

DialKeeper-2000 安全拨号认证网关 客户端使用手册(v1.4 版)



目录

1. 产品简介	4
2. 客户端软件包安装过程	4
2.1 客户端软件安装过程	4
2.2 智能卡驱动程序安装过程(可选)	5
2.3 Modem 驱动程序的安装	7
3. 客户端软件使用过程	7
3.1 服务器管理配置	7
3.2 修改对应配置文件	9
3.3 接入方式配置及证书配置	11
3.3.1 用户名口令方式接入配置	12
3.3.2 文件证书方式接入的配置和连接	13
3.3.3 智能卡方式接入的配置和连接	13
1.智能卡 common name 的查看	13
2.智能卡证书的接入验证	13
附录 客户端软件常见问题及解决方法	14
1 拨号客户端连接不上,提示错误码 797	14
2. 客户端提示错误码 680,没有拨号音	15
4. 提示"RAS 连接错误,无法找到 RAS 错误码"	16
5. 提示返回信息 tls-error, TLS handshake failed	16
6. 不能访问内网资源(ftp,telnet)	16
7. 客户端身份验证后,图标始终未变绿,提示"正在连接中"	16
8. 修改配置策略,无法保存,提示内存访问错误	17
9. 始终无法连接成功,图标一直在"连接中"状态	17
10. 连接成功,但是无法访问内网主机进行 telnet 等操作	17

图表目录

图表	1	软件包安装示意图-首页4
图表	2	软件包安装示意图-默认安装路径5
图表	3	软件包安装-安装客户端加密设备接口5
图表	4	智能卡驱动程序安装16
图表	5	智能卡驱动程序安装 26
图表	6	智能卡驱动程序安装 37
图表	7	智能卡驱动程序安装 4-安装完成重启系统7
图表	8	启动客户端主程序
图表	9	右键点击服务器管理菜单8
图表	10	服务器管理配置窗口8
图表	11	新建拨号区域的配置文件
图表	12	删除配置文件
图表	13	修改配置文件9
图表	14	客户端连接配置
图表	15	新建拨号连接110
图表	16	新建拨号连接 2-输入号码10
图表	17	新建拨号连接完成-输入拨号连接名称11
图表	18	用户名口令验证方式下的配置界面12
图表	19	用户名口令验证方式-验证窗口12
图表	20	拨号连接成功消息提示12
图表	21	连接状态信息察看13
图表	22	智能卡证书接入-PIN 码验证14

1. 产品简介

本文档为 Dialkeeper-2000 安全拨号认证网关的客户端软件使用手册。该软件提供了友 好的图形界面供拨号认证接入的用户使用,目前提供了用户名口令方式验证、加密文件证书 验证、智能卡验证三种验证方式。通过本软件,可实现对用户的高强度身份认证和数据加密、 防篡改,对用户实现严格的访问控制和保证内网系统的安全。

客户端软件通用的配置流程为:

1.在"服务器管理"菜单中增加配置文件名称(为便于标识,一般以拨号区域名称,如 某某网调拨号维护等命名)

2.选择对应配置文件,打开配置界面进行配置,选择对应的接入方式,并导入相应证书3.进行相应配置文件的拨号连接,点击"进行拨号"

4.连接及证书验证成功后,客户端进行内网资源的访问如 telnet/ftp 等操作。

注: 附录中提供了客户端常见的问题及解决方法,可供客户端用户参考。

2. 客户端软件包安装过程

2.1 客户端软件安装过程

双击 DK2000 安装程序文件弹出 license 窗口见下图,单击 cancel 按纽程序结束安装并退出。

🖢 DK2000 Setup	
navi-chilmac•m	License Agreement Please review the license terms before installing DK2000.
Press Page Down to see t Dialkeeper-2000 安全整 育。 任何侵犯版权的行为 何 部分以任何形式采用任 或扩散。	he rest of the agreement. 医号认证网关的教硬件设计版权归南骑集团公司信息系统分公司所 将被追究法律责任,未经版权所有者的书面离许不得将本手册的任 何手段电子的或机械的包括限相复制或录制或为任何目的进行复制
If you accept the terms of agreement to install DK20	f the agreement, click I Agree to continue. You must accept the 00.
	I Agree Cancel

图表 1 软件包安装示意图-首页

单击 browse 按纽选择要安装的路径(注意,请保持默认安装路径!)。

	Choose Install Location
ari-china.com	Choose the folder in which to install DK2000.
and select another folder.	Click Install to start the installation.
Destination Folder	
Destination Folder	Browse
Destination Folder	Browse
Destination Folder C:\Program Files\DK20 Space required: 3.2MB Space available: 887.8MB	Browse
Destination Folder CI\Program Files\DK20 Space required: 3.2MB Space available: 887.8MB	Browse,

