IBM® 客户端安全解决方案

客户端安全软件版本 5.3 管理员指南

IBM® 客户端安全解决方案

客户端安全软件版本 5.3 管理员指南

第一版（**2004** 年 **5** 月）

在使用该资料以及它支持的产品前，请确保阅读第 69 页的附录 A, 『客户端安全软件的美国出口条例』和第 77 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

该指南包含有关设置和使用与客户端安全软件一起提供的安全功能的信息。

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，『加密和解密文件和文件夹』”包含关于如何使用 IBM 客户端安全软件来保护敏感文件和文件夹的信息。

“第 3 章，『CSS 安全证书漫游』”包含关于如何配置 CSS 安全证书漫游网络、注册漫游客户机、授权和导入用户、同步用户数据和复原漫游网络的信息。

“第 4 章，『如何使用客户端安全软件』”包含关于如何使用客户端安全软件所提供的组件来设置 IBM 客户机用户所需的安全功能的示例。

“第 5 章，『授权用户』”包含关于客户机用户验证的信息，其中包含如何在 IBM 用户验证管理工具（UVM）中授权和删除用户。

“第 6 章，『使用 UVM 对用户授权后』”包含关于如何使用 Lotus Notes 的 UVM 保护，以及结合 Netscape 应用程序使用客户端安全软件设置操作系统登录的 UVM 保护的信息说明。

“第 7 章，『处理 UVM 策略』”包含关于如何编辑本地 UVM 策略、使用远程客户机的 UVM 策略和更改 UVM 策略文件的密码的说明。

“第 8 章，『其它安全管理员功能』”包含关于如何使用管理员实用程序来更改密钥存档位置、从存档复原密钥、恢复 UVM 口令以及启用或禁用 IBM 嵌入式安全芯片的说明。

“第 9 章，『客户机用户说明』”包含关于客户机用户在使用客户端安全软件时所执行的不同任务的说明。本章包含关于如何使用 UVM 登录保护、安全的电子邮件和用户配置实用程序的说明。

“第 10 章，『故障诊断』”包含您在使用该指南中所提供的说明时，克服可能遇到的已知限制和问题的有用信息。

“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』”包含密码标准，该标准适用于安全芯片密码的 UVM 口令和规则。

“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

该指南供执行以下操作的安全管理员使用：

- 为 IBM 客户机设置用户验证
- 为 IBM 客户机设置和编辑 UVM 安全策略
- 使用管理员实用程序为 IBM 客户机管理安全子系统（IBM 嵌入式安全芯片），以及相关设置

该指南还供 Tivoli Access Manager 管理员使用，他们将使用 IBM Tivoli Access Manager 管理 UVM 策略中提供的验证对象。Tivoli Access Manager 管理员必须能管理以下各项：

- Tivoli Access Manager 对象空间
- 验证、授权和安全证书获取过程
- IBM 分布式计算环境（DCE）
- IBM SecureWay Directory 轻量级目录访问协议（LDAP）

如何使用本指南

使用该指南为 IBM 客户机设置用户验证和 UVM 安全策略。该指南是*《客户端安全软件安装指南》*、*《结合客户端安全使用 Tivoli Access Manager》*和*《客户端安全软件用户指南》*的姊妹篇。可从 http://www.pc.ibm.com/us/security/secdownload.html IBM Web 站点下载该指南和客户端安全的所有其它文档。

对*《客户端安全软件安装指南》*的引用

本文档中提供对*《客户端安全软件安装指南》*的引用。在您可使用该指南前，您必须在 IBM 客户机上安装客户端安全软件。*《客户端安全软件安装指南》*中提供了安装该软件的说明。

对*《结合客户端安全使用 Tivoli Access Manager》*的引用

该文档中提供对*《结合客户端安全使用 Tivoli Access Manager》*的引用。将使用 Tivoli Access Manager 为 UVM 策略管理验证对象的安全管理员应该阅读*《结合客户端安全使用 Tivoli Access Manager》*。

