IBM® 客户端安全解决方案

结合 Tivoli® Access Manager 使用客户端安全软件版本 5.3

IBM® 客户端安全解决方案

结合 Tivoli® Access Manager 使用客户端安全软件版本 5.3

第一版（**2004** 年 **5** 月）

在使用本资料及其支持的产品之前，请务必阅读第 31 页的附录 A, 『客户端安全软件的美国出口条例』和第 39 页的附录 D, 『声明与商标』。对本手册所包含的内容，IBM 公司拥有最终解释权，如有变更，恕不另行通知。

目录

前言

本指南包含有关设置客户端安全软件以结合 IBM Tivoli Access Manager 使用的有用信息。

本指南结构如下：

“第 1 章, 『简介』”，包含该软件中所包含的应用程序和组件的概述，以及公钥基础结构（PKI）功能的描述。

“第 2 章, 『在 Tivoli Access Manager 服务器上安装客户端安全组件』”，包含在 Tivoli Access Manager 服务器上安装客户端安全支持的先决条件和说明。

“第 3 章, 『配置 IBM 客户机』”，包含配置 IBM 客户机以使用 Tivoli Access Manager 提供的验证服务的先决条件和说明。

“第 4 章, 『故障诊断』”，包含解决问题的有用信息，您在使用本指南提供的说明时可能碰到这些问题。

“附录 A, 『客户端安全软件的美国出口条例』”，包含有关该软件的美国出口条例信息。

“附录 B, 『密码和口令信息』”，包含适用于 UVM 口令的口令标准以及用于管理员密码的规则。

“附录 C, 『为系统登录使用 **UVM** 保护的规则』”，包含有关为操作系统登录使用 UVM 保护的信息。

“附录 D, 『声明与商标』”，包含法律声明和商标信息。

阅读本指南的对象

本指南是为那些在 IBM 客户机上使用 Tivoli Access Manager V3.9 来管理由用户验证管理工具（UVM）安全策略所设置的验证对象的企业管理员而提供的。

管理员必须了解以下概念和过程：

- SecureWay Directory 轻量级目录访问协议（LDAP）的安装和管理
- Tivoli Access Manager Runtime Environment 的安装和设置过程
- Tivoli Access Manager 对象空间的管理

如何使用本指南

使用本指南设置客户端安全支持以结合 Tivoli Access Manager 使用。本指南是*《客户端安全软件安装指南》*、*《客户端安全软件管理员指南》*和*《客户端安全用户指南》*的配套指南。

本指南及客户端安全的所有其它文档可以从 http://www.pc.ibm.com/us/security/index.html IBM Web 站点下载。

对《客户端安全软件安装指南》的引用

本文档提供对《客户端安全软件安装指南》的引用。安装和配置 Tivoli Access Manager 服务器并在客户机上安装了 Runtime Environment 后，使用《客户端安全软件安装指南》中的说明在 IBM 客户机上安装客户端安全软件。请参阅第 11 页的第 3 章，『配置 IBM 客户机』以获取更多信息。

对《客户端安全软件管理员指南》的引用

本文档提供对《客户端安全软件管理员指南》的引用。《客户端安全软件管理员指南》包含如何设置 IBM 客户机的用户验证和 UVM 策略的信息。安装客户端安全软件之后，使用《客户端安全软件管理员指南》来设置用户验证和安全策略。请参阅第 11 页的第 3 章，『配置 IBM 客户机』以获取更多信息。

附加信息

您可以从 http://www.pc.ibm.com/us/security/index.html IBM Web 站点获取附加信息和安全产品更新（如果可用）。

第 1 章 简介

感谢您选择装配有内置加密硬件的 ThinkPad™ 和 ThinkCentre™ 计算机，这些硬件与可下载的软件技术一起工作以便在客户机 PC 平台上提供很高的安全级别。这些硬件和软件统称为 IBM 嵌入式安全子系统（ESS）。硬件组件是 IBM 嵌入式安全芯片而软件组件是 IBM 客户端安全软件（CSS）。

客户端安全软件用于使用 IBM 嵌入式安全芯片来加密文件和存储加密密钥的 IBM 计算机。该软件由使 IBM 客户机系统能通过本地网络、企业或因特网使用客户端安全功能的应用程序和组件组成。

IBM 嵌入式安全子系统

IBM ESS 支持密钥管理的解决方案（例如公钥基础结构，PKI）并且由以下本地应用程序组成：

- 文件和文件夹加密（FFE）
- 密码管理器
- 安全 Windows 登录
- 多个可配置的验证方法，包括：
  - 口令
  - 指纹
  - 智能卡
  - 感应胸卡

为了有效使用 IBM ESS 的功能，安全管理员必须熟悉某些基本概念。以下部分描述基本安全概念。

IBM 嵌入式安全芯片

IBM 嵌入式安全子系统是提供额外级别的安全性来选择 IBM PC 平台的内置加密硬件技术。随着该安全子系统的出现，加密和验证过程从比较容易受攻击的软件转移并且移动到专用硬件的安全环境。它切实地提高了安全性。

IBM 嵌入式安全子系统支持：

- RSA3 PKI 操作，例如对隐私的加密和对验证的数字签名
- RSA 密钥生成
- 伪随机数生成
- 200 毫秒内的 RSA 功能计算
- 用于 RSA 密钥对存储的 EEPROM 内存
- 在规范 Vs. 1.1 中定义的全部 TCPA 功能
- 通过低针脚数量（LPC）总线与主处理器通信

IBM 客户端安全软件

IBM 客户端安全软件由以下软件应用程序和组件组成：

- 管理员实用程序：管理员实用程序是管理员用于激活或停用嵌入式安全子系统，并用于创建、存档和重新生成加密密钥和口令的界面。此外，管理员可以使用此实用程序将用户添加到客户端安全软件提供的安全策略。
- 管理员控制台：客户端安全软件管理员控制台使管理员能够配置安全证书漫游网络、创建并配置启用部署的文件以及创建非管理员配置和恢复概要。
- 用户配置实用程序：用户配置实用程序使客户机用户能够更改 UVM 口令、使 Windows 登录密码能够由 UVM 识别、更新密钥存档以及注册指纹。用户还可创建用 IBM 嵌入式安全子系统创建的数字证书的备份副本。
- 用户验证管理工具（**UVM**）：客户端安全软件使用 UVM 管理用于验证系统用户的口令和其它元素。例如，UVM 可使用指纹阅读器进行登录验证。客户端安全软件支持以下功能：
  - **UVM** 客户机策略保护：客户端安全软件使安全管理员能设置客户端安全策略，规定如何在系统上验证客户机用户。

    如果策略表明登录时需要指纹，而用户没有注册指纹，则他可以选择将指纹注册为登录的一部分。同样，如果需要指纹验证而没有连接识别器，UVM 将报告错误。另外，如果 Windows 密码未注册或注册不正确，那么使用 UVM，用户将有机会提供正确的 Windows 密码作为登录的一部分。
  - **UVM** 系统登录保护：客户端安全软件使安全管理员能通过登录界面控制计算机访问。UVM 保护确保只有安全策略识别的用户能够访问操作系统。

密码和密钥之间的关系

密码和密钥以及其它可选的验证设备一起发生作用以验证系统用户的身份。理解密码和密钥之间的关系对于理解 IBM 客户端安全软件如何工作至关重要。

管理员密码

管理员密码用于向 IBM 嵌入式安全子系统验证管理员。该密码（长度必须是 8 个字符）在嵌入式安全子系统的安全硬件范围内保留并且验证。一旦验证，管理员可以执行以下操作：

- 登记用户
- 启动策略界面
- 更改管理员密码

可以下列方式设置管理员密码：

- 通过 IBM 客户端安全安装向导
- 通过管理员实用程序
- 使用脚本
- 通过 BIOS 界面（仅 ThinkCentre 计算机）

具有创建并且维护管理员密码的策略很重要。如果管理员密码已泄漏或者忘记，则可以更改它。

对于那些熟悉可靠计算组织（Trusted Computing Group, TCG）概念和术语的人来说，管理员密码与所有者权限值相同。由于管理员密码与 IBM 嵌入式安全子系统关联，所以有时候它还称为*硬件密码*。

硬件公钥和私钥

IBM 嵌入式安全子系统的基本前提是它在客户机系统上提供强大的信任根。该根用于保护其它应用程序和功能。建立信任根的一部分是创建硬件公钥和硬件私钥。公钥和私钥（一起称为*密钥对*）在数学上以下列方式关联：

- 通过公钥加密的任何数据只能通过对应的私钥解密。
- 通过私钥加密的任何数据只能通过对应的公钥解密。

硬件私钥在安全子系统的安全、硬件范围内被创建、存储和使用。硬件公钥可用于各种用途（因此称为公钥），但它从不暴露在安全子系统的安全、硬件范围之外。硬件公钥和私钥是 IBM 密钥交换层次结构的关键部分，该层次结构在以后的部分中有所描述。

硬件公钥和私钥以下列方式创建：

- 通过 IBM 客户端安全安装向导
- 通过管理员实用程序
- 使用脚本

对于那些熟悉可靠计算组织（TCG）概念和术语的人来说，硬件公钥和私钥也可以称为*存储根密钥*（SRK）。

管理员公钥和私钥

管理员公钥和私钥是 IBM 密钥交换层次结构的整体部分。它们还允许在系统板或硬盘驱动器发生故障的情况下备份并且复原特定于用户的数据。

管理员公钥和私钥对于所有系统可以是唯一的，或者对于所有系统或系统组也可以是公共的。值得注意的是这些管理员密钥必须是受管的，所以选择使用唯一密钥还是使用已知密钥的策略十分重要。

可以下列方式之一创建管理员公钥和私钥：

- 通过 IBM 客户端安全安装向导
- 通过管理员实用程序
- 使用脚本

ESS 存档

管理员公钥和私钥允许在系统板或硬盘驱动器发生故障的情况下备份并且复原特定于用户的数据。

用户公钥和私钥

IBM 嵌入式安全子系统创建用户公钥和私钥以保护特定于用户的数据。当用户登记到 IBM 客户端安全软件时创建了这些密钥对。IBM 客户端安全软件的用户验证管理工具（UVM）组件透明地创建并且管理这些密钥。这些密钥根据登录到操作系统的 Windows 用户进行管理。

