用户管理

用户管理功能用于对使用 octoplant 系统的用户进行创建、权限、策略等的管理。

用户管理分为如下功能：

- 创建用户和组
- 权限管理
- 账户策略
- 用户同步
- 单点登录 SSO

创建用户和组

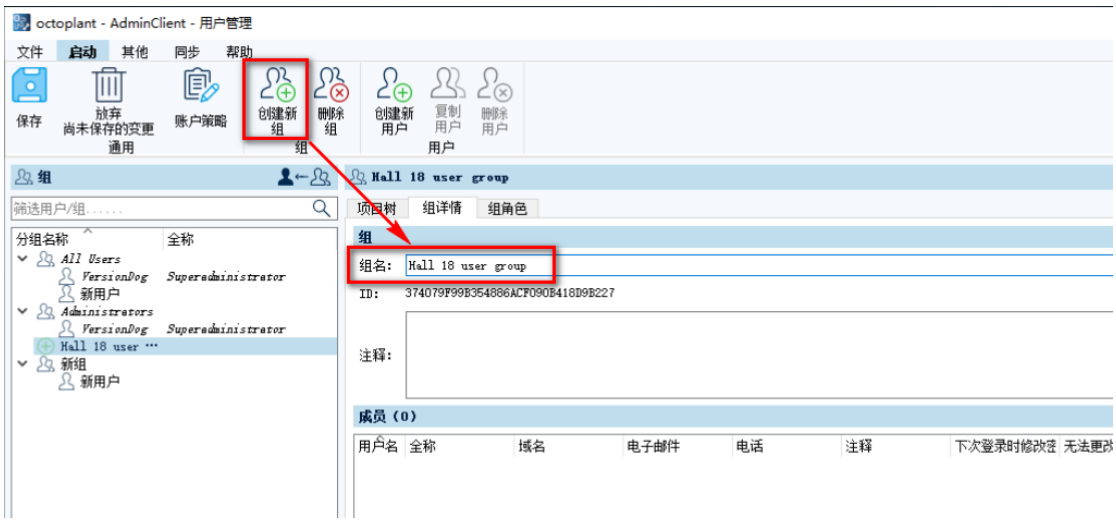
- 在 AdminClient 中打开*用户管理*
- 在用户管理界面或其它显示、选择用户/组的界面中， 

表示组视图， 

表示用户视图，  表示由用户视图切换为组视图，  表示由组视图切换为用户视图
- 筛选用户/组时，需要切换到用户视图或组视图

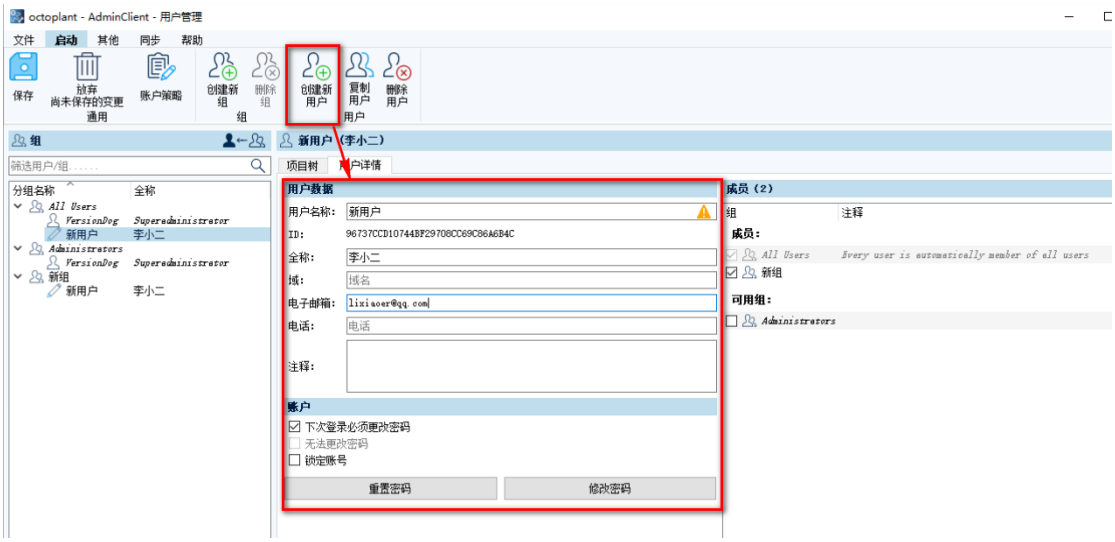
创建组

- 点击菜单栏的*创建新组*，即可新建一个组并弹出*组详情* 窗口
- *组详情* 窗口中，输入组名
- 如果要删除组，需要注意的是，All Users、Administrators 和当前登录用户所在的组不可删除