对*《客户端安全用户指南》*的引用

该文档中提供了对*《客户端安全用户指南》*的引用。管理员可使用该指南在使用客户端安全软件的 IBM 客户机上设置和维护 UVM 策略。在管理员设置用户验证和 UVM 安全策略后，客户机用户可阅读*《客户端安全用户指南》*，以了解如何使用客户端安全软件。

《用户指南》包含关于执行客户端安全软件任务（例如使用 UVM 登录保护、创建数字证书以及使用用户配置实用程序）的信息。

附加信息

您可从 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（在可用时）。

第 1 章 简介

无可挑剔的 ThinkPad™ 和 ThinkCentre™ 计算机装配有内置的加密硬件，它可以结合可下载的软件技术为客户机 PC 平台提供强大的安全级别。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）。

客户端安全软件设计用于使用 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

为了有效地使用 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取消激活嵌入式安全子系统，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、创建和配置启用部署的文件以及创建非管理员配置和恢复概要文件。
- 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。用户还可创建由 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。客户端安全软件启用以下功能：
  - **UVM** 客户机策略保护：客户端安全软件使安全管理员能够设置客户端安全策略，它规定了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 密码未向 UVM 注册或注册不正确，那么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够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协同工作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运行至关重要。

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 接口（仅限 ThinkCentre 计算机）

具有创建并且维护管理员密码的策略很重要。如果已泄露或者忘记管理员密码，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，所以有时候它又称为*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*根*信任。该根用于保护其它应用程序和功能。建立根信任的一部分是创建硬件公钥和硬件私钥。公钥和私钥（统称为*密钥对*）在数学上以下列方式相关联：

- 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。

在安全子系统的安全硬件范围内创建、存储和使用硬件私钥。硬件公钥可用于多种用途（因此称为公钥），但是它绝对不会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将有所描述。

硬件公钥和私钥的创建方式如下：

- 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 密钥交换层次结构整体的一部分。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，所以具有使用相对已知的密钥而言唯一的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 客户端安全软件时将创建这些密钥对。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*）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。

层次结构的下一个密钥“级别”（根以上）是管理员公钥和私钥或*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。如何管理这一密钥对取决于您想如何管理网络。由于管理员私钥在客户机系统（通过硬件公钥受保护）和管理员定义的位置中驻留，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。登记用户时会创建用户公钥和私钥（*用户密钥对*）并且会创建新的密钥“级别”。用户私钥已通过管理员公钥加密。通过硬件公钥加密管理员私钥。因此，要使用用户私钥，必须将管理员私钥（已通过硬件公钥加密）装入安全子系统。一旦装入芯片中，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使用。当前的 Windows 用户私钥（已通过管理员公钥加密）被传递到安全子系统中。还会将影响嵌入式安全子系统的应用程序所需要的任何数据传递到芯片中，在安全子系统的安全环境中进行解密和使用。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。这样提供了几乎无限量通过 IBM 嵌入式安全芯片进行保护的数据。

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。在任何给定时间内只能在安全子系统中存储一对密钥。在一次次进行引导时，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 嵌入式安全子系统中。相关的已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。

通过硬件公钥加密管理员私钥。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（已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量的用户；然而，最佳实践表明每台计算机限制登记 25 个用户会确保最佳性能。

IBM ESS 利用密钥交换层次结构，在该结构里，安全子系统的硬件公钥和私钥用来保护存储在芯片以外的其它数据。该硬件私钥在安全子系统中生成并且从不离开此安全环境。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，所以只能在此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能力确保了每个硬件密钥对在统计上都是唯一的。