IBM 密钥交换层次结构

IBM 嵌入式安全子系统体系结构的基本元素是 IBM 密钥交换层次结构。IBM 密钥交换层次结构的基础（或根）是硬件公钥和私钥。硬件公钥和私钥（称为*硬件密钥对*）是由 IBM 客户端安全软件创建并且从统计上讲在每台客户机上是唯一的。

层次结构上（在根的上面）下一个密钥“ 级别 ”是管理员公钥和私钥（*管理员密钥对*）。管理员密钥对可以在每台机器上都是唯一的，也可以在所有客户机或客户机子集上都相同。您如何管理该密钥对取决于您想如何管理网络。由于管理员私钥驻留在客户机系统中（通过硬件公钥受保护），在管理员定义的位置上，所以它是唯一的。

IBM 客户端安全软件将 Windows 用户登记到嵌入式安全子系统环境中。登记用户时会创建用户公钥和私钥（*用户密钥对*）并且创建新的密钥“ 级别 ”。用户私钥通过管理员公钥加密。管理员私钥通过硬件公钥加密。因此，要使用用户私钥，必须将管理员私钥（通过硬件公钥加密）装入安全子系统。一旦处于芯片中，硬件私钥会解密管理员私钥。管理员私钥现在在安全子系统中已作好使用准备以便将通过相应的管理员公钥加密的数据交换到安全子系统中进行解密和利用。当前的 Windows 用户私钥（通过管理员公钥加密）被传递到安全子系统中。利用嵌入式安全子系统的应用程序所需的任何数据也将传递到芯片中，在安全子系统的安全环境中进行解密和利用。用于向无线网络验证的私钥就是这样一个示例。

需要密钥时，密钥会交换到安全子系统中。加密的私钥会交换到安全子系统中，然后可以在芯片的受保护环境中使用。私钥从不在该硬件环境以外暴露或者使用。这使得 IBM 嵌入式安全芯片能够保护几乎无限的数据量。

之所以对私钥进行加密，是因为它们必需高度受保护并且 IBM 嵌入式安全子系统中的可用存储空间是有限的。任何给定时间内只能在安全子系统中存储一对密钥。在一次次引导时，只有硬件公钥和私钥保持存储在安全子系统中。为了允许多个密钥和多个用户，CSS 利用 IBM 密钥交换层次结构。需要密钥时，密钥会交换到 IBM 嵌入式安全子系统。相关的加密私钥会交换到安全子系统中，然后可以在芯片的受保护环境中使用。私钥从不在该硬件环境以外暴露或者使用。

管理员私钥通过硬件公钥加密。硬件私钥（仅在安全子系统中可用）用于解密管理员私钥。一旦管理员私钥在安全子系统中解密，就可以将用户私钥（通过管理员公钥加密）传递到安全子系统中并且通过管理员私钥解密。可以通过管理员公钥加密多个用户私钥。这样通过 IBM ESS 几乎允许系统上有无限的用户量；然而，最佳实践建议每台计算机限制登记 25 名用户确保最佳的性能。

IBM ESS 利用密钥交换层次结构（在该结构中，在安全子系统中使用硬件公钥和私钥）来保护存储在芯片以外的其它数据。硬件私钥在安全子系统中生成并且从不离开该安全环境。硬件公钥在安全子系统以外可用并且用于加密或保护其它数据块，例如私钥。一旦通过硬件公钥加密该数据，就只能通过硬件私钥将其解密。由于硬件私钥仅在安全子系统的安全环境中可用，所以只能在该相同的安全环境中对加密的数据进行解密和使用。值得注意的是每台计算机将会有一个唯一的硬件公钥和私钥。IBM 嵌入式安全子系统上的随机数功能确保了每个硬件密钥对在统计上是唯一的。

CSS 公钥基础结构（PKI）功能

客户端安全软件提供在您的业务中创建公钥基础结构（PKI）所需的所有组件，例如：

- 客户端安全策略上的管理员控制。在客户机级别验证最终用户是安全策略的重要方面。客户端安全软件提供了管理 IBM 客户机的安全策略必需的界面。此界面是“验证软件用户验证管理工具”（UVM）的一部分，该软件是客户端安全软件的主要组件。
- 公钥加密的加密密钥管理。管理员用客户端安全软件为计算机硬件和客户机用户创建加密密钥。当创建加密密钥时，它们通过密钥层次结构绑定到 IBM 嵌入式安全芯片，在该层次结构中，位于基本级别的硬件密钥用于加密位于上一个级别的密钥，包括与每个客户机用户关联的用户密钥。在 IBM 嵌入式安全芯片上加密和存储密钥会添加客户端安全必不可少的额外层，因为密钥被安全地绑定到计算机硬件。
- 由 **IBM** 嵌入式安全芯片保护的数字证书创建和存储。当您申请可用于数字签名或加密电子邮件消息的数字证书时，客户端安全软件使您能够选择 IBM 嵌入式安全子系统作为使用 Microsoft CryptoAPI 的应用程序的加密服务提供程序。这些应用程序包括 Internet Explorer 和 Microsoft Outlook Express。这确保数字证书的私钥在 IBM 嵌入式安全子系统中通过用户公钥加密。而且，Netscape 用户可选择 IBM 嵌入式安全子系统作为用于安全性数字证书的私钥生成器。使用公钥加密标准（PKCS）#11 的应用程序（例如 Netscape Messenger）可利用 IBM 嵌入式安全子系统提供的保护。
- 将数字证书传送到 **IBM** 嵌入式安全子系统的能力。IBM 客户端安全软件证书传送工具使您能够将使用缺省 Microsoft CSP 创建的证书传送到 IBM 嵌入式安全子系统 CSP。这样大大增加了为与证书关联的私钥提供的保护，因为它们现在将安全地存储在 IBM 嵌入式安全子系统上，而不是存储在易受攻击的软件上。

  注：受 IBM 嵌入式安全子系统 CSP 保护的数字证书无法导出到另一个 CSP。
- 密钥存档和恢复解决方案。一项重要的 PKI 功能是创建密钥存档，在原始密钥丢失或损坏的情况下可以从该存档复原密钥。IBM 客户端安全软件提供一个界面，该界面使您能够建立使用 IBM 嵌入式安全子系统创建的密钥和数字证书的存档，并且在需要时，复原这些密钥和证书。
- 文件和文件夹加密。文件和文件夹加密使客户机用户能够加密或解密文件或文件夹。这样就在 CSS 系统安全性措施的基础上提供了数据安全的增强级别。
- 指纹验证。IBM 客户端安全软件支持用于验证的 Targus PC 卡指纹阅读器和 Targus USB 指纹阅读器。为了能够正常运行，安装 Targus 指纹设备驱动程序之前，必须安装客户端安全软件。
- 智能卡验证。IBM 客户端安全软件支持某些智能卡作为验证设备。客户端安全软件使智能卡每次能够用作某个用户的验证标记。除非使用安全证书漫游，否则每个智能卡都绑定到系统。因为该智能卡必须随附密码（可能会泄漏），所以使用智能卡使您的系统更安全。
- 安全证书漫游。安全证书漫游使授权的网络用户能够使用网络上的任何计算机，就象是在使用自己的工作站一样。用户得到授权在任意客户端安全软件注册的客户机上使用 UVM 后，就能够将其个人数据导入到安全证书漫游网络中的任何其它注册的客户机中。其个人数据会在 CSS 存档以及任何曾经导入这些数据的计算机中得到自动更新和维护。对该个人数据的更新（诸如新的证书或口令更改）将立即在连接到漫游网络的所有其它计算机上可用。
- **FIPS 140 - 1** 认证。客户端安全软件支持 FIPS 140 - 1 认证的加密库。FIPS 认证的 RSA BSAFE 库用于 TCPA 系统。
- 口令失效。当每个用户添加到 UVM 中时，客户端安全软件都将建立特定于用户的口令和口令失效策略。

第 2 章 在 Tivoli Access Manager 服务器上安装客户端安全组件

在客户机级别上验证最终用户是一个重要的安全考虑因素。客户端安全软件提供了管理 IBM 客户机的安全策略必需的界面。该界面是验证软件（用户验证管理工具，UVM）的一部分，UVM 是客户端安全软件的主要组件。

可以用两种方法管理 IBM 客户机的 UVM 安全策略：

- 在本地使用驻留在 IBM 客户机上的策略编辑器
- 遍及企业，使用 Tivoli Access Manager

在客户端安全可以结合 Tivoli Access Manager 使用之前，必须已安装了 Tivoli Access Manager 的客户端安全组件。可以从 http://www.pc.ibm.com/us/security/index.html IBM Web 站点下载该组件。

先决条件

在 IBM 客户机和 Tivoli Access Manager 服务器之间建立安全连接之前，必须在 IBM 客户机上安装以下组件：

- IBM Global Security Toolkit
- IBM SecureWay Directory Client
- Tivoli Access Manager Runtime Environment

要获得关于安装和使用 Tivoli Access Manager 的详细信息，请参阅 http://www.tivoli.com/products/index/secureway_policy_dir/index.htm Web 站点上提供的文档。

下载和安装客户端安全组件

客户端安全组件可以免费从 IBM Web 站点下载。

要下载并在 Tivoli Access Manager 服务器和 IBM 客户机上安装客户端安全组件，请完成以下过程：

1. 使用 Web 站点上的信息，通过将您的型号与系统要求表中提供的型号匹配来确保 IBM 集成的安全芯片在您的系统上；然后单击 **Continue**。
2. 选择与您的机器类型相匹配的单选按钮并单击 **Continue**。
3. 创建用户标识，通过填充在线表单向 IBM 注册，并查看许可证协议；然后单击 **Accept Licence**。

