

三一运营过程体系文件

统一运维管理系统（UMA）用户操作手册

文档编号：

状态: ☐草稿 ☒发布 ☐修改



文档信息

撰写人	肖骁	文档版本:	2.1
撰写日期:	2014-10-20	版本发布日期:	2014-10-29
审批人:	贺东东	审批日期:	2014-8-28

修改记录

日期	修订人员	版本	备注
2014-8-28	肖骁	V1.0	初版发布
2014-9-28	肖骁	V2.0	快速上手使用部分修订, 格式调整
2014-10-28	肖骁	V2.1	新增部分问题解决方案



目录

1	引言	5
1.1	编写目的	5
1.2	适用范围	5
1.3	术语和定义	5
2	快速上手使用	5
2.1	首次访问 UMA	5
2.1.1	首次登陆	5
2.1.2	安装证书	6
2.1.3	安装 ActiveX 控件	8
2.1.4	将 UMA 添加到 IE 浏览器信任列表	9
2.1.5	安装 JRE (Java Runtime Environment)	10
2.2	简单访问	10
2.2.1	Web 界面简介	10
2.2.2	查找要访问的设备	11
2.2.3	访问设备	11
2.2.4	查看通知	12
2.3	修改账号密码	13
2.3.1	域账号密码修改	13
2.3.2	本地账号密码修改	14
3	深入了解	15
3.1	客户端环境	15
3.1.1	最佳客户端环境	15
3.1.2	客户端环境常见问题	15
3.2	SSH/Telnet 会话	16
3.2.1	在 Web 页面调用 SSH 客户端访问	16
3.2.2	直接使用 SSH 客户端工具访问	17
3.3	远程桌面 (RDP) 会话	20
3.3.1	访问 Windows 设备	20
3.3.2	修改 RDP 会话默认启动方式和分辨率	21



3.4	文件传输 (SFTP/SCP)	21
3.4.1	使用 FileZilla 进行文件传输	21
3.4.2	通过 rz/sz 进行文件传输	25
3.4.3	SCP 命令进行文件传输	27
3.5	XDMCP/Xfwd/VNC 会话	27
3.6	会话共享	28
3.6.1	支持的会话类型	28
3.6.2	如何发出邀请?	28
3.6.3	如何加入共享的会话	28
3.7	批量启动	28
3.7.1	如何使用批量访问	28
3.7.2	批量访问注意事项	28
3.8	命令复核	29
3.8.1	什么是命令复核?	29
3.8.2	如何对命令进行复核?	29
3.9	特殊的系统账号	29
3.9.1	self	29
3.9.2	any	29
3.10	账户设置	30
3.10.1	账户信息	31
3.10.2	自由修改密码	32
3.10.3	设备访问表格设置	33
更多		33



统一运维管理系统（UMA）用户操作手册

1 引言

1.1 编写目的

从普通用户的角度简单介绍如何使用统一运维管理系统（下文简称 UMA）。

1.2 适用范围

客户端环境的基本要求：

操作系统：Windows XP、Windows Vista 或者 Window 7；

浏览器：IE 7.0 以上版本的浏览器；

1.3 术语和定义

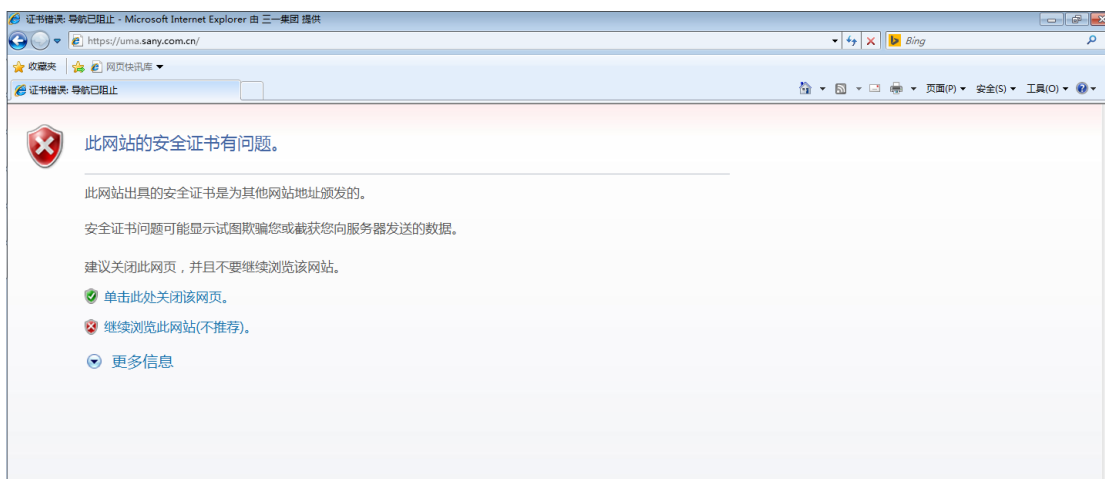
UMA：统一运维管理系统。

2 快速上手使用

2.1 首次访问 UMA

2.1.1 首次登陆

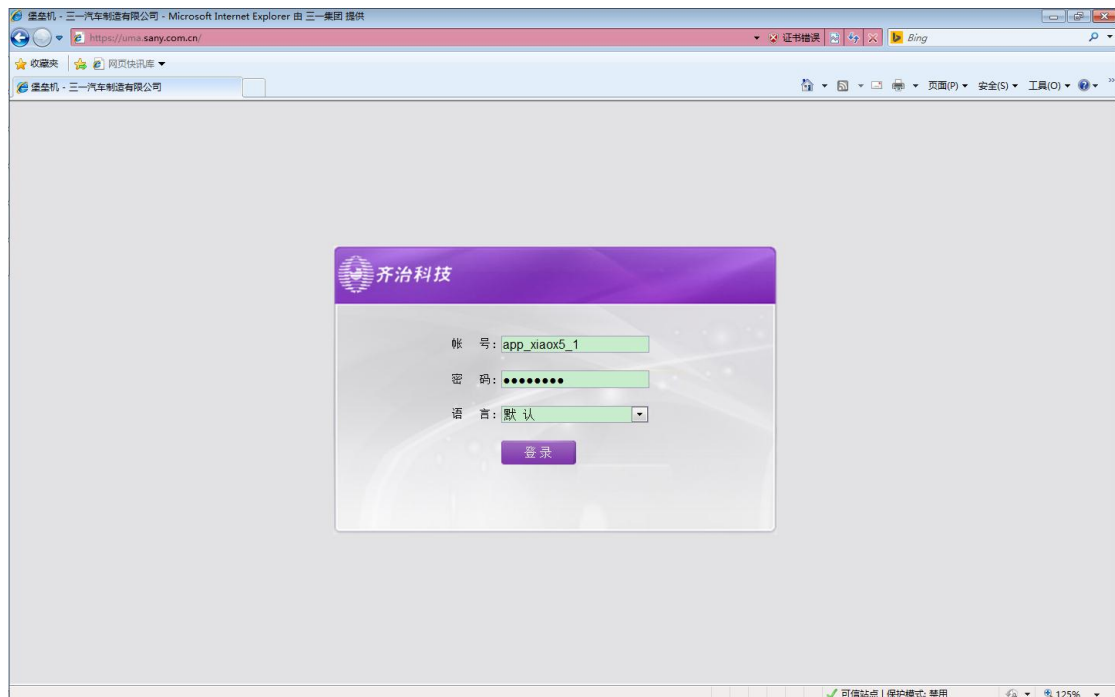
访问地址为 <https://uma.sany.com.cn>。回车后将会显示如下提示：



点击“继续浏览此网站（不推荐）”，将出现 UMA 的登录页面（未安装证书前，加载速度较慢，请耐心等待，具体证书安装方式见下文），如下图。输入用



于登录现有堡垒机的 APP 类账户和密码点击即可登录。



2.1.2 安装证书

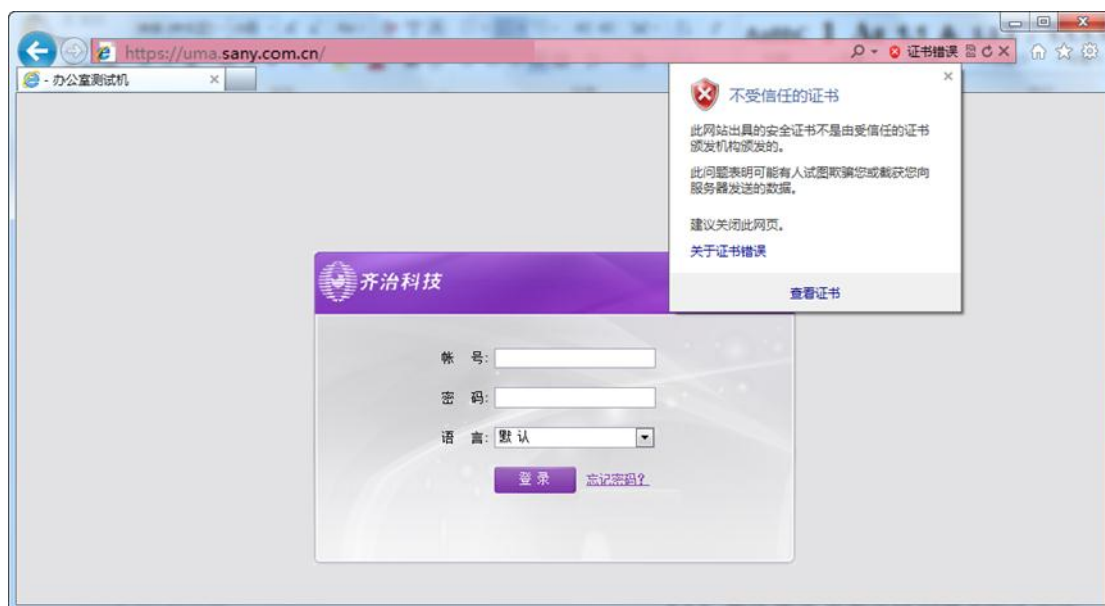
未安装证书的情况下，系统加载速度较慢，因此强烈建议优先安装证书文件，共需安装两个证书，分别为堡垒机 https 证书和堡垒机根证书，具体操作如下：

1) 安装 https 证书


输入地址后，点击“继续浏览网站”



