆页面图标和登陆信息更改 14
2.10 SSL VPN 配置的存盘 15
2.11 SSL VPN 连接方式 16
三. Array SSL VPN 双因素配置 16
3.1 动态码获取与绑定 17
3.1.1 手机端应用获取 17
3.1.2 绑定过程 18
3.1.3 密码获取 19
3.1.4 解除绑定 19
四. Array SSL VPN 账户硬件 ID 绑定 20

适用性声明:
本文档仅适用于云 Array SSL VPN 部署及配置

一. Array SSL VPN 创建与访问

1.1 部署 Array SSL VPN

Array SSL VPN 需要的虚拟机推荐配置

CPU：2 核（推荐）

内存：4GB（推荐）

带宽： 选择 0M 需要在公网 SLB 开通 443（登录 VPN）端口 和 8888（管理 VPN）端口

存储：默认存储

注：内存必须等于大于 2G。（不然，VPN 服务无法启动）

1.2 管理 Array SSL VPN

使用浏览器登录 https:// array 设备 VPN 外网 IP：8888

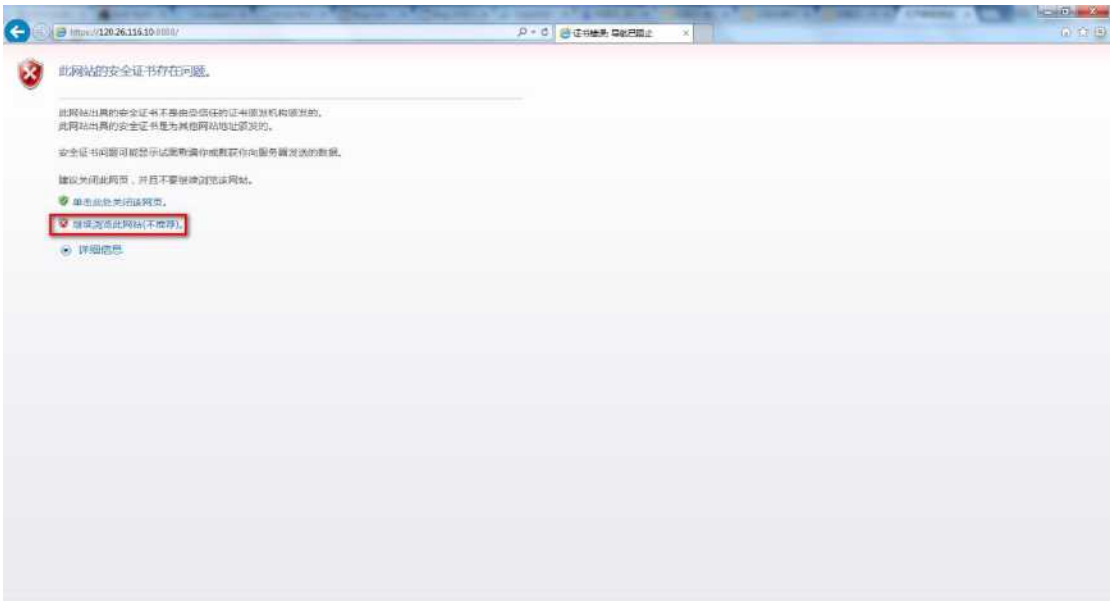
例：https:// 120.26.116.10:8888

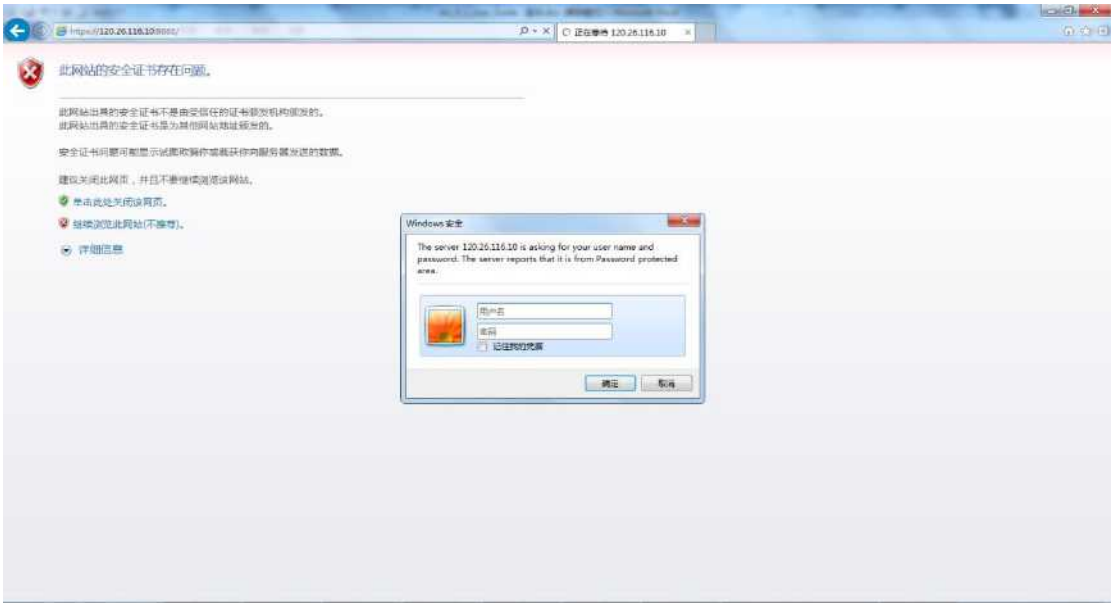
需要说明：

如果客户使用的是 SLB ,则需要在 SLB 开通 443(登录 VPN)端口 和 8888（管理 VPN 的 Web 控制台）端口

1.2.1 登录指导、管理员账号密码修改

在浏览器输入地址截图如下





管理员用户名和密码

Array SSL VPN 设备默认管理员账号： array 密码：admin

Enable 密码：默认未设置，直接点击 login 即进入 web 控制台。

管理员密码修改：

全局模式下 config 模式下-全局管理-双击管理员账户

修改完密码后点击保存，最后点击保存配置，将当前配置存盘

需要注意的是，配置模式只允许单管理员登陆，万一出现管理员在配置模式时非正常退出，导致再次登陆进入配置模式报错：