   您将被自动引导到客户端安全下载页面。
4. 遵循下载页面上的步骤来安装所有必需的设备驱动程序、自述文件、软件、参考文档和其它实用程序。
5. 通过完成以下过程安装客户端安全软件：

   a. 从 Windows 桌面上，单击开始 **>** 运行。

b. 在“运行”字段中，输入 d:\directory\csec50.exe，其中 d:\directory\ 是文件所处的盘符和目录。

c. 单击确定。

“欢迎使用 IBM 客户端安全软件 InstallShield 向导”窗口打开。

d. 单击下一步。

该向导将解压缩文件并安装该软件。安装完成后，将给您立即重新启动计算机或等到稍后再重新启动的选项。

e. 选择相应的单选按钮并单击确定。

6. 当计算机重新启动后，从 Windows 桌面上，单击开始 **>** 运行。
7. 在“运行”字段中，输入 d:\directory\TAMCSS.exe，其中 d:\directory\ 是文件所处的盘符和目录，或者单击浏览找到该文件。
8. 单击确定。
9. 指定目标文件夹，然后单击解压缩。

向导将把文件解压缩到指定的文件夹。有消息表明文件已成功解压缩。

10. 单击确定。

在 **Tivoli Access Manager** 服务器上添加客户端安全组件

pdadmin 实用程序是一个命令行工具，管理员可以用它来执行大多数 Tivoli Access Manager 管理任务。多个命令执行使管理员能够使用包含多个 pdadmin 命令的文件来执行一个完整的任务或一组任务。pdadmin 实用程序和管理服务器（pdmgrd）之间的通信是通过 SSL 保护的。pdadmin 实用程序作为 Tivoli Access Manager Runtime Environment（PDRTE）软件包的一部分来安装。

pdadmin 实用程序接受标识文件位置的文件名参数，例如：

```
MSDOS>pdadmin [-a <admin-user >][-p <password >]<file-pathname >
```

以下命令是如何在 Tivoli Access Manager 服务器上创建 IBM 解决方案对象空间、客户端安全操作和单个 ACL 条目的示例：

```
MSDOS>pdadmin -a sec_master -p password C:\TAM_Add_ClientSecurity.txt
```

请参考 *Tivoli Access Manager Base Administrator Guide* 以获得关于 pdadmin 实用程序及其命令语法的更多信息。

在 **IBM** 客户机和 **Tivoli Access Manager** 服务器之间建立安全连接

IBM 客户机必须在 Tivoli Access Manager 安全域中建立它自己的验证标识，以便从 Tivoli Access Manager 授权服务请求授权决定。

必须在 Tivoli Access Manager 安全域中为应用程序创建一个唯一标识。为了使验证标识执行验证检查，应用程序必须是远程 acl 用户组的成员。应用程序要联系其中一个安全域服务时，它必须首先登录到该安全域中。

svrsslcfg 实用程序使 IBM 客户端安全应用程序能够与 Tivoli Access Manager 管理服务器和授权服务器进行通信。

svrsslcfg 实用程序使 IBM 客户端安全应用程序能够与 Tivoli Access Manager 管理服务器和授权服务器进行通信。

svrsslcfg 实用程序执行以下任务：

- 创建应用程序的用户标识。例如，DemoUser/HOSTNAME
- 创建该用户的 SSL 密钥文件。例如，DemoUser.kdb 和 DemoUser.sth
- 把该用户添加到远程 acl 用户组

需要以下参数：

- **-f cfg_file** 配置文件路径和名称，使用 TAMCSS.conf
- **-d kdb_dir** 包含服务器的密钥环数据库文件的目录。
- **-n server_name** 预期的 IBM 客户机用户的实际 Windows 用户名／UVM 用户名。
- **-P admin_pwd** Tivoli Access Manager 管理员密码。
- **-s server_type** 必须指定为远程。
- **-S server_pwd** 新创建的用户密码。该参数是必需的。
- **-r port_num** 设置 IBM 客户机的侦听端口号。该参数在 Tivoli Access Manager Runtime 变量 SSL 服务器端口中为 PD 管理服务器指定。
- **-e pwd_life** 设置密码到期时间（以天数为单位）。

要在 IBM 客户机和 Tivoli Access Manager 服务器之间建立安全连接，请完成以下过程：

1. 创建一个目录并把 TAMCSS.conf 文件移动到该新目录。

   例如，`MSDOS> mkdir C:\TAMCSS MSDOS> move C:\TAMCSS.conf C:\TAMCSS\`

2. 运行 svrsslcfg 创建用户。

   MSDOS> svrsslcfg -config -f C:\TAMCSS\TAMCSS.conf -d C:\TAMCSS\ -n <server_name> - s remote -S <server_pwd> -P <admin_pwd> -e 365 -r 199

   注：用 IBM 客户机的预期的 UVM 用户名和主机名替换 <server_name>。例如：–n DemoUser/MyHostName。在 MSDOS 提示符下输入 “ hostname ” 可以找到 IBM 客户机主机名。svrsslcfg 实用程序将在 Tivoli Access Manager 服务器中创建一个有效条目，并为加密通信提供唯一的 SSL 密钥文件。

3. 运行 svrsslcfg 把 ivacld 的位置添加到 TAMCSS.conf 文件。

   缺省情况下，PD 授权服务器在端口 7136 上侦听。通过查看 Tivoli Access Manager 服务器上的 ivacld.conf 文件的 ivacld 节中的 tcp_req_port 参数可以验证它。获取正确的 ivacld 主机名很重要。使用 pdadmin server list 命令获得该信息。服务器名为：<server_name>-<host_name>。以下是运行 pdadmin server list 的示例：

```
MSDOS> pdadmin server list ivacld-MyHost.ibm.com
```

以下命令用于为上述显示的 ivacld 服务器添加复制条目。假设 ivacld 在缺省端口 7136 上侦听。

```
svrsslcfg -add_replica  -f <config file path> -h <host_name> MSDOS>svrsslcfg
-add_replica  -f C:\TAMCSS\TAMCSS.conf -h MyHost.ibm.com
```

第 3 章 配置 IBM 客户机

可以使用 Tivoli Access Manager 控制 IBM 客户机的验证对象之前，必须通过使用管理员实用程序（客户端安全软件随附的组件）来配置每个客户机。本部分包含配置 IBM 客户机的先决条件和说明。

先决条件

确保以下软件以下列顺序安装在 IBM 客户机上：

1. **Microsoft Windows** 支持的操作系统。您能够使用 Tivoli Access Manager 控制对于运行 Windows XP, Windows 2000 或 Windows NT Workstation 4.0 的 IBM 客户机的验证要求。
2. 客户端安全软件 **v3.0** 或更高版本。 安装该软件并启用 IBM 嵌入式安全芯片后，您可以使用客户端安全管理员实用程序设置用户验证并编辑 UVM 安全策略。要获得关于安装和使用客户端安全软件的详尽说明，请参阅*《客户端安全软件安装指南》*和*《客户端安全软件管理员指南》*。

配置 Tivoli Access Manager 设置信息

Tivoli Access Manager 安装在本地客户机之后，您可以通过使用管理员实用程序（客户端安全软件提供的软件组件）来配置 Access Manager 设置信息。Access Manager 设置信息包括以下设置：

- 选择配置文件的完整路径
- 选择本地高速缓存刷新时间间隔

要在 IBM 客户机上配置 Tivoli Access Manager 设置信息，请完成以下过程：

1. 单击开始 **>** 设置 **>** 控制面板 **> IBM** 嵌入式安全子系统。
2. 输入管理员密码，然后单击确定。

   您输入密码后，管理员实用程序主窗口打开。
3. 单击配置应用程序支持和策略按钮。

   显示 “ UVM 应用程序和策略配置 ” 屏幕。
4. 选中使用 **UVM** 的安全登录替换标准 **Windows** 登录复选框。
5. 单击应用程序策略按钮。
6. 在 Tivoli Access Manager 设置信息区域，选择到 TAMCSS.conf 配置文件的完整路径。例如，`C:\TAMCSS\TAMCSS.conf`

   Tivoli Access Manager 必须安装在客户机上以使该区域可用。
7. 单击编辑策略按钮。

   显示 “ 输入管理员密码 ” 屏幕。
8. 在提供的字段中输入管理员密码，然后单击确定。

显示“ IBM UVM 策略 ”屏幕。

9. 从“ 操作 ”下拉菜单中选择您要 Tivoli Access Manager 控制的操作。
10. 选中“ Access Manager 控制所选对象 ”复选框，以便在该框中出现选中标记。
11. 单击应用按钮。

    在下一次高速缓存刷新时发生更改。如果您需要立即发生更改，请单击刷新本地高速缓存按钮。

设置并使用本地高速缓存功能

选择 Tivoli Access Manager 配置文件后，可以设置本地高速缓存刷新时间间隔。由 Tivoli Access Manager 管理的安全策略信息的本地副本是在 IBM 客户机上维护的。您可以每隔（0-12）月或（0-30）天来安排本地高速缓存的自动刷新。

要设置或刷新本地高速缓存，请完成以下过程：

1. 单击开始 **>** 设置 **>** 控制面板 **> IBM** 嵌入式安全子系统。
2. 输入管理员密码，并单击确定。

   管理员实用程序窗口打开。要获得关于使用管理员实用程序的完整信息，请参阅*《客户端安全软件管理员指南》*。
3. 在管理员实用程序中，单击配置应用程序支持和策略按钮，然后单击应用程序策略按钮。

   显示“ 修改客户端安全策略配置 ”屏幕。
4. 请执行以下操作之一：
   - 要立即刷新本地高速缓存，单击刷新本地高速缓存。
   - 要设置自动刷新速率，在提供的字段中输入月（0-12）和天数（0-30），然后单击刷新本地高速缓存。将刷新本地高速缓存，并且将更新文件到期日期以表明何时会发生下一个自动刷新。

启用 **Tivoli Access Manager** 来控制 **IBM** 客户机对象

UVM 策略是通过通用策略文件控制的。称为 UVM 策略文件的通用策略文件包含 IBM 客户机系统上执行的操作（如登录到系统、清除屏幕保护程序或签名电子邮件消息）的验证要求。

在您能够启用 Tivoli Access Manager 控制 IBM 客户机的验证对象前，使用 UVM 策略编辑器编辑 UVM 策略文件。UVM 策略编辑器是管理员实用程序的一部分。

要点：启用 Tivoli Access Manager 来控制对象，则将对象控制授予 Tivoli Access Manager 对象空间。如果您这样做，则必须重新安装客户端安全软件以重新建立对该对象的本地控制。