创建用户

- 点击菜单栏的***创建新用户***，即可新建一个用户并弹出***用户数据*** 窗口
- ***用户数据*** 窗口中，用户名称为必填项，其余信息为选填项，如果需要接受邮件通知，则需要在电子邮箱信息栏中填写正确的电子邮箱地址
- 勾选***下次登录必须更改密码*** 时，该用户在下次登录会弹出修改密码的对话框
- ***默认情况下，无法更改密码*** 为不可选中状态，需要将账户策略中的密码过期改为无限期且***下次登陆必须更改密码*** 为非勾选状态才可变为可选中状态
- ***锁定账号*** 则会使该用户暂时无法访问 octoplant 系统
- 如果用户忘记了密码，则可以通过***重置密码*** 生成一个可见的随机密码，也可以通过***修改密码*** 生成一个新密码
- 勾选***成员***里的***可用组***将该用户分配到不同的用户组
- 如果要删除用户，需要注意的是，超级用户 versiondog 和当前登录用户不可删除
- 如果要增加多个相似账户，则可以点击***复制用户*** 来减少操作

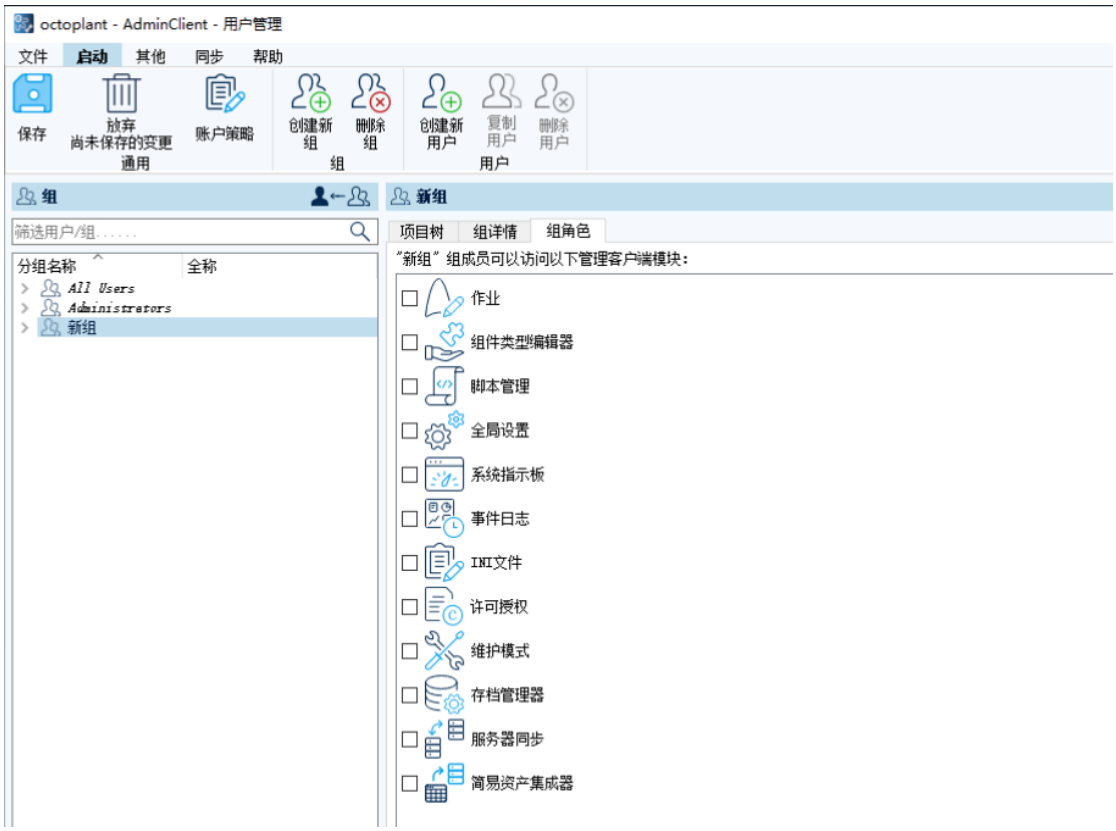


权限管理

用户/用户组的权限分为 octoplant 的功能使用权限和组件的读、写、增、删权限。

功能权限

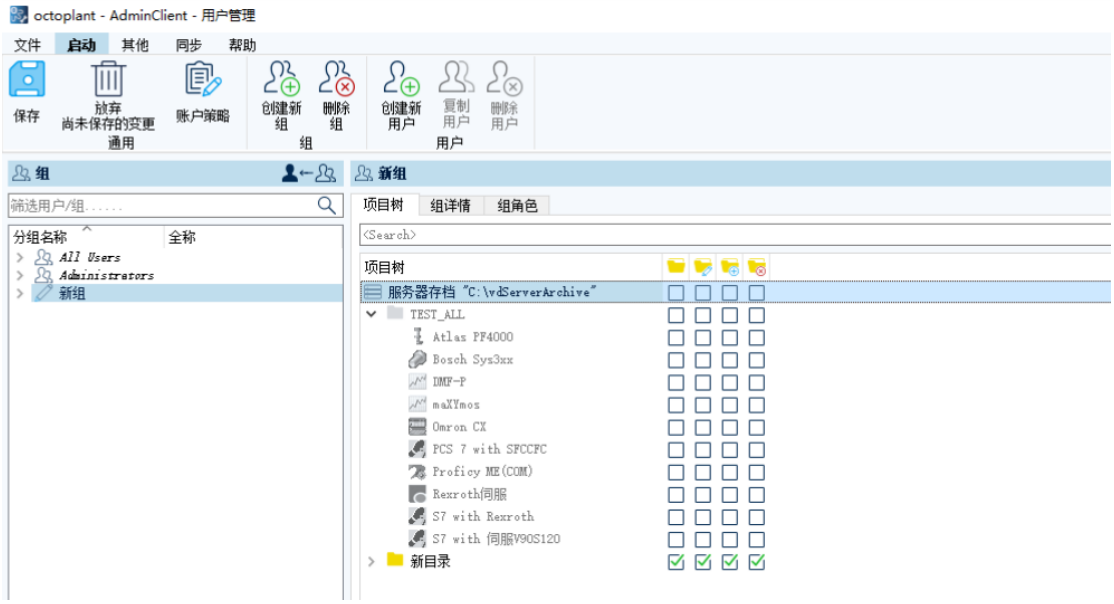
- 选择用户组，并打开***组角色*** 页面
- 为选择的用户组勾选相应的功能权限：作业、组件类型编辑器、脚本管理、全局设置、系统指示板、事件日志、INI 文件、许可授权、维护模式、存档管理器、服务器同步、简易资产集成器
- 功能权限是以用户组来进行分配的，用户组 Administrators 拥有完全权限
- 用户组下的用户可以继承到用户组的所有权限。如果用户同时属于多个用户组，则其权限相当于所有用户组权限的并集



