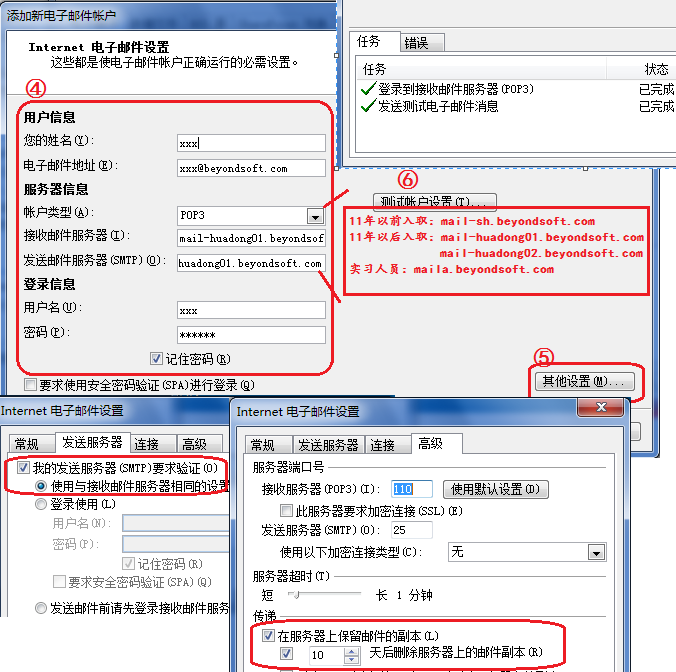
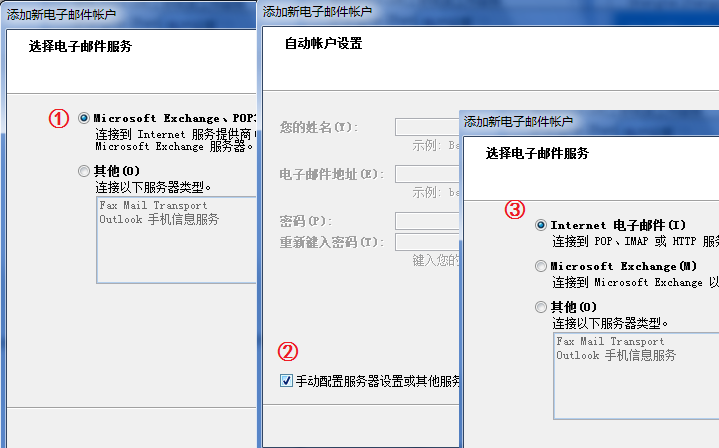
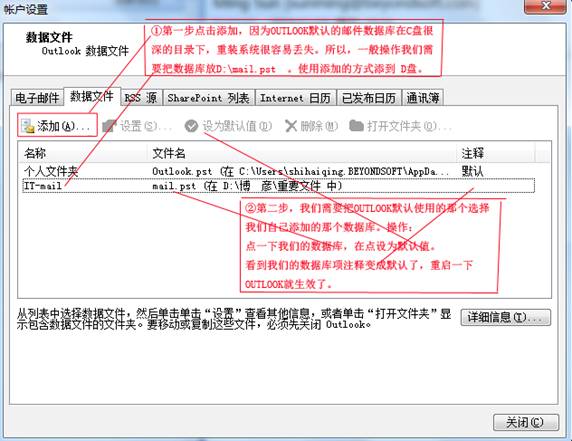
Outlook邮箱及数据文件配置

