赛蓝移动云管理员手册

Cylan Mobile Cloud

Administrator Manual

深圳市赛蓝科技有限公司

版权说明

本文的内容是赛蓝移动云接入方案。文中的资料、说明等相关内容的版权归深圳市赛蓝科技有限公司所有和保留。本文中的任何部分未经深圳市赛蓝科技有限公司（以下简称赛蓝科技）许可，不得转印、影印或复印、发行。

2009-2015© 版权所有 深圳市赛蓝科技有限公司

商标声明

本解决方案中所谈及的赛蓝科技产品的名称是赛蓝科技的商标。方案中涉及的其他公司的注册商标属各商标注册人所有，恕不逐一列明。

联系信息

深圳市福田区彩田北路民宁商务大厦 608

产品咨询热线：400-716-3232 0755-83073489

传真：0755-83073493

邮编：518035

目 录

1 产品简介

1.1 概述

赛蓝科技作为国家密码管理局批准的商用密码产品生产定点单位和销售许可单位，推出了自主研发的赛蓝科技移动云产品。目前，手机上的应用还是很有局限性，应用软件供应商很难在智能手机上开发其应用系统，如果想把 WINDOWS 平台上的应用软件移植到智能手机上，还存在很多技术上的难度，底层支持，浏览器支持，兼容性等问题非常明显，赛蓝的移动云应用平台给出了很好的解决方案，它借由赛蓝客户端去访问互联网上的应用服务器资源，它既能充分利用手机的便携性，续航时间和通信能力等众多天生优势，又不要求其具有较高的数据处理、计算和存储能力。一方面，运用远端“云计算”的高速处理能力来解决手机处理能力低下的问题；另一方面，利用“云存储”则可以解决手机存储能力不足的问题。

赛蓝移动云软件具备在任何地点、向任何用户交付任何应用的能力。它给将基于云的资源交付给用户，通过这个应用集中管理的平台，不断优化用户的应用性能和安全性，以应对不断变化的工作负载需求和基础架构可用性。从而使手机用户能够轻松访问其授权的应用和程序，可以提供足以媲美本地 PC 的丰富、完整的用户体验。赛蓝移动云软件的一般部署方式如下图所示。

1.2 客户端环境要求

客户端推荐使用的操作系统：android 2.1 及以上，IOS 3.0 及以上。

1.3 管理员配置环境要求

推荐使用浏览器：IE7，IE8，IE9，IE10

2 管理员配置

2.1 网络配置

2.1.1 基本配置

基本配置里面包括 4 个选项卡，分别显示网络接口，内网自动选路配置，域名服务器，PPPOE 拨号日志，如下图所示。

网络接口配置页面，通过点击相应网口编辑按钮，可修改该网络接口的接入方式，IP 地址，掩码，默认网关，MTU 值，线路权重，也可配置多个虚拟 IP 地址（即一个网口绑定多 IP 地址）。如下图所示：

接入方式项中，支持 3 种接入线路方式：静态 IP，DHCP，PPPOE。只有静态 IP 接入方式可配置虚拟 IP（即一个网口绑定多 IP 地址）。只有静态 IP 和 PPPOE

接入方式可配置线路权重。

线路权重：即线路负载均衡，只在有多条线路上网时起作用，该值针对内网通过 SGA 上网的用户，调节本线路占整体的比重，值越大比重越大。具体举例说明：如 eth0 为 PPPOE 拨号上网线路，线路权重设置为 3，eth1 也为 PPPOE 拨号上网线路，线路权重设置为 7，可理解为 2 条线路带宽看作一个整体值：10，eth0 占整体的 30%，eth1 占整体的 70%，即内网用户通过 SGA 上网，数据流会从这 2 条线路分别出去，30%的数据会走 eth0 出去，70%的数据会走 eth1 出去。这一说法只是一个大约的数据流分配走向，具体不会有那么精确。

点击内网自动选路配置，出现如下图：

如果是多网口上网时,可指定某 IP 或子网走某出口。配置如下：

点击域名服务器选项卡，配置 DNS 服务器 IP 地址，使 SGA 能正常解析域名。如下图：

点击 PPPOE 拨号日志选项卡，该页面只在网络接口配置有 PPPOE 拨号的时候有日志显示，记录各网络接口 PPPOE 拨号的信息，便于跟踪拨号状态。如下图：

2.1.2 高级配置

基本配置里面包括 3 个选项卡，分别是动态域名，主机解析，加入 AD 域。

动态域名选项卡页面如下图所示，系统预制了希网和花生壳 2 个免费域名客户端。

希网域名配置如下图：

用户账号：希网网站上，您申请域名所登录的有效账号；

登录密码：希网网站上，您申请域名所登录账号的密码；

描述：可为空；

绑定接口：绑定一个可以连接外网的 SGA 的接口；

动态域名：您将绑定在 SGA 设备上的有效域名；

更新频率：设置 SGA 系统将每几分钟去更新该域名所对应的 SGA 公网 IP 地址；

自动启动：勾选上启用后，SGA 系统每次启动将自动启动该域名客户端；

提交后，如需要马上启用该域名客户端，需要在返回页，操作项下点击启动。

花生壳域名配置如下：

用户账号：花生壳网站上，您申请域名所登录的有效账号；

登录密码：花生壳网站上，您申请域名所登录账号的密码；

描述：可为空；

绑定接口：绑定一个可以连接外网的 SGA 的接口；

Web 服务地址：花生壳的 Web 服务地址，可不做修改；

DDNS 服务器：花生壳的 DDNS 服务器地址，可不做修改；

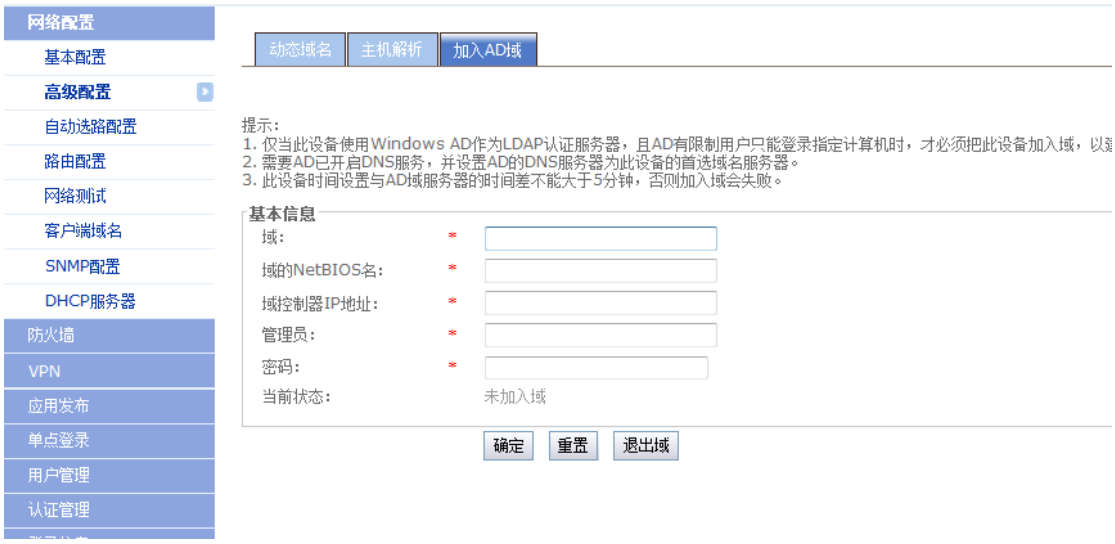
自动启动：勾选上启用后，SGA 系统每次启动将自动启动该域名客户端；

提交后，如需要马上启用该域名客户端，需要在返回页，操作项下点击启动。

主机解析选项卡页面如下图所示：

点击添加，弹出以下界面，配置 IP 地址、主机名或域名和别名的一个对应关系。

加入 AD 域选项卡如下图所示：



提示：1. 仅当此设备使用 Windows AD 作为 LDAP 认证服务器，且 AD 有限制用户只能登录指定计算机时，才必须把此设备加入域，以建立信任关系。若 AD 域用户可登录到所有计算机，则无需把此设备加入域，亦可进行认证。 2. 需要 AD 已开启 DNS 服务，并设置 AD 的 DNS 服务器为此设备的首选域名服务器。3. 此设备时间设置与 AD 域服务器的时间差不能大于 5 分钟，否则加入域会失败。

域：Windows AD 域的域名，如：punwar.cn

域的 NetBIOS 名：域控制器—属性---常规---域名 ，如：PUNWAR

域控制器 IP 地址：装有 AD 域服务器的地址 如：192.168.110.243

管理员：装有 AD 域服务器的管理员 如：administrator

密码：管理员对应的密码 如：*********

2.1.3 自动选路配置

如有两条或者两条以上的接入线路，可配置该功能，当用户访问其中一个线路的外网地址时，如这条访问线路没有另外一条速度快，用户访问页面会自动跳转到另外一条线路的外网地址上来打开 SGA 页面，如下图：

点击添加按钮，出来以下界面：

线路选择：选择便于识别的线路名称。

描述：可为空

启用：启用后改配置才生效。

线路 IP 或域名：填写有效的，外网能正常访问到的线路 IP 或域名

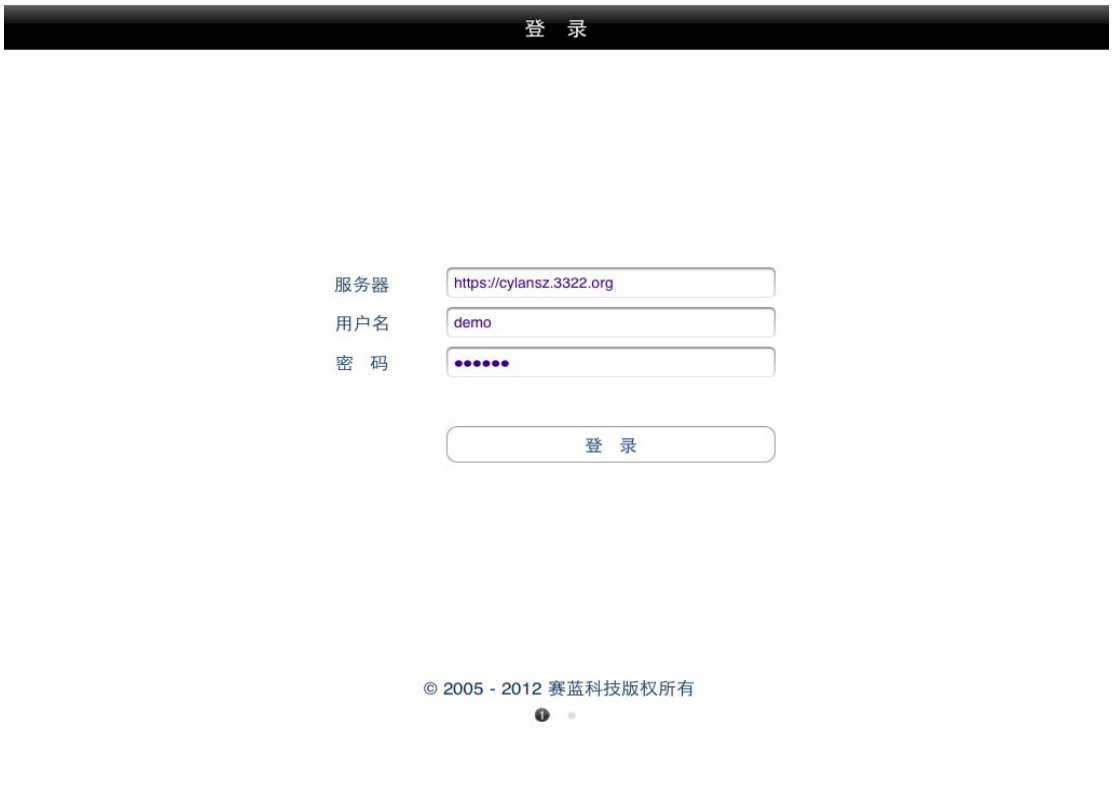
HTTPS 端口：填写 SGA 前台访问端口。

2.1.4 网络测试

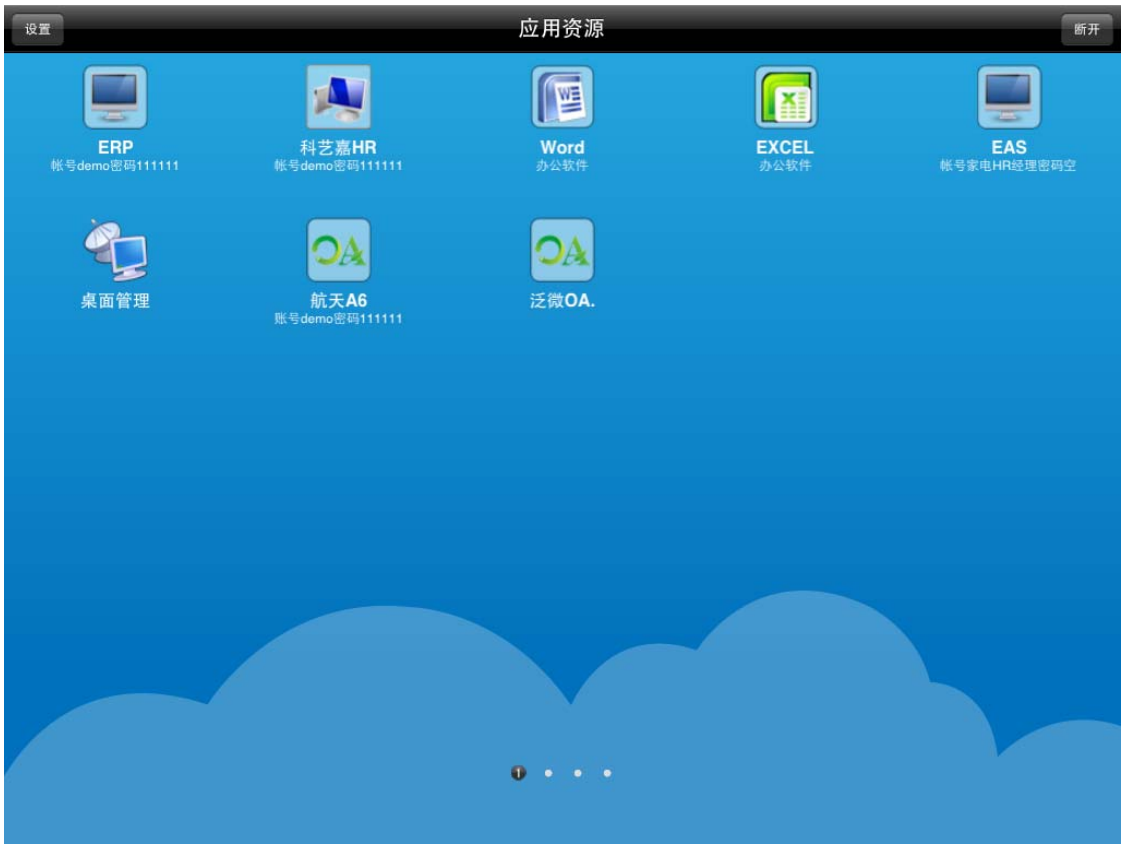
该页面提供 Ping 测试， Traceroute（路由追踪），URL=>IP（域名解析功能），Port Test（端口测试）。

2.1.5 登录实例

以上信息配置好后如果在内网使用直接在客户端填写内网地址，如果使用外网访问就需要在客户端填写服务器域名地址，然后填写上用户名和密码之后点击登录，以 ipad 为例，如下图所示：



点击登录按钮，登录到资源列表，如下图所示：



2.2 应用发布

2.2.1 CAB 应用

CAB 应用发布选项卡：

条件过滤，可针对已经发布的 CAB 应用资源，根据名称，描述，IP 地址，状态进行单独、组合、模糊、精确等查询。

添加/配置 CAB 应用资源，点添加后，出现以下配置界面：

名称：CAB 应用资源在系统和用户界面的显示名称。

描述：可为空。

排序优先级：值越大在前台资源列表中的显示位置越靠前,不填或为 0 则按

默认排序。

启用：是否启用该资源。

终端服务器地址：要发布的 CAB 应用服务器的 IP 地址。可以填写多个终端服务器地址，以实现负载均衡。

使用方式：CAB 应用所走的隧道方式。有 TCP，IP，内网方式三个选择项。

端口：终端服务的端口号，默认是 3389。

应用账户：包含使用设备账号，手动绑定账号，使用默认账号。

使用设备账号：如选择这一项，表示应用账户直接使用 SGA 设备内的账户进行登录，此种情况下 iCylanAPP 会在相应服务器自动创建相应具有远程桌面登录权限的账号进行匹配使用，用户会自动登录相应的 CAB 应用资源。此种方法，Windows 登录和手机客户端共用一套账号和密码。