必须在访问控制中重置管理员账户 config 模式：

系统管理-访问控制-config 模式：重设到初始值

Enable 密码设置：

系统管理-访问控制-新的 Enable 密码

二. Array SSL VPN 常用配置维护

2.1 License 申请与导入

部署 0 元镜像的试用用户需要提前申请测试 license，购买含并发用户镜像无需申请。申请方式如下：

在登录界面找到序列号，发邮件联系厂商可申请 30 天临时 license 供测试使用。

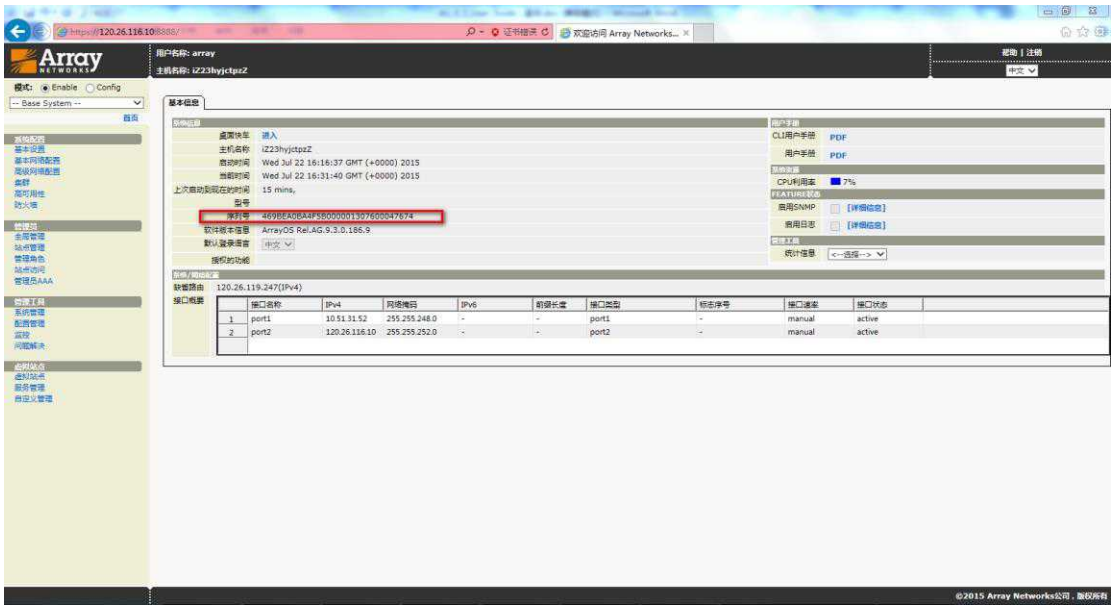
申请测试 license 请发送至以下邮件：

liubin@arraynetworks.com.cn

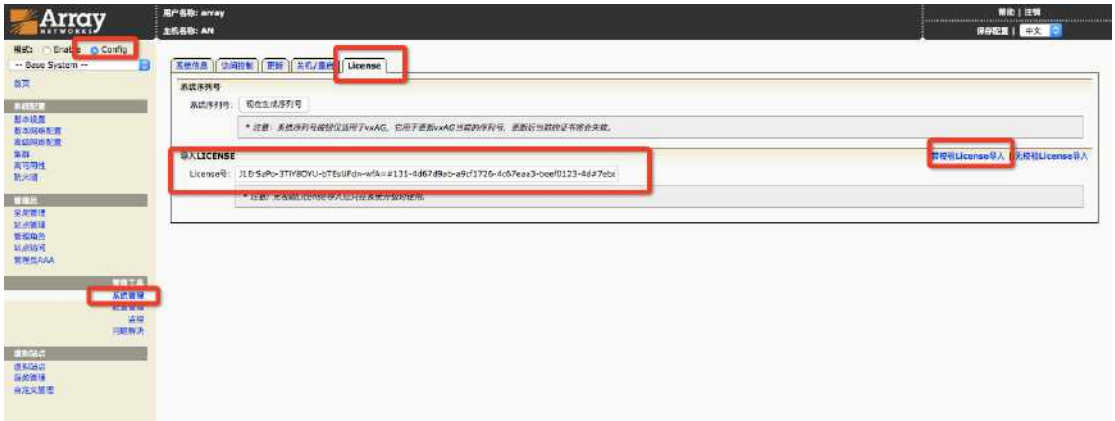
发送测试 license 申请请备注公司名、联系人姓名和手机号码，并把实际测试并发用户写明，若未写明一律按照 5 个并发数申请。