第一步 outlook邮箱配置



第二部 数据文件配置



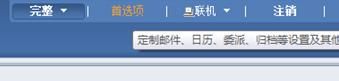
邮箱密码及域（ERP）密码的修改

1. **邮箱密码修改：**

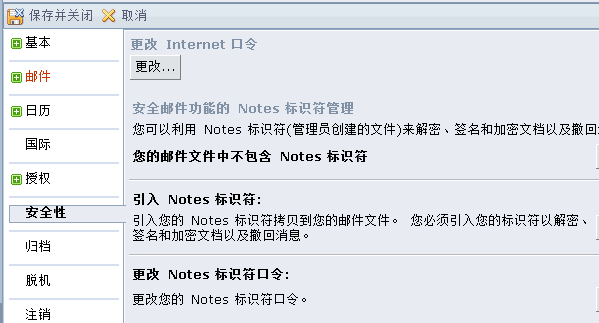
1、根据邮件服务器地址登录web版邮箱

如mail-huadong01.beyondsoft.com

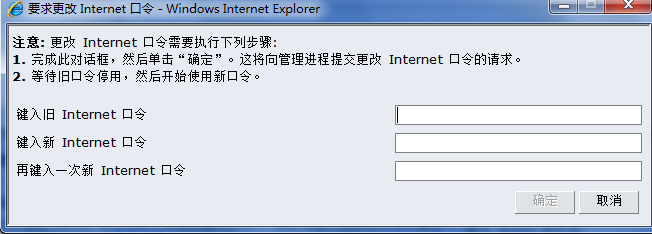
2、点击右上角的首选项，进入设置



3、选择安全性，更改internet口令



4、点击更改，进行密码更改



1. **域密码更改：**

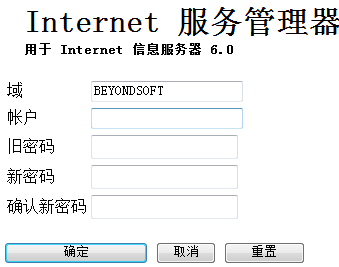
对于域用户

直接CTRL+ALT+DELETE,在弹出的更改密码选项中更改即可

对于未加域的用户

访问<https://changepwd.beyondsoft.com/iisadmpwd>

在internet服务管理器中修改



注：1、因为密码同步需要时间，所以在密码修改后一段时间内会出现旧密码和新密码都可以登录的现象，这是正常的。

2、为确保信息安全，密码有效时间为开通或修改密码后的180天，请注意时间及时修改，以免带来不便！

**博彦科技员工信息安全50条**

**通讯与操作**

* 禁止在办公区域内使用未授权软件；
* 确保安装并及时（15天之内）更新操作系统补丁；
* 确保安装杀毒软件并保持更新（15天之内）为最新版本；
* 电脑中毒后第一时间切断网络连接并通知IT部门；
* 重要数据必须及时备份并定期进行测试；
* 禁止使用“未授权”可移动存储设备（包括但不限于USB存储器、MP3/MP4/PSP、移动硬盘，软盘、可擦写CD/DVD光盘等设备）；
* 禁止将 “已授权”的可移动存储设备转借他人；
* 未经授权不得使用BT、电驴下载、P2P等下载软件；
* 不得故意遮挡或损坏公司监控设备造成监控障碍；

**访问控制**

* 所有员工办公机器都必须加入工作域；
* 离开座位时，电脑必须锁屏；
* 确保设置密码（邮件、共享、域用户、锁屏），且口令需具备一定复杂度；
* 未经批准，不得将Hub/Switch等设备接入公司网络；
* 未经批准，不得私自进行服务器访问授权；
* 严禁在会议室内及白板上遗留资料（纸质、电子资料）
* 不得故意将计算机屏幕面向窗口或玻璃门导致涉密资料有泄露的风险

**信息安全行为准则**

* 所有员工应观察系统和服务中或可疑的信息安全弱点，发现可疑安全弱点或发生信息安全事故时，员工须及时上报信息安全委员会；
* 不得抢劫、盗窃公司、客户涉密信息；
* 不得出现以出卖公司信息牟利，对公司利益造成损害的企业间谍行为；
* 不得向外部人员透漏与工作相关的任何信息；
* 向外部（客户、合作商、供应商等）提供涉密资料时，首先获得直接主管许可，然后向信息owner部门申请；
* 不得在电梯、汽车、餐厅、酒店大堂等公共场所接听涉及公司机密的重要电话，必须接听时请到相对空旷或不易被窃听的地方；
* 如遇到不确定的操作或问题，请上报领导或信息安全委员会。
* 严禁蓄意或违反规定的人为操作而导致火灾、爆炸、断电或其他灾难性事故‘

**物理与环境安全**

* 下班做到五关：关门、关窗、关空调、关灯、关计算机（除非有特殊要求）；
* 在办公室必须佩带公司颁发的贴有照片的门卡，使用门卡出入；
* 临时卡卡带颜色必须区别于员工卡卡带颜色；
* 严禁借用别人的员工卡及门禁卡出入；
* 严禁强制打开访问控制门或“未授权”用某器件支撑门；
* 严禁“尾随”、“潜入”办公区域；
* 非公司员工未经登记、许可，严禁擅自进入公司内部；
* 严禁未经批准在公司任何区域拍照、录像；

**人员安全**

* 确保所有人员（正式员工、实习生、劳务人员、合作方）都签有保密协议或保密条款；
* 积极参与公司信息安全培训；
* 配合公司信息安全委员会季度审计，并做相应改进；
* 不得违反《博彦科技员工保密协议》；
* 严禁员工非因公外出时携带涉密资料；
* 严禁蓄意发布并传播损害客户及公司及客户利益的信息和内容；
* 员工关系变动时必须做好涉密资产的移交和清理；
* 员工关系变动时确保其相应访问权限的调整；
* 严禁伪造他人名义发送Email或发送要求转发给多人的恶作剧邮件；
* 未经授权，不得发送全员邮件；

**资产安全**

* 未经批准，不得私自转借、交换个人计算机或其他可移动存储设备；
* 禁止员工下班后将笔记本电脑搁置在桌面；
* 确保所持工作文件经过安全等级识别并标明密级(部门文件密级设定参考公司标准)；
* 未经批准，禁止拷贝、保存、共享与本岗位无关的涉密资料；
* 不得持有与本岗位无关的涉密资料；
* 涉密资料必须妥善保管，不得放在未保护或易泄露的地方；
* 禁止将打印的涉密文档留在打印机旁，员工必须在1分钟内将其取走；
* 当文档不再需要时（特别是涉密文档），必须做销毁处理；