手动绑定账号：如选择这一项，表示应用账户可以与终端服务器上具有远程桌面登录权限的账号，进行手动绑定，拥有相应资源的用户组中的用户可以手动绑定 Windows 登录账号，需要在 CAB 用户绑定页面进行相应绑定，此处的 SGA 设备前台登录用户名、密码和绑定 Windows 登录账号、密码可以不同。

使用默认账号：如选择这一项，表示应用账户可以使用终端服务器上具有远程桌面登录权限的账号自动登录使用。**注：**选择此项时，需要填写默认登录账号、密码。

登录后工作目录：登录 CAB 系统后启动的程序的工作目录。

登录后启动程序：登录 CAB 系统后启动的执行程序名。

图标：该资源在前台的显示图标。自定义图标可在应用发布----图标管理模块页面上传。

移动云配置：登录 CAB 系统后可以启动多个程序，这里提供了启动 3 个程序。

是否启用持久缓存：适用于手机客户端中出现界面刷新不频繁的应用；界面刷新频率很高的应用。勾选后，则表示开启缓存，可能降低应用运行速度。

关联 SSO：关联相应 SSO 资源，再配合赛蓝 iCylanAPP Server 使用。可以直接用手持终端登录 SSO 资源，第一次输入用户名和密码后，以后访问无需再次输入即可登录使用。

窗口大小：CAB 应用资源框前台显示的分辨率大小调节。有全屏，1024 X 768，800 X 600，788 X 564，640 X 480 以及手动设置六个选择项。

颜色深度：CAB 应用显示的颜色。有 24，16，15，8 四个选择项。

共享剪贴板：选择是否共享用户客户机的剪贴板。

共享打印机：选择是否共享用户的打印机，分别有 3 个选择项：共享所有，共享默认，不共享。

使用 WINDOWS 组合键： 有在远程计算机上，在本地计算机上，在全屏模式下三种选项。

在远程计算机上：即只要鼠标箭头在 CAB 窗口内，使用 WINDOWS 组合键，将只对 CAB 窗口有效。

在本地计算机上：即鼠标箭头即使在 CAB 窗口内，使用 WINDOWS 组合键，有些 WINDOWS 组合键将对 CAB 窗口和你本地计算机都有效（如输入法的切换），但是在 CAB 全屏模式下，可使用 alt+tab 键切换本地计算机的应用窗口。

只在全屏模式下：即全屏模式下，WINDOWS 组合键只在 CAB 窗口有效；非全屏模式下，WINDOWS 组合键对 CAB 窗口和本地计算机都有效。

强制使用服务器配置：选中该项，在使用智能手持终端登录访问应用时，会强制客户端使用服务器的配置参数。

本地设备映射：提供磁盘映射，串口映射和并口映射；

注意：如勾选了“使用 windows 远程桌面客户端”，磁盘映射只要映射一个磁盘，默认所有磁盘都会映射到服务器端。串口映射和并口映射也是一样。

CAB 服务配置选项卡：

CAB 服务配置选项卡页面如下图所示。

自动登录：当启用此项，用手机访问前台资源，且只有一个资源时，会自动跳过资源列表页面直接访问资源。

帐号同步：启用此项，当在 SGA 建立用户，该用户就会自动同步到装有 iCylanAPPServer 的服务器上。

CAB 服务端口：默认是 1234，CAB 服务器安装 iCylanAPP Server 服务后会连接此端口。如果 SGA 设备放在路由器或防火墙后面，需要转发 1234 端口到设备相应接口上。

IcylanApp server 详细配置请参看附录一

CAB 用户绑定：

CAB 用户绑定页面如下图所示：

此页面可以导出用户关联列表，按照相应格式编辑后导入。可以查看用户关联情况和解除 CAB 绑定。

注：若导入文本中包含中文字符，需转换为 UTF-8 格式的文本文件。

2.2.2 视频资源

随时随地的监控录像功能，无论身在何处，任何密码授权的用户通过身边的手机客户端联网连接到监控网点，可以看到任意监控网点的即时图像并根据需要录像，避免了地理位置间隔原因造成监督管理的不便。

注：目前视频资源只支持 android 客户端

点添加后出现下列配置页面：

名称：视频资源在系统和用户界面的显示名称。

描述：可为空。

排序优先级：值越大在前台资源列表中的显示位置越靠前,不填或为 0 则按默认排序。

启用：是否启用该视频资源。

URL 地址：内网中能访问到视频监控软件的地址

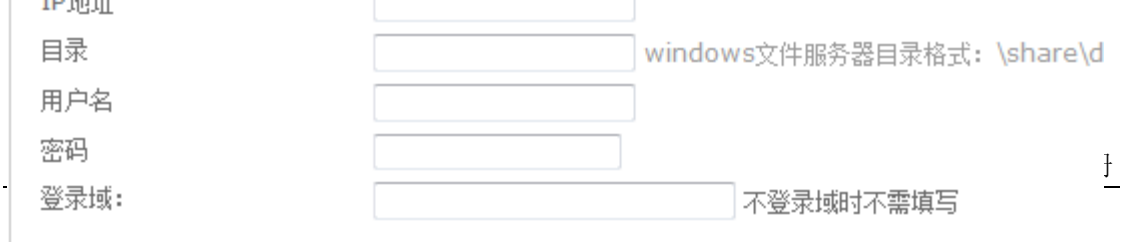
图标：该资源在前台的显示图标。自定义图标可在应用发布——图标管理模块页面上传。

2.2.3 IBOX

用户使用 PC 或手机客户端访问服务器时，支持从该服务器下载文件，远程打开并且支持从本地上传文件到服务器端。配置如下图所示：

启用 IBOX：勾选后，即可启用该功能。

用户独立配置：勾选后配置 ibox 则需要在创建用户页面进行配置，如下图所示 ，配置方法和非用户独立配置相同。



存储系统类型：默认选择 windows 文件服务器。如果有专门存放文件的网络文件服务器，可以选择 

IP 地址：该存储服务器的内网地址

目录：存放上传下载文件的文件夹目录。注意：windows 文件服务器目录格式：\share\doc，网络文件服务器目录格式：/share/doc

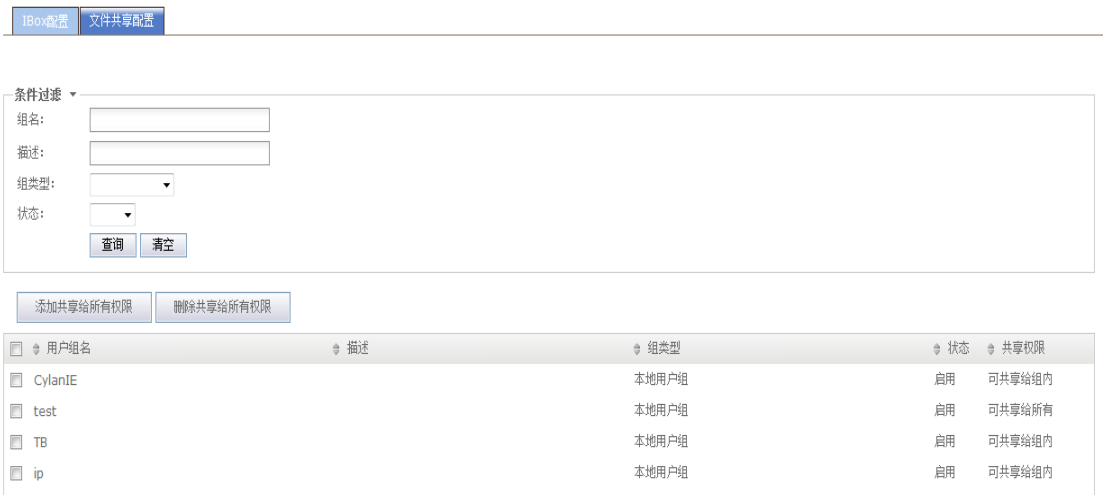
用户名：能访问到该服务器的用户

密码：能访问到该服务器的用户对应的密码

登录域：如果要登录该服务器的域则填写该服务器的登录域

状态：显示绿色字体已挂载则成功挂载了 ibox，红色字体未挂载则没有成功挂载 ibox。

文件共享配置列表可以将共享的文件添加到共享给其他组和组内的权限。共享给组内的文件，组内的用户可以互相查看。共享给所有的文件，其他组内的成员也能够查看。



以上信息配置好后，使用手机客户端登录前台地址， 比如以 ipad 为例，在服务器地址栏输入 cylansz.3322.org,用户名密码输入 demo/111111，点击登录按钮后进入资源列表，向左滑动到 ibox 页面，如下图所示：

注：如果在 SGA 移动云管理平台没有配置相应的信息，该手机客户端 ibox 页面将不会显示任何信息

2.2.4 图标管理

资源在前台显示的图标都可以由用户自己定制，然后在这个模块页面上传即可。配置应用的时候，选择相应的图标名称来对应各个应用。如下图所示：

注：请上传符合规定的图片大小和格式。

2.3 单点登录

2.3.1 模版配置

条件过滤，可针对已经发布的单点登录资源，根据名称，描述，状态进行单独、

组合、模糊、精确等查询。

注意：单点登录的使用是需要您本身能访问该单点登录所发布的资源的前提下使用的，即您要能通过自身网络，TCP 应用或者隧道应用下能访问到该资源，才能正常的使用单点登录打开您所要访问的系统。

添加/配置模板配置资源，点添加后，出现以下配置界面：

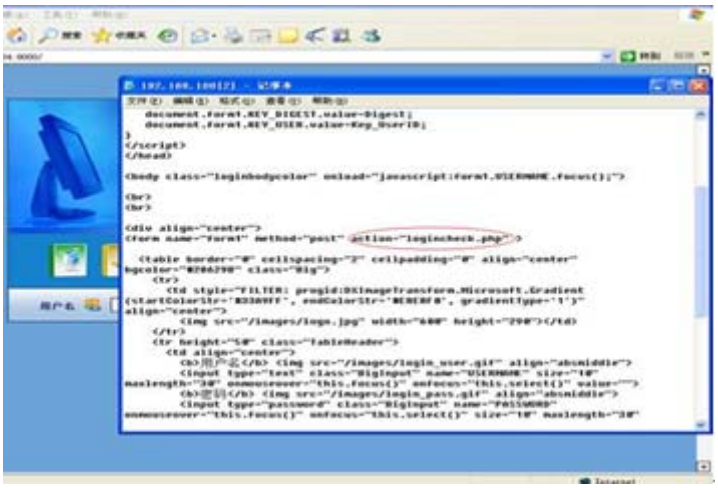
登录页模板选择“带附加码的登录页”，出现如下图所示页面：

资源名称：模板配置资源在系统和用户界面的显示名称。

描述：可为空。

是否启用：是否启用该模板配置资源。

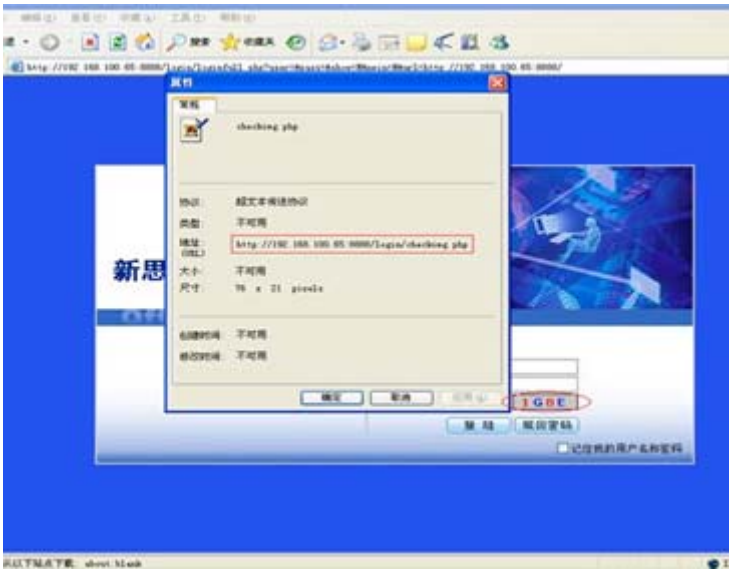
提交地址：以下图为例，右击登录页，选择查看源文件，在源文件里找到 action 所指向的页面名称，action 指向了 logincheck.php 页，所以提交地址填写：http://192.168.90.80/index.asp。



登录页模板：系统内置两个模板，一个是用户名密码登录页，一个是带附加码的登录页。如选择带附加码的登录页模板，下面会出来附加码图片地址项。

点击该项旁边的添加模板，出来以下界面：

附加码图片地址：获取方式如下图所示：右击附加码图片，选择属性，在地址一项中可获取附加码地址。



Charset：即登录界面的编码方式。可选择的方式有三种：GB2312，UTF-8，Big5。

提交方法：有两种：一种为 get，一种为 post，上面的为 post 方法。

提交参数：如果登录页面只有用户名和密码填写框，选择用户名密码登录页模板

用户标签处填写便于前台用户辨认和看到的标签名称，表单元素名为登录页源码文件中所有 input 开头的函数中对应的 name 字段中的名称。

默认值为所有用户登录该 OA 系统的默认账号等；用户可修改？下有 3 个选择项，分别是：可修改，必须修改，不可修改，通常登录页上需要用户填写或选择的为可修改或依据您的需求选择必须修改，附加码等系统自动产生的为必须修改。

密码字段：该选项可满足用户在前台重新配置页面录制用户名密码时，输入密码项不以明文显示出来。

注意：如果选择“必须修改”或“不可修改”项，前台用户在重新录制页面将看不到该项标签显示。

如复杂系统需要发布单点登录，请联系产品开发商的技术人员。

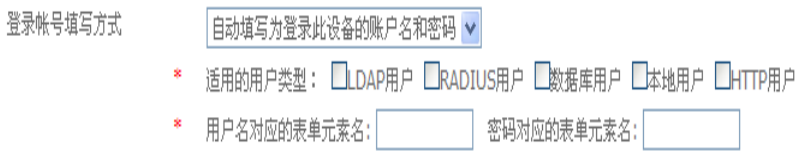
登录帐号填写方式：

该方式有三种：

1）用户首次访问之前预先设置。选择该项，前台用户第一次访问该助手单点登录资源，会弹出用户名密码等信息的录入页面，填写好后，下次再访问时，即

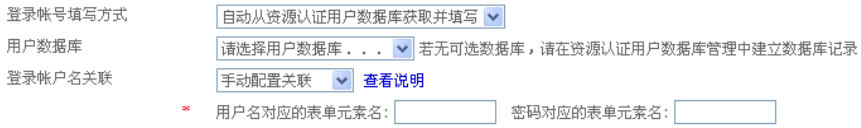
直接用第一次录入的信息登录发布的系统。

2）自动填写为登录此设备的账户名和密码。可复选适用这样使用的用户类型。如下图所示。



选择该项后，前台用户第一次访问该助手单点登录资源，会弹出录入信息框，但是用户不需要录入用户名密码，只需要录入其他信息即可，填写好后，下次在访问时，即直接用登录手机客户端的账户和密码来登录该单点登录资源系统。

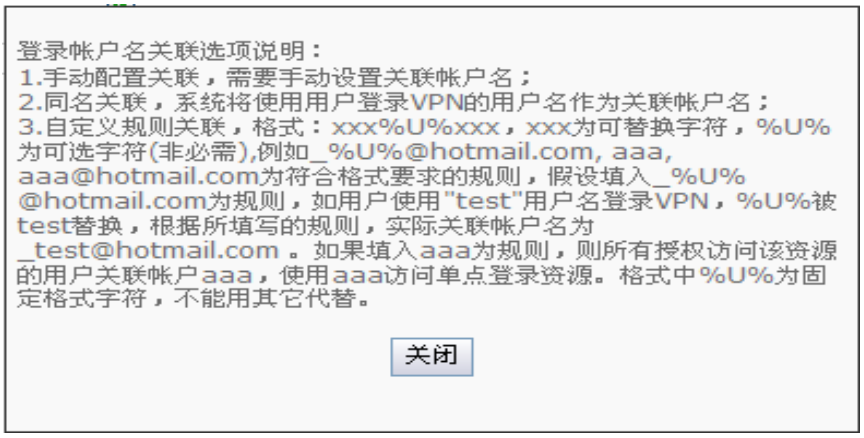
3）自动从资源认证用户数据库获取并填写。该功能可直接从第三方数据库中取账户密码作为单点登录资源的登录账户密码。如下图：该项要与下面将介绍的资源认证用户数据库和资源账户关联结合使用。