点击浏览器地址栏中的“证书错误”—“查看证书”，然后在弹出的证书界面点“安装”，“下一步”—“下一步”...即可。

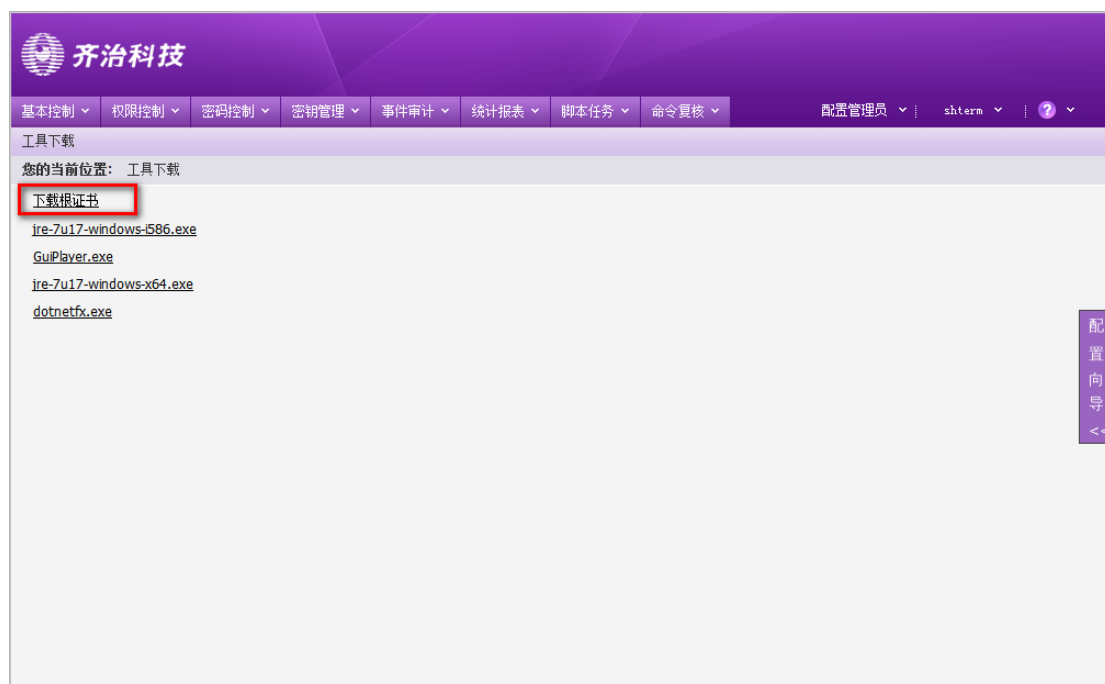


2) 导入根证书

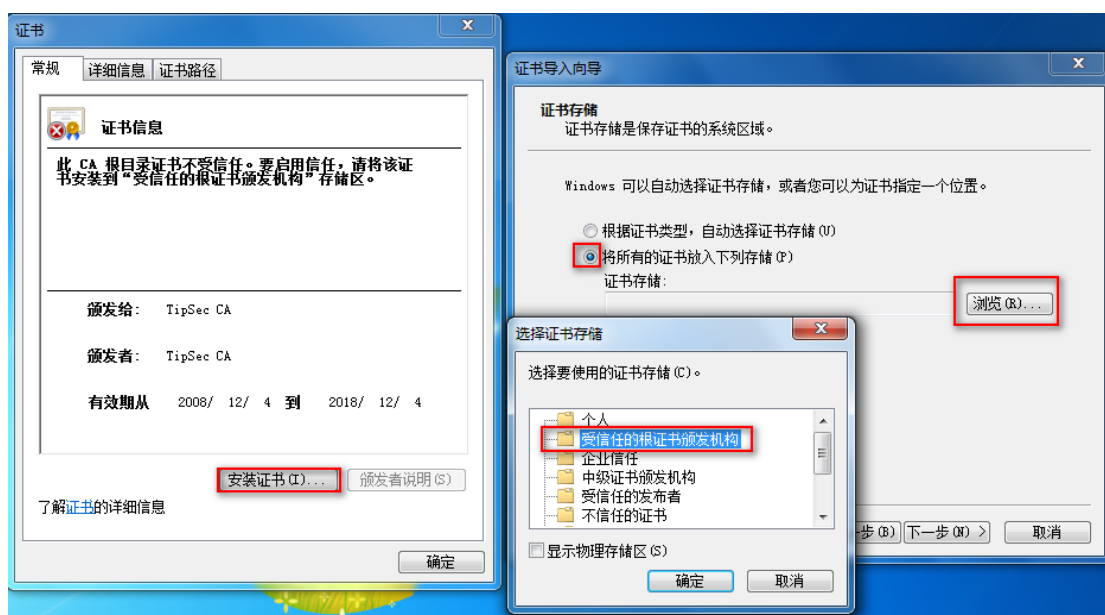
进入系统后，在页面右上角的下拉菜单中点击“工具下载”，在工具下载页面，下载根证书到本地；



提示：“工具下载”界面除根证书可以下载外，还可下载多个有效工具，如UMA 系统专用的 JRE、UMA 的 IE 控件、Linux 下的文件传输工具 FileZilla 等。

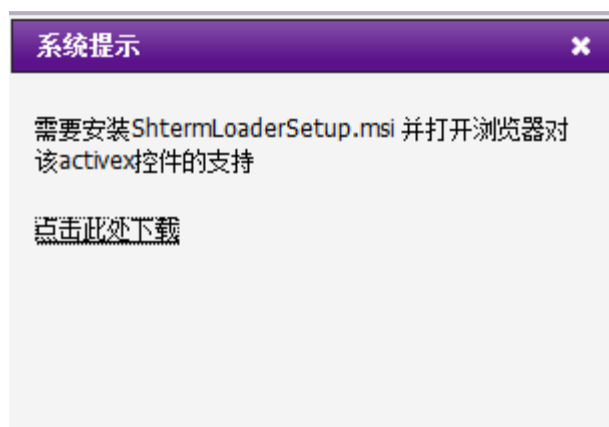


双击下载根证书文件，在“证书”窗口点击“安装证书”—“下一步”；在证书向导窗口中选择把根证书安装到“受信任的根证书颁发机构”。完成后重启浏览器即可。



2.1.3 安装 ActiveX 控件

使用 IE 浏览器首次访问，将会收到系统提示要求安装 ActiveX 控件，如下图所示：



按照提示下载并安装控件，完成后重启浏览器并重新登录。

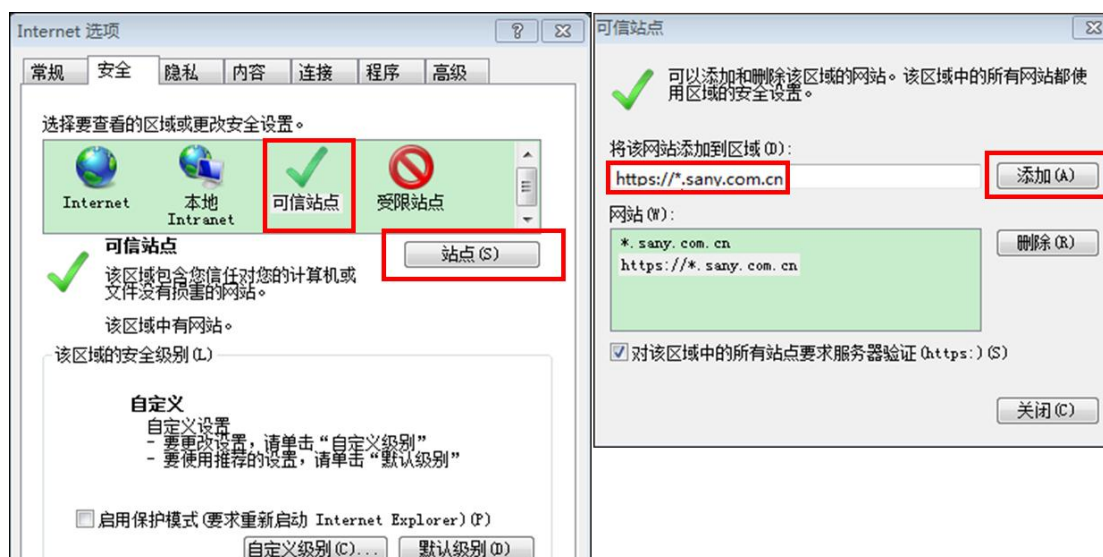
提示：如果提示“此安装程序需要.NET Framework 版本”，可以点击页面右上角问号，在“工具下载”中下载 dotnetfx.exe 并安装。

2.1.4 将 UMA 添加到 IE 浏览器信任列表

要使用 ActiveX 控件必须将 UMA 添加到 IE 浏览器的信任列表。如果 UMA 不在浏览器信任列表，将会收到以下提示：



处理方式如下图：打开 IE 浏览器的“Internet 选项”，进入“安全”选项卡中，选中可信站点，并单击“站点”，将 https://*.sany.com.cn 添加到“可信站点”中。





2.1.5 安装 JRE (Java Runtime Environment)

要完整使用 UMA，建议安装 JRE1.6 或以上版本。请检查是否已经安装，如果未安装请从 UMA 的“工具下载”中下载并安装。请点击 UMA 页面右上角问号标志，在“工具下载”中下载“jre-7u17-windows-i586.exe”，并进行安装。

提示：推荐使用堡垒机自带的 java 版本进行安装，否则在使用一些第三方工具如 FileZilla 时可能出现调用失败。

2.2 简单访问

普通用户可以通过 UMA 的 Web 站点访问授权目标设备，本节简要介绍如何访问通过 UMA 的 Web 站点访问目标设备。

2.2.1 Web 界面简介

下图是普通用户登录 UMA 后的页面视图：



为了便于表述使用橘黄色标记将页面分为 4 个区域：

左上①为菜单栏，包含设备访问、命令复核两个主菜单；

右上②，用户角色、当前用户和帮助菜单（问号标志），可以切换用户角色、退出登录、设置用户账号、下载常用工具、查看版本信息；

左下③，访问规则组列表（请点击“按访问规则分组”），点击后右下④区域



可以显示相应的设备。

右下④，可访问设备清单，默认为最近访问的设备清单，点击左侧规则（部门）可以显示相应的规则（部门）下的设备。

注意：Web 页面的超时时间为 30 分钟，如果登录后超过 30 分钟无任何新的 Web 请求会话将自动退出。

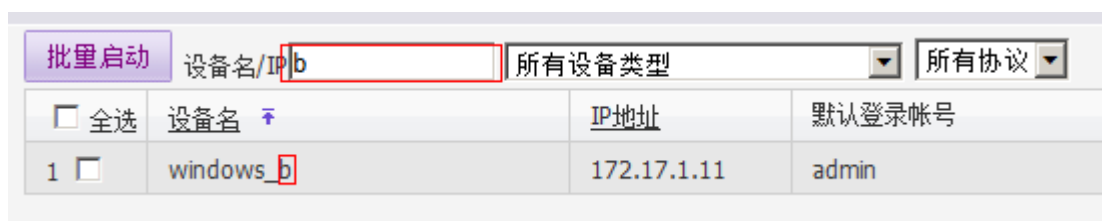
2.2.2 查找要访问的设备

登录 UMA 后，默认会打开最近访问页面，该页面会列出最近或者部分可访问设备。如果列表中没有，可以通过以下几种方式查找设备：

- 1) **按访问规则分组查看设备：**在设备访问页面左侧点击相应规则可查看该规则下的设备，目前在部门未启用的情况下，建议按此方式访问设备，如下图：



- 2) **按部门分组查看设备：**该功能暂未启用。
- 3) **搜索和过滤设备：**可在设备清单栏上的“设备名/IP”搜索框，按照设备名或者 IP 进行模糊搜索，或者通过设备类型及协议进行过滤。如下图：