图表 2 软件包安装示意图-默认安装路径

单击 install 按钮弹出软件安装界面,程序开始安装 DialKeeper-2000 安全拨号认 证网关客户端相关的程序和组件,如下图安装客户端加密设备接口,选择"仍然继续" 进行安装。

1	正在为此硬件安装的软件:
	naridiallink Adapter VI
	没有通过 Windows 徽标测试,无法验证它同 Windows XP 的相容性。(<u>告诉我为什么这个测试很重要。</u>)
	继续安装此软件会立即或在以后使系统支得不稳定。 Bigrosoft 建议您现在停止此安装,并同硬件供应商
	肤系,以获得通过 Tindows 额体测试的软件。

图表 3 软件包安装-安装客户端加密设备接口

2.2 智能卡驱动程序安装过程(可选)

如果使用智能卡证书验证的用户,则必须安装智能卡的驱动程序,其他种类的用户(文件证书用户、用户名口令方式验证的用户)则不必安装。

智能卡驱动程序的安装,双击智能卡驱动程序,弹出如下图所示的菜单。

▼atchSAFE 安装程序	×
TatchSAFE	
按 PAGE DOWN 键以查看协议的剩余部分。	
·	
安装和使用WatchSAFE安全套件需要接受以下条款:	
本协议是您(个人或单一实体)与握奇数据系统有限公司之间关于客户端网络 安全产品WatchSAFE的法律协议。	
客户端网络安全产品WatchSAPE的版权归握奇数据系统有限公司所有。本套	
- 未经授权擅自复制或散布本军件产品的部分或全部,将承受产厉的民事和刑事 处罚,对已知的违反者将给予法律范围内的全面制载。	
」 您是否接受上述"许可证协议"的所有条款? 如果选择"否",安装程序将关闭。 若要安装 WatchSAFE,您必须接受此协议。	
InstallShield	
<上一步®) 是(1) 否(1)	

图表 4 智能卡驱动程序安装 1

选择是弹出如下图所示的目录,选择要安装的目的文件夹或使用默认安装,单击下 一步,弹出菜单。

WatchSAFE 安裝程序	
TatchSAFE	
安装程序将在以下文件夹中安装 WatchSAFE。	
要安装到此文件夹,请单击"下一步"。 要安装到其它文件夹,请单击"浏览" ,然后选择其它文件夹。	
_ 目的地文件夹	
C:\Program Files\Watchdata\WatchSAFE 浏览 @)	
InstallShield	
< 上一步 (B) 下一步 (B) 取消	i

图表 5 智能卡驱动程序安装 2

智能卡读写设备选择"握奇电子钥匙",单击 next 按钮进入程序以及组件安装过程, 安装结束弹出如下图的窗口。

TatchSAFE 安装程序
选择智能卡读写设备
若要安装相关读写器的驱动程序,请单击它旁边的按钮。
○ 握奇串行口智能卡读写器
○ 握奇USB智能卡读写器
● 握奇电子钥匙
○ 其他智能卡读写器
InstallShieldCancelCancel

图表 6 智能卡驱动程序安装 3

选择是按钮重新启动计算机完成智能卡读写设备驱动程序的安装。

▼atchSAFE 安装程序	
	InstallShield Tizard 完 InstallShield Wizard 已成功安装 WatchSAFE,在使 用该程序之前,必须重新启动计算机。 C 不,稍后再重新启动计算机。 从驱动器中取出所有磁盘,然后单击"完成"以完成安 装。
	< 上一步 (B) 完成 取消

图表 7 智能卡驱动程序安装 4-安装完成重启系统

2.3 Modem 驱动程序的安装

客户端用户根据自己不同的 modem 型号安装自己的 modem 驱动程序(略)。

3. 客户端软件使用过程

用户在进行拨号连接前要注意以下四点:

- 一、dialkeeper-2000 安全拨号认证网关客户端正确安装。
- 二、客户端 modem 驱动程序的正确安装
- 三、进行了拨号号码及证书等的正确配置,详细见后面的描述

如客户端使用遇到一些问题,请参见 附录 客户端软件常见问题及解决方法

3.1 服务器管理配置

DialKeeper-2000 安全拨号认证网关客户端安装完成后,双击桌面的客户端程序

"DialKeeper-2000 电力系统专用安全拨号接入系统.exe"程序,在系统托盘上可见客户端程序图标,如下图所示:



图表 8 启动客户端主程序

如图第一个红色的图标,右键弹出菜单单击"服务器管理",如下图所示:



图表 9 右键点击服务器管理菜单

打开的服务器管理窗口如下所示,在服务器名称文本框中可输入您想要建立的拨号区域 名称,如"某某网调拨号维护",点击新建按钮,建立新的配置文件。

12 服务署管理	
服务器资源列表 拔号加密连接配置文件:nvpn	
服务器名称 请在此输入配置文件的名称	
新建 修改 删除	退出

图表 10 服务器管理配置窗口

服务器资源列表	拨号加密连接配置文件.nvpn 某某阿调拨号维护.nvpn	
服务器名称	某某网调拨号维护	
xc2#	247 101113	3834

图表 11 新建拨号区域的配置文件

欲删除某一拨号区域配置,可以在服务器资源列表中点击对应的配置文件名称,然

后点击删除按钮,以删除软件自带的默认配置文件为例,点击"拨号加密连接配置文件",点击删除按钮,经确认后删除配置文件,如下图所示:

服务器资	原列表 <u>拨号加密连</u> 某某网调拨	接配置文件 nvp 号维护.nvpn	on : 1
	警告		9
	· · · · · · · · · · · · · · · · · · ·	●除配置文件吗 否(28) ┃	
服务器名	称 拔号加密连	接配置文件	
316240	4230	nnire 1	3834

图表 12 删除配置文件

欲修改某配置文件名称,可直接点击"服务器资源列表"中的文件名称,然后, 在"服务器名称"栏中输入新的名称,点击"修改"按钮,进行配置文件名称的修改。

3.2 修改对应配置文件

右键任务栏上的图标,可进行指定配置文件的修改,如下图所示:



图表 13 修改配置文件

		.
添加	编辑	删除
接入方式		
🦰 用户名密码 🍣	🔓 文件证书 👔	🍵 🤨 智能卡 💆
证书配置		
证书配置 智能卡主题名		
证书配置 智能卡主题名 CA 证书(或)		浏览导入

打开的客户端连接配置窗口如下所示,包括拨号设置及证书设置等:

图表 14 客户端连接配置

单击添加按钮弹出如下图所示窗口:

新建连接向导	×
注接类型 选择连接类型。	2
 透到专用网络 (C) 用我的电话线 (周制解调器或 ISDN)连接。 通过 Internet 连接到专用网络 (C)- 创建通过 Internet 的虚拟专用网 (VPN) 连接或通道。 直接连接到另一台计算机 (C)- 使用我的串行、并行或红外端口连接。 通过或常连接到网络 (B) 通过我的宽带连接来连接 	
< 上一步 (B) 下一步 (B) > 取消)

图表 15 新建拨号连接1

选择拨到专用网络单击下一步见下图所示。

新建连接向导	
要拔的电话号码 您要连接的电话号码是什么?	LA LA
在下面输入电话号码。 电话号码 @): 	
您可能需要包含"1"或区号,或两者。如果您不确定是否需要这些 外的号码,请用您的电话拨此号码。如果您听到调制解调器声,则表 您拨的号码正确。	另 ē明
< 上一步 (2)) 下一步 (2) > 〔	取消

图表 16 新建拨号连接 2-输入号码

在电话号码窗口输入服务端的电话号码单击下一步,点击"不使用我的智能卡"(即

不使用 windows 系统自带的智能卡认证)

「建连接向导	
智能卡 您可以把您的智能卡用于此连接。	۶.
您可以配置此连接来使用您的智能 卡用在此连接。	卡登录到远程网络。选择是否把您的智能
○使用我的智能卡(凹)	
⊙不使用我的智能卡 @)	
	< 上一步 (B) 下一步 (B) > 取消

新建连接向导	
已完成 向导已准备好创建连接。	\$
输入此连接的名称: 【某市调拨号】	
单击"完成"来把它存入网络连接文件夹。 要在以后编辑此连接,诸选择它,然后单击"文件" 菜单下的"属性"。	
<上→步(8)	完成 取消