用户数据库：选择此处，需先在资源认证用户数据库模块先建立数据库资源。

登录账户名关联：包括手动配置关联，同名关联，自定义规则关联。可点击旁边的查看说明了解其使用。其中手动配置关联需要结合资源账户关联模块用。

点击查看说明，如下图：



图标：该资源在前台的显示图标。自定义图标可在应用发布——图标管理模块页面上传。

2.3.2 助手配置

助手单点登录通常可以应用于有登录界面简单的 WEB 系统(不支持有验证码的 web 系统认证等)，如简单的 OA，web 邮箱等，支持 C/S 与 B/S 的单点登录，如 C/S 架构的用友 U8，金蝶 KIS 等系统，B/S 架构的泛微 OA 以及邮箱等。使用之前先下载配置助手工具，来录制相关应用对应的 XML 文件。下载的助手工具中有详细说明。

添加/配置助手配置资源，点添加后，出现以下配置界面：

资源名称：助手配置资源在系统和用户界面的显示名称。

描述：可为空。

是否启用：是否启用该助手配置资源。

上传配置文件：浏览制作好的 XML 文件路径并选择此文件上传。

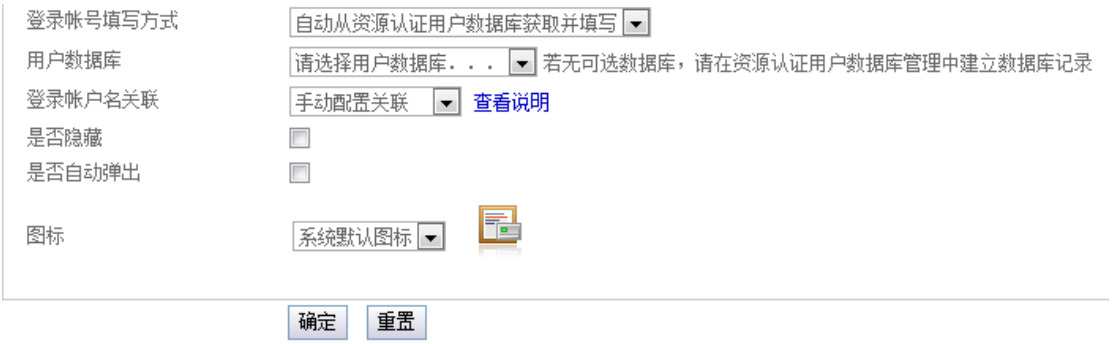
登录帐号填写方式：该方式有三种：

1）用户首次访问之前预先设置。选择该项，前台用户第一次访问该助手单点登录资源，会弹出用户名密码等信息的录入页面，填写好后，下次再访问时，即直接用第一次录入的信息登录发布的系统。

2）自动填写为登录此设备的账户名和密码。如下图：可复选适用这样使用的用户类型。

选择该项后，前台用户第一次访问该助手单点登录资源，会弹出录入信息框，但是用户不需要录入用户名密码，只需要录入其他信息即可，填写好后，下次在访问时，即直接用登录手机客户端的账户和密码来登录该单点登录资源系统。

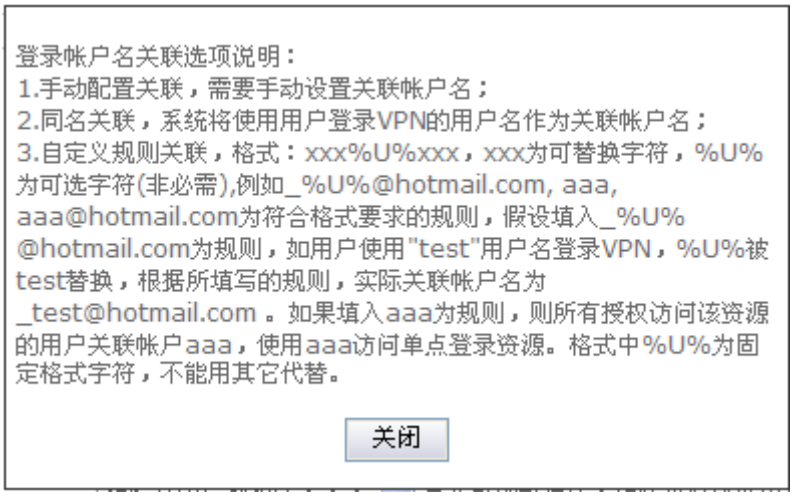
3）自动从资源认证用户数据库获取并填写。该功能可直接从第三方数据库中取账户密码作为单点登录资源的登录账户密码。如下图：该项要与下面将介绍的资源认证用户数据库和资源账户关联结合使用。



用户数据库：该处选择，需要先在资源认证用户数据库模块先建立数据库资源。

登录账户名关联：此处有三项选择：手动配置关联，同名关联，自定义规则关联。可查看旁边的说明链接了解其使用。其中手动配置关联需要结合资源账户关联模块使用。该关联配置是将要用在单点登录资源的数据库账户与 SGA 系统账户做关联。

点击查看说明，如下图：



图标：该资源在前台的显示图标。自定义图标可在应用发布----图标管理模块页面上传。

SSO 配置实现实例

以内网访问一个 OA 系统为例，进入单点登录——助手配置页面，点击添加，如下图：

点击上图中的添加，出来以下界面，在资源名称处填写助手单点登录资源前台显示名称，在上传配置文件处通过浏览按钮，选择用助手工具制作出来的 XML 文件路径，配置以上这些即可。其他配置项需要根据 web 系统的具体情况来配置。

提交后，将在助手配置页面出现一条新的记录：

发布的资源只对应相应的用户组，不对应单个的用户，用户要能访问到相应的资源，需要将用户先加入资源所在的用户组里才能访问到。

现在要用户 demo 能访问到上面配置的助手 SSO 资源，要先将单点登录工具录制的 XML 文件与该应用关联，如下图所示：

在关联 SSO 选项栏里选择录制的 XML 文件，提交后使用客户端登录，第一次登录 SSO 资源需要用户配置 SSO 信息，以 ipad 为例，如下图所示：

点确定之后显示设置以保存，如图所示：

下次使用 SSO 资源的时候，系统将自动为页面上的用户名和密码填写上然后登录。

2.3.2 资源认证用户数据库

点击添加按钮，进入以下界面：

名称：数据库服务器在系统中的标识名称。

描述：可为空。

是否启用：是否启用该数据库服务器资源。

类型：选择数据库的类型，有四种选择，分别是 MYSQL,Oracle,Sybase，Microsoft SQL Server。

IP 地址：数据库服务器的 ip 地址。

端口：数据库服务器的端口，MYSQL 默认端口是 3306,Oracle 默认端口是 1521,Sybase 默认端口是 5000，Microsoft SQL Server 端口 1433。

登录名：连接数据库的帐号。

登录密码：连接数据库的密码。

库名：要连接的数据库库名。

表名：要连接的数据库表名。

用户名字段：用户名在数据库中的字段名。

密码字段：密码在数据库中的字段名。

2.3.3 资源账户关联

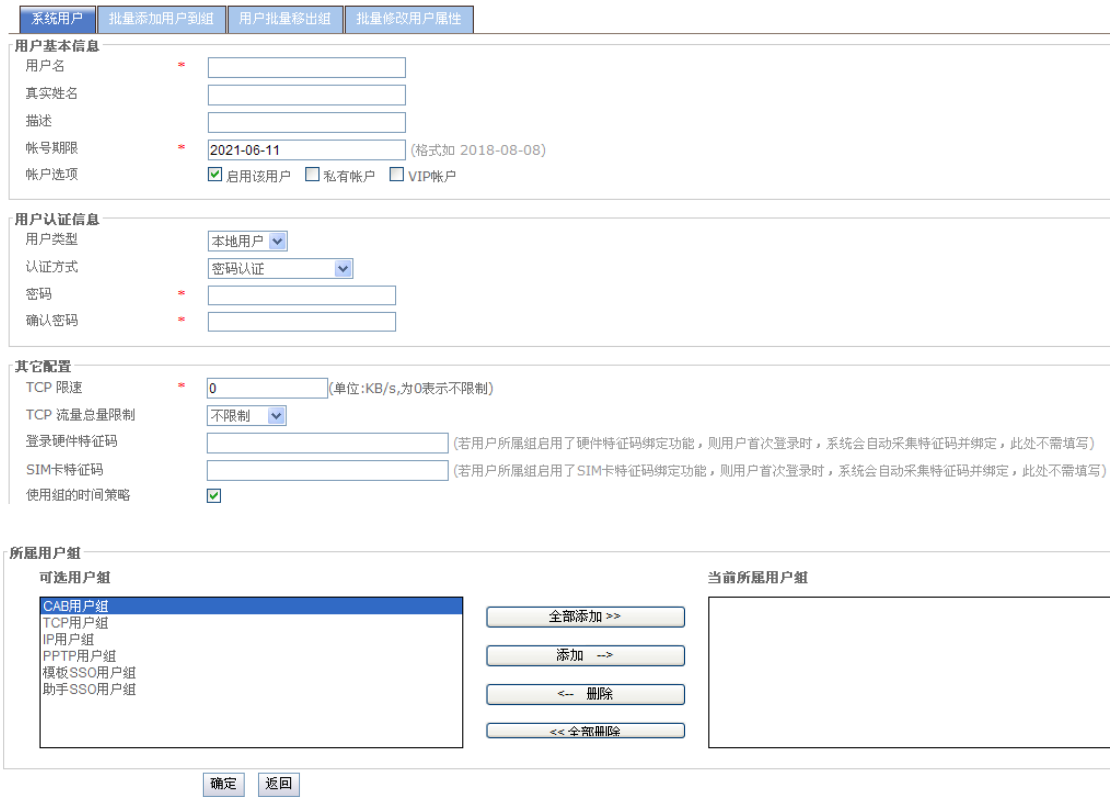
如有单点登录资源配置了自动从资源认证用户数据库获取并填写项，并且选择手动配置关联，则需要配置该功能模块。该关联配置是将要用在单点登录资源的数据库账户与 SGA 系统账户做关联。

2.4 用户管理

2.4.1 系统用户

条件过滤，可针对已经存在的系统用户，根据名称，所属用户组，用户类型，认证类型，真实姓名，描述，证书序列号，VIP 账户，状态进行单独、组合、模糊、精确等查询。

点击添加，出来以下界面：



用户名：用户登录前台的登录名称。

真实姓名：可为空。

E-Mail：该项需要在认证管理---认证策略下，勾选启用邮箱认证服务才会出现。该功能详细介绍请参加附录。

描述：可为空

账号期限：账号可以使用的有效年限。默认是当前时间+10 年，用户在该期限内可以正常使用，超过该期限，帐号为过期状态，用户无法用该帐号登录。请在系统管理－－时间设置里把时间设置准确。

账户选项：勾选“启用该用户”，该帐号为启用状态，可以正常使用，没有勾选“启用该用户”，该帐号为禁用状态，用户无法使用该帐号登录。

勾选“私有账户”，即同一时间，该账户只能一个用户登录。

勾选“VIP 账户”，即该用户不受组和站点的最大登录数限制。

匿名账户选项需要在认证管理---认证策略下，勾选匿名访问策略项才会出

现。该功能详细介绍请参加附录。

用户类型：该处能选择的用户类型共有 7 个，除本地用户外，其余类型需要勾选认证管理——认证策略下的相关认证服务才会出现。在此出现的 6 种用户类型有：本地用户，LDAP 用户，RADIUS 用户，数据库用户，指纹认证用户，HTTP 用户，本地令牌认证。

认证方式：5 种认证方式，分别是：密码认证，密码和证书认证，证书绑定认证，密码或证书绑定认证，密码和证书绑定认证。

密码认证：该用户使用其用户名和密码进入前台。

密码和证书认证：用户不但需要用户名和密码进行验证，还需要带上能通过 SSL 系统里的 CA 根证验证的用户证书，该用户才可以进入前台。

注：该证书只要 CA 能认到，就可以，不需要绑定在用户配置里。

证书绑定认证：该用户使用给其绑定的证书进入前台。

密码或证书绑定认证：该用户既可以使用他的用户名和密码进入前台，也可以使用给他绑定的证书进入前台。

密码和证书绑定认证：该用户不但需要用户名和密码进行验证，还需要带上给他绑定的证书进入前台。

注：该用户的用户名密码和该证书绑定认证，缺一不可。

辅助认证方式：此项需要在认证管理——认证策略下，勾选您需要的辅助认证策略才会出现，并且辅助认证策略只能同时选择一个，只有 Ukey 认证和短信认证勾选后才会出现。令牌认证勾选后会出现在认证管理模块下面。

其它配置：

TCP 限速：该功能可限制该用户每次登录手机客户端资源访问页面使用隧道的流量，仅限 TCP 协议流量。(单位:KB/s,为 0 表示不限制)

TCP 流量总量限制：该功能项可按照每日，每周，每月来限制该用户使用隧道的总 TCP 协议流量。

登录硬件特征码：如果用户所属组勾选使用机器码绑定策略，则用户首次登录时，系统会自动采集用户手持终端上的 CPU，网卡等信息来生成唯一标识该电脑的特征码并自动绑定。绑定后，只有这个特征码对应的手持终端才能使用这个账户进行登录。

SIM 卡特征码：如果用户所属组勾选使用 SIM 卡绑定策略，则用户首次登录时，系统会自动采集智能手持终端的 SIM 信息并自动绑定。绑定后，只有这个特征码对应的手持终端才能使用这个账户进行登录。

该功能使用说明：第一次配置时，管理员只需把绑定硬件特征码的勾上即可。用户在第一次成功登录后，SGA 设备会对应登录的用户记录下第一个使用该账户登录电脑的特征码信息到缓存区，如果需要永久的绑定该电脑，还需要在其他设备用该账户登录前再成功登录一次。

使用组的时间策略：勾选此项后，该用户的登录时间将采用他所在组的时间登录所属站点。如果该用户加入了多个组，时间策略为所有组时间叠加后的时间。

自定义开放时间：如果勾选上面的“使用组的时间策略”，该项将消失，反之，用户将使用自己的时间策略登录所属站点。

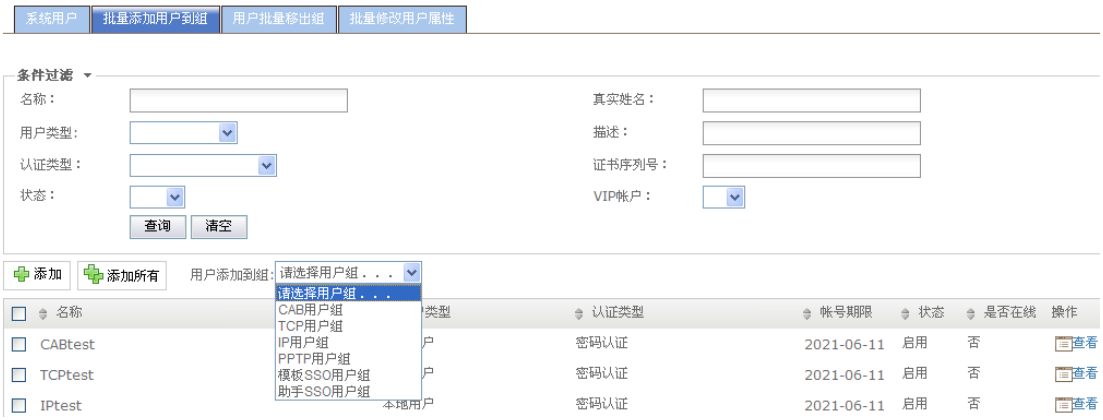
所属用户组：选择用户所在的用户组。如果用户所在的用户组被禁用了，则用户登录到前台，将无法看见和使用该用户组的任何资源。