组件权限

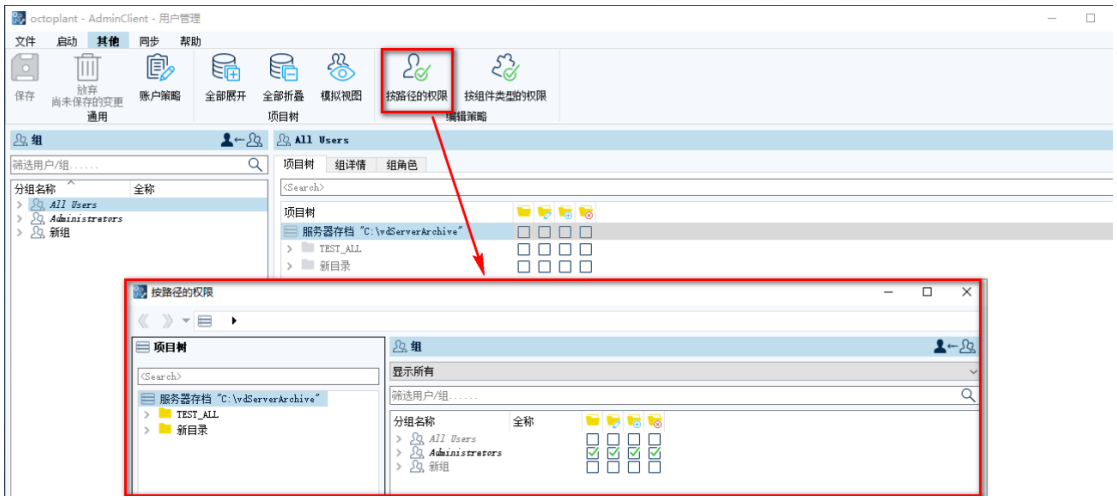
1.按照用户/用户组分配权限

- 选择用户组，并打开*项目树* 页面
- 选择用户/用户组，勾选目录或组件的读、写、增、删权限
- 按照权限高低排序，删>增>写>读，例如勾选删权限，则会同时拥有读、写、增权限
- 如果勾选目录的权限，对目录下的组件也会拥有相同的权限