注：如果没有 license，服务将不可用。

序列号显示位置：

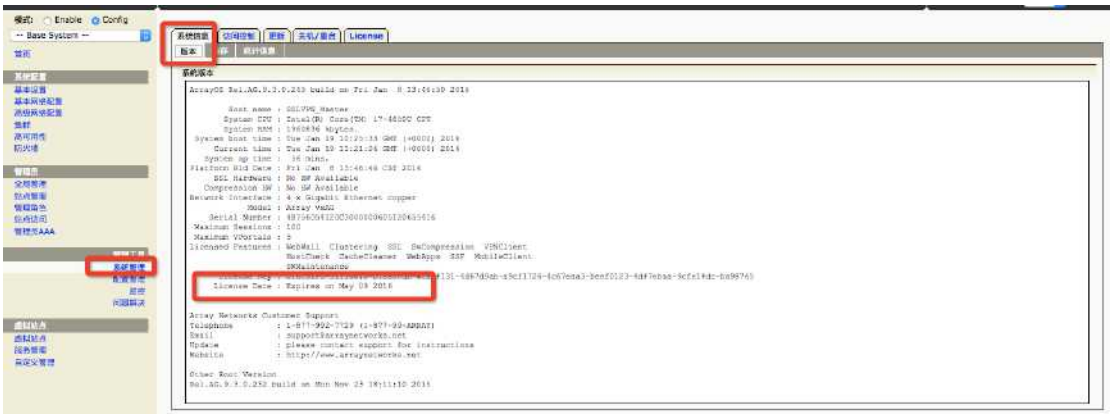


导入 license，注意需要带校验导入 license。



导入成功后请立即重启虚拟机，等管理页面能够正常登录后，继续后续操作。

查看 license 到期时间：

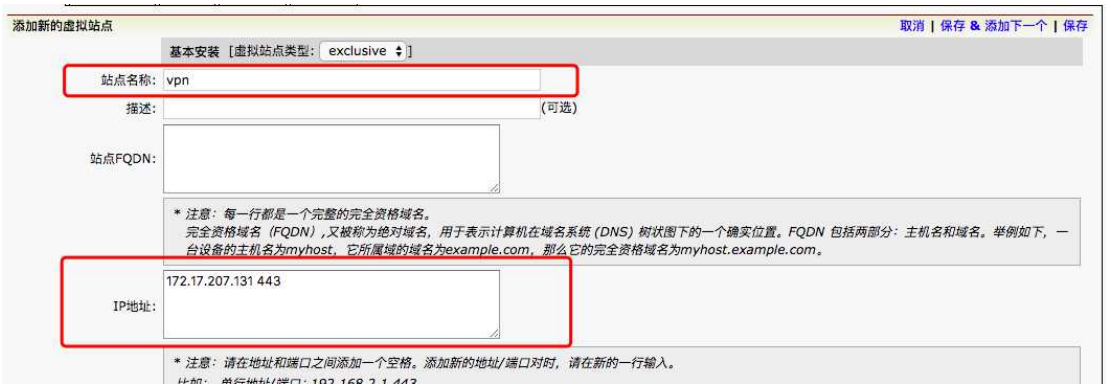


注意：购买含并发镜像无需考虑 license 许可问题，该步骤可以忽略。

2.2 SSL VPN 虚拟站点建立

首先我们需要创建一个虚拟站点，进入全局模式 config 模式下->虚拟站点->添加站点：

站点名称：自定义



生成自签发证书，证书信息填写自定义即可（该服务器证书在浏览器中未受信，若有受信证书可以直接在创建虚拟站点时导入）

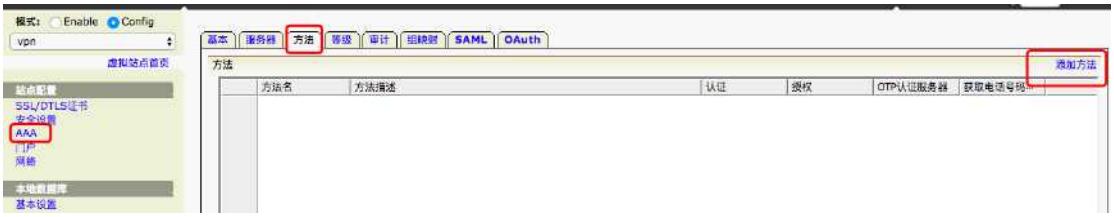
填写完以上信息后点击保存。

这样我们就能在左上角下拉菜单中看到我们新创建的虚拟站点了。选中虚拟站点可以进入站点模式下配置相关的 VPN 配置。

2.3 本地数据库认证建立

array 管理员登陆->切换到 vpn 站点->AAA->服务器->本地数据库->启用本地数据服务器->应用修改

AAA->方法->添加方法



方法名：自定义

认证选择 vpn（默认数据库启用后，本地数据库名称和站点名称相同）

最后点击保存。

以上为本地数据库认证启用方式，如果有其他认证方式要求，请咨询 lizy@arraynetworks.com.cn

2.4 SSL VPN 建立

SSL VPN 访问区域配置：

array 用户登陆->切换到 vpn 站点->Config 模式->VPN->通用设置->VPN 资源->添加

资源：自定义

网络类型 VPN 资源项：填写需要通过 SSL VPN 接入后管理的 IP 地址或 IP 地址段，点击添加，可以多次添加。

最后点击保存。

SSL VPN 客户端分配地址池配置：

VPN->通用设置->Netpool->增加 Netpool

Netpool 名称：自定义

启用 NAT 选项说明：勾选启用 nat 后，用户端分配的 netpool 地址经过 SSL VPN 会 nat 成站点服务 ip；

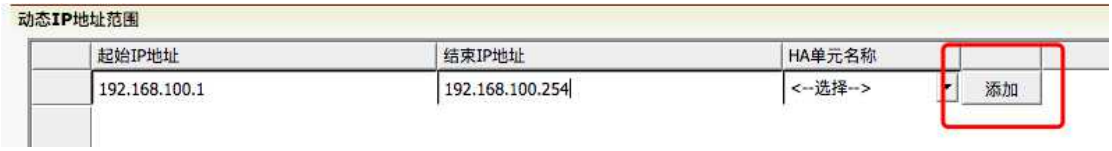
不勾选代表使用路由模式，源地址为 VPN 实际分配给客户端的 netpool 地址，为了支持路由模式正常工作，必须在内部指定一条 vpn 分配地址池的目的路由。