2.2.3 访问设备

使用鼠标点击设备可展开设备的可用服务（协议），如下图，点击①后，会弹



出②“服务”：

<input type="checkbox"/> 全选	设备名	IP地址	默认登录帐号	设备类型	简要说明
1 <input type="checkbox"/>	10.0.24.1 ①	10.0.24.1	test	General Linux	HRM应用服务器
服务	<div>  SFTP  ssh ② </div>				
2 <input type="checkbox"/>	10.0.24.10	10.0.24.10	any	General Linux	olm在线学习系统应用服务器

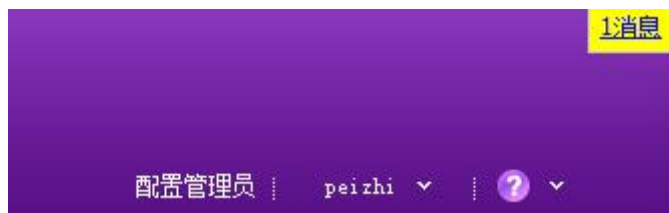
在②中，通过左键单击服务图标可以以默认账号（上一次成功访问的账号）访问该服务，右键单击图标可以打开服务的高级选项（如选择登陆账号、调整分辨率、磁盘映射等）。

提示：

- 1) 除“any”账号外，其他登录账号前带有“*”的，均为代填密码的账号。
- 2) 部分访问规则要求填写备注信息，需要填写访问目的后方可继续访问；
- 3) 如果管理员启动了双人授权，需要授权人输入授权密码后方可使用；
- 4) 关于各种服务的详细使用说明请参考“深入了解”中的相关内容。

2.2.4 查看通知

当用户被赋予工单审批人、命令复核人或双人授权人权限之后，在右上角“消息”会显示未查看的消息数。



点击“消息”，查看相关信息；点“详细”可以进行授权和驳回操作。



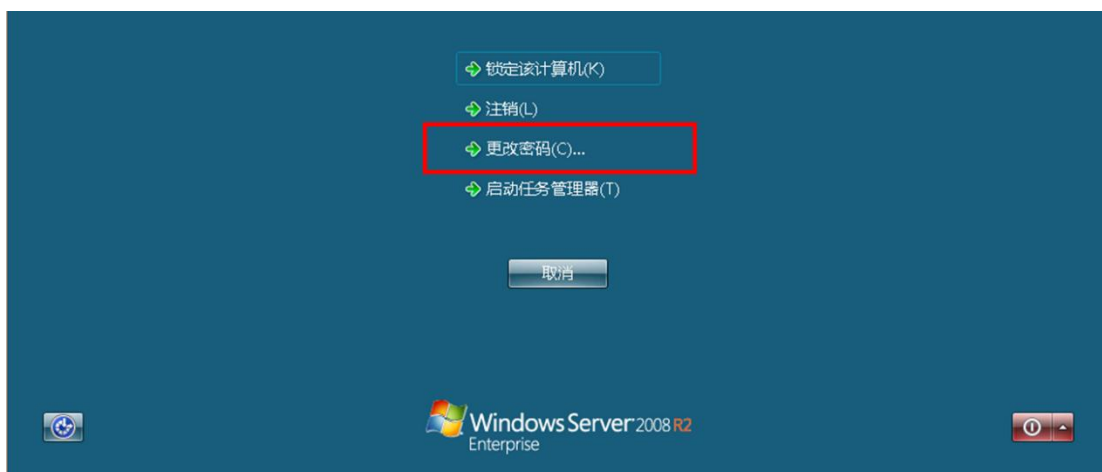


2.3 修改账号密码

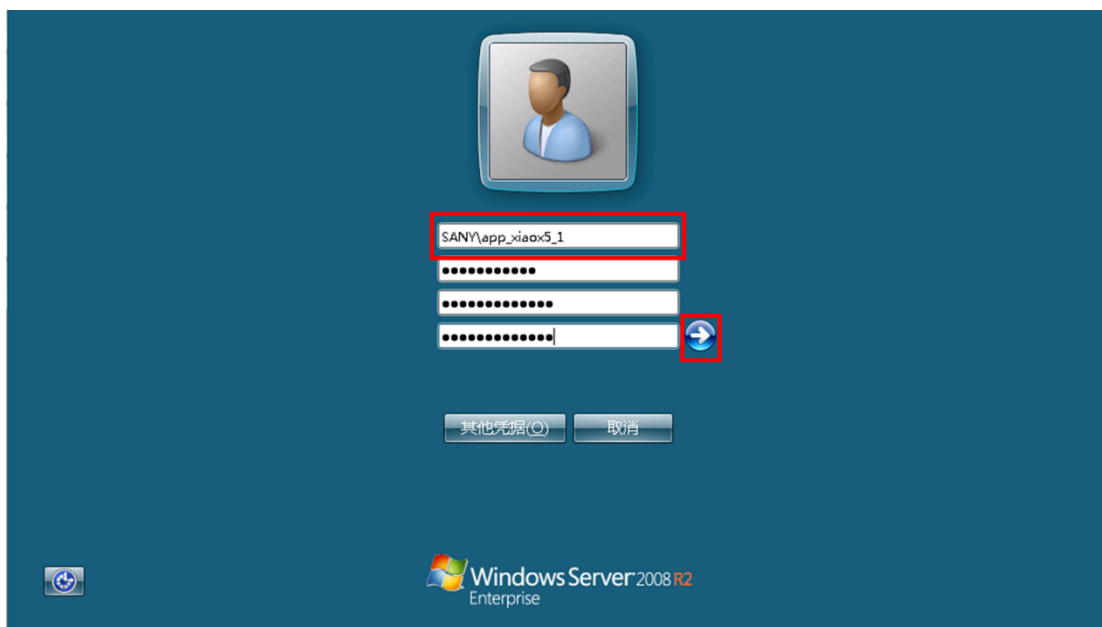
2.3.1 域账号密码修改

目前 UMA 系统默认使用三一域中的管理员类域账号（如 app_XX_1，x86-XX）登陆，如需修改账号密码，请在三一域中进行修改。操作方式如下：

- 1) 在个人办公电脑或已加域的服务器中按 **ctrl+Alt+Delete**，进入如下界面，选择“更改密码”。



- 2) 将待修改的账号变更为 **app** 账号，如下图所示，填入旧密码及更改的新密码即可，按确认键即可。



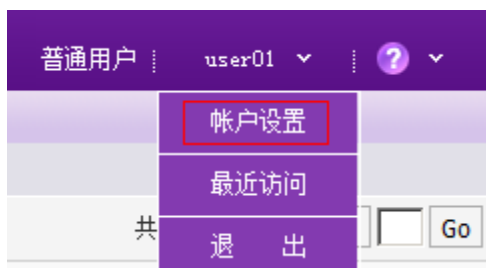
提示：如 app 账号密码已过期，该改密方式不再可行。请各位通过 OA 流程“集团固化流程/IT 类/公共应用权限/IT 系统用户密码重置申请”来重置流程。



2.3.2 本地账号密码修改

对于极少部分的本地用户，为了账号安全，账号密码有效期均为 90 天，密码到期前十天会收到提醒，过期后 10 天内依然允许使用老密码登录后重设密码。普通用户修改密码的方法如下：

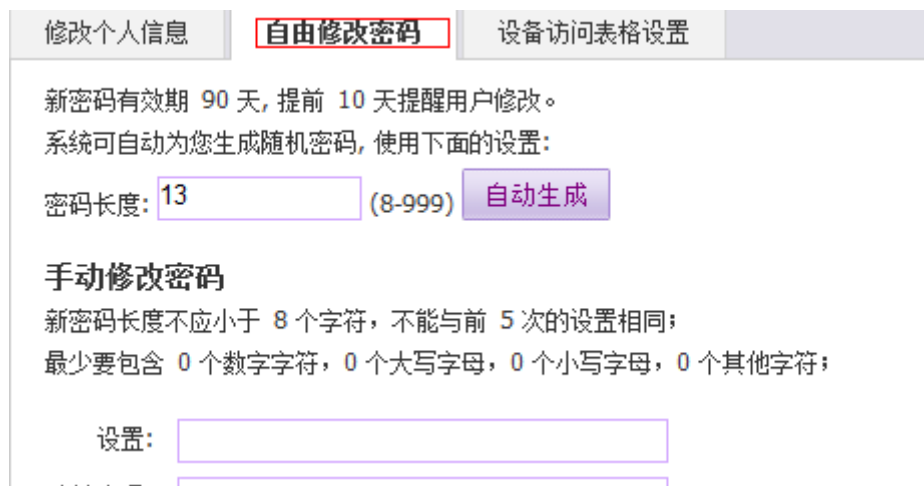
登录 UMA 后点击页面右上角当前用户名，如下图：



在下拉菜单中点击“账户设置”，如下图：



输入当前密码后点击“确定”，在打开的页面中选择“自由修改密码”，如下图：





可以选择自动生成密码，也可以选择手工输入新密码（请注意页面中管理员设定的密码复杂度要求）。

提示：如果登录 UMA 时的身份验证方式不是本地（native），将无法在此修改密码，详情请咨询系统管理员。

3 深入了解

本部分将深入完整的介绍 UMA 的普通用户可能遇到的各种问题，建议根据需要选择性的阅读和查看相关内容。

3.1 客户端环境

3.1.1 最佳客户端环境

操作系统：Windows XP、Vista 或者 7，32bit/64bit

浏览器：IE 7 及以上版本，并将 https://*.sany.com.cn 加入 IE 加入受信任站点，安装堡垒机 https 证书和 UMA 的根证书（在工具下载中下载并按照提示安装即可）；