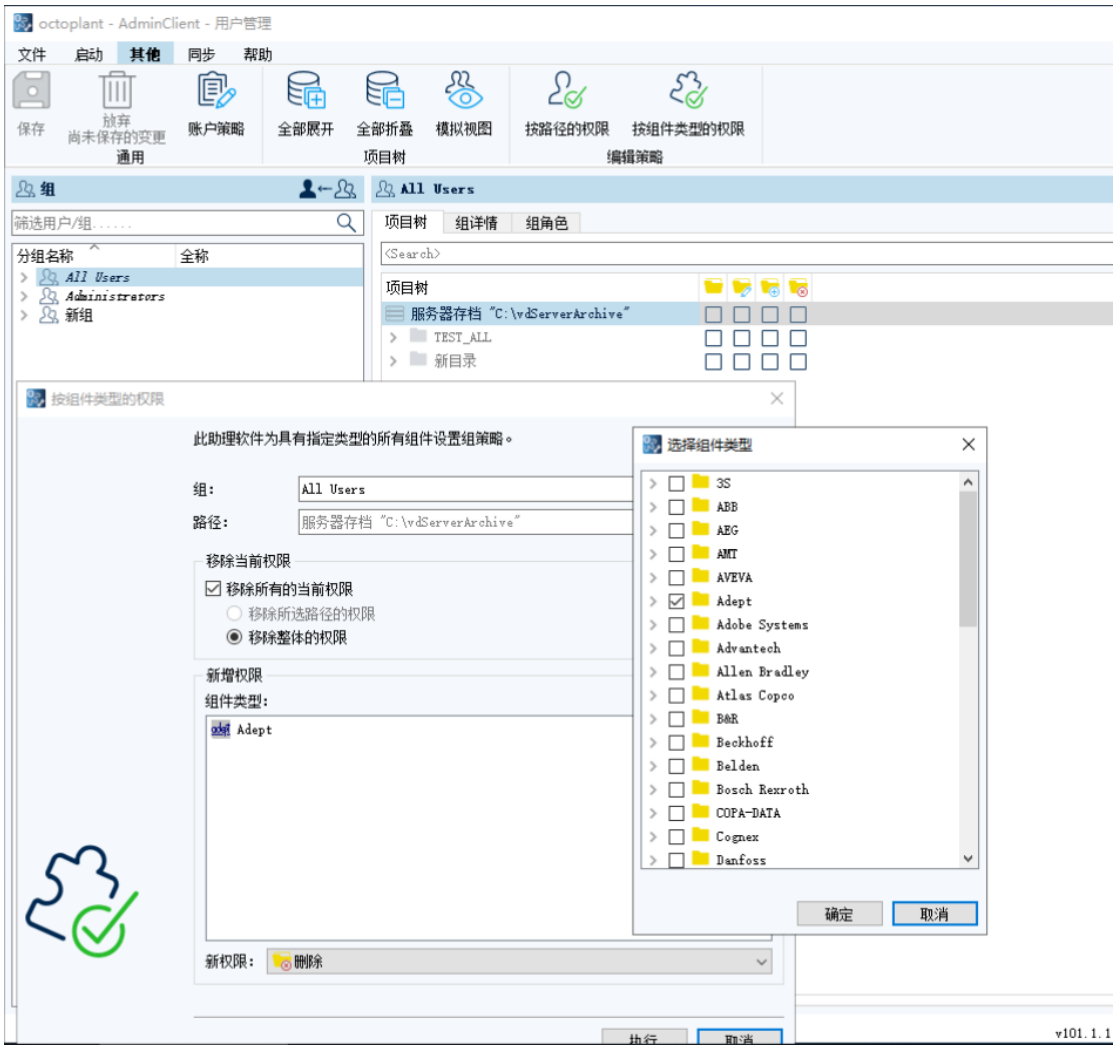
2.按照路径分配权限

- 在选项卡*其他* 中，点击*按路经的权限* 则可以为目录和组件配置不同用户的权限



3.按照组件类型分配权限

- 选择用户组，点击***按组件类型的权限***
- 选择需要设置权限的路径。如果需要移除权限，则勾选***移除所有的当前权限***，并选择***移除所选路径的权限*** 或***移除整体的权限***
- 在



账户策略

点击菜单栏***账户策略*** 可以设定用户对 octoplant 系统的登录配置。

- ***授权***
- ***通过访问管理授权*** ：适用于只在 octoplant 中添加用户的情形
- ***通过操作系统授权*** ：适用于只用域账户登录 octoplant 的情形
- ***通过操作系统和访问管理授权*** ：适用于既包含域账户、又包含添加用户的情形
- ***单点登录*** ：当选择***通过操作系统授权*** 时，可以选择单点登录

- ***密码***：设定密码的有效期限制、密码的历史记录、随机或特定密码作为新帐户或重置帐户的默认密码，以及用户是否必须在首次登录时更改密码

- ***密码策略***：可以设定密码的长度要求和复杂度要求

- ***锁定账户*** ：设定是否开启锁定账户功能，以及锁定的条件、锁定的时间

- ***被删除的用户*** ：匿名化已删除的用户数据
- ***删除用户时匿名处理*** ：从数据苦衷删除用户的全名、电子邮件、电话和备注
- ***同时对用户名匿名处理*** ：从数据库中删除用户的用户名
- ***对所有以前删除的用户进行匿名处理*** ：根据删除规则对以前的用户进行匿名处理