添加系统用户成功后可以如下所示：（以添加 CABTest 用户为例）

可在上图所示页面对 CABtest 账户进行编辑，查看，删除等操作。登录记录按钮。可查看账户 CABtest 最近 5 次的登录记录，CAB 账户按钮可为 CABtest 账户绑定属于它的 CAB 资源自动登录账户，前提是需要 CABtest 账户下有可以访问的 CAB 资源。

批量添加用户到组选项，如下图。

在这里，可以批量添加已有用户到特定组。



用户批量移出组选项卡如下图所示：

选择当前用户组，在下面列表会出现该组里面的所有用户，这时你可对该组的用户进行查看和删除动作。

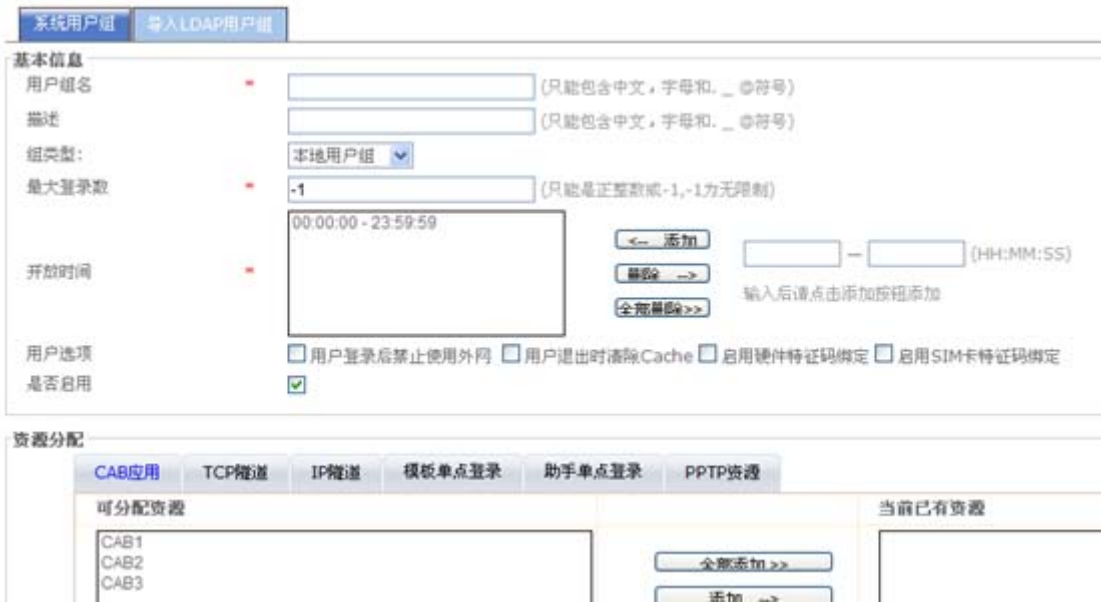
批量修改用户属性选项卡如下图所示。

在这里，可以批量修改用户的账号期限，启用账户选项，私有账户选项，TCP 限速设置，TCP 流量总量限制，清除已绑定硬件特征码或手持终端 SIM 卡特征码。

2.4.2 系统用户组

条件过滤，可针对已经有的用户组，根据组名，描述，组类型，状态进行单独、组合、模糊、精确等查询。

点击添加，出来以下界面：



用户组名：在系统里显示的用户组的名称。

描述：可为空。

组类型：该处能选择的组类型共有 3 个，除本地用户组外，其余类型需要勾选认证管理——认证策略下的相关认证服务才会出现。在此出现的 3 种用户类型有：本地用户组，LDAP 用户组，HTTP 用户组。

最大登录数：限制该组同时在线的用户数。-1 为无限制。该项设置受系统本身的用户许可数和站点最大登录数的限制，即系统本身用户许可数优先级大于站点最大登录数，站点最大登录数优先级大于用户组的最大登录数。

开放时间：限制该组一天内能正常访问的时间段，默认是全天任何时间。原则上，用户开放时间范围应该在用户组的开放时间之内。

用户选项：主要用来配置用户组中用户的登录策略，包含四个选项，即用户登录后禁止使用外网，用户退出时清除 Cache，启用硬件特征码绑定，启用 SIM 卡特征码绑定。

是否启用：是否启用该组。

资源分配：分配该组能访问的应用资源。

添加系统用户组成功后可以如下所示：（以添加 CAB 用户组为例）

可在上图中对 CAB 用户组做编辑，查看，删除操作。

2.4.3 导入/导出用户

该功能模块可从第三方数据库，LDAP 服务器及文本文件中批量导入用户到 SGA 系统用户中，同样也可以将 SGA 中的系统用户导出到文本文件，并批量更新

用户的配置信息。

该模块包括四个选项卡：从数据库导入，从 LDAP 服务器导入，导入文件，导出/更新。

从数据库导入页面如下图：

选择数据库：有新建数据库连接和已有数据库连接可选择。选择已有数据库连接需要首先在认证管理——认证策略下，勾选启用数据库认证服务，然后在认证管理——数据库认证模块中配置好相关数据库信息（具体配置请参照下面介绍的数据库认证页面配置说明）。这时再到从数据库导入页面选项卡选择已有数据库连接，即可看到在数据库认证页面配置好的数据库。

SGA 系统暂时只支持 MYSQL，Oracle，Sybase 和 Microsoft SQL Server 四种数据库的用户导入。

点击从数据库导入选项卡，配置相关选项。以下我们以新建数据库连接为例：

上图中选择新建数据库连接，然后数据库项再选择 Microsoft SQL Server，配置好相关信息后，可点击测试连接按钮检查数据库是否可以正常连接上，如下图：

点击下一步进入下个阶段，如下图：

上图中，用户名对应字段和密码对应字段项中，会出现数据库表里面的所有

字段选项，你只需把数据库中的字段名与系统用户的字段名做个对应即可导入你想要的用户信息。

可以根据用户实际需求可以选择使用证书认证，导入真实姓名，证书序列号等，其他不需要导入项配置好后，所有用户将使用相同的配置。

在导入第三方数据库用户时，还可以字段名对用户表中的用户进行筛选导入。

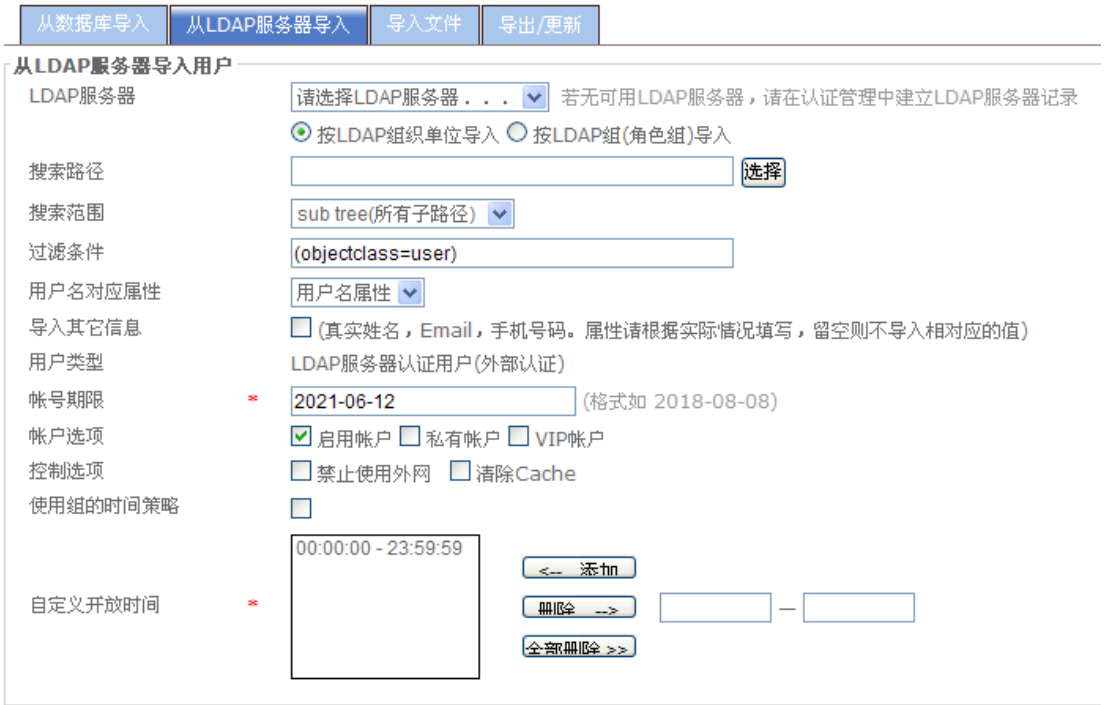
从 LDAP 服务器导入页面如下图：

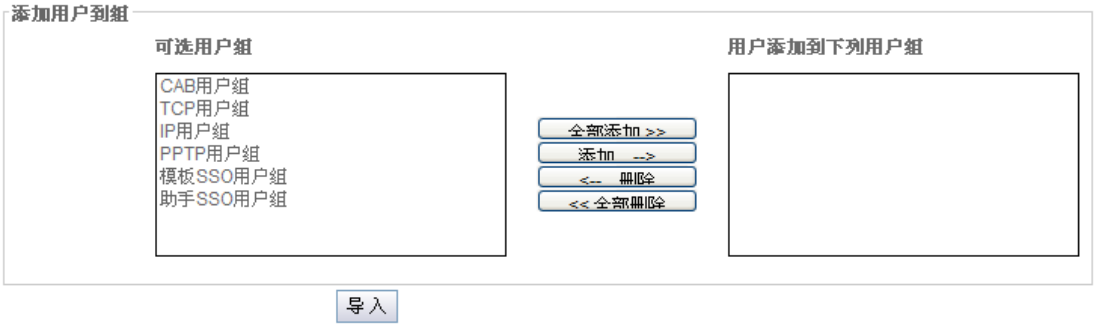
要使用此功能，首先需要在认证管理——认证策略中，勾选启用 LDAP 服务器认证，然后在认证管理——LDAP 认证模块页面中配置好 LDAP 服务器资源。

做好以上配置后，可进入从 LDAP 服务器导入选项卡，在 LDAP 服务器项选择你要导入的 LDAP 服务器。按照要求配置下面各项。

其中搜索路径项，可以按照你选择的按 LDAP 组织单位导入还是按 LDAP 角色组导入。

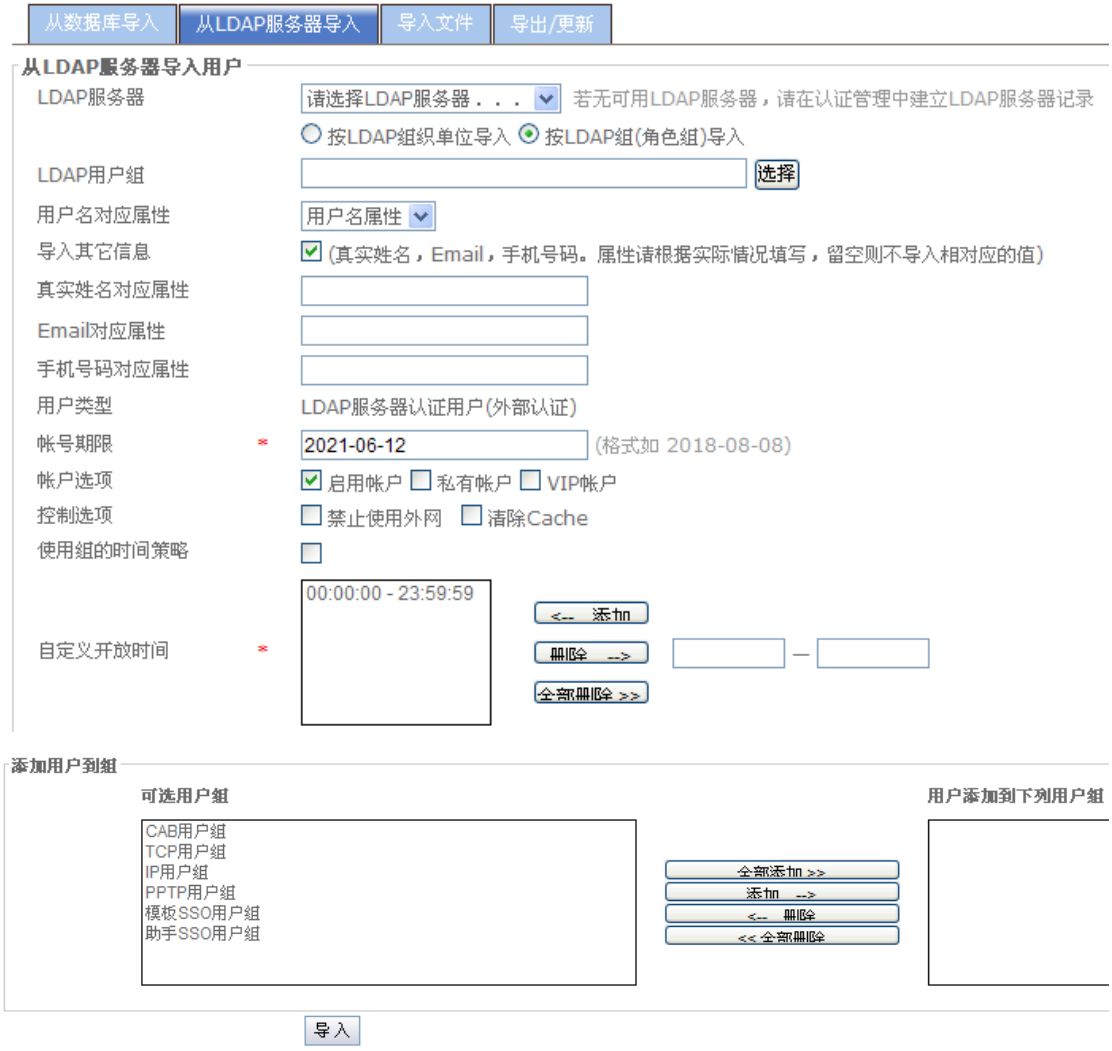
如果选按 LDAP 组织单位导入，如下图所示。点击选择按钮自动搜索，并可在搜索完毕后的弹出框中自行选择后自动填入。





按照以上要求进行配置后，点击导入即可。

如果选择按 LDAP 组（角色组）导入，如下图所示。点击选择按钮自动搜索，并可在搜索完毕后的弹出框中自行选择后自动填入。



用户名对应属性：可选择用户名属性或登录名属性。

配置完对应信息，点导入即可。

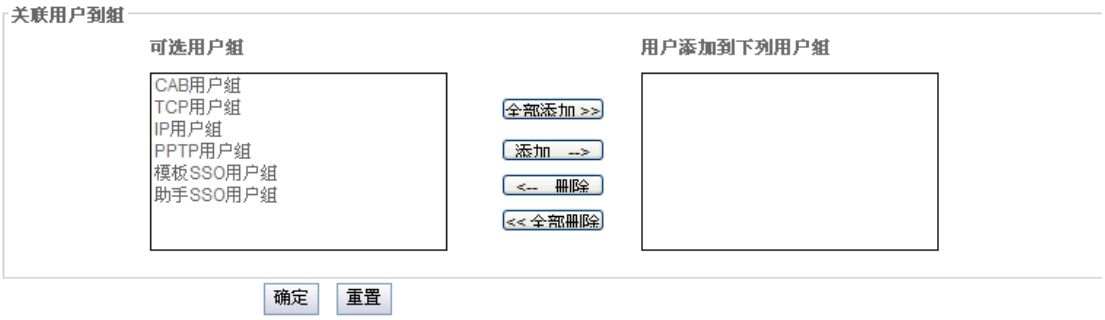
如果使用的数据库不在 SGA 支持范围内，或者第三方存储用户系统不在 SGA 支持访问内，可使用文本文件导入方式来批量导入用户信息，你只需要在其他系统中将用户信息导出成文本文件格式，或者手工编辑用户信息到文本文件格式即可。

导入文件选项卡页面如下图：

在导入的文本文件中，每个字段数据以列的形式排列，文本中列与列之间以英文半角逗号(,)隔开，逗号前后不要有空格，注意：若包含中文需把文本文件另存为 UTF-8 编码格式。可导入用户名，密码，真实姓名，证书序列号，描述，手机号码，email 七个字段。

注意：导入文本文件需至少包含用户名、密码，或用户名、证书序列号。如果你导入的某个唯一属性（如用户名，证书序列号等）已经在 SSL 设备中存在了，该条已经存在的信息将无法导入，并且返回错误提示，但是其他正确的信息仍然可以被导入。