请根据实际网络环境挑选部署模式

最后点击保存。

双击新建的 netpool 名称

在动态 IP 地址范围中填写对应的地址区间并点击添加（此处我用了 192.168.100.0/24 这个段地址）

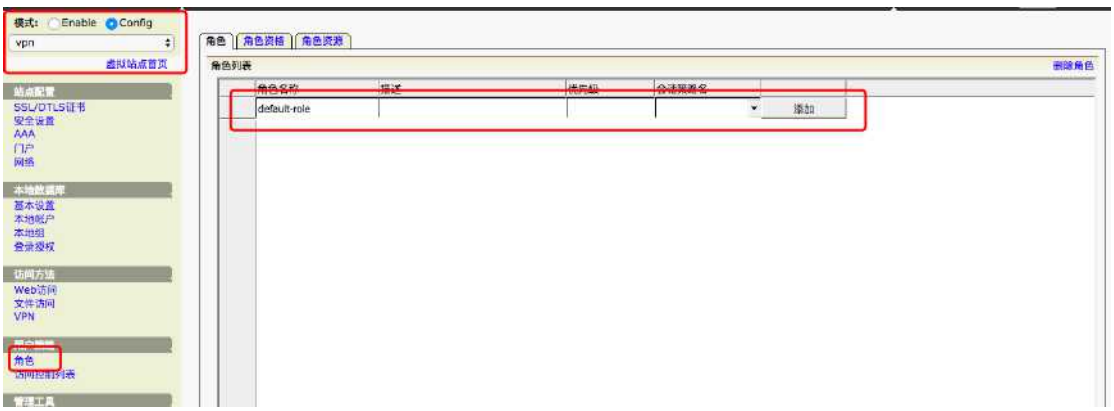


最后启用 SSL VPN 功能，VPN->SSL VPN>勾选启用 VPN->应用修改，

2.5 角色的建立

在之前我们已经建立了认证，SSL VPN 的资源和分配地址段，我们需要将这些元素联系起来，通过创建角色完成我们最后的配置步骤：

array 用户登陆->切换到 vpn 站点->Config 模式->角色->填写角色名称->添加



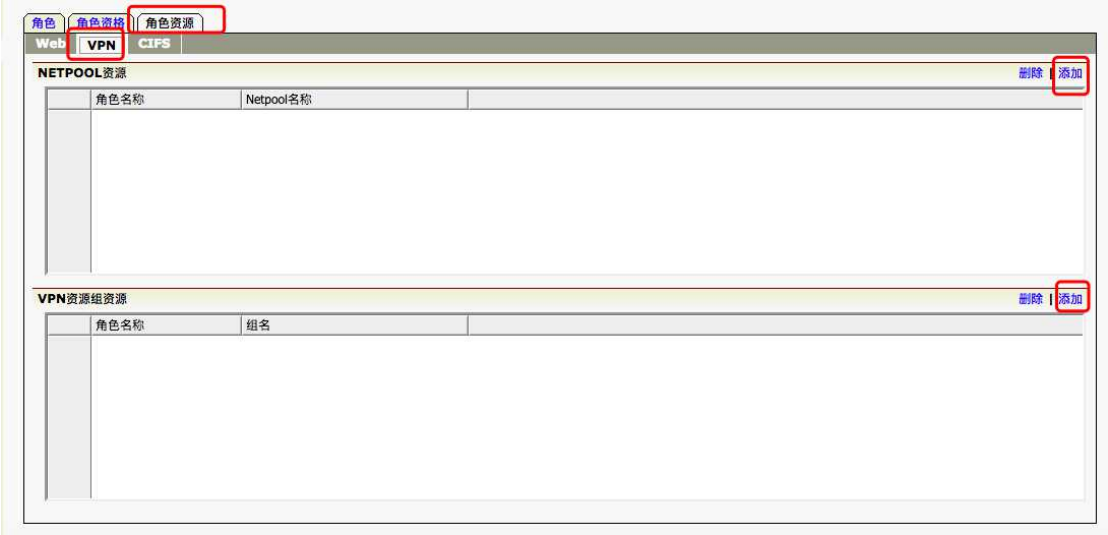
在角色中至少要定义一个角色资格

角色资格->添加

资格名称：自定义

最后关联角色的 VPN 资源

角色资源->VPN->NETPOOL 资源->添加



VPN 资源组资源->添加

以上我们已经完整的定义了整个 SSL VPN 的配置。最后我们要把配置存盘（这点非常重要，否则重启配置会丢失）

全局模式下->Config 模式->保存配置->保存全局和所有虚拟站点配置

2.6 添加本地用户账号

以上我们已经配置完了 SSL VPN 服务，下来我们通过添加账户就可以开始使用 Array SSL VPN 业务了。