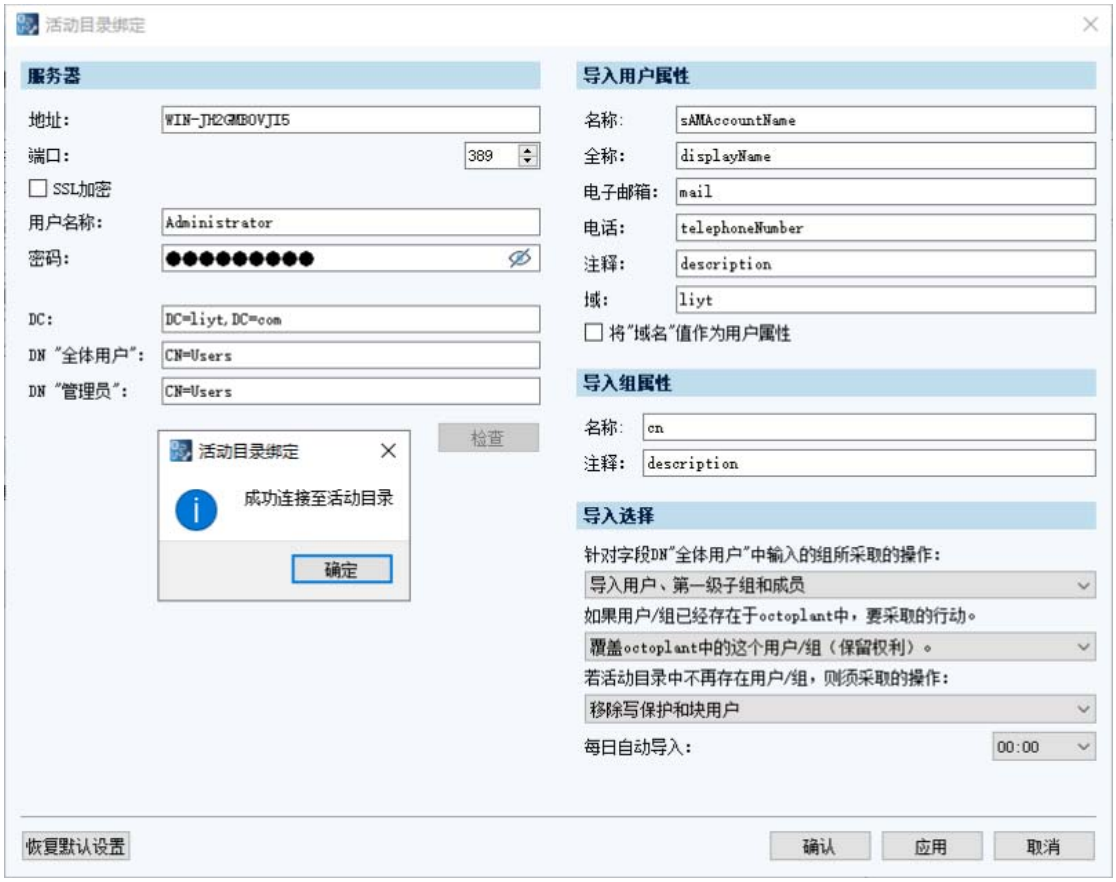
- ***杂项***

- ***可以本地登录*** ：允许客户端在未能连接到服务器时进行本地登录

用户同步

用户同步功能可以将域账户导入 octoplant 系统，从而符合相关的安全管理要求。

在菜单栏*同步→配置* 可以设定 octoplant 与 AD 域服务器的绑定信息。



- ***服务器***
- ***地址*** ：输入 AD 域服务器的 IP、名称或域名。
- ***端口*** ：加密连接默认端口 636，非加密连接默认端口 389，可以修改
- ***SSL 加密*** ：默认采用 LDAP 协议与 AD 域服务器建立联系。勾选后将使用 LDAPS 协议
- ***用户名称*** ：访问 AD 域服务器的用户名称，用户名格式：<用户名>或<域>\<用户名>或<用户名>@<域>
- ***密码*** ：访问 AD 域服务器的用户密码
- ***DC*** ：域的 DNS 名称
- ***DN“全体用户”*** ：从 AD 域服务器导入的用户或用户组
- ***DN“管理员”*** ：从 AD 域服务器导入到管理员组的用户或用户组

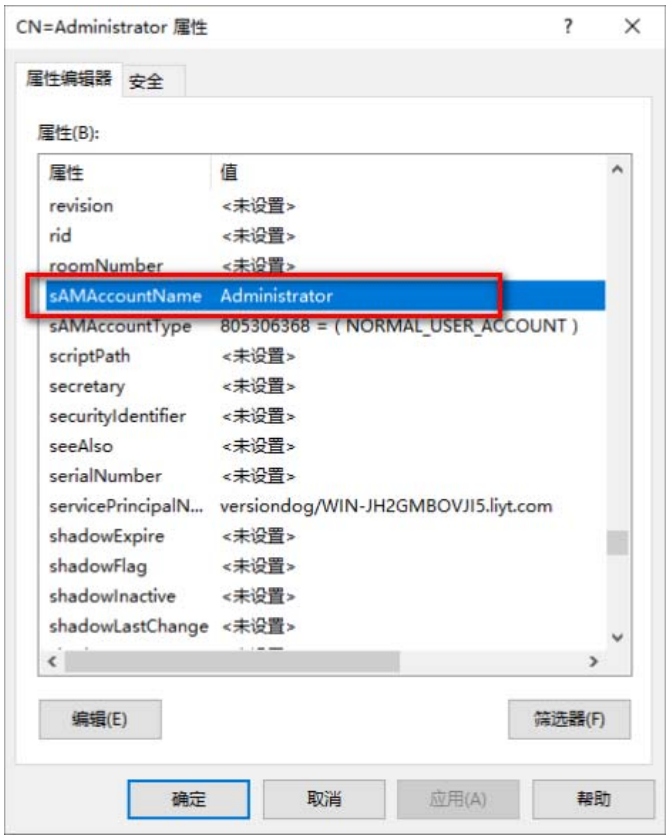
如果访问路径 DC、CN、OU 等名称包含特殊字符，则需要在特殊字符前添加转义字符。如 CN=W+D，需要输入 CN=W\+D。

可以通过 Get-ADGroup <group name>和 Get-ADUser <user name>来查看 AD 组和 AD 用户信息。

```
PS C:\Users\Administrator> get-ADGroup users


DistinguishedName : CN=Users,CN=Builtin,DC=liyt,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Users
ObjectClass       : group
ObjectGUID        : 498915b6-8c84-412e-a448-d36e2506f3d3
SamAccountName    : Users
SID               : S-1-5-32-545


PS C:\Users\Administrator> get-ADuser Administrator


DistinguishedName : CN=Administrator,CN=Users,DC=liyt,DC=com
Enabled           : True
GivenName         :
Name              : Administrator
ObjectClass       : user
ObjectGUID        : c1e644be-e591-407a-a682-a01a109fe00c
SamAccountName    : Administrator
SID               : S-1-5-21-139314877-1273306518-1774971213-500
Surname           :
UserPrincipalName :
```