编辑本地 **UVM** 策略

尝试编辑本地客户机的 UVM 策略之前，确保至少有一个用户在 UVM 中登记。否则，在策略编辑器试图打开本地策略文件时将显示错误消息。

编辑本地 UVM 策略并只在编辑它的客户机上使用它。如果您在其缺省位置安装客户端安全，则本地 UVM 策略存储为 \Program Files\IBM\Security\UVM_Policy\globalpolicy.gvm。仅添加到 UVM 的用户可以使用 UVM 策略编辑器。

注：如果您设置 UVM 策略以要求用于验证对象（如操作系统登录）的指纹，则添加到 UVM 的用户必须注册其指纹以使用该对象。

要启动 UVM 策略编辑器，请完成以下管理员实用程序过程：

1. 单击配置应用程序支持和策略按钮，然后单击应用程序策略按钮。

   显示“ 修改客户端安全策略配置 ”屏幕。
2. 单击编辑策略按钮。

   显示“ 输入管理员密码 ”屏幕。
3. 在提供的字段中输入管理员密码，然后单击确定。

   显示“ IBM UVM 策略 ”屏幕。
4. 在“ 对象选择 ”选项卡上，单击操作或对象类型，然后选择您要为其指定验证要求的对象。

   有效操作的示例包括系统登录、系统解锁和电子邮件解密；对象类型的示例是获取数字证书。
5. 对于您选择的每个对象，选择 **Tivoli Access Manager** 控制所选对象，为该对象启用 Tivoli Access Manager。

   要点：如果启用 Tivoli Access Manager 来控制对象，则将控制授予 Tivoli Access Manager 对象空间。如果您以后要重新建立对该对象的本地控制，则必须重新安装客户端安全软件。

   注：编辑 UVM 策略时，通过单击策略摘要可以查看策略摘要信息。
6. 单击应用保存您的更改。
7. 单击确定退出。

编辑和使用远程客户机的 UVM 策略

要在多个 IBM 客户机上使用 UVM 策略，请编辑和保存一个远程客户机的 UVM 策略，然后将 UVM 策略文件复制到其它 IBM 客户机上。如果您在客户端安全的缺省位置安装它，UVM 策略文件将存储为 \Program Files\IBM\Security\UVM_Policy\remote\globalpolicy.gvm。

把以下文件复制到要使用该 UVM 策略的其它远程 IBM 客户机：

- \IBM\Security\UVM_Policy\remote\globalpolicy.gvm
- \IBM\Security\UVM_Policy\remote\globalpolicy.gvm.sig

如果您在客户端安全软件的缺省位置安装它，则前述路径的根目录是 \Program Files。将这两个文件复制到远程客户机的 \IBM\Security\UVM_Policy\ 目录路径。

第 4 章 故障诊断

以下部分的信息有助于防止、识别和纠正您在使用客户端安全软件过程中可能会遇到的问题。

管理员功能

本部分包含管理员在设置和使用客户端安全软件时可能会觉得很有用的信息。

IBM 客户端安全软件仅能在具有 IBM 嵌入式安全子系统的 IBM 计算机上使用。该软件由应用程序和组件组成，这些应用程序和组件使 IBM 客户机能通过安全硬件而不是通过易受攻击的软件保护他们的敏感信息。

授权用户

客户机用户信息受保护之前，IBM 客户端安全软件必须安装在客户机上，并且用户必须获得授权使用该软件。易于使用的安装向导指导您逐步完成整个安装过程。

要点：在安装过程中，必须授权至少一个客户机用户使用 UVM。如果在最初安装客户端安全软件时没有授权任何用户使用 UVM，则您的安全设置将不被应用并且您的信息将不受保护。

如果在没有授权任何用户的情况下您完成了安装向导，请关闭并重新启动您的计算机；然后从 Windows “开始”菜单运行客户端安全安装向导，并授权一名 Windows 用户使用 UVM。这将使 IBM 客户端安全软件能够应用您的安全设置并保护您的敏感信息。

删除用户

当您删除用户时，用户名在管理员实用程序中的用户列表中被删除。

设置 BIOS 管理员密码（ThinkCentre）

在 Configuration/Setup Utility 中可用的安全设置使管理员能执行以下操作：

- 启用或禁用 IBM 嵌入式安全子系统
- 清除 IBM 嵌入式安全子系统

注意：

- 清除 IBM 嵌入式安全子系统后，所有存储在子系统上的加密密钥和证书都会丢失。

因为通过计算机的 Configuration/Setup Utility 可以访问您的安全设置，所以请设置管理员密码来阻止未授权用户更改这些设置。

要设置 BIOS 管理员密码：

1. 关机并重新启动计算机。
2. 当屏幕出现 Configuration/Setup Utility 提示时，按 **F1**。

   打开 Configuration/Setup Utility 主菜单。

3. 选择 **System Security**。
4. 选择 **Administrator Password**。
5. 输入您的密码并按键盘上的向下箭头。
6. 再次输入您的密码并按向下箭头。
7. 选择 **Change Administrator password** 并按 Enter 键；然后再次按 Enter 键。
8. 按 **Esc** 键退出并保存设置。

在您设置了 BIOS 管理员密码之后，每次您尝试访问 Configuration/Setup Utility 时都出现提示。

要点：请将您的 BIOS 管理员密码的记录存放在安全的地方。如果您丢失或忘记了 BIOS 管理员密码，则您无法访问 Configuration/Setup Utility，且您在不卸下计算机外盖并移动系统板上跳线的情况下无法更改或删除 BIOS 管理员密码。请参阅计算机随附的硬件文档以获取更多的信息。

设置超级用户密码（**ThinkPad**）

IBM BIOS Setup Utility 中可用的安全设置使管理员能够执行以下任务：

- 启用或禁用 IBM 嵌入式安全子系统
- 清除 IBM 嵌入式安全子系统

注意：

- 在安装或升级客户端安全软件之前，在某些型号的 ThinkPad 上必须临时禁用超级用户密码。

在设置了客户端安全软件后，请设置一个超级用户密码以阻止未授权的用户对这些设置的更改。

要设置超级用户密码，请完成以下过程之一：

示例 **1**

1. 关机并重新启动计算机。
2. 当屏幕出现 Setup Utility 提示时，按 F1。

   Setup Utility 主菜单打开。
3. 选择 **Password**。
4. 选择 **Supervisor Password**。
5. 输入您的密码并按 Enter 键。
6. 再次输入您的密码并按 Enter 键。
7. 单击 **Continue**。
8. 按 F10 保存并退出。

示例 **2**

1. 关机并重新启动计算机。
2. 当“To interrupt normal startup, press the blue Access IBM button”（要中断正常启动，请按蓝色的 Access IBM 按键）消息显示时，请按蓝色的 Access IBM 按键。

Access IBM predesktop Area 打开。

3. 双击 **Start setup utility**。
4. 使用方向键浏览菜单以选择 **Security**。
5. 选择 **Password**。
6. 选择 **Supervisor Password**。
7. 输入您的密码并按 Enter 键。
8. 再次输入您的密码并按 Enter 键。
9. 单击 **Continue**。
10. 按 F10 保存并退出。

在您设置了超级用户密码之后，每次您尝试访问 BIOS Setup Utility 时会出现提示。

要点：将超级用户密码保存在安全的地方。如果您丢失或忘记了超级用户密码，则无法访问 IBM BIOS Setup Utility，而且无法更改或删除密码。请参阅计算机随附硬件文档以获取更多的信息。

保护管理员密码

管理员密码保护对管理员实用程序的访问权。保护管理员密码以禁止未授权的用户更改管理员实用程序中的设置。

清除 **IBM** 嵌入式安全子系统（**ThinkCentre**）

如果您希望从 IBM 嵌入式安全子系统擦除所有的用户加密密钥并且清除子系统的管理员密码，则必须清除该芯片。在清除 IBM 嵌入式安全子系统前，请阅读下面的信息。

注意：

- 清除 IBM 嵌入式安全子系统后，所有存储在子系统上的加密密钥和证书都会丢失。

要清除 IBM 嵌入式安全子系统，请完成以下过程：

1. 关机并重新启动计算机。
2. 当屏幕出现 Setup Utility 提示时，按 F1。

   Setup Utility 主菜单打开。
3. 选择 **Security**。
4. 选择 **IBM TCPA Feature Setup**。
5. 选择 **Clear IBM TCPA Security Feature** 并按 Enter 键。
6. 选择 **Yes**。
7. 按 F10 并选择 **Yes**。
8. 按 Enter 键。计算机将重新启动。

清除 **IBM** 嵌入式安全子系统（**ThinkPad**）

如果您希望从 IBM 嵌入式安全子系统擦除所有的用户加密密钥并且清除管理员密码，则必须清除该子系统。在清除 IBM 嵌入式安全子系统前，请阅读下面的信息。

注意：

- 清除 IBM 嵌入式安全子系统后，所有存储在子系统上的加密密钥和证书都会丢失。

要清除 IBM 嵌入式安全子系统，请完成以下过程：

1. 关闭计算机
2. 当您重新启动计算机时，按住 Fn 键。
3. 当屏幕出现 Setup Utility 提示时，按 F1。

   Setup Utility 主菜单打开。
4. 选择 **Config**。
5. 选择 **IBM Security Chip**。
6. 选择 **Clear IBM Security Chip**。
7. 选择 **Yes**。
8. 按 Enter 键继续。
9. 按 F10 保存并退出。

CSS V5.2 的已知问题或限制

以下信息可能有助于使用客户端安全软件 V5.2 的功能。

漫游限制

使用 CSS 漫游服务器

当任何人试图登录 CSS 漫游服务器时将出现 CSS 管理员密码提示。然而，计算机在没有输入该密码的情况下也能够正常使用。

在漫游环境中使用 IBM 安全密码管理器

在一个系统上使用 IBM 客户端安全密码管理器存储的密码能够在漫游环境内用于其它系统上。当用户在漫游网络中登录到另一个系统上（如果存档可用），则从存档中自动检索新条目。因此，如果用户已经登录到一个系统上，他必须注销并重新登录，然后任何新条目才能在漫游网络上可用。