登录 VPN 设备后，创建需要使用的 VPN 账户：

array 用户登陆->切换到 vpn 站点->Config 模式->本地数据库->本地账户->添加

2.7 登录 VPN 系统

添加完用户浏览器登陆主机外网 ip 到用户登陆界面。注意 :同样需要在 SLB 上映射 443 端口。才可以通过外网进行访问登录。

例：https://39.107.76.227

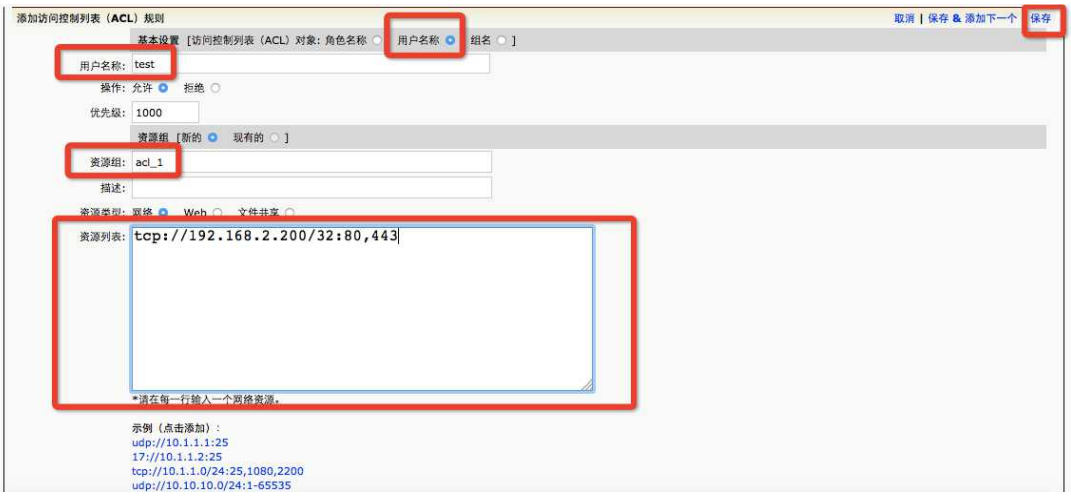
2.8 VPN 账号权限配置

默认情况下，用户正常登录后，能够访问 VPN 可访问区域网段中的所有应用，如果需要给具体的某个用户定义 ACL，按如下方式定义：

array 用户登陆->切换到 vpn 站点->Config 模式->用户策略->访问控制列表->基本 ACL->ACL 规则

添加具体明细 ACL：

访问控制列表选基于用户名的方式，选择本地数据库中具体的用户名，资源组名称随机定义，资源列表根据以下示例添加。添加完成后，默认行为是 deny，以下截图是针对 test 这个用户只开放 192.168.2.200 这个地址的 80 和 443 端口。注意：针对当前登录用户更改权限后，需要让此用户注销重新登录，才能分配到新更改后的权限。（若用户量比较大，可以选择基于本地组分配 ACL 资源）