- ***导入用户属性***

- 名称(sAMAccountName)、全称(displayName)、电子邮箱(mail)、电话(telephoneNumber)、注释(description)。括弧内为默认值



- ***域*** ： AD 域服务器的域名
- ***将“域”值作为用户属性*** ： 默认不勾选，域的 NetBIOS 将会输入，可以读取和使用任意的用户属性

➢ ***导入组属性***

名称(cn)、注释(description)

➢ ***导入选项***

- 针对字段 DN 全体用户 中输入的组所采取的操作：
  - ✓ ***导入用户、第一级子组和成员（默认选项）***
  - ✓ ***导入用户、组和成员***
  - ✓ ***导入用户（不导入组或成员）***
- 如果用户/组已经存在于 octoplant 中，要采取的行动：
  - ✓ ***覆盖 octoplant 中的用户/组（保留权利）***
  - ✓ ***跳过用户/组***
- 如果 AD 域服务器中不再存在用户/组，则须采取的操作：
  - ✓ ***移除写保护和阻止用户（默认）***：在 octoplant 中保留用户和组，并且锁定用户
  - ✓ ***移除写保护*** ： 在 octoplant 中保留用户和组，用户
  - ✓ ***删除用户/组*** ： 在 octoplant 中删除用户和组，
- ***每日自动导入*** ： 开始每日自动导入的时间

➢ ***检查*** ： 此按钮可以检测与 AD 域服务器的绑定信息是否正确

在配置完成后，需要点击菜单栏***同步 →激活*** 来激活自动导入功能，也可以点击菜单栏***同步 →现在导入*** 来执行一次手动导入。

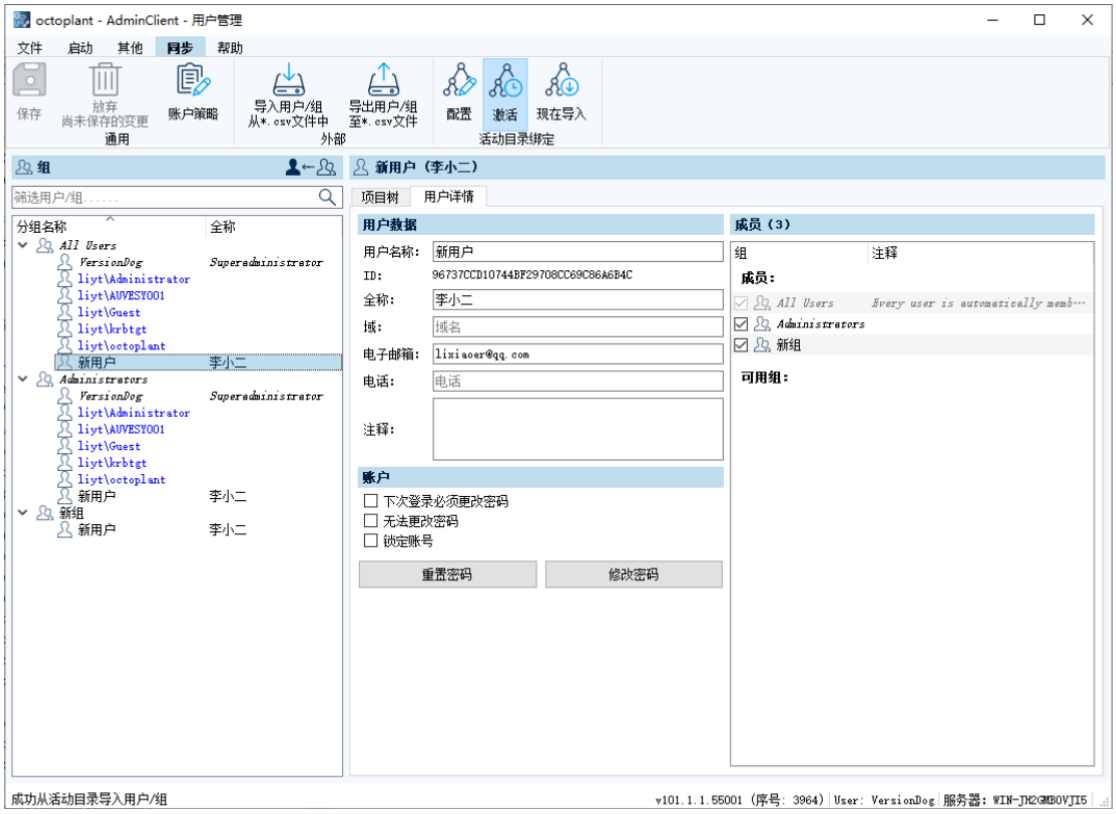
新导入到 octoplant 的用户和组将在用户管理中以蓝色显示并只读。若要删除只读状态和颜色标记，取消菜单栏***同步 →激活***。