Internet Explorer 证书和漫游刷新延迟

Internet Explorer 证书在存档中每 20 秒刷新一次。当漫游用户生成了新的 Internet Explorer 证书时，该用户在另一个系统上导入、复原或更改其 CSS 配置之前必须等待至少 20 秒。在 20 秒刷新时间间隔之前尝试任何这些操作将导致证书丢失。同样，如果当证书生成时用户没有连接到存档，则该用户在连接到存档后应该等待 20 秒以确保证书在存档中更新。

Lotus Notes 密码和安全证书漫游

如果启用 Lotus Notes 支持，则用户的 Lotus Notes 密码将由 UVM 存储。用户将无需输入他们的 Notes 密码就可以登录到 Lotus Notes 上。他们将被要求提供他们的 UVM 口令、指纹、智能卡等（取决于安全策略的设置）以获得对 Lotus Notes 的访问。

如果用户从 Lotus Notes 内部更改了其 Notes 密码，Lotus Notes 标识文件则随新密码更新并且新 Notes 密码的 UVM 副本也将更新。在漫游环境中，用户的 UVM 安全证书将在用户能访问的漫游网络上的其它系统上可用。如果有更新密码的 Notes 标识文件也不能用于其它系统，则 Notes 密码的 UVM 副本可能与漫游网络中其它系统上的标识文件中的 Notes 密码不匹配。如果该情况发生，用户将无法访问 Lotus Notes。

如果用户带有更新密码的 Notes 标识文件也不能用于另一个系统，则应该将更新的 Notes 标识文件复制到漫游网络中的其它系统上，这样标识文件中的密码将与 UVM 存储的副本匹配。或者，用户能从“开始”菜单中运行“修改安全设置”，并将 Notes 密码改回原来的值。Notes 密码随后能通过 Lotus Notes 再次更新。

在漫游环境中登录时安全证书的可用性

当存档位于网络共享的位置上时，一旦用户有权访问该存档，则最新的用户安全证书集就从存档中下载下来。登录时用户还无权访问网络共享，因此在系统登录完成之前用户还无法下载最新的安全证书。例如，如果在漫游网络中的另一个系统上更改 UVM 口令，或者在另一个系统上注册新的指纹，则这些更新在登录过程完成之前将不可用。如果更新的用户安全证书不可用，则用户应该尝试以前的口令或其它注册的指纹以登录到系统。登录完成后，用户的更新安全证书将可用并且新的口令和指纹将向 UVM 注册。

感应胸卡限制

启用带有 **Xyloc** 感应胸卡的安全 **UVM** 登录保护

要成功启用带有 CSS 感应胸卡支持的安全 UVM 登录保护，您必须按以下顺序安装组件：

1. 安装客户端安全软件。
2. 使用 CSS 管理员实用程序启用安全 UVM 登录保护。
3. 重新启动计算机。
4. 安装 Xyloc 软件进行感应胸卡支持。

注：如果首先安装了 Xyloc 感应胸卡软件，则不显示客户端安全软件登录界面。如果该情况发生，则您必须卸载客户端安全软件和 Xyloc 软件，然后按照以上说明的顺序重新安装它们以复原 UVM 安全登录保护。

感应胸卡和 **Cisco LEAP** 支持

同时启用感应胸卡保护和 Cisco LEAP 支持可能导致意外后果。建议不要在同一系统中安装或使用这些组件。

Ensure 软件支持

客户端安全软件 5.2 需要感应胸卡用户将他们的 Ensure 软件升级到 Ensure V7.41。当从客户端安全软件的以前版本开始升级时，请在升级到客户端安全软件 5.2 之前升级您的 Ensure 软件。

复原密钥

在执行密钥复原操作后，您必须重新启动计算机才能继续使用客户端安全软件。

本地和域用户名

如果域用户名和本地用户名相同，则您应该对两个帐户都使用相同的 Windows 密码。IBM 用户验证管理工具对每个标识只存储一个 Windows 密码，因此用户应该在本地和域登录时使用相同的密码。如果不是这样，则在启用了 IBM UVM 安全 Windows 登录替换时，在本地和域登录间切换时将提示他们更新 IBM UVM Windows 密码。

CSS 不提供使用同一个帐户名登记不同的域和本地用户的功能。如果试图用同一个标识登记不同的本地和域用户，则显示以下消息：选定的用户标识已经配置。CSS 不允许在一个系统中对同一个域和本地用户标识进行不同的登记，这样同一个用户标识将仅有权访问同一个安全证书集，如安全证书、存储的指纹等。

重新安装 Targus 指纹软件

如果除去或重新安装了 Targus 指纹软件，则在客户端安全软件中启用指纹支持所需的注册表条目必须手动添加以启用指纹支持。下载包含所需条目的注册表文件（atplugin.reg）并双击它将注册表条目合并到该注册表中。在提示时，单击“确定”以确认该操作。必须重新启动系统以便客户端安全软件识别更改并启用指纹支持。

注：您必须具有系统的管理员权限以添加这些注册表条目。

BIOS 超级用户口令

IBM 客户端安全软件 5.2 和更早版本不支持一些 ThinkPad 系统上的 BIOS 超级用户口令功能。如果启用 BIOS 超级用户口令，则任何对安全子系统所做的启用和禁用操作必须在 BIOS Setup 中进行。

使用 Netscape 7.x

Netscape 7.x 与 Netscape 4.x 的工作方式不同。在启动 Netscape 后不会立即出现口令提示。或更确切地说，PKCS#11 模块只在需要时才装入，这样口令提示只在执行需要 PKCS#11 模块的操作时才出现。

使用软盘存档

如果在配置安全软件时您指定软盘作为存档位置，则当配置过程写数据到软盘时会有长时间的延迟。一些其它介质，例如网络共享或 USB 存储钥匙，可能是很好的存档位置。

智能卡限制

注册智能卡

在用户可以使用智能卡成功验证之前必须向 UVM 注册该卡。如果一张卡分配给多个用户，则只有最近注册该卡的用户才能使用该卡。因而，智能卡应该只注册给一个用户帐户。

验证智能卡

如果智能卡需要验证，UVM 将显示需要该智能卡的对话框。当将智能卡插入阅读器，将显示需要智能卡 PIN 的对话框。如果用户输入不正确的 PIN，UVM 将再次要求智能卡。必须取出并重新插入智能卡后才能再次输入 PIN。用户必须继续取出和重新插入智能卡直到输入该卡正确的 PIN。

加密后在文件夹上显示加号（+）字符

在加密文件或文件夹后，Windows 资源管理器可能在文件夹图标前显示外部的加号（+）字符。该额外字符在刷新资源管理器窗口后将消失。

Windows XP 受限用户的限制

Windows XP 受限用户无法更新其 UVM 口令、Windows 密码或使用 User Configuration Utility 更新其密钥存档。

其它限制

本部分包含关于与客户端安全软件相关的其它已知问题和限制的信息。

结合 Windows 操作系统使用客户端安全软件

所有 **Windows** 操作系统都有以下已知的限制：如果在 UVM 中登记的客户机用户更改了其 Windows 用户名，将丢失所有客户端安全功能。用户将不得不在 UVM 中重新登记新的用户名并请求所有新的安全证书。

Windows XP 操作系统有以下已知的限制：在 UVM 中登记的、其先前的 Windows 用户名已更改的用户将无法被 UVM 识别。UVM 将指向以前的用户名，而 Windows 将只识别新用户名。即使在安装客户端安全软件之前已更改 Windows 用户名，也会发生此限制。

结合 Netscape 应用程序使用客户端安全软件

授权失败后 **Netscape** 打开：如果 UVM 口令窗口打开，则在可以继续操作前必须输入 UVM 口令，然后单击确定。如果输入了不正确的 UVM 口令（或对指纹识别提供了一个不正确的指纹），则显示错误消息。如果您单击确定，则 Netscape 将打开，但您将无法使用由 IBM 嵌入式安全子系统生成的数字证书。您必须退出并重新进入 Netscape，并在可以使用 IBM 嵌入式安全子系统证书之前，输入正确的 UVM 口令。

不显示算法：如果在 Netscape 中查看 IBM 嵌入式安全子系统 PKCS#11 模块，则不选择该模块支持的所有散列算法。IBM 嵌入式安全子系统 PKCS#11 模块支持以下算法，但在 Netscape 中查看时不标识为受到支持：

- SHA-1
- MD5

IBM 嵌入式安全子系统证书和加密算法

提供以下信息来帮助识别有关可以结合 IBM 嵌入式安全子系统证书使用的加密算法的问题。请参阅 Microsoft 或 Netscape 的资料，以获取有关结合其电子邮件应用程序使用的加密算法的当前信息。

当从一个 **Outlook Express**（**128** 位）客户机发送电子邮件至另一个 **Outlook Express**（**128** 位）客户机时：如果您使用带有 128 位的 Internet Explorer 4.0 或 5.0 版本的 Outlook Express 发送加密的电子邮件至其它使用 Outlook Express（128 位）的客户机，则使用 IBM 嵌入式安全子系统证书加密的电子邮件消息仅可使用 3DES 算法。

当在一个 **Outlook Express**（**128** 位）客户机与一个 **Netscape** 客户机间发送电子邮件时：从一个 Netscape 客户机至一个 Outlook Express（128 位）客户机的 RC2（40）、RC2（64）或 RC2（128）加密请求总是使用 RC2（40）算法返回至 Netscape 客户机。

在 **Outlook Express**（**128** 位）客户机中某些算法可能不可用：某些 RC2 算法以及其它算法可能不能结合 IBM 嵌入式安全子系统证书使用，这取决于如何配置或更新您的 Outlook Express （128 位）版本。请参阅 Microsoft 的资料以获取有关结合您的 Outlook Express 版本使用的加密算法的当前信息。

为 **Lotus Notes** 用户标识使用 **UVM** 保护

如果在 **Notes** 会话内部切换用户标识，则 **UVM** 保护将无法进行：您可以仅为 Notes 会话的当前用户标识设置 UVM 保护。要从已启用 UVM 保护的用户标识切换为另一个用户标识，请完成以下过程：

1. 退出 Notes。
2. 禁用当前用户标识的 UVM 保护。
3. 进入 Notes 并切换用户标识。要获得关于切换用户标识的信息，请参阅您的 Lotus Notes 文档。