其他：安装“工具下载”中提供的 JRE 版本，安装 Shtermloader，安装 .NET Framework 2.0。

关于以上环境的设置方法可以参考 2.1 中的介绍。

3.1.2 客户端环境常见问题

为了方便灵活的设置客户端环境，本节列举相关的常见问题：

3) 是否支持 Unix/Linux 和其它非 Windows 操作系统？

支持。但是无法使用部分 Windows 下特有的功能，比如 mstsc 方式访问 Windows 设备、RemoteAPP.....。

4) 是否必须使用 IE 浏览器？

否。UMA 可兼容大多数主流的浏览器，可以使用 Firefox、Chrome 或者其他浏览器访问 UMA（需要安装 JRE）。但是如果希望使用 Shtermloader ActiveX 控件加速启动速度，建议使用 IE。

5) 必须要安装 Java 吗？

建议安装。除非只使用 SecureCRT、Putty、FileZilla 等客户端工具访问字



符类设备，不访问 UMA 的 Web 页面，否则请务必安装。

6) 是否必须安装 Shtermloader ActiveX 控件？

否，Shtermloader ActiveX 控件可以优化设备访问页面的速度和 Windows 设备访问相关的功能，因此如果使用 IE 浏览器时，会强制要求安装。如果不安装，可以使用非 IE 浏览器通过安装 Java 访问 UMA。

7) 是否必须安装 .NET Framework？

否，如果不需要使用 RemoteAPP 功能则不需安装。

8) 安装 Shtermloader ActiveX 控件后是否依然需要安装 Java？

依然需要，如果需要使用下列功能依然需要安装 Java：Java 模式的 RDP 和 RDPAPP 会话、Jterm 方式的字符会话访问、会话共享、RDP 以外的其他图形会话。

9) 是否支持 64 位的 IE 浏览器？

支持。

10) 客户端需要访问 UMA 的那些端口？

默认情况下需要访问 UMA 的下列端口：

TCP/22，用于 SSH/Telnet/FTP/SFTP/SCP 协议的访问；

TCP/443，用于访问 UMA 的 Web 站点；

TCP/5899，用于访问各种图形会话的访问；

TCP/3389，用于 mstsc 模式的 RDP 会话访问。

3.2 SSH/Telnet 会话

3.2.1 在 Web 页面调用 SSH 客户端访问

通过 Web 启动 SSH 或者 Telnet 会话时，可直接调用 SecureCRT 或者 Putty，默认调用软件可通过修改账户设定进行调整：

- 1) 点击页面右上角账户名称下的“账户设置”菜单；
- 2) 输入当前密码，并确定；
- 3) 在“修改个人信息”选项卡中，修改“字符会话客户端”为 SecureCRT 或者 Putty，完成后点击确定即可。

注意：



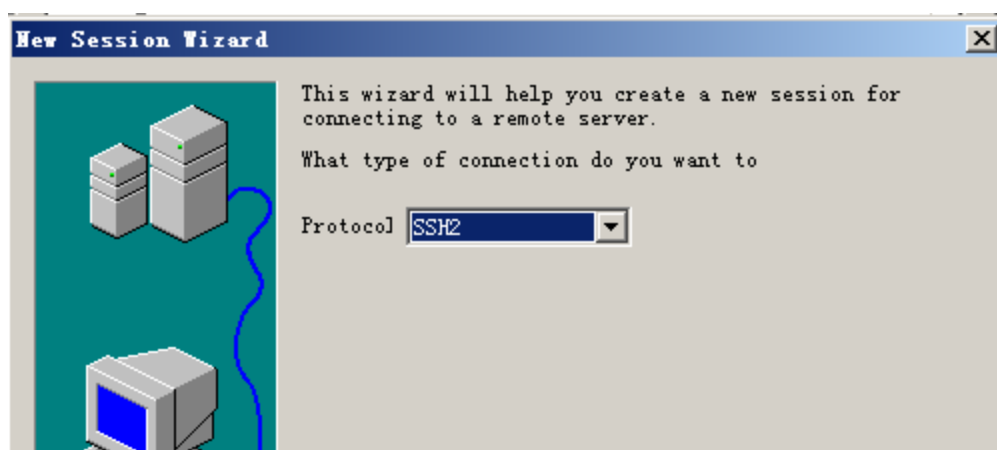
- 1) 使用 SecureCRT 作为字符会话客户端，将会调用本地的该软件，因此计算机上必须已经安装 SecureCRT，首次使用将提示您选择软件路径。
- 2) 如果操作系统不是 Windows，设置 SecureCRT 或者 Putty 作为客户端后，UMA 将使用系统自带的 Jterm 作为实际的终端。

3.2.2 直接使用 SSH 客户端工具访问

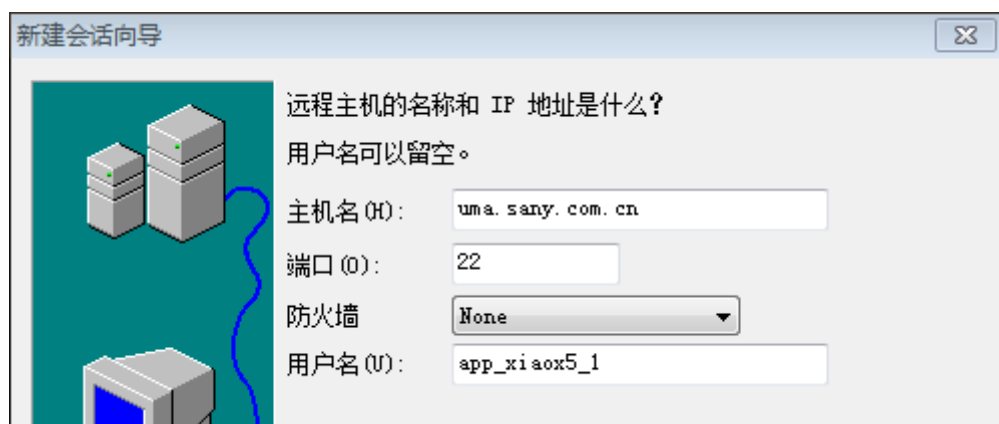
UMA 允许普通用户使用任何兼容 SSH V2 协议的客户端工具，通过访问 UMA 的 22 端口后，进一步访问目标设备的 SSH 和 Telnet 服务。该访问方式无需在 web 页面进行登录。这些工具包括：SecureCRT、Putty、Xshell、OpenSSH 等兼容 SSH，且仿真方式可调整为 Xterm 的客户端。

以下以 SecureCRT 为例介绍如下访问：

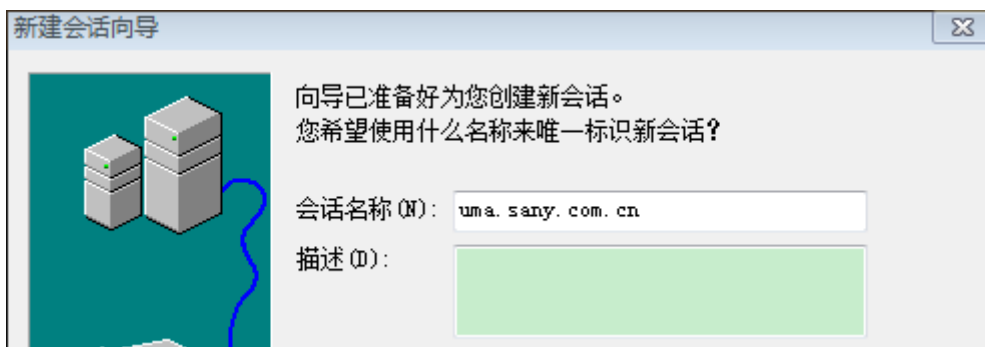
- 1) 打开 SecureCRT，新建连接，选择协议为 SSH2，如下图：



- 2) 设置主机名 (Hostname) 为 UMA 的 IP 或者域名，端口 (Port) 为 22，用户名 (Username) 为登录 UMA 的用户账号。如下图：



- 3) 设置会话名称 (Session) 为任意名称，如 UMA：



- 4) 完成后点击连接 (connect)，在登录对话框中输入密码，点击“OK”，即可登录。



- 5) 登录后依次选择规则、设备和系统账号后即可访问目标设备。

```
1: 规则1
2: 规则3
0: all
Select group: 1

1: linux-1 (192.168.5.201)
2: linux-2 (192.168.5.202)
Select server: 1

1: enable
2: root
Select account: 2

SHTerm 2.4.6-r337
Copyright (c) 2005-2011, QiZhi Technologies. All Rights Reserved.
License granted to Test Customer.
Valid from 2012-02-15 to 2013-02-15.
#####welcome#####
*****
Last login: Mon Feb 27 14:40:43 2012 from 192.168.4.177
root@ss-201 ~1#
```

- 6) 如果出现如下图报错，需要将 SSH 客户端的仿真方式改为 Xterm。



```
14: 10.0.48.5 (10.0.48.5) JOA接口服务器
15: csxolm01v-ap (10.0.24.4) 在线学习 应用服务器
16: csxolm02v-ap (10.0.24.5) OLM 流媒体服务器
Select server: 1

1: any
2: * test 测试账号
Select account: 2

SHTERM 2.6.3-35fa58f3
Copyright (c) 2005-2011, Qizhi Technologies. All Rights Reserved.
License granted to Sany Auto.
Valid from 2014-08-01 to 2014-11-20.
Error: only support xterm terminal

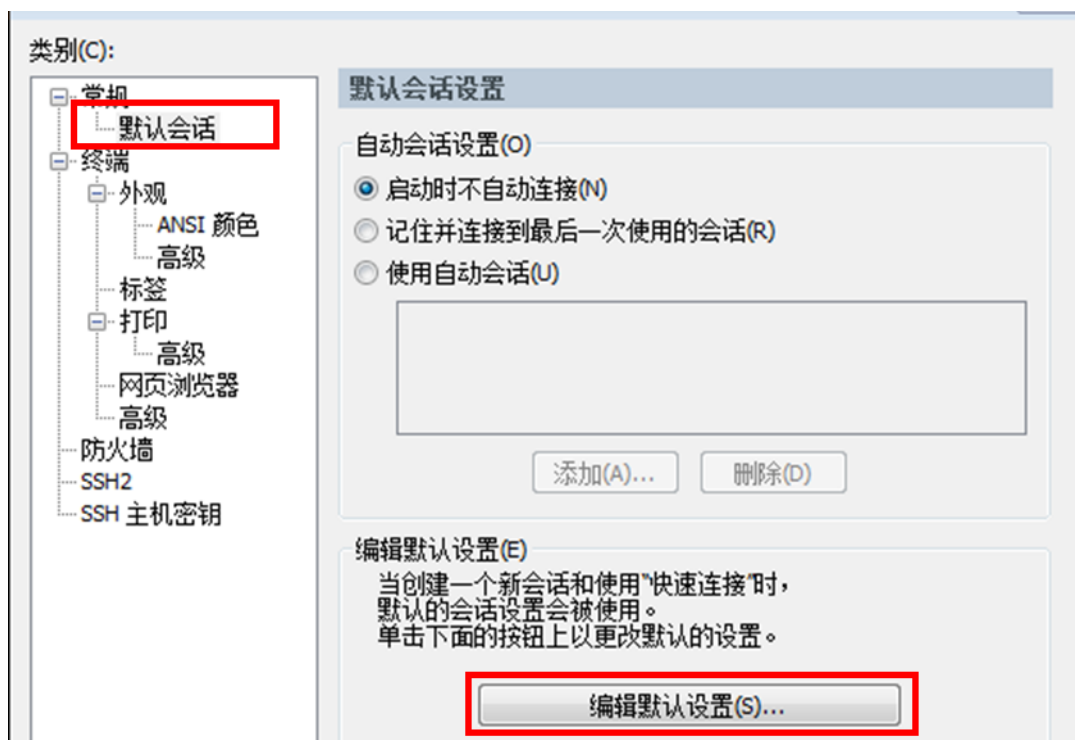
Session closed, press ENTER to start over again or q,Q to exit.
```