点击浏览按钮选择对应文本文件后，点击下一步进入下图所示页面：



以上按照需求都配置确认好后，点确定即可导入文本文件中的用户信息。

导出/更新选项卡页面如下图所示：

如果要将系统用户都导出到文本文件，可在导出用户项中，右击下载地址链接，选择目标另存为即可（建议使用目标另存为保存是为了保留原格式，防止其他格式的文本文件在导入时出错）。导入的格式是按照 SGA 内定的格式编排的，如没必要，不建议用户改动格式，因为要使用设备的文件导入更新用户功能，只支持设备本身导出格式的文件导入。

只是批量修改用户信息的某项值时，可在该页导出的文本文件中直接改相应的值内容，然后保存，再在该页面中导入即可。

2.4.4 管理员账户

条件过滤，可针对已经创建的管理员，根据名称，描述，管理员类型，状态进行单独、组合、模糊、精确等查询。

添加/配置系统管理员，点添加后，出现以下配置界面。

名称：管理员登录后台的登录名称。

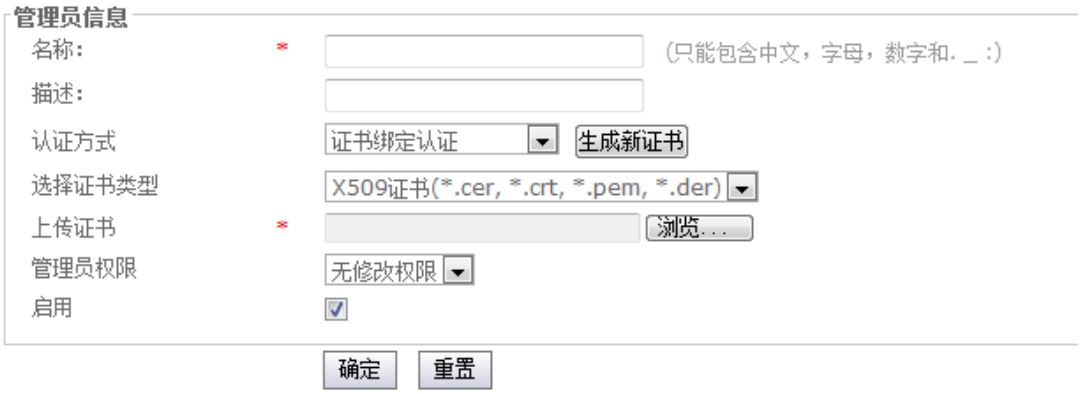
描述：可为空。

认证方式：5 种认证方式，分别是：密码认证，密码和证书认证，证书绑定认证，密码或证书绑定认证，密码和证书绑定认证。

密码认证：该管理员使用他的用户名和密码进入后台。

密码和证书认证：管理员不但需要用户名和密码进行验证，还需要带上能通过 SGA 系统里的 CA 根证验证的用户证书，该管理员才可以进入后台。注：该证书只要 CA 能认到，就可以，不需要绑定在用户配置里。

证书绑定认证：该管理员使用给他绑定的证书进入后台。如下图所示，需要选择证书类型和上传证书。



密码或证书绑定认证：该管理员既可以使用他的用户名和密码进入后台，也可以使用给他绑定的证书进入后台。如下图所示：

密码和证书绑定认证：该管理员不但需要用户名和密码进行验证，还需要带上给他绑定的证书进入后台。注：该管理员用户名密码和该证书绑定认证，缺一不可。

选择证书类型：证书类型分 X509 证书和 P12 证书，根据用户需求进行选择。

上传证书，私钥保护口令：上传相应的用户证书，如果证书类型选择的是 P12 格式，则还需要输入用户证书相应的私钥保护口令，无口令可不输。

如在认证管理——认证策略中，勾选了辅助认证策略中的使用 UKey 认证，则该页面还会多出辅助认证方式项。

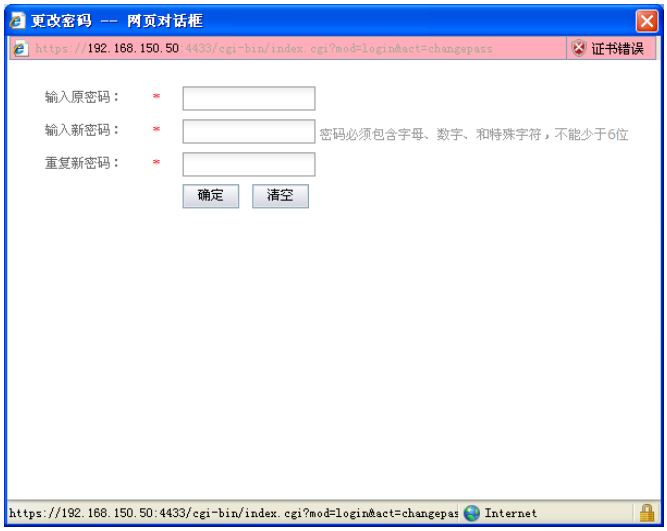
管理员权限：管理员权限分为可修改配置和无修改权限。当选择可修改配置

时，会出现可见菜单配置页面。如下图所示。

如果指定管理员只可操作网络配置相关信息。如下图所示：

启用：是否启用该管理员账户。

此外，点击页面右上角的更改密码（出现下图所示），也可以对管理员用户的密码进行修改。



2.5 认证管理

2.5.1 认证策略

认证策略模块页面如下图所示：

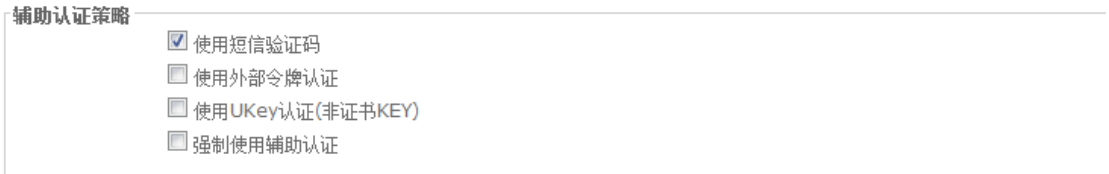
辅助认证策略：

此项可于下面三项中的任意一项复选，勾选此项后，前台登录认证方式只能是下面勾选的三项辅助认证方式之一。

强制使用辅助认证：勾选此项，在登录到 SGA 移动云平台时，则必须经过辅助认证才能登录。

使用短信验证码

在认证管理——认证策略里面，辅助认证策略下勾选“使用短信验证码（启用后 SSL 将不能使用串口进行配置）”，如下图所示：可由用户自定义短信提示的内容，内容为空则发送的短信中只有 6 位数字验证码。



勾选了使用短信验证码后，在用户管理----系统用户配置页面将会过出来手机号码配置项，如下图：

把上图系统用户配置页面的必填项填写完提交后，并填写上手机号码，确定提交后，该用户账户选项——私有账户的勾会自动勾上，即有短信认证的账户同一时间只能登录一个。

使用该用户登录前台，在手机客户端输入用户名和密码后，会弹出要求获取和填写短信密码的界面，以 iphone 为了，如下图所示。

这时会有一条关于验证码的短信息发送到该用户对应的手机上，在短信密码框中输入您收到的短信验证码，点确定便可正常登录到前台资源访问页面进行操作。

注意：如果您在 20 分钟内没有输入短信密码登录，系统将自动回到登录页面，用户必须重新登录，重新获取短信密码。如果 60 秒内未收到短信，可重新点击获取短信密码按钮。

使用外部令牌认证：勾选此项后，在认证管理下会出现外部令牌认证模块。在外部令牌认证配置页面配置好后，前台用户可使用外部令牌认证登录。

使用 UKey 认证：勾选此项后，在用户管理---系统用户配置界面可以出现相关配置项。有配置该认证方式的用户，需要用该认证方式进行认证。这里的 UKey 不是证书 KEY，而是一种密码 KEY。

用户锁定策略：

该项可设置账户在多少时间连续错误登录多少次后会被锁定。

解锁策略有超时解锁，并设置锁定时间，还有管理员解锁。

管理员解锁如下图所示：

如果有使用 E-Mail 地址登录错误被锁定的邮箱账户，也可勾选最下面项，同时把邮箱账户对应的系统用户一起锁定。

认证服务配置：

启用 LDAP 认证服务：

在管理后台显示该模块，需要在认证管理——认证策略中，勾选启用 LDAP 认证服务。

添加/配置 ldap 服务器。点添加后，出现以下配置界面：

服务器名：ldap 服务器在系统中的标识名称。

描述：可为空。

是否启用：是否启用该 ldap 认证服务器资源。

服务器 IP 地址：ldap 服务器的 IP 地址。

服务器端口：ldap 服务的端口号，默认为 389。

匿名绑定：勾选此项，可不用配置后面的用户名，密码，前提是 LDAP 服务

器支持匿名搜索目录。

用户名，密码，确认密码：连接 ldap 服务器的账户/密码，建议使用管理员帐号。

Ldap 服务器类型：提供 WINDOWS 域服务器和普通 LDAP 服务器两项选择。

Ldap 协议版本：支持版本 2 和版本 3。

根 DN：当配置好以上项目之后，确认 ldap 服务器也正常，即可点击“获取”按钮，如果能获取到根 DN，即绑定 ldap 服务器成功，用户可根据需要选择一个合适的根 DN；如果不成功，会弹出不成功的提示框，并提醒用户可能造成绑定不成功的原因。也可以自己手工填写根 DN。

用户名属性，登录名属性，组名属性，用户属组属性，组属用户属性：如果你是 WINDOWS 域服务器，这些信息默认即可；如果是其他 ldap 服务器，可按实际情况进行配置。

筛选条件：用户可根据自己的要求填写过滤字段信息。

密码 MD5 加密：对相应用户密码启用 MD5 加密，防止破解。

认证测试：LDAP 用户名和密码认证测试，并提供相应验证结果。

提交 LDAP 资源后，会在用户管理——系统用户里面多出一条 LDAP 认证默认用户，如下图：

有了这个用户，可以针对 LDAP 用户加入系统用户组，以及一些用户的基本配置，并且 LDAP 服务器上的账户可以正常登录到手机客户端。

启用 RADIUS 认证服务：

要在管理后台显示该模块，需要在认证管理——认证策略中，勾选启用 RADIUS 认证服务。

添加/配置 RADIUS 服务器。点添加后，出现以下配置界面：

名称：Radius 服务器在系统中的标识名称。

描述：可为空。

启用：是否启用该 Radius 认证服务器资源。

服务器地址：Radius 服务器的 IP 地址。

服务器端口：Radius 服务的端口号，默认为 1812。

共享密钥：连接 Radius 服务器的密码。

NAS-IP-ADDRESS（本端 IP 地址）：SSL 和 Radius 服务器通讯的地址。

CALLING-STATION-ID（本端 ID）：本端地址的 ID 号，默认 1115551212。

认证测试：Radius 用户名和密码认证测试，并提供相应验证结果。

提交RADIUS资源后,会在用户管理系统用户里面多出一条RADIUS默认用户，如下图：

可以针对 RADIUS 用户加入系统用户组，以及一些用户的基本配置，并且RADIUS 服务器上的账户可以正常登录到手机客户端。

启用 HTTP 认证服务：

在管理后台显示该模块，需要在认证管理——认证策略中，勾选启用 HTTP 认证服务。

添加/配置 HTTP 服务器。点击添加按钮，出现如下配置界面：

提交HTTP 资源后，会在用户管理——系统用户里面多出一条HTTP 默认用户，如下图：

可以针对 HTTP 用户加入系统用户组，以及进行一些用户的基本配置，并且 HTTP 认证账户可以正常登录到手机客户端。

启用数据库认证服务：

要在管理后台显示该模块，需要在认证管理——认证策略中，勾选启用数据库认证服务。

添加/配置数据库服务器。点击添加按钮，出现如下配置界面：

服务器名：数据库服务器在系统中的标识名称。

描述：可为空。

是否启用：是否启用该数据库服务器资源。

数据库类型：可以有四种选择类型，分别是 MYSQL,Oracle,Sybase，Microsoft SQL Server。

IP 地址：数据库服务器的 IP 地址。

端口：数据库服务器的端口，MYSQL 默认端口是 3306，Oracle 默认端口是 1521，Sybase 默认端口是 5000，Microsoft SQL Server 端口 1433。

登录名：连接数据库的帐号。

登录密码：连接数据库的密码。

库名：要连接的数据库库名。

表名：要连接的数据库表名。

用户名字段：用户名在数据库中的字段名。

密码字段：密码在数据库中的字段名。

密码加密方法：有不加密，PASSWORD，MD5，SHA5，ENCRYPT 加密方法可以选择。

提交数据库资源后，会在用户管理——系统用户里面多出一条数据库默认用户，如下图：

有了这个用户，可以针对数据库用户加入系统用户组，以及一些用户的基本配置，并且数据库服务器上的账户可以正常登录到手机客户端。

启用邮箱认证服务：

启用该项后，会在认证管理模块下出现邮箱认证子模块，然后进入认证管理——认证配置界面，如下图：

添加/配置邮箱服务器。点击添加按钮，出现如下配置界面：以 163 邮箱为例。

确定提交后，即邮箱服务器配置好了，还需要将某个用户的 163 邮箱对应某个系统用户，启用该功能后，会在系统用户——用户界面多出一项 E-Mail 的配置项，如下图：将 cylantest@163.com 邮箱对应到 test 用户的 E-Mail 项中：

这时可以在手机客户端使用 cylantest@163.com 账户，密码为登录这个邮箱的密码来登录手机客户端了。

启用统一认证服务：

要在管理后台显示该模块，需要在认证管理——认证策略中，勾选启用统一认证服务。

添加/配置统一服务器。点击添加按钮，出现如下配置界面：

提交统一认证资源后，会在用户管理——系统用户里面多出一条统一认证默认用户，如下图：

可以针对统一用户加入系统用户组，以及一些用户的基本配置，并且统一认证服务器上的账户可以正常登录到手机客户端。

启用本地令牌认证：

启用该项后，会在认证管理模块下出现本地令牌认证子模块， 登录管理后台，点击认证管理---本地令牌认证---添加----令牌 SN----令牌 SN 信息--确定。配置方法如下图所示：

令牌 SN：动态口令牌唯一硬件 ID 号，如下图所示

令牌 SN 信息：根据令牌 ID 号可向赛蓝索取对应 SN 信息。令牌 SN 信息和 ID 号对应格式

797054471
SS000060797054471E28D1E87284765036139998661 39FD621F1ED0882F680E3D56A0A2364EFED8C7D4262688C509FEF8534B4FC4F1A2FE5593AF29C1686D5E1E451CA1735FF1E1876B0A958608D02800FEDB69494CAFBF8925C99E25C7986A550E85EAEFBB7B12890E85EAEFBB7B12890E85EAEFBB7B12890E85EAEFBB7B12890E85EAEFBB7B1289==

添加令牌账号完成后，测试同步令牌时间。

点击同步令牌时间，填入对应的口令后点击确定，提示同步成功说明配置正确。

令牌口令如下图所示：

建立账号使用本地令牌登录：用户管理--系统用户—添加，如下图所示

用户添加完成后，可在认证管理—本地令牌认证处查看账号关联信息，如下图所示

用户可通过账号：demo, 密码：动态口令牌得数字，登录访问用户所在组的资源，

注：动态令牌口令变更频率为 1 分钟/次。

启用 OTP 令牌认证：

启用该项后，会在手机客户端上开启手机令牌的功能。下面以 Cylan 公司为中国电信定制的 android 客户端手机令牌为例，首先在系统用户配置页面-用户类型选择 OTP 令牌认证用户如下图所示：