   如果要为已切换至的用户标识设置 UVM 保护，则继续执行步骤 4。
4. 进入由客户端安全软件提供的 Lotus Notes 配置工具，并设置 UVM 保护。

用户配置实用程序限制

Windows XP 在某些环境下强加访问限制，限制客户机用户可用的功能。

Windows XP Professional

在 Windows XP Professional 中，客户机用户限制可能适用于以下情况：

- 客户端安全软件安装在后来转换为 NTFS 格式的分区上
- Windows 文件夹在后来转换为 NTFS 格式的分区上
- 存档文件夹在后来转换为 NTFS 格式的分区上

在以上情况中，Windows XP Professional 的受限用户可能无法执行以下用户配置实用程序任务：

- 更改其 UVM 口令
- 更新向 UVM 注册的 Windows 密码
- 更新密钥存档

Windows XP Home

Windows XP Home 的受限用户在以下任何一种情况中将无法使用用户配置实用程序：

- 客户端安全软件安装在 NTFS 格式的分区上
- Windows 文件夹在 NTFS 格式的分区上
- 存档文件夹在 NTFS 格式的分区上

Tivoli Access Manager 限制

当选择了 Tivoli Access Manager 控制时，不禁用拒绝对所选对象的所有访问复选框。在 UVM 策略编辑器中，如果选择了 **Access Manager** 控制所选对象使 Tivoli Access Manager 能够控制验证对象，则不禁用拒绝对所选对象的所有访问复选框。尽管拒绝对所选对象的所有访问复选框保留为活动状态，它不能被选择来覆盖 Tivoli Access Manager 控制。

错误消息

在事件日志中生成与客户端安全软件相关的错误消息：客户端安全软件使用一个可在事件日志中生成错误消息的设备驱动程序。与这些消息关联的错误不会影响计算机的正常操作。

如果拒绝对一个验证对象的访问，则 **UVM** 调用由关联的程序生成的错误消息：如果 UVM 策略设置为拒绝对一个验证对象（例如电子邮件解密）的访问，表明访问被拒绝的消息将根据所使用软件的不同而有所差异。例如，来自 Outlook Express 的表明拒绝访问验证对象的错误消息与来自 Netscape 的表明拒绝访问的错误消息是不同的。

故障诊断图表

以下部分提供的故障诊断图表可在您使用客户端安全软件遇到问题时提供帮助。

安装故障诊断信息

以下故障诊断信息可能在您安装客户端安全软件过程中遇到问题时向您提供帮助。

问题症状	可能的解决方案
在软件安装过程中显示错误消息	操作
在安装软件时显示消息，询问您是否要除去所选应用程序及其全部组件。	单击确定退出窗口。再次开始安装过程来安装客户端安全软件的新版本。
安装过程中显示消息，表明您必须升级或删除该程序。	执行下列操作之一： • 如果已安装客户端安全软件 5.0 之前的版本，则选择删除并使用 IBM BIOS Setup Utility 清除该安全子系统。 • 否则，选择升级并继续安装。
由于未知管理员密码的原因，拒绝安装访问	操作
在启用 IBM 嵌入式安全子系统的 IBM 客户机上安装软件时，IBM 嵌入式安全子系统的管理员密码未知。	清除安全子系统以继续安装。

管理员实用程序故障诊断信息

如果您在使用管理员实用程序时遇到问题，以下故障诊断信息可能会有帮助。

问题症状	可能的解决方案
在管理员实用程序中输入和确认您的 **UVM** 口令后，“ 下一步 ”按钮不可用。	操作
将用户添加至 UVM 时，在管理员实用程序中输入和确认您的 UVM 口令后，下一步按钮可能不可用。	单击 Windows 任务栏上的信息项并继续该过程。
更改管理员公钥时显示错误消息	操作
当您清除嵌入式安全子系统，然后复原密钥存档时，如果您更改管理员公钥，则可能显示错误消息。	将用户添加到 UVM 并请求新的证书（如果适用）。
尝试恢复 **UVM** 口令时显示错误消息	操作

问题症状	可能的解决方案
当您更改管理员公钥，然后尝试恢复用户的 UVM 口令时，可能显示错误消息。	请执行以下操作之一： • 如果不需要用户的 UVM 口令，则不需要任何操作。 • 如果需要用户的 UVM 口令，则您必须将用户添加到 UVM，并请求新的证书（如果适用）。
当您尝试保存 **UVM** 策略文件时显示错误消息	操作
当您尝试通过单击应用或保存来保存 UVM 策略文件（globalpolicy.gvm）时，显示错误消息。	退出错误消息、再次编辑 UVM 策略文件以进行更改，然后保存文件。
当您尝试打开 **UVM** 策略编辑器时显示错误消息	操作
当前用户（登录到操作系统）尚未添加到 UVM 时，UVM 策略编辑器将不打开。	将用户添加到 UVM 并打开 UVM 策略编辑器。
当您正在使用管理员实用程序时显示错误消息	操作
当您正在使用管理员实用程序时，可能显示以下错误消息： 当尝试访问 IBM 嵌入式安全子系统时，发生缓冲区 I/O 错误。这可以通过重新引导来改正。	退出错误消息并且重新启动计算机。
当更改管理员密码时显示禁用芯片的消息	操作
当您尝试更改管理员密码，并且在输入确认密码后按 Enter 键或 Tab > Enter 键时，将启用禁用芯片按钮并显示禁用芯片确认消息。	请执行以下操作： 1. 从禁用芯片确认窗口退出。 2. 要更改管理员密码，请输入新的密码，输入确认密码，然后单击更改。在输入确认密码后不要按 Enter 键或 Tab > Enter 键。

用户配置实用程序故障诊断信息

如果您在使用用户配置实用程序时遇到问题，以下故障诊断信息可能会有帮助。

问题症状	可能的解决方案
受限用户在 **Windows XP Professional** 中无法执行某些用户配置实用程序功能	操作
Windows XP Professional 受限用户可能无法执行以下用户配置实用程序任务： • 更改其 UVM 口令 • 更新向 UVM 注册的 Windows 密码 • 更新密钥存档	这是 Windows XP Professional 的已知限制。此问题没有解决方案。
受限的用户在 **Windows XP Home** 中无法使用用户配置实用程序	操作

问题症状	可能的解决方案
Windows XP Home 的受限用户在以下任何一种情况中将无法使用用户配置实用程序： • 客户端安全软件安装在 NTFS 格式的分区上 • Windows 文件夹在 NTFS 格式的分区上 • 存档文件夹在 NTFS 格式的分区上	这是 Windows XP Home 的已知限制。此问题没有解决方案。

特定于 **ThinkPad** 的故障诊断信息

如果在 ThinkPad 计算机上使用客户端安全软件时遇到问题，以下故障诊断信息可能会有帮助。

问题症状	可能的解决方案
当尝试客户端安全管理员功能时显示错误消息	操作
在尝试执行客户端安全管理员功能后会显示错误消息。	必须禁用 ThinkPad 超级用户密码以执行某些客户端安全管理员功能。 要禁用超级用户密码，请完成以下过程： 1. 按 F1 访问 IBM BIOS Setup Utility。 2. 输入当前超级用户密码。 3. 输入新的空白超级用户密码，并且确认空白密码。 4. 按 Enter 键。 5. 按 F10 保存并退出。
不同的 **UVM** 感知指纹传感器不正确工作	操作
IBM ThinkPad 计算机不支持多个 UVM 感知指纹传感器彼此交换。	请勿切换指纹传感器型号。远程工作时，请使用与在扩展坞中工作时相同的型号。

Microsoft 故障诊断信息

结合 Microsoft 应用程序或操作系统使用客户端安全软件遇到问题时，以下故障诊断图表中的信息可能对您有帮助作用。

问题症状	可能的解决方案
屏幕保护程序仅在本地屏幕上显示	操作
使用 Windows Extended Desktop 功能时，即使对您的系统及其键盘的访问已被保护，客户端安全软件屏幕保护程序也仅显示在本地屏幕上。	如果显示任何敏感信息，在调用客户端安全屏幕保护程序之前，在扩展桌面上最小化窗口。
客户端安全对于在 **UVM** 中登记的用户无法正常工作	操作
登记的客户机用户可能已更改其 Windows 用户名。如果发生这种情况，则丢失所有客户端安全功能。	在 UVM 中重新登记新的用户名并请求所有新的安全证书。
注：在 Windows XP 中，在 UVM 中登记的、其先前 Windows 用户名已更改的用户将无法被 UVM 识别。即使在安装客户端安全软件之前已更改 Windows 用户名，也会发生此限制。	

问题症状	可能的解决方案
使用 **Outlook Express** 读加密的电子邮件时发生问题	操作
由于发送方和接收方使用的 Web 浏览器的加密长度差异，所以无法解密加密的电子邮件。	验证以下情况： 1. 发送方使用的 Web 浏览器的加密长度与接收方使用的 Web 浏览器的加密长度兼容。 2. Web 浏览器的加密长度与客户端安全软件的固件所提供的加密长度兼容。
使用来自某地址（该地址具有多个与其关联的证书）的证书时发生问题	操作
Outlook Express 可以列出与单个电子邮件地址关联的多个证书，并且这些证书中的一部分证书可能成为无效的证书。如果与证书关联的私钥在生成证书的发送方计算机的 IBM 嵌入式安全子系统上不再存在，则证书可能变为无效证书。	要求接收方重新发送其数字证书；然后在 Outlook Express 的地址簿中选择该证书。
尝试数字签名电子邮件消息时产生故障消息	操作
如果电子邮件消息的撰写者尝试数字签名电子邮件消息，而撰写者并不具有与他或她的电子邮件帐户关联的证书，则显示错误消息。	使用 Outlook Express 中的安全设置指定要与该用户帐户关联的证书。有关更多信息，请参阅为 Outlook Express 提供的文档。
Outlook Express（**128** 位）仅使用 **3DES** 算法加密电子邮件消息	操作
在结合 128 位版本的 Internet Explorer 4.0 或 5.0 使用 Outlook Express 的客户机之间发送加密的电子邮件时，仅可使用 3DES 算法。	有关结合 Outlook Express 使用的加密算法的当前信息，请参阅 Microsoft 的文档。
Outlook Express 客户机返回以不同算法加密的电子邮件消息	操作
使用 RC2（40）、RC2（64）或 RC2（128）算法加密的电子邮件消息从使用 Netscape Messenger 的客户机发送到使用 Outlook Express（128 位）的客户机。从 Outlook Express 客户机返回的电子邮件消息将采用 RC2（40）算法加密。	不需要操作。从 Netscape 客户机到 Outlook Express（128 位）客户机的 RC2（40）、RC2（64）或 RC2（128）加密请求总是使用 RC2（40）算法返回到 Netscape 客户机。请参阅 Microsoft 的资料以获取有关结合您的 Outlook Express 版本使用的加密算法的当前信息。
硬盘驱动器发生故障后在 **Outlook Express** 中使用证书时产生错误消息	操作
通过使用管理员实用程序中的密钥复原功能可以复原证书。一些证书（例如 VeriSign 提供的免费证书）在密钥复原后可能不会复原。	在复原密钥后，请执行以下操作之一： • 获取新证书 • 在 Outlook Express 中再次注册证书权限
Outlook Express 不更新与证书关联的加密长度	操作
当发送方选择了 Netscape 中的加密长度并将签名的电子邮件消息发送到结合 Internet Explorer 4.0（128 位）使用 Outlook Express 客户机时，返回的电子邮件的加密长度可能不匹配。	从 Outlook Express 的地址簿中删除关联的证书。再次打开签名的电子邮件并且将证书添加到 Outlook Express 的地址簿中。
在 **Outlook Express** 中显示错误解密消息	操作