修改方式如下：

点击 SecurCRT 菜单中“选项”的“全局选项”。

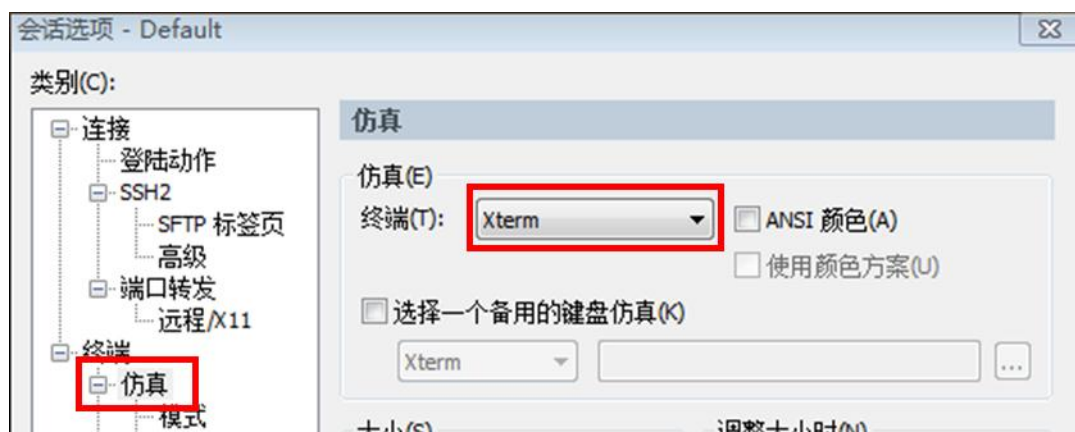


弹出的对话框中，点击“默认会话”，然后选择“编辑默认设置”。





然后在其中选择“仿真”，将终端的方式改成 Xterm。



提示：

- 1) 在选择访问规则、设备和系统账号时可以使用“/”+“关键词”进行模糊搜索，例如/24.1 可以匹配到 IP 为 10.0.24.1 的设备；
- 2) 在选择设备和系统账号时可以输入菜单中的序号进行选择，也可以直接输入设备名、IP、系统账号名进行选择；
- 3) 按 2 次回车可返回上一级菜单；
- 4) 在任意选择菜单中均可以使用 ping 命令检查目标设备网络是否正常。

3.3 远程桌面（RDP）会话

3.3.1 访问 Windows 设备

访问 windows 设备，通过堡垒机 web 界面中访问目标设备 RDP 服务：

- 1) 在设备访问中找到要访问的设备；
- 2) 点击目标设备的 RDP 图标。
- 3) 如果已经访问过 UMA，将按照上一次访问时使用的系统账号和启动方式启动会话，如果没有访问过，UMA 将弹出高级菜单，如下图：



**提示：**

- 1) 屏幕大小：指启动会话的屏幕大小
- 2) Console：与 `mstsc /admin` 或者 `mstsc /console` 功能一致
- 3) `mstsc`：是否使用微软的客户端访问，默认为勾选状态，如果取消勾选将使用 java 访问的 `applet` 访问
- 4) 磁盘映射：是否要映射本地磁盘到远程计算机。

注意：

可能无法看到 `console` 和磁盘映射选项，表明管理员禁用了相关功能。

3.3.2 修改 RDP 会话默认启动方式和分辨率

如果希望修改 RDP 的默认启动方式和屏幕分辨率，请按照以下方法完成：

- 1) 点击页面右上角账户名称下的“账户设置”菜单；
- 2) 输入当前密码，并确定；
- 3) 在“修改个人信息”选项卡中，修改“图形会话分辨率”、“图形会话默认分辨率”和“RDP 会话默认启动方式”。

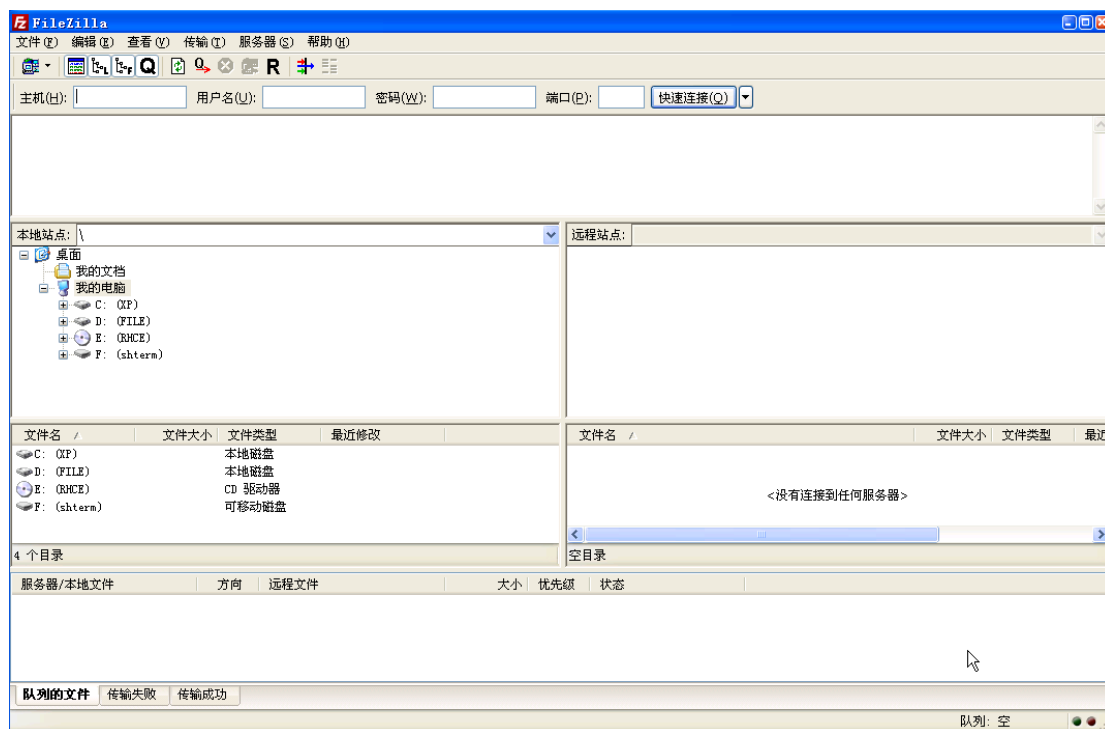
3.4 文件传输（SFTP/SCP）

UMA 支持对 SFTP/SCP 的访问，为了安全无论最终目标设备使用何种协议，要通过 UMA 进行文件传输，必须使用兼容 `sftp/scp` 协议的客户端工具先访问 UMA。推荐使用 FileZilla、SCP 命令访问 UMA 的文件传输服务。使用方法简介如下：

3.4.1 使用 FileZilla 进行文件传输

方式 1：要使用 FileZilla 进行文件传输，在设备密码已代填的情况下，可按以下方式操作：

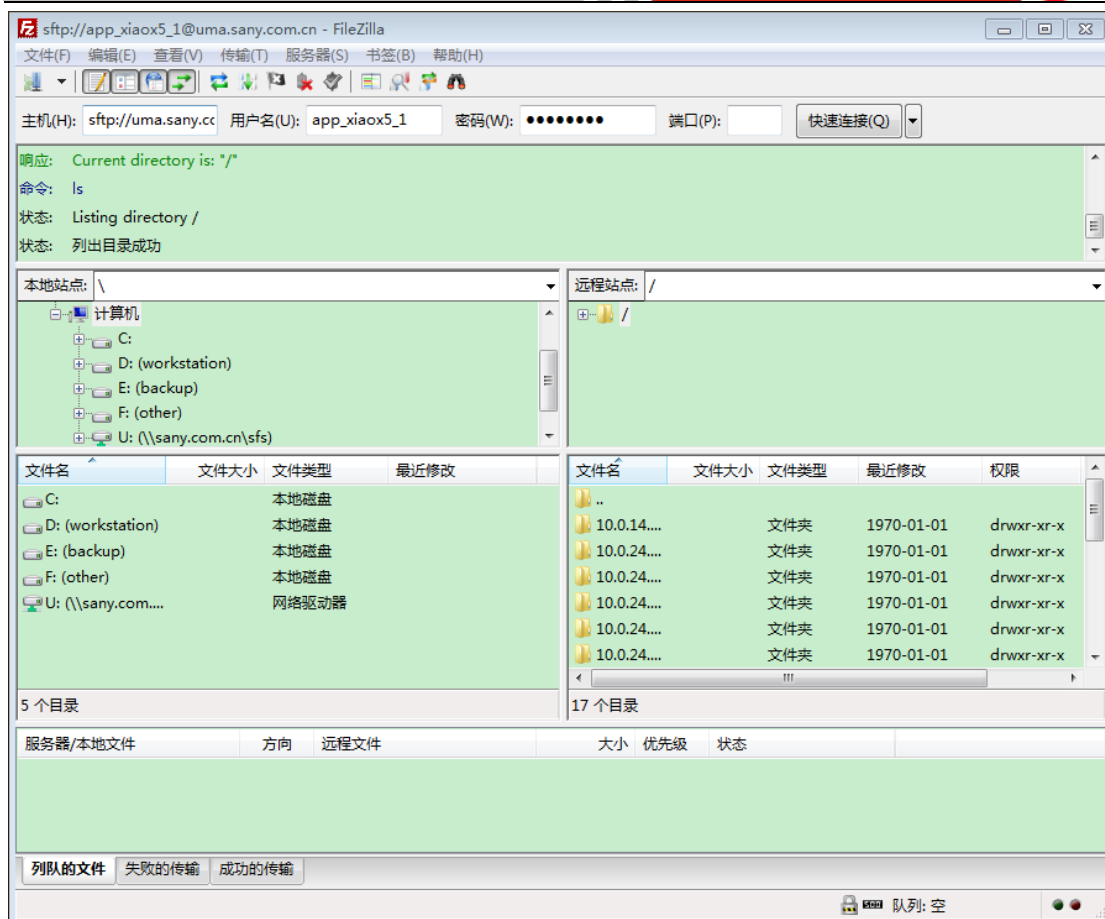
- 1) 安装并运行 FileZilla 后（可在“工具下载”中进行下载），出现如下界面：