2.9 登陆页面图标和登陆信息更改

在站点模式下，以下界面标注处能够更改登陆页面语言和 Logo 图标：

以下界面标注处可以修改登陆页面的登陆信息和欢迎页面的登陆标题和信息

2.10 SSL VPN 配置的存盘

以上添加的配置只会保存在内存中，我们必须将现有的配置保存至硬盘中，便于 ESC 重启后能够正常加载配置，保证配置没有丢失：

Base System 下点击保存配置，选择保存全局和所有虚拟站点配置，并点击确认。

站点模式下直接点击保存配置即可。

2.11 SSL VPN 连接方式

请详细阅读 Array SSL VPN 客户端使用手册

三. Array SSL VPN 双因素配置

Array SSL VPN 提供三种密码认证方式：**静态密码，动态密码，静态密码+动态密码。**

静态密码：最基本的认证模式，登陆密码为添加用户时设置的密码。

动态密码：利用 Array OTP 手机应用与站点及用户绑定后生成的 6 位数动态密码登陆

静态密码+动态密码：密码格式为静态密码与动态密码连接（例：静态密码为 secret，获取当前动态密码为 123456，则登陆密码为 secret123456）。

配置：array 用户登陆->切换到 default_site->Config 模式->站点配置->AAA->服务器->本地数据库->LocalDB 认证模式->应用修改

3.1 动态码获取与绑定

3.1.1 手机端应用获取

IOS 系统在 Apple Store 搜索 MotionProOTP 应用安装。

Android 系统可在 360 手机助手或小米应用商城下载 MotionProOTP 应用。

链接如下：

http://zhushou.360.cn/detail/index/soft_id/3083541?recrefer=SE_D_MotionProOTP

http://app.xiaomi.com/details?id=com.arraynetworks.authentication&ref=search

3.1.2 绑定过程

以 Android 系统为例打开后如下图所示，iOS 系统过程基本相同。

服务器地址：为前文所说 VPN 登陆界面（https://服务器地址）中的服务器地址。

端口：默认为 443

用户名：该用户登陆 VPN 时的用户名。

密码：添加用户时设置的密码，即静态密码。

3.1.3 密码获取

绑定成功后如下图所示，密码为 30S 更新一次。

3.1.4 解除绑定

客户端解除绑定：

VPN 管理端强制解除绑定：

在本地账户中选择对应的账户，将自定义信息 1 中的字符串删除即可。

四. Array SSL VPN 账户硬件 ID 绑定

需要实现用户认证账户与登录终端设备的绑定。

首先进入站点模式下，点击本地数据库中登录授权：

设置前先建立好本地组，推荐方式 machineid 和 macany。

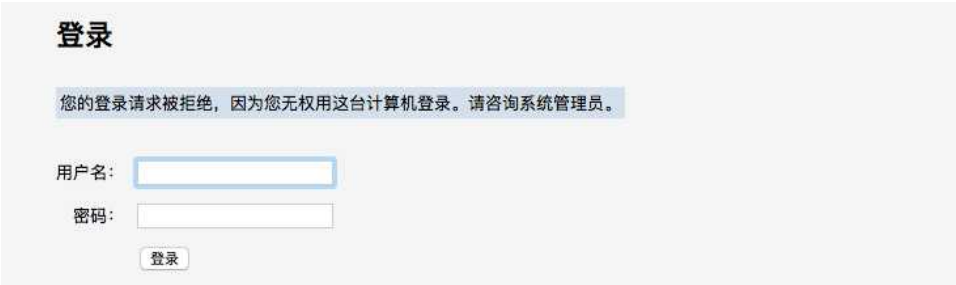
必须开启自动收集，自动审批可根据实际情况开启或不开启。

若开启自动审批功能，单个账户允许的终端绑定数量由硬件 ID 限制的数量决定。

可以在授权请求中看到账户和终端绑定的授权信息：

若自动审批功能不开启，默认状态是 deny，需要管理员进行放行。

deny 状态下会提示：



解除账户的终端绑定，选中对应账户绑定条目后点击拒绝即可。