问题症状	可能的解决方案
通过双击消息，您可在 Outlook Express 中打开它。在某些情况下，当您太快地双击加密的消息时，会出现解密错误消息。	关闭消息，并再次打开加密的电子邮件消息。
同样，当您选择加密的消息时可能在预览窗格中显示解密错误消息。	如果在预览窗格中出现错误消息，则不需要任何操作。
当您在加密的电子邮件上两次单击“发送”按钮时显示错误消息。	操作
使用 Outlook Express 时，如果您两次单击“发送”按钮发送加密的电子邮件消息，则显示错误消息，表明无法发送消息。	关闭错误消息，然后单击发送按钮一次。
当您请求证书时显示错误消息	操作
当使用 Internet Explorer 时，如果您请求使用 IBM 嵌入式安全子系统 CSP 的证书，则可能收到错误消息。	再次请求数字证书。

Netscape 应用程序故障诊断信息

结合 Netscape 应用程序使用客户端安全软件遇到问题时，以下故障诊断图表中的信息可能对您有帮助作用。

问题症状	可能的解决方案
读加密的电子邮件时发生问题	操作
由于发送方和接收方使用的 Web 浏览器的加密长度差异，所以无法解密加密的电子邮件。	验证以下情况： 1. 发送方使用的 Web 浏览器的加密长度与接收方使用的 Web 浏览器的加密长度兼容。 2. Web 浏览器的加密长度与客户端安全软件的固件所提供的加密长度兼容。
尝试数字签名电子邮件消息时产生故障消息	操作
当在 Netscape Messenger 中未选择 IBM 嵌入式安全子系统证书，并且电子邮件消息的作者尝试使用证书签名消息时，显示错误消息。	使用 Netscape Messenger 中的安全设置来选择证书。打开 Netscape Messenger 时，单击工具栏上的安全图标。“安全信息”窗口打开。单击左面板中的 **Messenger**，然后选择 **IBM** 嵌入式安全芯片证书。有关更多信息，请参阅由 Netscape 提供的文档。
电子邮件消息使用不同的算法返回到客户机	操作
使用 RC2（40）、RC2（64）或 RC2（128）算法加密的电子邮件消息从使用 Netscape Messenger 的客户机被发送到使用 Outlook Express（128 位）的客户机。从 Outlook Express 客户机返回的电子邮件消息将采用 RC2（40）算法加密。	不需要操作。从 Netscape 客户机到 Outlook Express（128 位）客户机的 RC2（40）、RC2（64）或 RC2（128）加密请求总是使用 RC2（40）算法返回到 Netscape 客户机。请参阅 Microsoft 的资料以获取有关结合您的 Outlook Express 版本使用的加密算法的当前信息。
无法使用由 **IBM** 嵌入式安全子系统生成的数字证书	操作

问题症状	可能的解决方案
由 IBM 嵌入式安全子系统生成的数字证书不可用。	验证打开 Netscape 时是否输入了正确的 UVM 口令。如果您输入了不正确的 UVM 口令，则显示错误消息表明验证失败。如果您单击确定，则 Netscape 打开，但您将无法使用由 IBM 嵌入式安全子系统生成的证书。您必须退出并重新打开 Netscape，然后输入正确的 UVM 口令。
在 **Netscape** 中没有替换来自同一个发送方的新数字证书	操作
当多次接收到来自同一发送方的数字签名的电子邮件时，与电子邮件关联的第一个数字证书未被覆盖。	如果您接收到多个电子邮件证书，则只有一个证书是缺省证书。在 Netscape 中使用安全功能删除第一个证书，然后重新打开第二个证书或要求发送方发送另一个签名的电子邮件。
无法导出 **IBM** 嵌入式安全子系统证书	操作
在 Netscape 中无法导出 IBM 嵌入式安全子系统证书。Netscape 中的导出功能可用于备份证书。	转至管理员实用程序或用户配置实用程序以更新密钥存档。当您更新密钥存档时，创建与 IBM 嵌入式安全子系统关联的所有证书的副本。
硬盘驱动器发生故障后尝试使用复原的证书时产生错误消息	操作
通过使用管理员实用程序中的密钥复原功能可以复原证书。一些证书（例如 VeriSign 提供的免费证书）在密钥复原后可能不会复原。	复原密钥后，获取新的证书。
Netscape 代理程序打开但导致 **Netscape** 失败	操作
Netscape 代理程序打开但关闭了 Netscape。	关闭 Netscape 代理程序。
如果您尝试打开 **Netscape**，则 **Netscape** 延迟	操作
如果您添加 IBM 嵌入式安全子系统 PKCS#11 模块，然后打开 Netscape，则在 Netscape 打开之前将发生短暂延迟。	不需要操作。该延迟是出于提供信息的目的。

数字证书故障诊断信息

如果在获取数字证书时遇到问题，则以下故障诊断信息可能会有帮助。

问题症状	可能的解决方案
在数字证书请求过程中 **UVM** 口令窗口或指纹验证窗口多次显示	操作
UVM 安全策略规定用户在获取数字证书之前提供 UVM 口令或指纹验证。如果用户尝试获取证书，将多次显示要求 UVM 口令或指纹识别的验证窗口。	每次打开验证窗口时输入您的 UVM 口令或识别您的指纹。
显示 **VBScript** 或 **JavaScript** 错误消息	操作
当您请求数字证书时，可能显示与 VBScript 或 JavaScript 相关的错误消息。	重新启动计算机，并再次获取证书。

Tivoli Access Manager 故障诊断信息

如果在结合客户端安全软件使用 Tivoli Access Manager 过程中遇到问题，以下故障诊断信息可能会有帮助。

问题症状	可能的解决方案
本地策略设置不符合服务器上的那些设置	操作
Tivoli Access Manager 允许 UVM 不支持的某些位配置。因此，本地策略要求可以覆盖管理员在配置 PD 服务器时所做的设置。	这是一个已知限制。
Tivoli Access Manager 设置项不可访问	操作
在管理员实用程序的“策略设置”页面上无法访问 Tivoli Access Manager 设置和本地高速缓存设置项。	安装 Tivoli Access Manager Runtime Environment。如果未在 IBM 客户机上安装 Runtime Environment，则“策略设置”页面上的 Tivoli Access Manager 设置将不可用。
用户的控制对于用户和组都有效	操作
配置 Tivoli Access Manager 服务器时，如果您将用户定义到组，并且打开了遍历位，则用户的控制对于用户和组都有效。	不需要操作。

Lotus Notes 故障诊断信息

如果在结合客户端安全软件使用 Lotus Notes 时遇到问题，以下故障诊断信息可能会有帮助。

问题症状	可能的解决方案
为 **Lotus Notes** 启用了 **UVM** 保护后，**Notes** 无法完成其自身的设置	操作
使用管理员实用程序启用 UVM 保护之后，Lotus Notes 无法完成设置。	这是一个已知限制。 必须在使用管理员实用程序启用 Lotus Notes 支持之前配置和运行 Lotus Notes。
当您尝试更改 **Notes** 密码时显示错误消息	操作
在使用客户端安全软件时更改 Notes 密码可能显示错误消息。	重试密码更改。如果这不起作用，则重新启动客户机。
随机生成密码后显示错误消息	操作
当您执行以下操作时可能显示错误消息： • 使用 Lotus Notes 配置工具为 Notes 标识设置 UVM 保护 • 打开 Notes 并使用 Notes 提供的功能来更改 Notes 标识文件的密码 • 在您更改密码后立即关闭 Notes	单击确定关闭错误消息。不需要任何其它操作。 与错误消息相反，密码已更改。新的密码是由客户端安全软件创建的随机生成的密码。Notes 标识文件现在用随机生成的密码加密，并且用户不需要新的用户标识文件。如果最终用户再次更改密码，UVM 将为 Notes 标识生成新的随机密码。

加密故障诊断信息

如果在使用客户端安全软件 3.0 或更高版本加密文件时遇到问题，以下故障诊断信息可能会有帮助。

问题症状	可能的解决方案
不能解密先前加密的文件	操作
使用客户端安全软件的先前版本加密的文件在升级到客户端安全软件 3.0 或更高版本之后不能解密。	这是一个已知限制。 安装客户端安全软件 3.0 或更高版本*之前*，您必须解密使用客户端安全软件的先前版本加密的所有文件。由于客户端安全软件 3.0 的文件加密实现中的更改，客户端安全软件 3.0 无法解密使用客户端安全软件先前版本加密的文件。