- a) “主机”中输入 uma.sany.com.cn 或 10.0.96.66;
- b) “用户名”中填写 UMA 用户账号;
- c) “密码”中填写用户账号密码;
- d) “端口”中填写 sftp 协议端口: 22;
- e) 点击“快速连接”, 出现如下画面:



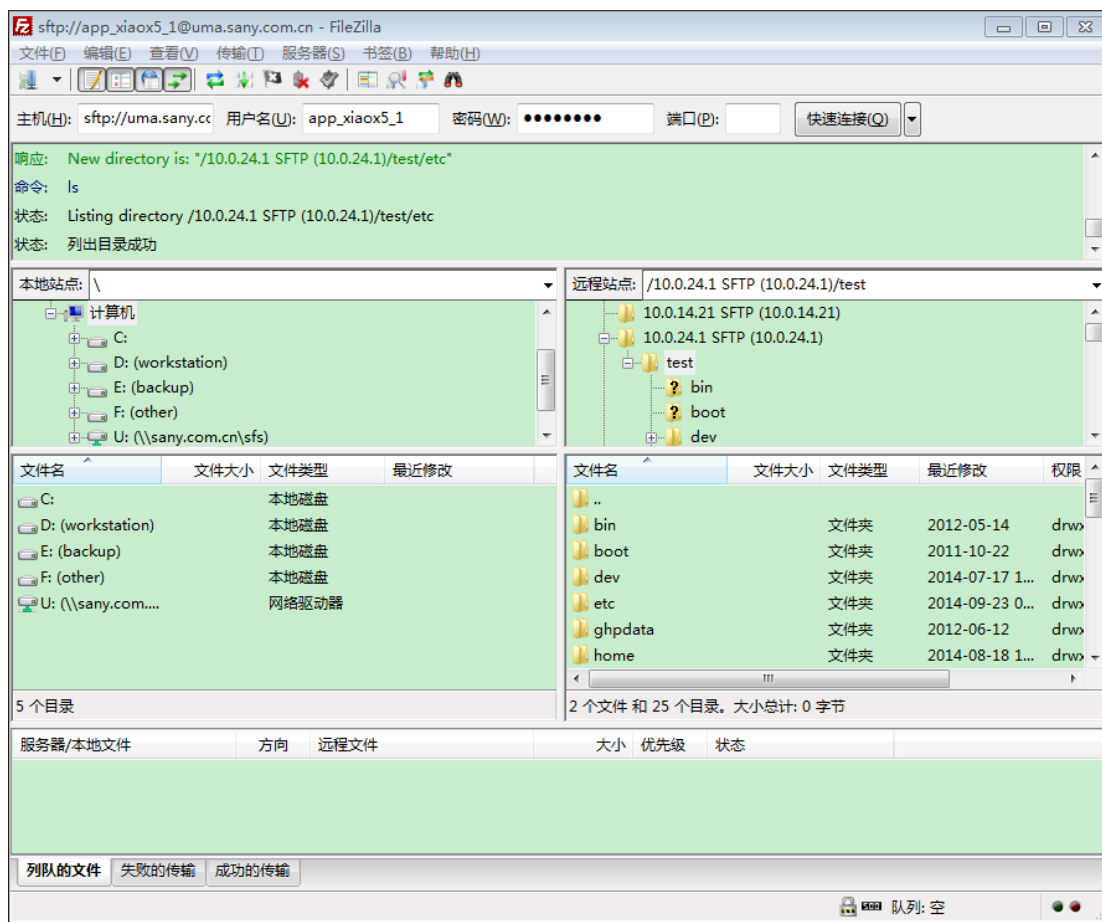
- 2) 勾选“总是信任该主机, 并将该密钥加入缓存”, 点击“确定”, 出现如下画面:



3) 在“文件名”列表中，点击相应的设备，出现如下画面：



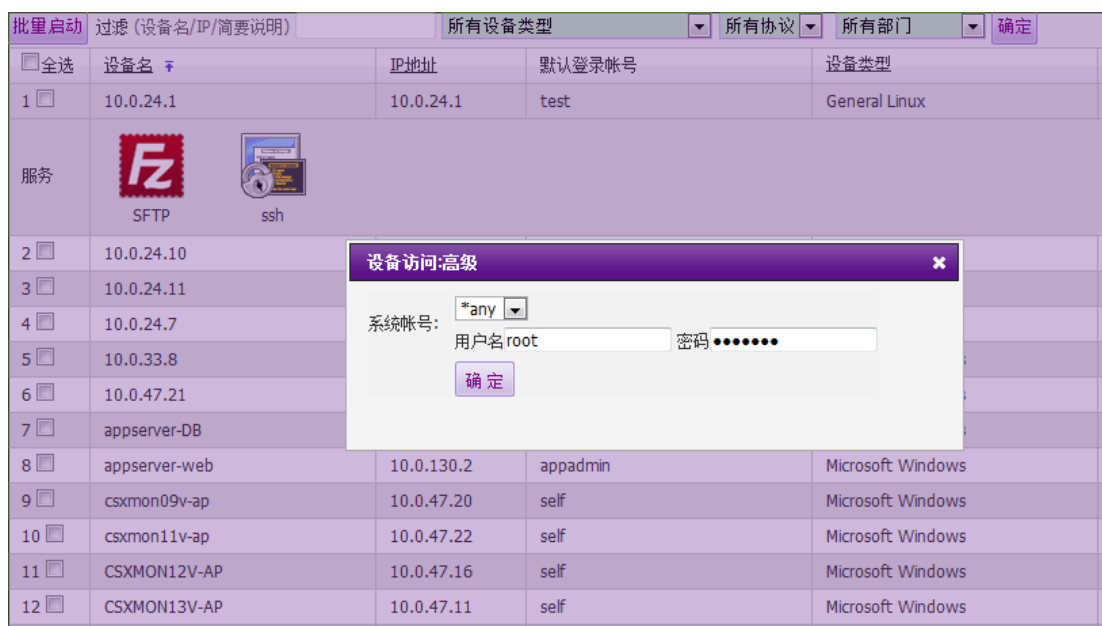
4) 点击相应的“系统账号”，出现如下画面：



此时已进入目标的根目录，可以选择进入相应的目录进行文件上传与下载。

方式 2: 在密码未代填的情况下，可按如下方式操作：

在 web 页面中，右键点击 SFTP，账号选择为“any”，填入用户名和密码，即可弹出 FileZilla，按方式 1 描述的方式即可进行文件传输。





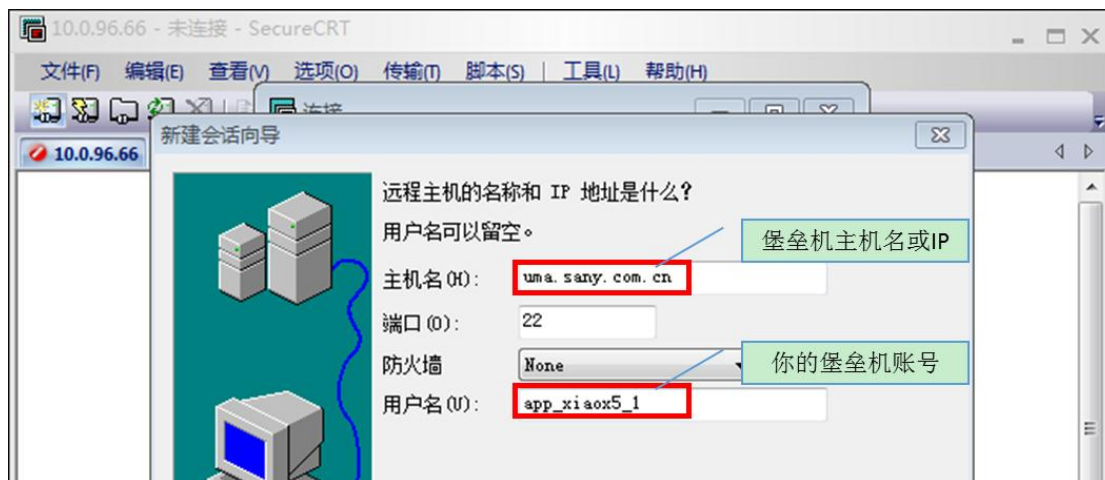
3.4.2 通过 rz/sz 进行文件传输

前提条件:

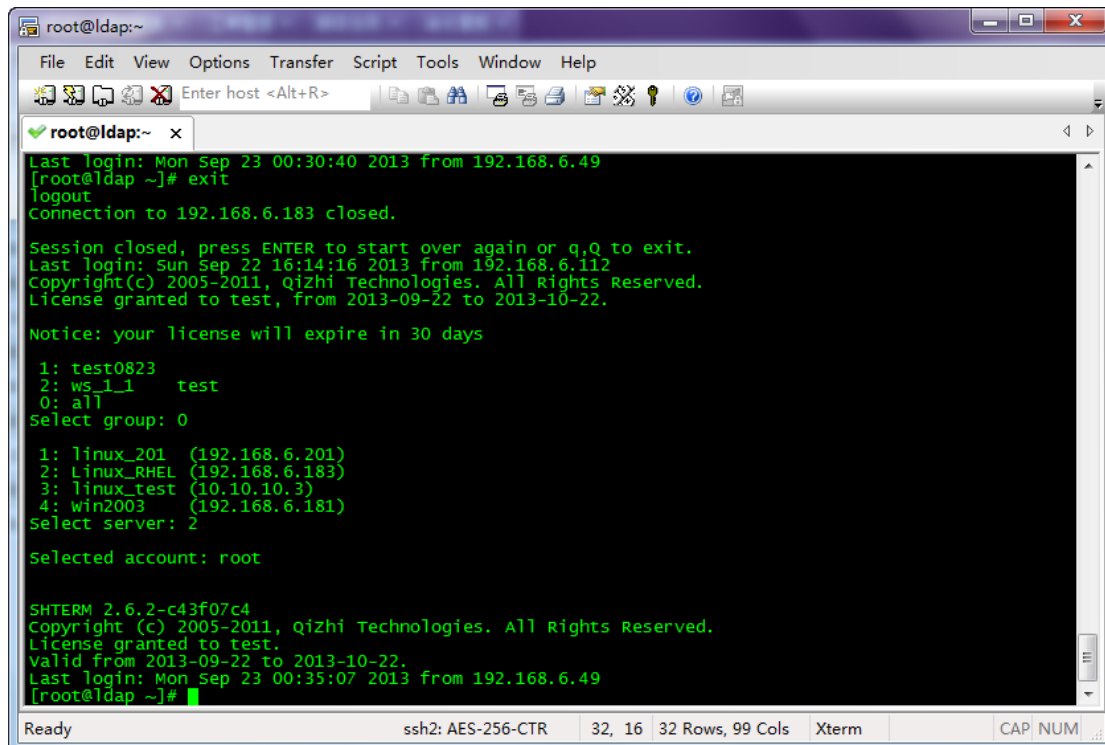
- 1) 目标设备上安装了 lrzsz 软件包;
- 2) 使用的 ssh 客户端支持 zmodem 协议;

以 SecureCRT 为例:

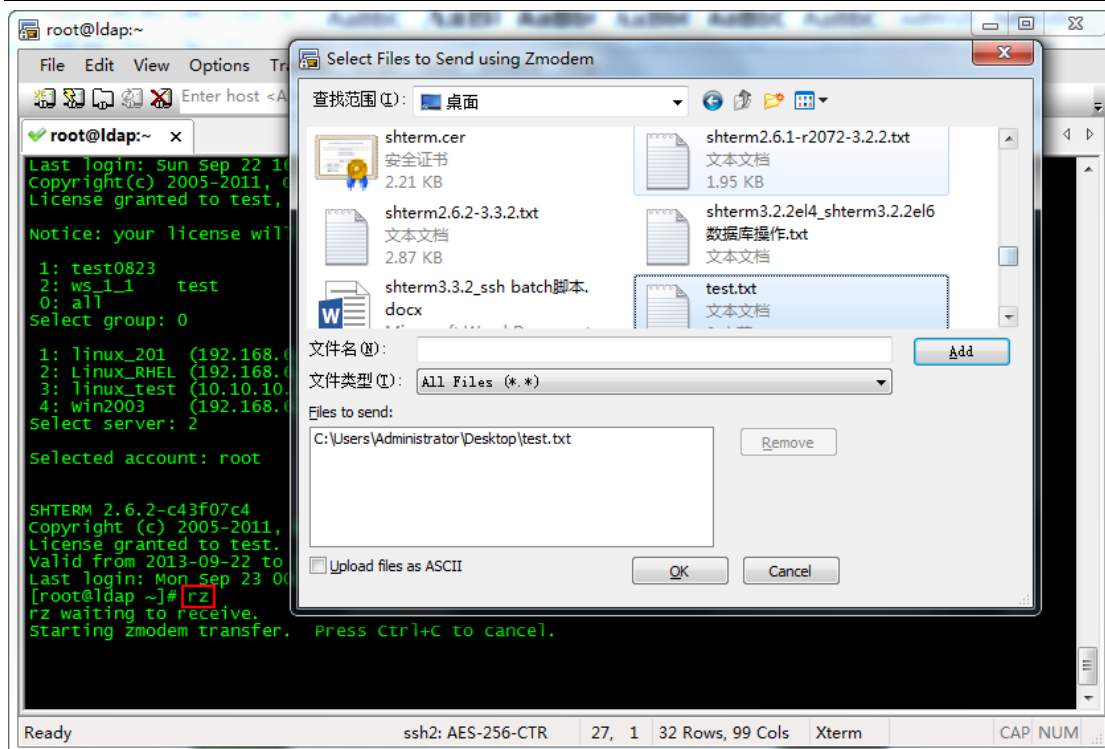
- 1) 通过 SecureCRT 登陆堡垒机;



- 2) 登入一台目标设备

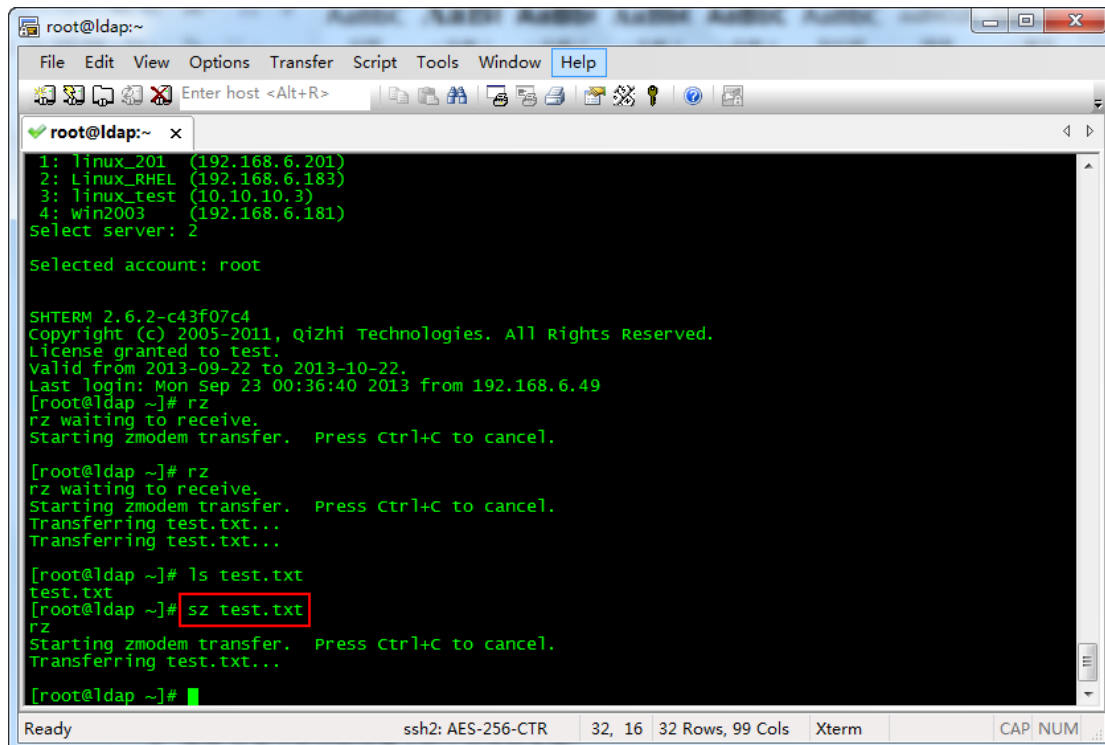


- 3) 使用 rz 命令向目标设备上传文件



输入 rz 命令之后,选择要上传的文件(test.txt),然后点击“OK”即可把 test.txt 上传到目标设备上。

4) 使用 sz 命令把目标设备上的文件传到本地;命令格式 sz <文件全名>



文件下载到“我的文档”文件夹里面的“下载”文件夹下（具体可以查看 Options-Session Options 中的 x/y/z modem 相关的设置。



3.4.3 SCP 命令进行文件传输

使用 scp 命令通过 UMA 向目标设备传输文件与直接使用 scp 命令向目标设备传输文件是基本相同的，只是通过 UMA 向目标设备传输文件时，远端地址的格式不同。其格式如下：

UMA 用户账号@UMA 主机地址：/目标设备地址/目标设备上的系统账号/目标设备上的目录

比如：

UMA 用户账号为：app_xiaox5_1

UMA 的主机地址为：10.0.96.66

目标设备地址为：10.0.24.1

目标设备的系统账号为：root

要进行文件操作的目标设备目录为：/var/www/

那么远端地址为：

app_xiaox5_1@ 10.0.96.66:/ 10.0.24.1/var/www/

举例来说，如果 app_xiaox5_1（用户账号）要通过 UMA（10.0.96.66）将本机的/root/new.css 上传到目标设备（10.0.24.1）的/var/www 目录中，并命名为 default.css，可以使用如下命令：

```
#scp /root/new.css app_xiaox5_1@10.0.96.66:/10.0.24.1/var/www/default.css
```

回车后，输入 app_xiaox5_1 的用户账号密码即可。

反之，如果 app_xiaox5_1（用户账号）要通过 UMA（10.0.96.66）将目标设备（10.0.24.1）的/var/www 目录中 default.css，下载到本机的/root/目录，并命名为 new.css，可以使用如下命令：

```
#scp app_xiaox5_1@10.0.96.66:/10.0.24.1/var/www/default.css /root/new.css
```

回车后，输入 app_xiaox5_1 的用户账号密码即可。

3.5 XDMCP/Xfwd/VNC 会话

XDMCP 协议，使用方法与 Java 模式的 RDP 会话基本相同，但该协议不支持系统账号密码代填，使用该协议必须知道目标设备的系统账号的密码；

Xfwd 协议，使用方法与 Java 模式的 RDP 会话基本相同；

VNC 协议，使用方法与 Java 模式的 RDP 会话基本相同，如果管理员未设



置 VNC 密码系统会要求手工输入密码。

3.6 会话共享

会话共享是指两个用户共享同一图形会话，用于协同任务或者远程协助。

3.6.1 支持的会话类型

支持非 mstsc 方式的 RDP 和 rdpapp 会话，xdmcp 会话、xfwd 会话、vnc 会话（使用密码代填）。

不支持任何字符会话和 mstsc 模式的 RDP 和 rdpapp 会话

3.6.2 如何发出邀请？

- 1) 会话要求必须有一个符合支持的会话列表中的活动会话；
- 2) 打开“设备访问”-“会话共享”中的我的会话中找到要共享的会话，点击“邀请”；
- 3) 选择一个用户后点击“发出邀请”；
- 4) 通知邀请对象。