点击确定之后，在手机令牌服务器处填写 192.168.110.90，用户名 otp，密码 111111，该密码在激活绑定之后就失效，如下图所示：

点击激活绑定之后，就需要生成动态密码，使用生成的动态密码登录服务器，如下图所示：

注：生成的动态密码只能使用一下，下次登录需要再次生成动态密码

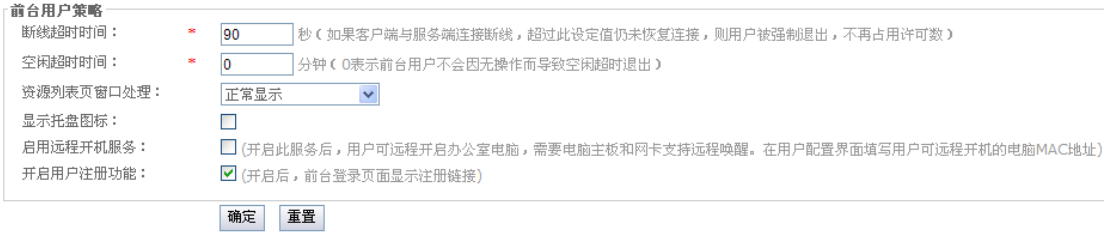
双用户名密码认证：

即用户采用双因素认证方式，勾选认证服务配置中相应认证服务，相应认证方法即会出现在认证方式中，用户可以根据需求自己选择。当使用这种方式时，

用户使用第一种认证方式分配资源使用权限。

2.5.2 前台策略

前台用户策略模块目前手机客户端支持远程开机服务的功能。如下图所示。



启用远程开机服务：开启此服务后，用户可远程开启办公室电脑，需要电脑主板和网卡支持远程唤醒。在用户配置界面填写用户可远程开机的电脑 MAC 地址)。

2.6 登录信息

2.6.1 在线用户

条件过滤，可根据用户名称精确和模糊查询下面已登录用户列表中您需要查询的用户信息。

该页会显示已经登录前台用户的信息和数量，并且可以由管理员强制断开某个在线用户或全部在线用户。

2.6.2 用户登录记录

可查看所有登录过的用户的登录信息，如登录名称，用户类型，最后登录 IP，最后登录时间，最后退出时间，登录次数等，还可以点击对应用户后面的查看按钮，查看对应用户最近 5 次的登录记录。也可对用户登录记录进行删除操作。

2.6.3 在线管理员

该页面可查看正在登录系统的系统管理员和站点管理员登录的信息，如管理员名称，类型，所属站点，登录时间和登录 IP。

2.7 证书中心

2.7.1 CA 配置

出厂时，SGA 设备上有一套自建的证书文件，包括 CA 根证，服务器证书，证书销毁列表，可进入 CA 配置页面查看证书的信息，如下图：用户可以不修改此证书，直接使用。设备支持多 CA 认证（三个 CA），还可以在此配置其它 CA 信息。

注：手机客户端目前只支持自建证书用户登录

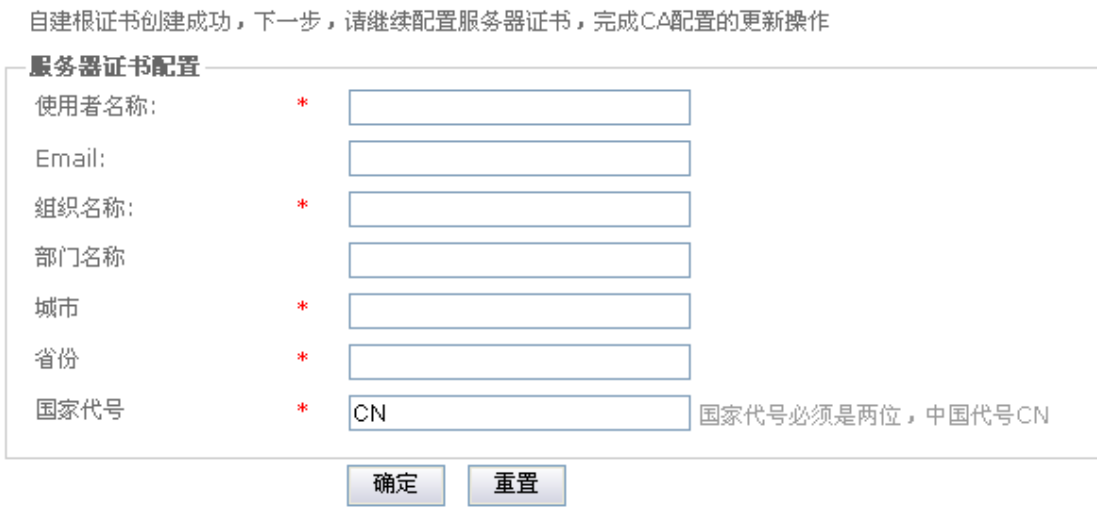
用户如果要修改证书，可点击“更新 CA 配置”，进入以下界面：

注意：在配置证书的时候，请务必现在系统管理——系统配置——时间设置里，将时间设置准确。

证书创建方式分两种：一、自建证书，二、导入第三方签发的证书。

我们选择自建证书，用户只要填写好下面的信息，点提交，SGA 系统便可根据您提交的信息生成 CA 根证书。

CA 根证书生成后，会自动跳转到服务器证书的生成界面，如下图：



用户填写好需要填写的信息，确定后，将会自动重启系统服务，用户可刷新 SGA 页面重新回到 CA 配置页面，可查看到您刚才生成的证书信息，自建证书的生成将会自动为 CA 根证生成证书销毁列表。

注意：自建 CA 和自建服务器证书必须一气呵成，该次自建证书的生成才会有效。

如果用户有自己的一套证书，也可以在 SGA 系统上导入自己的证书，选择导入第三方签发的证书出现以下界面：

系统支持 X509，P12，P7B 格式的根证书的导入，注意：根证书只有导入私钥文件，才能在 SGA 系统里面的证书生成页面生成用户证书。如果不需要通过 SGA 系统生成、签发与导入 CA 根证匹配的用户证书，可不导入根证书的私钥。

服务器证书的导入支持 X509 和 P12 格式，服务器证书可不导入。需要注意的是：服务器证书一定要是上面导入根证书签发的。特别注意：服务器私钥文件不支持 WINDOWS 系统证书机构下生成的.pvk 格式的文件，您可以在 WINDOWS 系统证书机构生成一个 P12 格式的服务器证书导入到 SGA 系统里面。如果是 WINDOWS 下生成的服务器证书，请在生成证书的时候，选择类型为“服务器证书”，客户端证书类型是不能在此作为服务器证书导入的。

证书销毁列表配置处可不做配置，如果用户需要导入证书销毁列表，需要注意的是：该证书销毁列表一定要与上面导入的服务器证书和 CA 根证书相匹配，

并且证书销毁列表的生成时间不能过期，否则 SGA 系统将会提示导入第三方证书不成功。

如果用户导入的根证书是带私钥的，提交后，SGA 系统会系统为该 CA 根证书生成证书销毁列表。

如果是 JKS 格式的私钥，请参照以下链接的文档说明，将它转换为 PEM 格式的私钥：

http://developers.sun.com.cn/Java/using_ssl_with_glassfish_v2.html

2.7.2 生成证书

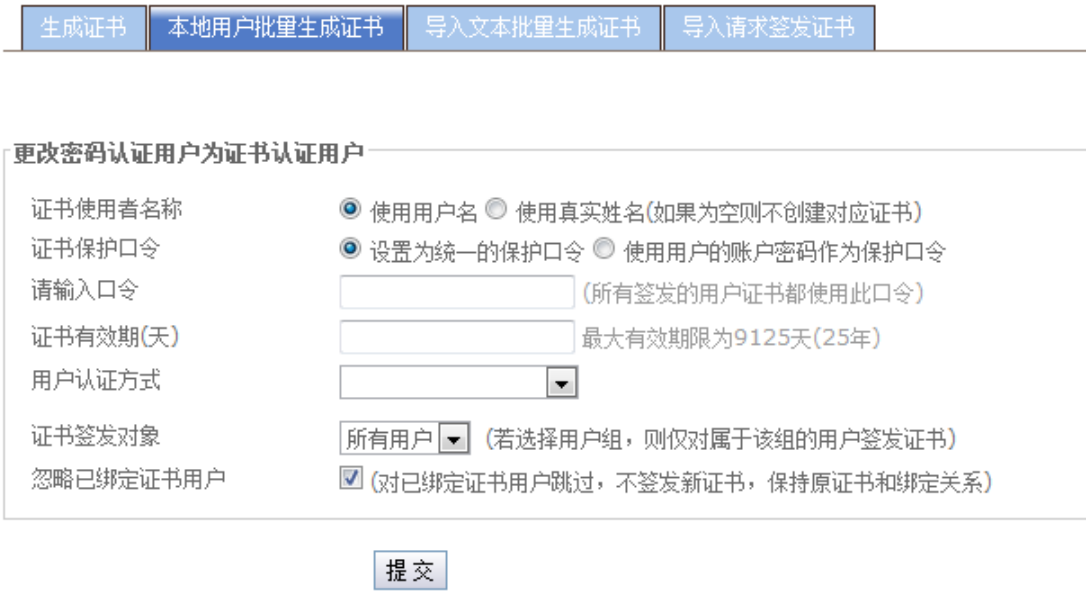
支持本地生成证书，本地用户批量生成证书，导入文本批量生成证书，导入请求签发文件生成证书。

如果使用的是 SGA 自建证书或者您导入了带私钥的第三方 CA 根证书，则代表 SGA 系统可以签发用户证书。在导入请求签发证书选项卡中，我们可以导入证书请求工具生成的证书请求文件，来为用户签发不带私钥的用户证书。

生成证书选项卡如下图所示：

如果是 SGA 系统自建证书，或者导入的第三方 CA 根证书带私钥，管理员可通过证书生成页面，直接在 SGA 系统里面生成和签发用户证书，填写好下面信息后，点提交，将会出来用户证书下载页面，管理员可以通过下载下来的证书在 SGA 系统里面配置绑定证书用户，并把该用户证书发放给最终用户。

本地用户批量生成证书如下图所示：



证书使用者名称：1. 使用用户名 2. 使用真实姓名，真实姓名需保证唯一，且不能为空，如果为空则不创建对应证书。

证书保护口令：1. 设置为统一的保护口令。此时需要设置相应的用户口令。

2. 使用用户的账户密码作为保护口令。选择此项，不需要设定用户证书口令，直接使用用户的账户密码作为保护口令。

请输入口令：用户登录证书的统一口令。

证书有效期：证书的有效期限，最大为 9125 天（25 年）。

用户认证方式：包含证书绑定认证，密码或证书绑定认证，密码和证书绑定认证。

证书签发对象：可以针对所有用户，也可以针对不同组的用户，如选择用户组，则仅对属于该组的用户签发证书。

忽略已绑定证书用户：勾选此项，则对已绑定证书用户跳过，不签发新证书，保持原证书和用户之间的绑定关系。

导入文本批量生成证书如下图所示：

在此页面可以批量导入文本证书，设置所有签发用户证书保护口令。注：文本中用户名与部门之间以英文半角（,）隔开，逗号前后不要有空格，且文件必须另存为 UTF-8 编码格式。

导入请求签发证书如下图所示：

如果使用的是 SGA 自建证书或者您导入了带私钥的第三方 CA 根证书，则代表 SGA 系统可以签发用户证书。在导入请求签发证书页面，我们可以导入证书请求工具生成的证书请求文件，来为用户签发不带私钥的用户证书。

导入证书请求文件，点击签发，会出现用户证书下载页面，管理员可将下载下来的用户证书发放给相应的最终用户。

2.7.3 证书列表

批量生成证书页面可查看已签发证书列表，并提供下载，吊销和删除证书。已签发证书选项卡如下图所示。在此页面可以查看已签发证书，下载，吊销和删除证书。

2.7.4 证书吊销

只有使用的是 SGA 自建证书或者您导入了带私钥的第三方 CA 根证书，才能吊销用户证书。

如下图：将用户证书导入后，选择吊销原因，点击吊销，即可吊销该用户证书，该吊销的用户证书信息会记录到吊销列表，被吊销的用户证书在 SGA 系统上将不能正常使用，通过验证。

可点击“下载最新证书吊销列表”链接来下载最新的吊销列表。

注意：要是吊销列表马上生效，即被吊销的证书立刻就不能正常使用，需要手动在系统管理——关机重启页面，点击重启系统按钮，来重新启动系统服务。

2.7.5 在线证书状态服务

可在该页面设置外部证书吊销文件地址，来实现时时获取吊销证书信息。

2.8 页面定制

2.8.1 页面定制

页面定制页面可定制手机客户端登录页面的 Logo，以及移动云管理平台顶部横幅 Logo 如下图所示：

在导入 logo 文件处选择您制作好的 logo 图片，点击提交，您选择的 logo 图片将显示在“未上传自定义 logo”处，如要使替换的 logo 生效，还需勾选“启用自定义 Logo”，点击提交。如要还原系统 logo，可将“启用自定义 Logo”后的钩去掉，点击提交即可。

前台页面定制和后台页面定制可以分别更换前、后台的 logo，而且是彻底的改变，系统恢复出厂设置时也会保持更改后的 logo。该功能需谨慎使用，最好有网页制作经验的人来操作。或联系厂家技术人员。

2.9 系统管理

2.9.1 系统配置

系统配置模块包括以下选项卡：自动升级，服务端口配置，时间设置，用户许可设置。

自动升级配置页面如下图所示：

可以自动检测到最新版本，进行自动升级。默认是启用的状态，升级完后自动重启。可以根据需要自行配置。可以手动设置更新时间。可以手动检查是否有最新版本进行更新处理。

服务端口配置页面如下图所示：

可设置前台 http 重定向，修改前台和后台 https 端口，设置端口合一。

http 重定向只对前台登录有效，勾选“启用 http”，则用户登录前台可直接在 IE 地址栏输入 http://ip 或域名的方式访问前台，页面会自动跳转到 https://ip 或域名的方式来访问手机客户端。如果是外网用户需要使用 http 重定向功能来访问 SGA，管理员需要把 http 端口和 https 端口同时映射到 SGA 接口上。前台 http 和 https 端口可由管理员按需要更改。

如果您想修改前台或后台的 https 端口，可将 443 或 4433 修改成您需要的端口，修改后您访问手机客户端或后台的方式将是：https://IP 地址或域名：端口号，例如您将 SGA 前台 https 端口 443 修改成 8043，访问的域名是 abc.3322.org，您访问 SGA 前台的方式为：https://abc.3322.org:8043，并且如果您将 SGA 放在路由器或防火墙的后面，您则需要把 TCP8043 端口映射到 SGA 的接口上。

启用端口合一：即 IP 隧道、TCP 隧道端口的合一。不勾选，如果您将 SGA 放在路由器或防火墙的后面，您则需要把 IP 隧道和 TCP 隧道端口映射到 SGA 的接口上。勾选使用 UDP 模式，建立 IP 隧道后可以加速 IP 隧道的访问。

时间设置选项卡：需要手工设置系统时间，并支持使用时间服务器同步，如下图：

注意：在配置时间服务器同步之前，请确认您的 SGA 与外网是连通的，并且配置了有效的 DNS。

用户许可设置选项里的序列号将根据您购买的用户许可数由厂商提供，如果您购买的是 10 个用户许可证，则表示同一时间只能 10 个用户能登录到 SGA 前台系统。提交正确的序列号后，系统将会重启 SGA 服务。

PC 客户端用户许可数：是指可接入 PC 用户数量。移动云用户许可数是指接入手持智能终端的个数，

硬件 SGA 用户许可设置页面：

软件版 SGA 用户许可设置页面：

软件版 SGA 需要配合 cylan 开发的 ilicence 进行使用，许可中心配置的域名或 IP 需要填写安装 ilicence 服务器的 ip 或域名，端口默认为 50302 端口。