~~名称中包含 versiondog 或 AUVESY（大写或小写）的用户将在导入过程中被忽略。~~

可以导入的用户数量取决 license 规模限制。

通过字段 ***DN 全体用户*** 导入到 octoplant 中的用户/组没有初始权限，需要给用户/组分配权限。

通过字段 ***DN 管理员*** 导入的用户将自动分配到 ***Administrators*** 组和 ***All Users*** 组。



单点登录 SSO

单点登录 SSO 可以使用登录到 windows 上的域账户自动登录 octoplant。

- ***使用*** 单点登录 SSO 功能需要以下条件：
- ***用户同步*** 功能需要开启
- 登录到 windows 上的域账户需要存在于 AD 域服务器上
- 在***账户策略*** 中激活单点登录
- 在客户端登录界面的服务器配置中开启单点登录
- 启动服务 vdogmasterservice 的用户需要设置 SPN 属性

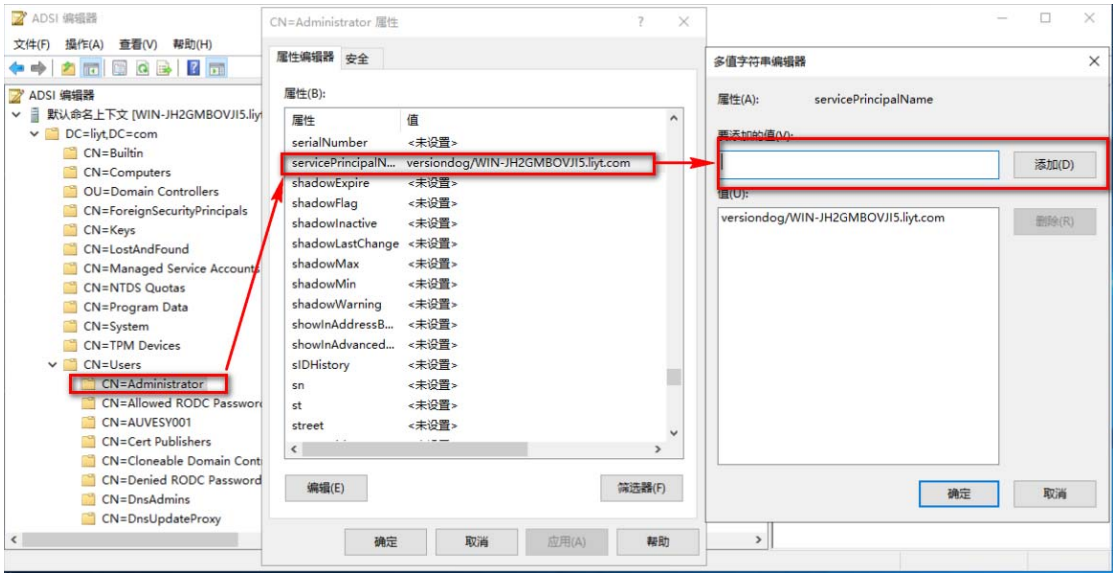
- ***设置 SPN 属性***

- 自动设置

  如果启动服务 vdogmasterservice 的用户在 AD 域服务器中具有觉有读写权限，则 octoplant 会自动设置 SPN 属性

- 手动设置

  在 AD 域服务器的用户属性中手动添加 SPN 属性



- ***取消单点登录 SSO***

  在客户端中***登出*** 用户后，在登陆界面的服务器配置中取消单点登录功能。