# 廊坊BigData环境VPN拨入指导

吴淑荣/00197720

2012-08-07

1. **概述**

廊坊BIGDATA的VPN帐号管理系统目的是为了解决OpenVPN用户授权问题，其使用微软的活动目录（Active Directory）作为前台，提供VPN帐号的的管理授权工作，相对于传统的OpenVPN用户管理方式，使用活动目录的方式在提高了系统易用性的同时，也极大地提高了系统的安全性：

* 可视化用户管理。
* 可对用户管理进行分级授权，提高了VPN帐号管理效率。
* 用户可以自己修改密码。
* 强制用户使用AD的密码策略，增加了系统安全性。

1. **VPN管理系统角色**

VPN管理系统包括3个角色：

* ***系统管理员角色：*** 拥有整个系统的最高权限，通过权限委派的方式对下级OU管理员进行授权，可授的权限包括帐号的创建、修改、删除、禁用及密码修改等。
* ***OU管理员角色：***OU为“Organization Unit”的简称，OU管理员则负责本OU内VPN用户的授权管理工作，其权限由系统管理员授予。
* ***VPN用户：***VPN用户是此系统的最终用户，通过使用AD帐号，VPN用户可通过OpenVPN方式远程拨入廊坊BigData环境。

1. **OU管理员的权限及职责：**

本指导的阅读受众为VPN拨入用户。

***权限：***VPN拨入权限有OU管理员授予

***职责：***

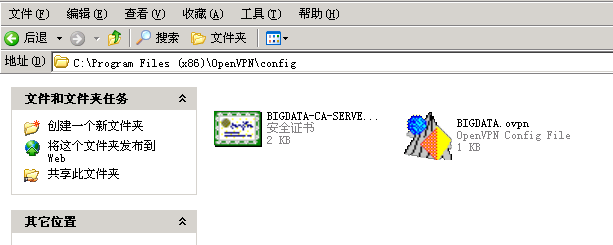
* + **VPN帐号不得借与他人使用**
  + **帐号密码不得以电子明文方式保存或写在字条上保存**
  + **原则上用户应对自己帐号的所有操作负责**
  + **如帐号不再使用，需主动联系OU管理员禁用或删除该帐号**

1. **客户端下载**

可通过“<http://openvpn.se/files/install_packages/openvpn-2.0.9-gui-1.0.3-install.exe>”下载，禁止从其它地方下载OpenVPN客户端，以免误安装被植入木马的软件。

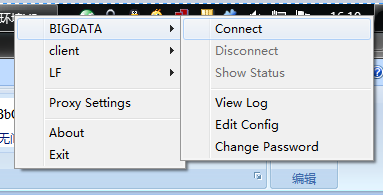
1. **VPN配置文件**

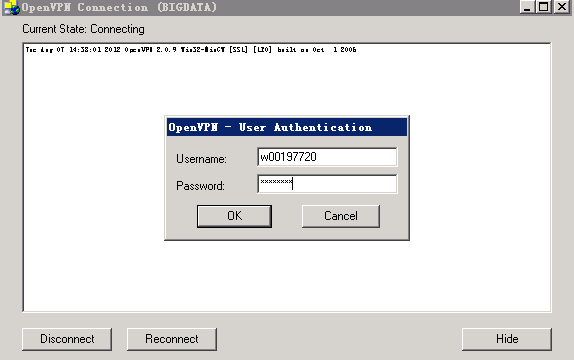
把压缩包里的文件解压到一下目录：



1. **VPN拨入**

打开OpenVPN客户端，右键选择相应的配置文件，并点击“connect”按钮：

****



1. **网络访问**

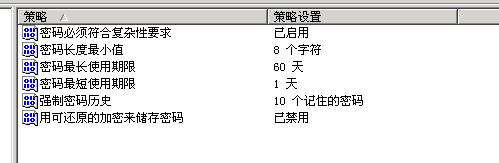
VPN拨入成功后系统会自动添加一条10.120.4.0/23的主机路由指到廊坊，用户可通过ping 2.0.0.1验证VPN是否通畅，如有问题请联系OU管理员。

1. **密码修改**

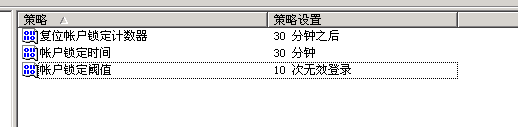
用户首次登陆或帐号密码重置后，需登录<https://10.120.5.112/pass>修改自己的帐号密码，原则上不允许通过管理员修改密码。用户如忘记密码，需联系OU管理员进行重置。



帐号密码需满足复杂性要求（字母、数字及特殊字符组合，长度8个字符以上），密码有效期为60天，密码到期后账号会自动锁定，届时请联系OU管理员解锁：

****

在30分钟内登录失败次数达到10次后，帐号会自动被锁定30分钟：

****