3.6.3 如何加入共享的会话

- 1) 在“设备访问”-“会话共享”页面“我收到的邀请”中找到需要加入的会话，点击“加入”。
- 2) 会话启动后即可多个人同时操作一个会话。

3.7 批量启动

3.7.1 如何使用批量访问

UMA 支持批量启动多个不同目标设备相同服务名称会话，具体方法如下：

- 1) 在设备访问页面选择多个要访问的设备；
- 2) 点击“批量访问”。

3.7.2 批量访问注意事项

- 1) VNC 和 XDMCP 会话不支持批量访问；
- 2) 需要进行双人授权的设备无法使用批量访问功能；
- 3) 无默认系统账号的设备无法使用批量访问（无复选框），需要先手工访



问一次该设备后才可以使用批量访问功能。

3.8 命令复核

3.8.1 什么是命令复核？

命令复核是指管理员为了防止高危命令被随意执行，通过 UMA 设定相应的规则，当用户需要执行符合设定规则的命令时必须经过复核。

如果在访问字符会话执行某些命令时出现：“shterm: this command needs manager's confirm, are you sure? [Y/n]”，说明要执行的命令需要进行复核，输入 Y 并回车即可以发出请求。

3.8.2 如何对命令进行复核？

如果收到了他人的命令符合请求，请访问“命令复核”，对请求进行审核。

3.9 特殊的系统账号

3.9.1 self

登录目标设备时如果选择 **self** 系统账号，则堡垒机会使用用户登录堡垒机的账号和密码登陆目标设备。适用于用堡垒机和目标设备都使用 AD、LDAP 或其他认证服务器进行统一认证的情况。

3.9.2 any

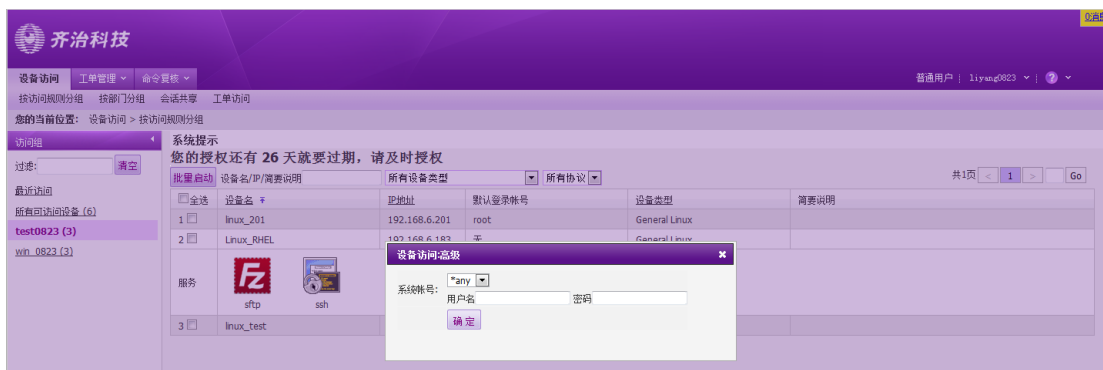
登录目标设备时如果选择 **any** 系统账号，则堡垒机只打开目标设备登录框，不进行登录操作，需要用户自己输入系统账号和密码进行登录。

例如：

1) windows 设备访问时选 **any** 系统账号，则会停留在 windows 登陆界面让用户自己输入账号和密码；

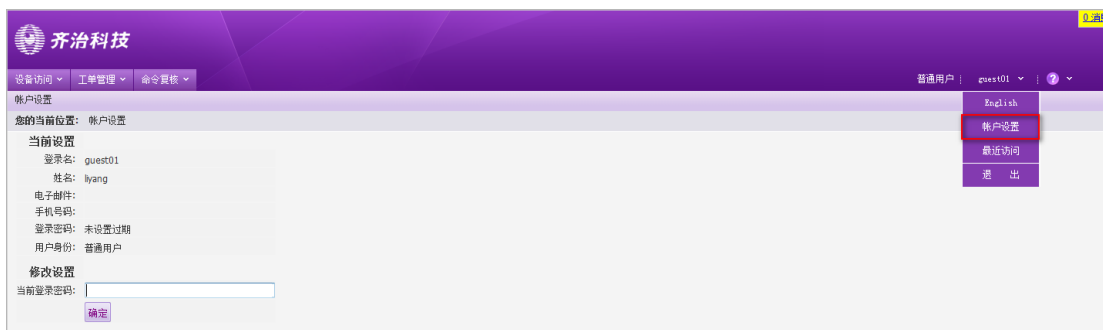


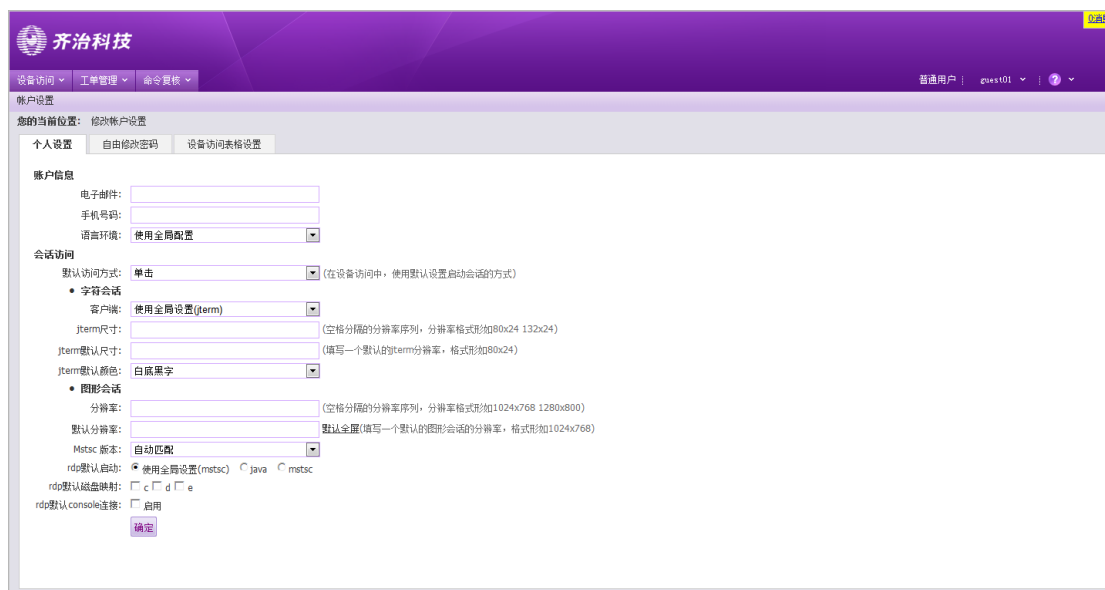
2) 在 web 界面访问 ftp, sftp, Xfwd 服务时选择 any 账号则会弹出密码框让用户自己填写账号密码;



3.10 账户设置

在当前账号的下拉菜单中选择“账户设置”,需要输入当前密码才能“账户设置”页面;





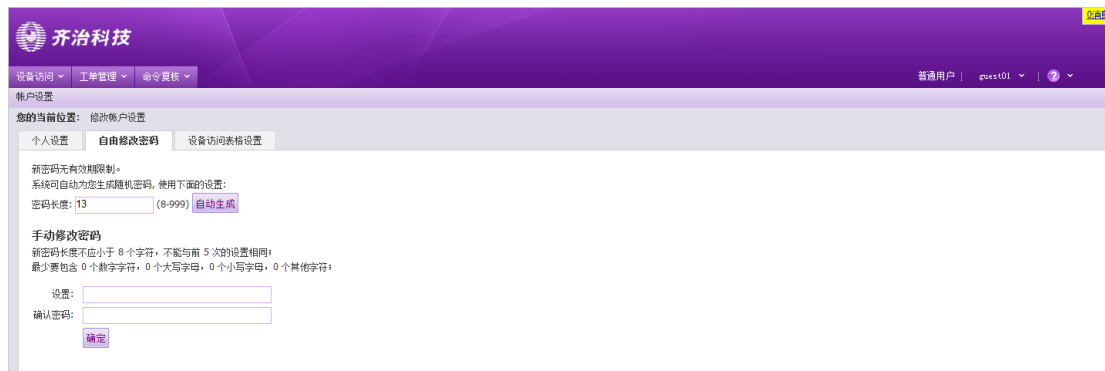
3.10.1 帐户信息

- 1) **邮箱地址：**设置自己的邮箱地址，要求该邮箱能收到堡垒机发送的邮件（可选）；
- 2) **手机号码：**填写自己的手机信息（可选）；
- 3) 手机号码和语言环境（支持简体中文和英文两种语言）
- 4) **会话访问：**
 - a) **默认访问方式：**设置使用单击还是双击启动会话；
 - b) **字符会话**
 - **客户端：**Jterm（基于 java 的客户端，在 web 界面中直接调用）、Putty（堡垒机自带）和 SecureCRT（需自己先在本地安装）。
 - **Jterm 尺寸、Jterm 默认尺寸和 Jterm 默认颜色**可以根据自己的使用习惯设置，这些设置只有在客户端选择为 Jterm 时才生效。
 - c) **图形会话**
 - **分辨率：**设置开启 RDP 会话时窗口的大小；
 - **默认分辨率：**设置默认分辨率之后，在访问目标设备时，右键点击可以选择该分辨率；
 - **mstsc 版本：**建议不要修改，不同的 windows 系统的 RDP 的协议版本有所不同，最好留给堡垒机自己去判断；



- RDP 默认启动：提供两个方式 mstsc 和 java。mstsc 为微软的远程桌面工具，使用体验比较好；java 方式是调用堡垒机自带的 java 工具；
- RDP 默认磁盘映射：把本地硬盘映射到目标设备里面去，设置默认磁盘映射后每次访问目标设备时不用再手动选择映射本地磁盘；
- RDP 默认 console 连接：设置是否使用 console 模式开启 RDP 会话；

3.10.2 自由修改密码



堡垒机提供了两种修改密码方式：自动生成和手动修改。

自动生成：如上图，先设置密码长度，然后“自动生成”，堡垒机会自动修改密码为一个随机字符串。

提示：

- 1) 自动生成密码之后，请记录下自动生成的随机密码，否则下次无法登陆堡垒机。
- 2) 手动修改密码：需要手动输入两次密码，并且设置的密码要满足超级管理员设置的密码复杂度要求才能修改成功。



3.10.3 设备访问表格设置

字段名	是否显示
部门	<input type="checkbox"/>
字符终端	<input type="checkbox"/>
图形终端	<input type="checkbox"/>
文件传输	<input type="checkbox"/>
最后登录时间	<input type="checkbox"/>

提交

勾选设备的属性字段后在访问列表中设备信息里面会多出这些属性栏。

更多

其它未尽事宜，请联系系统管理员 xiaox5@sany.com.cn。