UVM 感知设备故障诊断信息

如果在使用 UVM 感知设备时遇到问题，以下故障诊断信息可能会有帮助。

问题症状	可能的解决方案
UVM 感知设备停止正常工作	操作
UVM 感知的安全设备（例如智能卡、智能卡阅读器或指纹阅读器）运行不正常。	请确认系统是否已正确配置设备。配置设备后，您可能需要重新引导系统以正确启动服务。 有关设备故障诊断的信息，请参阅设备文档或联系设备供应商。
UVM 感知设备停止正常工作	操作
当您从通用串行总线（USB）端口断开 UVM 感知设备的连接，然后重新将设备连接到 USB 端口时，则设备可能不能正确工作。	在设备重新连接到 USB 端口后重新启动计算机。

附录 A. 客户端安全软件的美国出口条例

IBM 客户端安全软件软件包已由 IBM 出口管理办公室（ERO）复查，而且根据美国政府出口管理的要求，IBM 已提交相应的文档，并从美国商业部获取高达 256 位加密支持的零售分类许可，用于除美国政府禁运的那些国家或地区以外的国际分发。美国和其它国家或地区的条例依据各自的国家或地区政府而更改。

如果您无法下载客户端安全软件软件包，请联系您当地的 IBM 销售办事处以与您的 IBM 国家或地区出口条例协调员（ERC）核实。

附录 B. 密码和口令信息

本附录包含有关密码和口令的信息。

密码和口令规则

当处理安全系统时，有许多不同的密码和口令。不同的密码具有不同的规则。本部分包含有关管理员密码和 UVM 口令的信息。

管理员密码规则

安全管理员无法更改支配管理员密码的规则。

以下规则是关于管理员密码的：

长度　密码必须刚好是八个字符。

字符　密码必须仅包含字母数字字符。允许字母与数字的组合。不允许特殊的字符，如空格、!、？ 、%。

属性　请设置管理员密码以在计算机中启用 IBM 嵌入式安全芯片。每次您访问管理员实用程序和管理员控制台时必须输入该密码。

不正确的尝试

如果您输入十次不正确的密码，计算机会锁定 1 小时 17 分钟。如果在经过这段时间后，您又输入了十次不正确的密码，计算机将锁定 2 小时 34 分钟。您每输入十次不正确的密码，计算机禁用的时间就会加倍。

UVM 口令规则

IBM 客户端安全软件使安全管理员能够设置管理用户 UVM 口令的规则。为提高安全性，UVM 口令可以更长并且可以比传统的密码更具唯一性。UVM 口令策略由管理员实用程序来控制。

管理员实用程序中的 UVM 口令策略界面使安全管理员能通过简单的界面来控制口令标准。UVM 口令策略界面使管理员能确定以下口令规则：

注：以下括号中提供了每个口令标准的缺省设置。

- 确定是否设置允许的最小字母数字字符数（是，6）

  例如，允许设置为“6”个字符时，`1234567xxx` 是无效的密码。
- 确定是否设置允许的最小数字字符数（是，1）

  例如，设置为“1”时，`thisismypassword` 是无效密码。
- 确定是否设置允许的最小空格数（无最小值）

  例如，设置为“2”时，`i am not here` 是无效密码。
- 确定是否使口令能以数字开始（否）

  例如，缺省情况下，`1password` 是无效密码。

- 确定是否使口令能以数字结束（否）

  例如，缺省情况下，password8 是无效密码。
- 确定是否允许口令包含用户标识（否）

  例如，缺省情况下，UserName 是无效密码，其中 UserName 是用户标识。
- 确定是否确保新的口令与前 x 个口令不同，其中 x 是可编辑的字段（是，3）

  例如，缺省情况下，如果您的最后三个密码中的任何一个是 mypassword，则 mypassword 是无效密码。
- 确定口令是否可以包含来自前一个密码的任何位置多于三个的连续相同的字符（否）

  例如，缺省情况下，如果您的前一个密码是 pass 或 word，则 paswor 是无效的密码。

管理员实用程序中的 UVM 口令策略界面也能够使安全管理员控制口令的失效。UVM 口令策略界面使管理员能够在以下口令失效规则中进行选择：

- 确定是否在一定天数后，使口令失效（是，184）

  例如，缺省情况下口令将在 184 天后失效。新口令必须与已确定的口令策略相符。
- 确定口令是否会失效（是）

  如果选择了该选项，口令将永不失效。

用户登记时在管理员实用程序中检查口令策略，并且还在用户从客户机实用程序更改口令时检查该策略。与前一个密码相关的两个用户设置将重新设置并且将除去任何口令历史。

以下一般规则是关于 UVM 口令的：

长度　口令的长度最多可以是 256 个字符。

字符　口令可包含键盘输入字符的任何组合，包括空格和非字母数字字符。

属性　UVM 口令不同于您用于登录操作系统的密码。UVM 口令可结合其它验证设备使用，如 UVM 感知指纹传感器。

不正确的尝试

如果在会话过程中多次输入不正确的 UVM 口令，则计算机将实行一系列反攻击延迟。这些延迟在以下部分中指定。

TCPA 和非 TCPA 系统上的失败计数

下表显示 TCPA 系统的反攻击延迟设置：

尝试次数	下次失败时的延迟
15	1.1 分钟
31	2.2 分钟
47	4.4 分钟
63	8.8 分钟

尝试次数	下次失败时的延迟
79	17.6 分钟
95	35.2 分钟
111	1.2 小时
127	2.3 小时
143	4.7 小时

TCPA 系统不区分用户口令和管理员密码。任何使用 IBM 嵌入式安全芯片的验证遵守相同的策略。最大超时为 4.7 小时。TCPA 系统延迟不会超过 4.7 小时。

非 TCPA 系统区分管理员密码和用户口令。在非 TCPA 系统上，管理员密码在 10 次失败尝试后有 77 分钟的延迟；用户密码在 32 次失败尝试后只有 1 分钟的延迟，然后在每 32 次失败尝试后锁定时间加倍。

重新设置口令

如果用户忘记其口令，则管理员可以使用户能够重新设置其口令。

远程重新设置口令

要远程重新设置密码，请完成以下过程：

- 管理员

  远程管理员必须执行以下操作：

  1. 创建新的一次性密码并且向用户传达该密码。
  2. 将数据文件发送给用户。

     可以通过电子邮件将数据文件发送给用户，可以将它复制到可移动介质上（例如软盘）或者可以将它直接写入用户存档文件（假定用户可以访问该系统）。该加密文件用于匹配新的一次性密码。

- 用户

  用户必须执行以下操作：

  1. 登录到计算机上。
  2. 当提示需要口令时，选中 “ 忘记口令 ” 复选框。
  3. 输入远程管理员传达的一次性密码并且提供管理员所发送的文件的位置。

     UVM 验证文件中的信息与所提供的密码匹配后，就授予用户访问权。然后直接提示用户更改口令。

这是所建议的重新设置已丢失口令的方式。

手动重新设置口令

如果管理员可以转到用户忘记其口令的系统，则管理员可作为管理员登录到该用户的系统，向管理员实用程序提供管理员私钥并且手动更改用户的口令。要更改口令，管理员不必知道用户的旧口令。

附录 C. 为系统登录使用 UVM 保护的规则

UVM 保护确保只有已为特定 IBM 客户机添加到 UVM 的那些用户能够访问操作系统。Windows 操作系统包含提供登录保护的应用程序。尽管 UVM 保护设计为与那些 Windows 登录应用程序平行工作，但是 UVM 保护根据操作系统的不同而不同。

UVM 登录界面替换操作系统登录，以便每次用户尝试登录系统时 UVM 登录窗口打开。

在您为了系统登录设置和使用 UVM 保护前，阅读以下提示：

- 当启用 UVM 保护时，请勿清除 IBM 嵌入式安全芯片。如果您清除了 IBM 嵌入式安全芯片，则硬盘的内容变成不可用，这样您必须重新格式化硬盘驱动器，并重新安装所有软件。
- 如果您在管理员实用程序中清除用 **UVM** 的安全登录替换标准 **Windows** 登录复选框，则在无 UVM 登录保护的情况下系统返回到 Windows 登录过程。
- 您可以选择选项来指定允许为 Windows 登录应用程序输入正确密码的最大尝试次数。该选项不适用于 UVM 登录保护。对于您可设置允许输入 UVM 口令的尝试次数没有限制。

附录 D. 声明与商标

该附录提供 IBM 产品的法律声明以及商标信息。

声明

本信息是为在美国提供的产品和服务编写的。

IBM 可能在其他国家或地区不提供本文档中讨论的产品、服务或功能特性。有关您当前所在区域的产品和服务的信息，请向您当地的 IBM 代表咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或暗示只能使用 IBM 的产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务，则由用户自行负责。

IBM 公司可能已拥有或正在申请与本文档内容有关的各项专利。提供本文档并未授权用户使用这些专利的任何许可。您可以用书面方式将许可查询寄往：

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

本条款不适用英国或任何这样的条款与当地法律不一致的国家或地区：
International Business Machines Corporation “按现状”提供本出版物，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关非侵权、适销和适用于某种特定用途的保证。某些国家或地区在某些交易中不允许免除明示或暗含的保证。因此本条款可能不适用于您。

本信息中可能包含技术方面不够准确的地方或印刷错误。此处的信息将定期更改；这些更改将编入本出版物的新版本中。IBM 可以随时对本信息中描述的产品和／或程序进行改进和／或更改，而不另行通知。

本程序的被许可方如果要了解有关程序的信息以达到如下目的：(i) 允许在独立创建的程序和其他程序（包括本程序）之间进行信息交换，以及 (ii) 允许对已经交换的信息进行相互使用，请与下列地址联系：IBM Corporation, Department 80D, P.O. Box 12195, 3039 Cornwallis, Research Triangle Park, NC 27709, U.S.A. 只要遵守适当的条件和条款，包括某些情况下的一定数量的付费，都可获得这方面的信息。

本资料中描述的许可程序及其所有可用的许可资料均由 IBM 依据 IBM 客户协议、IBM 国际程序许可协议或任何同等协议中的条款提供。

商标

IBM 和 SecureWay 是 IBM 公司在美国和／或其他国家或地区的商标。

Tivoli 是 Tivoli Systems Inc. 在美国和／或其他国家或地区的商标。

Microsoft、Windows 和 Windows NT 是 Microsoft Corporation 在美国和／或其他国家或地区的商标。

其它公司、产品和服务名称可能是其它公司的商标或服务标记。

中国印刷