图表 17 新建拨号连接完成-输入拨号连接名称

在连接名称中输入建立的连接名称 (最好起容易辨别的名称)。单击完成按纽。

3.3 接入方式配置及证书配置

在客户端连接配置的"接入方式"中选择对应的接入方式,有以下三种,无论哪一种方

式,都要配置 Ca 证书。

1.用户名口令认证:用户名口令在连接建立时进行验证输入

2.文件证书认证: 需预先配置导入客户的加密证书

3.智能卡证书认证: 需填写客户智能卡证书的 common name

注:无论是 Ca 证书或客户加密证书,在服务器管理配置中名称都不能重复,否则,请先进 行改名,然后从客户端界面导入。

3.3.1 用户名口令方式接入配置

拨号连接	【某市调拨号	-
添加	,	
娶入方式		
 ・ 用户名密码 	88. O 文件证书 📿	○ 複銀卡 🔼
● 用户名密码 ↓	😤 ° 文件证书 []	🧲 智能卡 💆
唆入方式 ● 用户名密码 正书配置	😤 🤉 文件证书 []	○智能卡 🔼
唆入方式 ● 用户名密码 → 正书配置 智能卡主题名 ↓	😤 ° 文件证书 📻	○智能卡 🔼
 廣入方式 用户名密码 正书配置 智能卡主趨名 CA 证书(或) 	83. 6 文件证书 🗂	C 智能卡 🛃 浏览导入

图表 18 用户名口令验证方式下的配置界面

点击浏览导入窗口,导入正确的 ca 证书,单击确定按钮,用户名口令方式接入配置结束。右键点击对应配置文件的"进行拨号",即可进行拨号连接,如下是用户名口令验证的对话框:

	DK2000 - User Authentication	
• 可访问资源	пра:	
	密码:	

图表 19 用户名口令验证方式-验证窗口

验证成功后,会有对应提示信息,如下图:

ų)	某某	市调拔号	維护	已经连	接.	×
					_	J

图表 20 拨号连接成功消息提示

点击"察看状态",可看到该用户的访问控制权限信息,包括网络层及应用层的权限信息,如下图所示:

	当前状态	》:已注接					
Wed	Jun 0	1 10:51:09	2008 无:0:%	证证书成功:	depth=1,	/C=CN/ST=JS/L:	=NANJ ING/
Wed	Jun 0	1 10:51:09	2008 无:0:验	证证书成功:	depth=0,	/C=CN/ST=ZHEJ	IANG/L=HA
Wed	Jun 0	1 10:51:12	2008 DK2000	客户端安全认	【证接入成:	叻	
<							>
) []	访问资	渡					
土印	(H) 10 D	「奴 保: tcp	telnet	192,168.1	.21 23	eth0	
1			108 C 12 C 11 C 10 C 10	168 1 21 21	eth0		
		tcp	ftp 192.	100.1.21 21			
应月	过滤信	tcp 息(禁止):	ftp 192.	100.1.21 21	1 YEAR 24 74		
应月]过滤信	tcp (息(禁止): telu	ftp 192. net 192.16	8.1.21 kil	l scada		
应用]过滤信	tcp 急(禁止): telu ftp	ftp 192. net 192.16 192.168.1	8.1.21 kil .21 get	l scada passwd		

图表 21 连接状态信息察看

然后,客户端用户就可以进行内网实际主机的操作了

3.3.2 文件证书方式接入的配置和连接

客户端连接配置→ 接入方式中选择"文件证书",并导入客户证书(P12)证书(后缀 名为 pfx 或 p12 的证书)。

文件证书必须是 pkcs#12 格式,由管理员提供,同时提供给客户的还有证书的保护口令, 这是使用证书的重要验证和保护手段,在连接建立时输入验证。(注:有关内容参见服务器 端使用手册中的附录有关内容,使用证书工具或电力调度证书系统进行证书的生成)

3.3.3 智能卡方式接入的配置和连接

1.智能卡 common name 的查看

智能卡驱动程序安装过程见 2.2 节的阐述。

将智能卡插在主机 usb 端口上, 然后打开 IE→ 工具 →Internet 选项 → 内容 →证书 →个人, 进行证书 common name 的察看。如果不能辨别, 可以打开智能卡的软件, 点击"证 书察看"按钮, 进行证书 common name 的察看。

2.智能卡证书的接入验证

智能卡证书的接入参见用户名密码方式接入,在接入过程中会弹出下图提示用户输入智能卡 PIN 码。输入 PIN 码单击确定按钮即可,注意,如果连续输入 10 次错误,智能卡将锁死,只能由调度证书系统重新签发才能生效。



图表 22 智能卡证书接入-PIN 码验证

附录 客户端软件常见问题及解决方法

1 拨号客户端连接不上,提示错误码 797

弹出窗口如图一,提示"不能建立到远程计算机的连接,因为没有找到调制解调器,或者调制解调器忙。"