Ilicence 详细安装配置请参看附录二

2.9.2 配置管理

导入/导出配置选项卡。可以导出和导入设备配置。导入配置后，系统会重启，重启后，请用导入的配置里面的登录参数登录 SGA 系统。

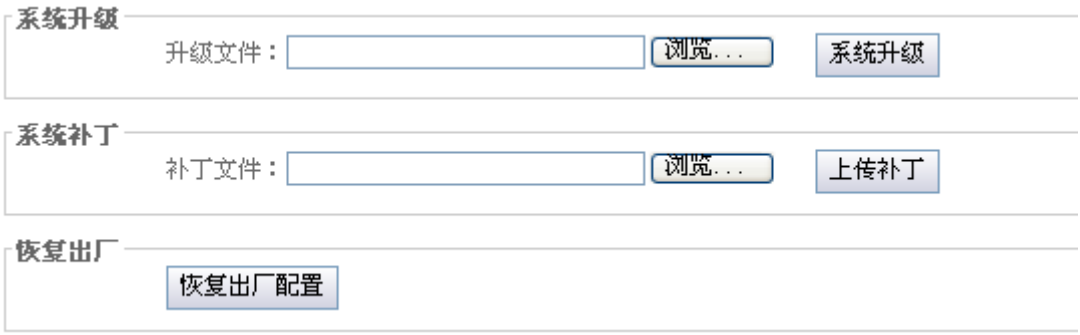
历史备份选项卡。可以对配置进行备份。

2.9.3 系统升级/恢复出厂

系统升级页面可恢复出厂配置和进行系统的升级以及上传补丁文件，注意：

恢复出厂配置，系统升级和上传补丁的过程中不能断电，系统将自动重启。

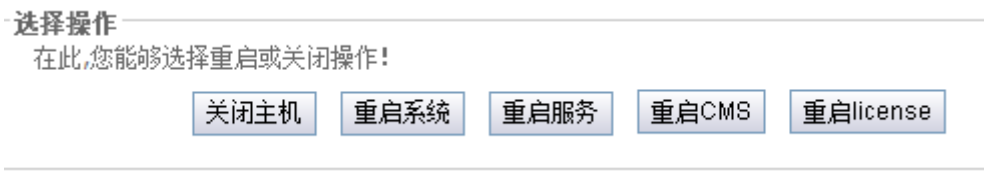
恢复出厂设置，重启完后，管理员可以通过 eth0 口 IP：192.168.0.254 或 eth1 口 IP：192.168.1.254，端口 4433 来访问后台并配置。成功升级和上传补丁后，系统会重新启动，管理员可通过之前访问的接口参数来继续访问后台。



系统升级完毕后，可以通过页面右上角的系统信息来查看当前版本，如下图所示：

2.9.4 关机重启

在软件版 SGA 上，执行关闭主机，重启主机，重启系统，重启 CMS，重启 licence；重启系统是只把 SGA 服务重启，不重启网卡之类的服务。



在硬件版 SGA 执行关闭主机，重启主机，重启系统

2.10 日志中心

2.10.1 系统日志

日志中心会显示系统的所有日志信息，并对日志做了分类，可显示管理日志，错误日志，信息日志，调试日志。

2.10.2 日志服务器

也可以配置外部接受日志的日志服务器。选择日志服务器选项卡，如下图：

添加/配置日志服务器，点添加后，出现以下界面：

服务器 IP：日志服务器的 IP 地址。

服务器端口：日志服务的端口，默认为 514。

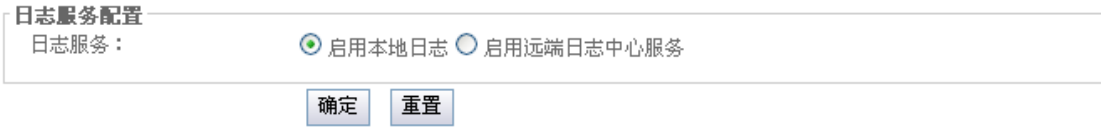
日志级别：级别选项有：all，critical，error，warning，notice，info，debug。

匹配规则：选项有：级别之上，等于，不等于。

2.10.3 日志服务配置

日志服务配置页面可以启用本地日志和启用远程日志中心服务。

启用本地日志选项卡如下图所示：



启用远端日志中心服务选项卡如下图所示：

服务器 IP 地址：日志服务器的 IP 地址。

服务器端口：日志服务的端口，默认为 514。

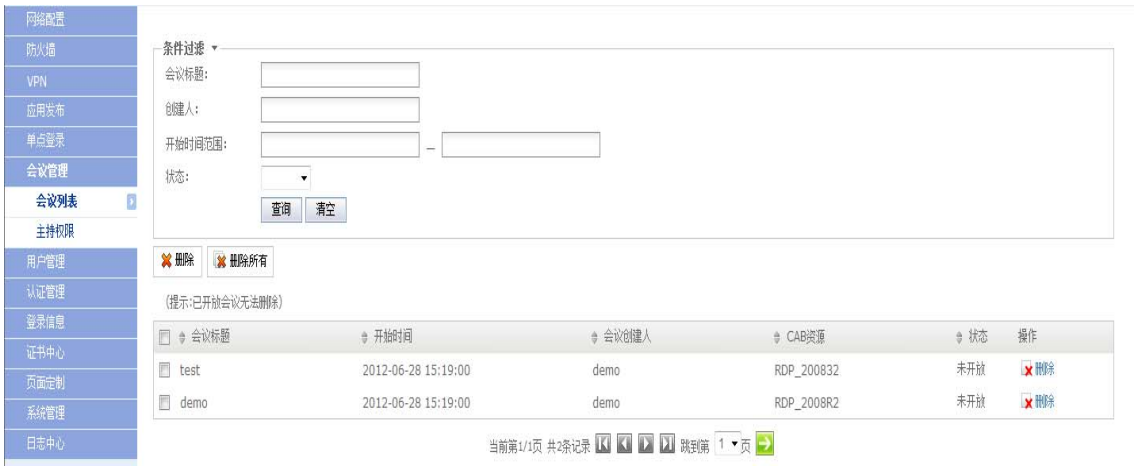
用户名：连接日志服务器的用户名。

密码：连接日志服务器的密码。

2.11 会议管理

2.11.1 会议列表

条件过滤，可针对会议标题、创建人、开始时间范围、状态包括以开放和未开放，进行单独、组合、模糊、精确等查询。



会议列表：显示的是在手机客户端建立的开放和没有开放的会议，管理员可以对建立的会议进行删除操作。

注：已开始的会议不能进行删除操作

2.11.2 主持权限

主持权限：条件过滤可以可针对用户名称、真实姓名、所属用户组、用户类型进行单独、组合、模糊、精确等查询。

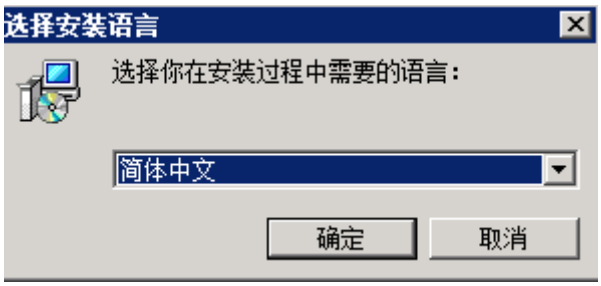
在主持权限页面，管理员可以对用户添加和删除主持会议的权限，具有主持会议权限的用户可以在手机客户端创建会议。

如在客户端创建一个 demo 的会议，如下图所示：

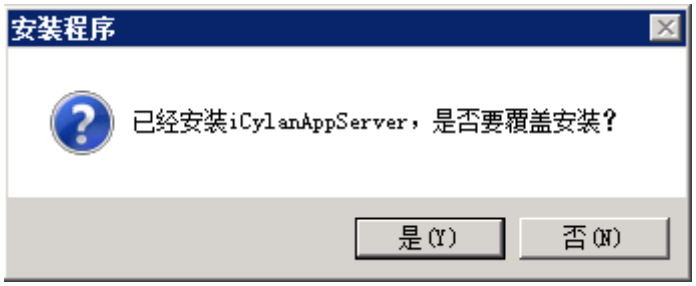
点击确定之后，将会在手机客户端和移动云管理平台显示该会议的信息，如下图所示：

附录一 iserver 安装和配置

双机 IcylanAppserver 出现如下图所示：



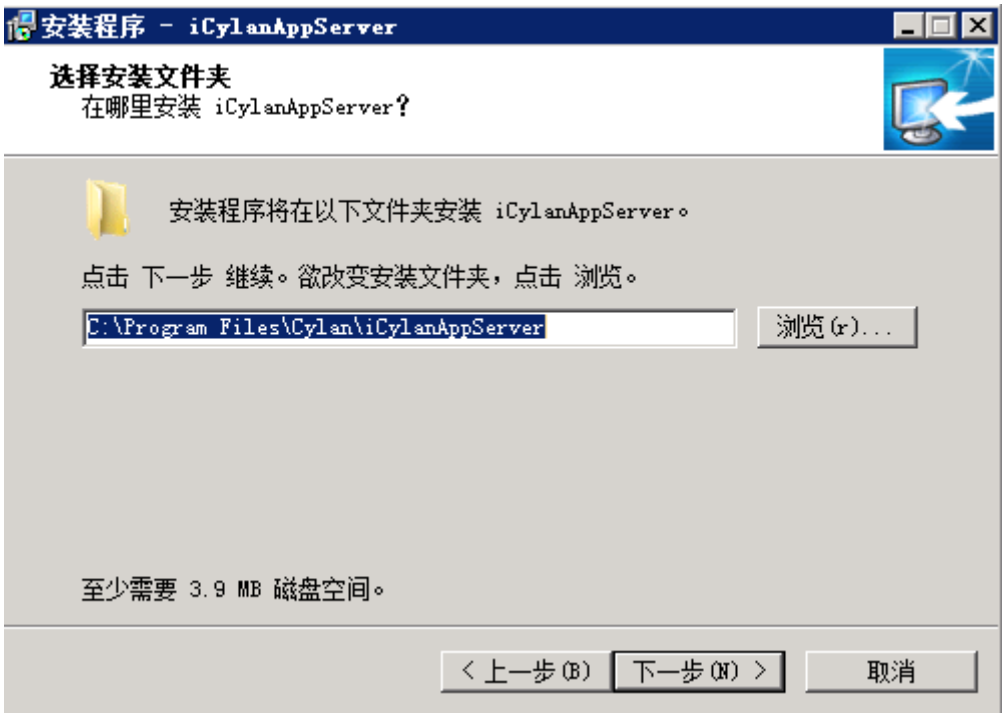
用户可以根据环境进行语言设置，目前我们提供了中文和英文两种安装语言，点击确定之后如果是覆盖安装则会出现如下提示信息：



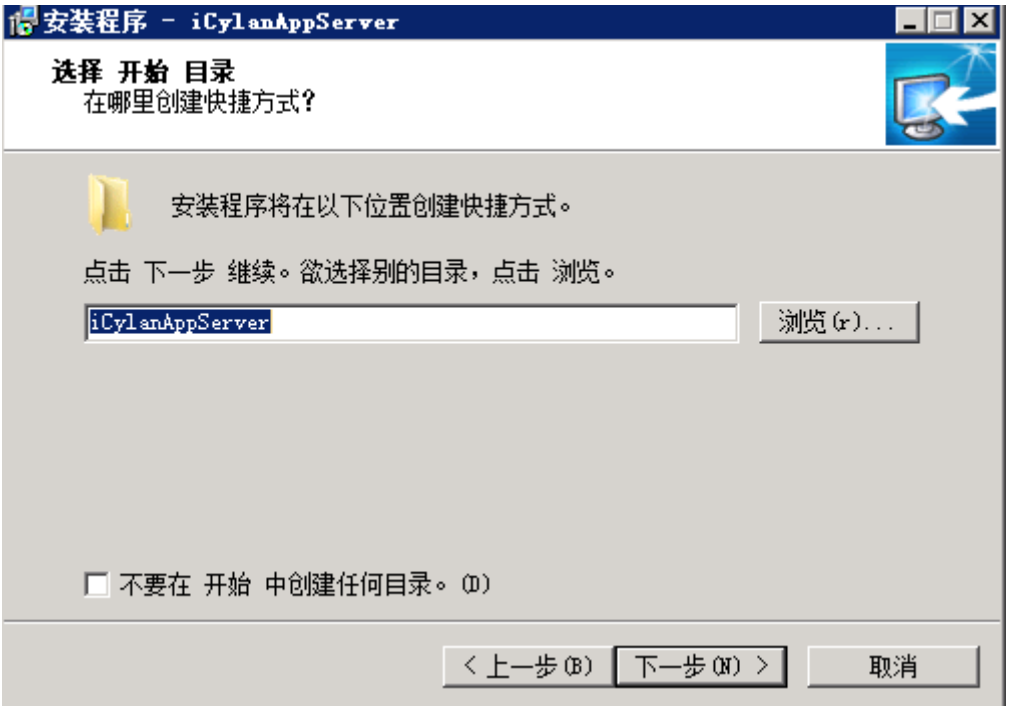
点击是之后直接跳转到安装页面

如果是第一次安装则会出现如下提示：

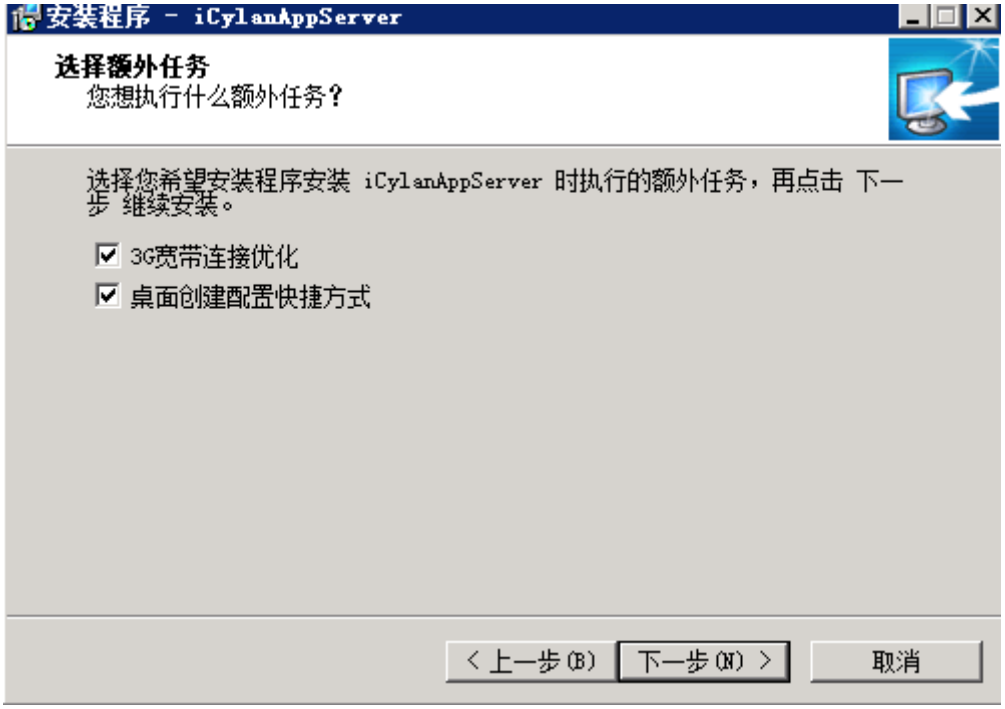
点击下一步



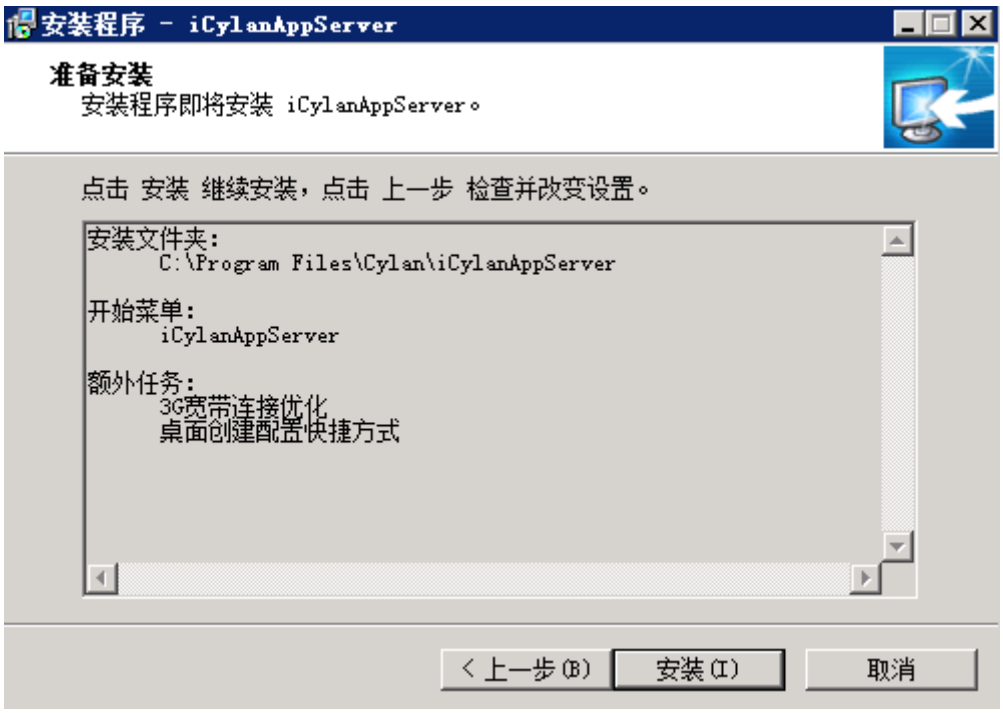
这一步用户可以选择安装文件的位置，这里我们选择默认的位置，点击下一步



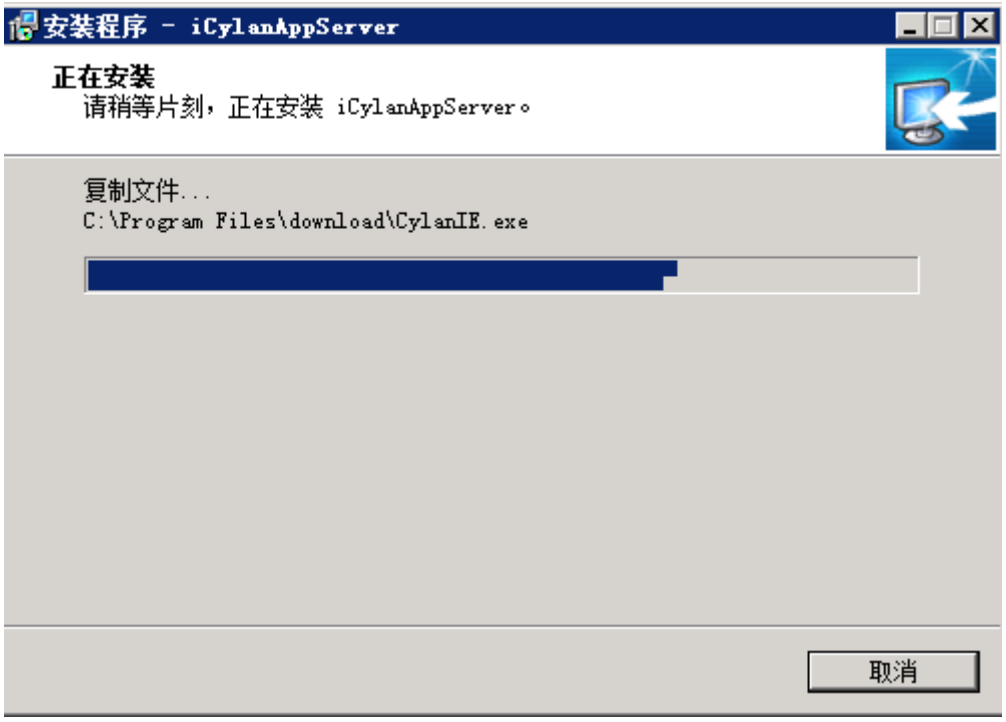
这一步用户可以选择在哪里创建快捷方式，这里我们选择默认，点击下一步



这一步用户可以选择一些额外的任务，这里我们选择默认设置，点击下一步



这一步提醒用户软件准备安装，点击安装，软件就进入安装状态



等待安装完成后就出现如下配置页面

服务器状态：主机名显示的是主机名称；运行状态显示的是与 SGA 连接状态，显示正常则与 SGA 连接成功，显示失败则没有与 SGA 连接成功；版本显示的是当前软件的版本号

服务器地址：SGA 设备 IP 地址。

服务器端口：默认是 1234，SGA 设备和 CAB 服务器的连接端口。因为 SGA 和 CAB 服务器本身处在一个内网中，因此，如果 SGA 设备放在防火墙或路由器后面，无需转发 1234 端口到设备相应接口上。SGA 的端口和此端口需保持一致，所以两项要至少更改一个。

本地监听端口：监听服务器状态的端口。

鼠标双击速度：通过滑动滑动条可以改变在客户端双击的速度

窗口最大化： 勾选后，在客户端打开的窗口以最大化显示

配置完成后关闭窗口显示如下信息

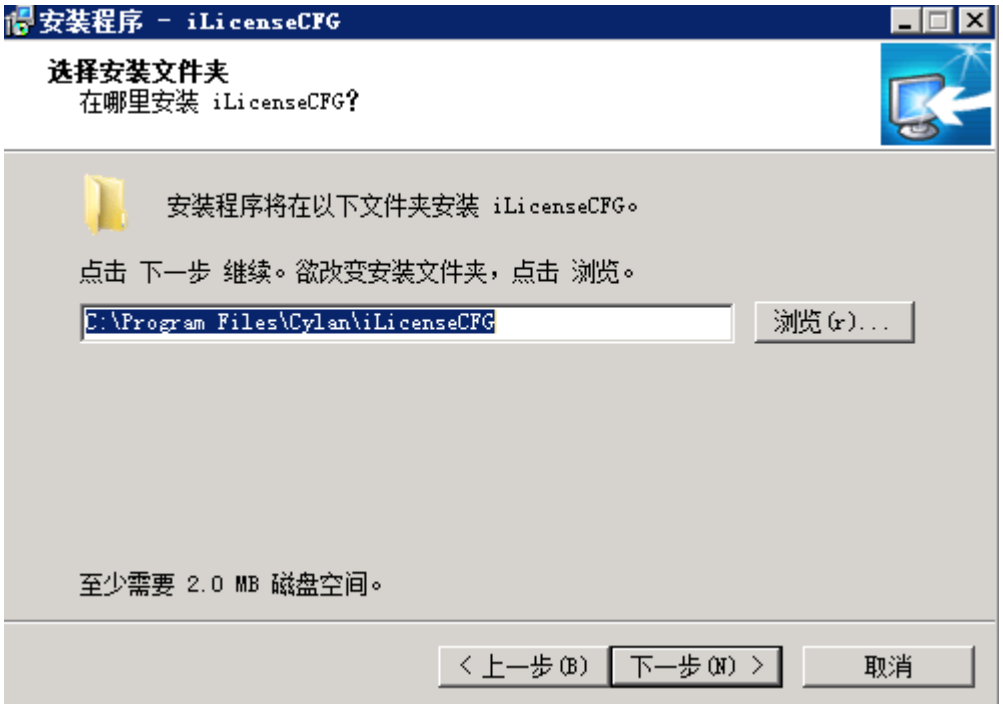
用户可以选择是否现在进行重新启动，点击完成按钮，icylanAppserver 就安装完成

附录二 ilicence 安装和配置

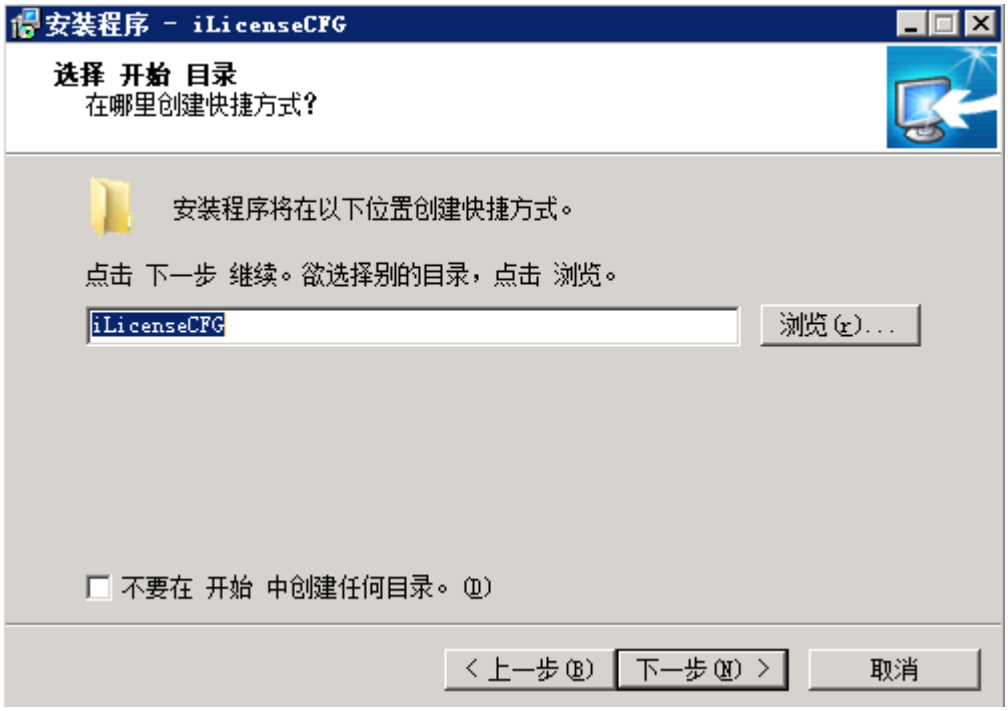
双机 Ilicence 

出现如下图欢迎页面：

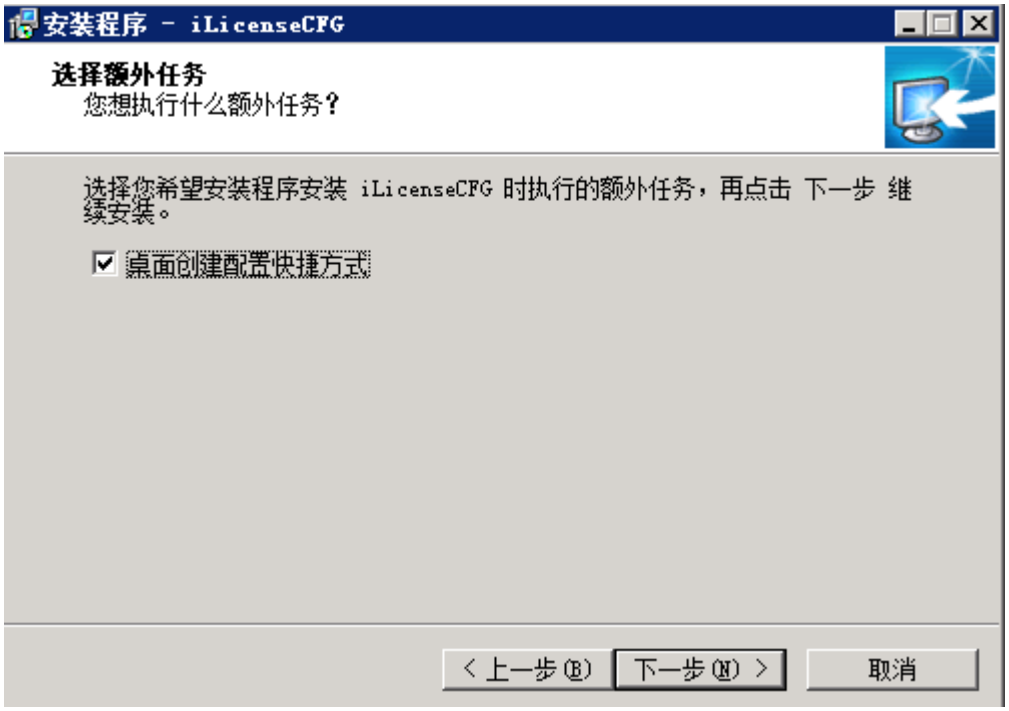
点击下一步，出现下图



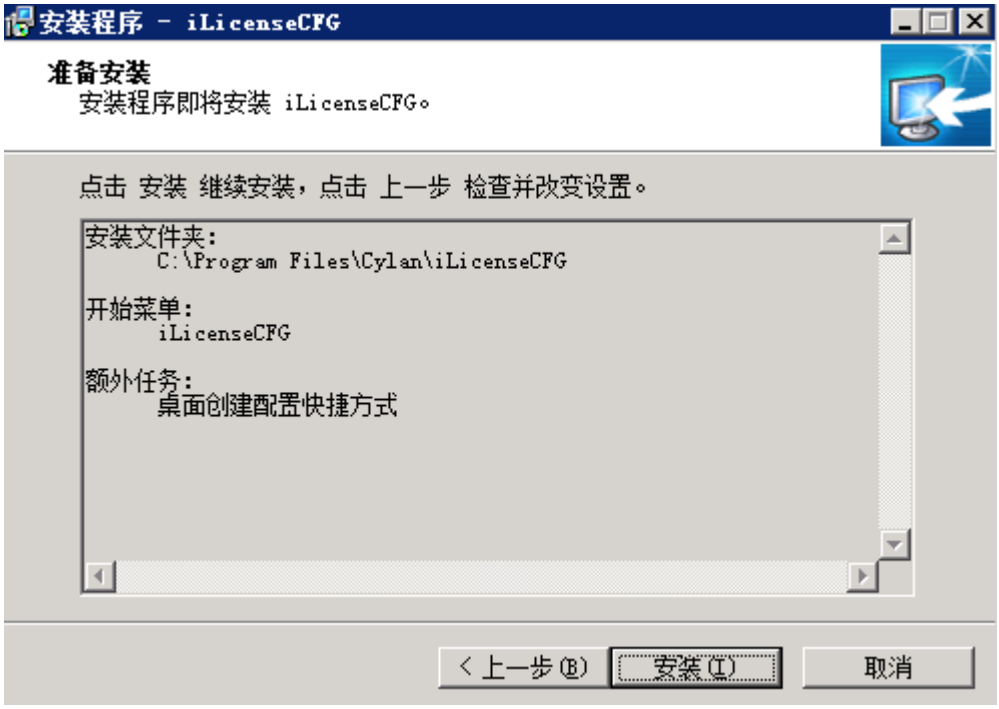
这一步用户可以选择安装软件的位置，这里我们选择默认位置，点击下一步



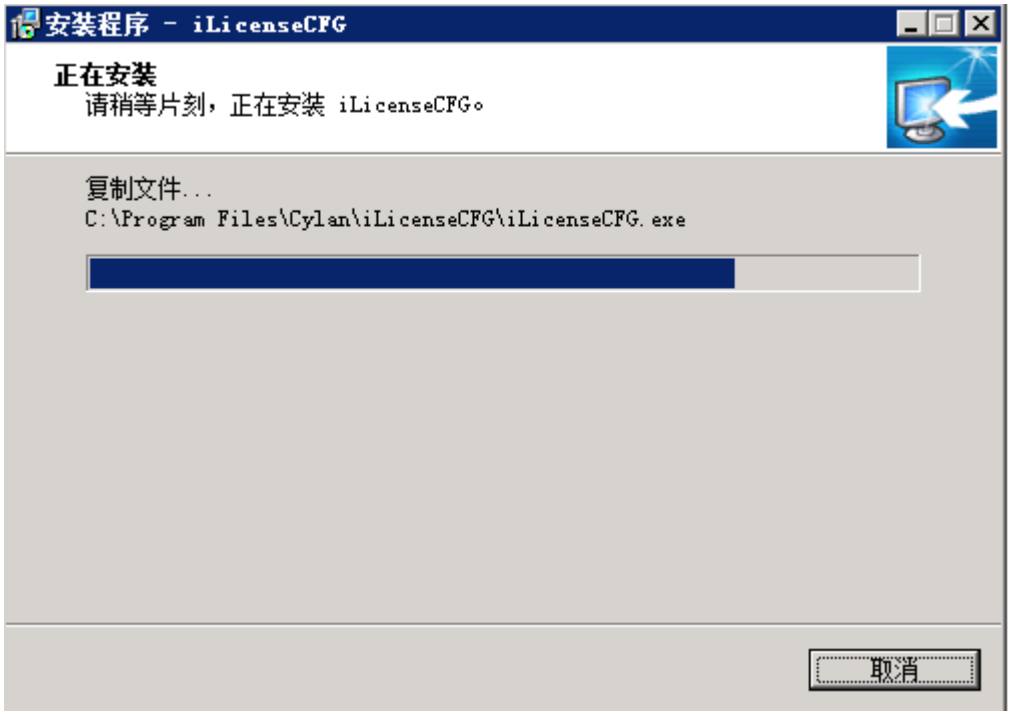
这一步用户可以选择在哪里创建快捷方式，这里我们选择默认，点击下一步



这一步用户可以选择额外的任务，点击下一步进入准备安装页面



该页面在安装之前显示前面步骤用户所做的设置，点击安装进入安装页面



等待安装完成就进入配置页面，Ilicence 配置如图所示：

服务配置下的序列号是厂家根据用户提供的硬件 ID 以及需要购买许可数量所提供的。填上序列号之后，点击保存，再点击关闭按钮出现下图所示信息看，整个安装过程结束


安装程序 - iLicenseCFG
完成 iLicenseCFG 安装向导
iLicenseCFG的安装已完成。点击图标可执行本程序。
点击 完成 退出安装向导。
完成(F)

手册声明：关于对本产品产生的任何问题，请联系赛蓝技术支持！谢谢！