消息		X
<u>.</u>	BAS连接错误: 获取到BAS连接的错误消息 错误码:1997, 不能建立到远程计算机的连接,因为没有找到调制解调器,或者调制解调器忙。需要更多协助,请单击"详细信息" 在帮助和支持中心查找此错误号。	,或
	補定	

解决办法: 1 确保调制解调器驱动安装成功

- 2 调制解调器开关已经打开
- 3 在设备管理中能够检查到调制解调器
- 4 在设备管理器中检查调制解调器是否正常,方法如下:
 - 点击下图中的"属性"

□ 设备管理器	
文件 (E) 操作 (A) 查看 (Y) 帮助 (H)	
- =	
+ → → → → → → → → → →	
+ シ> 键盘 + Da 人体学输入设备 扫描检测硬件改动 (A)	
+ ② 声音、视频和游? 屈性 (B) + 1) 最振知其它指针;	
+ ← 通用申行总线控制器 + ■學 网络适配器 + ■學 系统设备 + ■ 显示卡	

属性中的"诊断"属性页中,点击"查询调制解调器",会显示"正同调制解调器通讯…",

	SPORT CONTRACTOR	
守	📙 设备管理器	5600FY MODEM 尾性 ? 🗙 - 🗆 🗶
	文件 (£) 操作 (A) ← → ■ 四 - 思 CJY + ③ DVD/CD-RC + ③ DVD/CD-RC + ④ SCSI 和 I	常規 週制解週器 診断 高級 認知程序 详細信息 週制解週器信息
	+	前令 195
	 + < ・ (型) 人体学術) + (型) 声音、現 + ・ (型) 原标和目行) + ・ ・	查询调制解调器 @) 日志记录 □附加到日志 @) 前梢候
		取消

● 然后若能在"命令"和"响应"中有很多命令的显示(如下图)说明 modem

正常; 否则 modem 不正常;

5600FY MODEM 居性	2 🔀
常规 调制解调器 诊断 调制解调器信息	高級 驱动程序 详细信息
字段 值 硬件 ID SERENUM\TOP1002	
命令 响应 ATGOVIEO 成功 AT+FCLASS=? 0,1,8	~
日志记录	查询调制解调器(Q)
□ 附加到日志 (2)	[查看日志 ₩]
	确定 取消

2. 客户端提示错误码 680, 没有拨号音

弹出窗口如图二,没有拨号音。



解决办法:

确保本地电话线路正常,用电话机测试。

3. 提示错误码 678, 远程计算机没有反应



解决办法:

1.右键拨号连接图标,单击修改配置文件,编辑拨号的电话号码,确保电话号码为远程 接入服务器的电话号码。确定,重新连接。

2. 以电话机模拟测试,去拨远方的号码,看是否正常

3.如还不成功请和服务器管理员联系,确保拨号网关处于开启状态

4. 提示"RAS 连接错误,无法找到 RAS 错误码"

解决办法:

检查远程服务器的号码是否配置正确,或直接使用电话拨打该号码,看是否正确。

5. 提示返回信息 tls-error, TLS handshake failed

解决办法:

检查客户端证书是否配置正确,是否为管理员分配的证书、或重新导入证书。

6. 不能访问内网资源(ftp,telnet)

1.察看 gui 界面上资源信息,看是否允许访问对应的内网资源,如果没有,则询问服务器管理员,对自己的访问控制是否设置正确

2.联系服务器管理员,看是否拨号网关到内网交换机的网线没有连接

7. 客户端身份验证后, 图标始终未变绿, 提示"正在连接中"

解决办法:

- 打开控制面板→ 管理工具 →服务 ,关闭服务 "Routing and remote access"
- 还有一种可能是系统防火墙软件导致,请检查客户端防火墙的策略, 或暂时停止防火墙服务进行测试

8. 修改配置策略,无法保存,提示内存访问错误

解决办法:

此种情况一般出现在 win2000 平台,请联系南瑞信息公司,提供最新的 v1.4 以上版本的客户端软件,客户端版本可右键点击相应图标的菜单"关于 DK2000"进行版本的察看。

9. 始终无法连接成功,图标一直在"连接中"状态

解决办法:

检查客户端主机的防火墙软件如"瑞星"或"卡巴斯基"等安全策略设置,或者直接关闭进行再次尝试。

10. 连接成功,但是无法访问内网主机进行 telnet 等操作

解决办法:

- 右键点击图标的"察看状态"菜单,在状态栏的可访问资源中察看是否开通了访问 权限,否则通知系统管理员进行权限的放开
- 如果1不能解决问题,请联系系统管理员看是否拨号网关已经将网线连上内网的交换机。