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。
- 公钥密码术的加密密钥管理。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，其中基本级别硬件密钥用于加密其上的密钥，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以用户公钥加密。而且，Netscape 用户可选择 IBM 嵌入式安全子系统作为用于安全性的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，如 Netscape Messenger，可利用 IBM 嵌入式安全子系统提供的保护。
- 把数字证书转移到 **IBM** 嵌入式安全子系统的能力。IBM 客户端安全软件证书转移工具使您能够将使用缺省 Microsoft CSP 创建的证书转移到 IBM 嵌入式安全子系统 CSP。这样大大增加了为与证书相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界面，使您能够建立由 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。为正常的运行，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能够作为单个用户的一次性验证标记使用。除非使用安全证书漫游，否则每个智能卡都绑定到系统。因为该智能卡必须与密码（可能会损坏）一起提供，所以需要智能卡使您的系统更安全。
- 安全证书漫游。安全证书漫游使得到授权的网络用户能够使用网络上的任何计算机，就象是自己的工作站一样。用户得到授权在任意注册了客户端安全软件的客户机上使用 UVM 后，就能够将其个人数据导入到安全证书漫游网络中的其它任何注册的客户机中。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，客户端安全软件建立特定于用户的口令和口令失效策略。

第 2 章 加密和解密文件和文件夹

加密技术使用户能够保护他们计算机上包含的敏感数据。加密文件确保了在没有满足指定的安全要求的情况下，没有人可以访问加密文件中的信息。加密文件还可以保护通过因特网或网络发送的文件中的敏感数据。

IBM 客户端安全软件使用户能够以下列方法加密和解密敏感文件和文件夹：

- 使用客户端安全软件应用程序的单个文件 " 右键单击 " 加密。

  该功能是下载的基本 IBM 客户端安全软件的一部分。
- 使用 **IBM** 文件和文件夹加密实用程序的透明、实时的文件和文件夹加密。

  注：为了启用该功能，必须下载 IBM 文件和文件夹加密（FFE）实用程序。必须在您安装 IBM 文件和文件夹加密实用程序*之前*安装 IBM 客户端安全软件。

右键单击加密

客户端安全软件的基本右键单击加密功能使用户能够使用他们的鼠标右键单击按键保护敏感文件。要利用该功能，不需要下载其它软件。用该功能加密的文件将具有以下特征：

- 每次您希望使用加密的文件时都必须手动将其解密，为了再次保护它，在完成时手动将其加密。每次加密或解密文件时都必须调用 UVM 策略。这些要求对选定文件的加密和解密提供强大的手动控制，但是该严格保护对于每次使用加密文件时不希望提供密码、指纹或智能卡的用户就不太方便。
- 文件可以加密状态发送到远程位置；然而，它们只能在其加密的计算机上进行解密，因为用于加密文件的密钥对于该计算机上的 IBM 嵌入式安全子系统是唯一的。

通过右击菜单可手工加密和解密文件。当文件以这种方式加密时，加密操作将 `.$enc$` 扩展名追加到文件。然后这些加密的文件可以安全地存储在远程服务器上。在再次使用右键单击功能将其解密前，它们将保持加密，并且应用程序不能使用它们。

透明的实时加密（FFE 加密）

可从 IBM 客户端安全 Web 站点下载 IBM 文件和文件夹加密（FFE）实用程序来启用客户端安全软件的透明、实时的加密功能。FFE 提供了比 CSS 的 " 右键单击 " 基本加密功能更加方便、透明的加密格式。还可以使用鼠标的右键单击按键调用使用 FFE 的文件和文件夹加密。用 FFE 加密的文件和文件夹将具有以下特征：

- UVM 策略只需要在启动时调用。这对选定文件提供了更方便的加密和解密方式，因为您*不*需要在每次希望使用加密文件时提供密码、指纹或智能卡。
- 当应用程序打开使用文件和文件夹加密实用程序加密的文件时，该文件自动解密。当保存使用文件和文件夹加密实用程序加密的文件时，该文件自动加密。
- 用文件和文件夹加密（FFE）实用程序加密的文件可以发送到远程位置；然而，它们将以解密状态发送。

在保护或取消保护文件夹后，重新启动操作系统时，Check Disk 实用程序可能会运行。使用计算机前，请等待系统检查完成。

下载了 FFE 实用程序的用 UVM 登记的用户可通过右键单击界面选择要保护或取消保护的文件夹。这将加密文件夹或它的子文件夹中包含的所有文件。当文件以这种方式保护时，文件名不会添加任何扩展名。当应用程序访问加密文件夹中的文件时，文件将解密到内存并且在保存于硬盘之前将重新加密。

任何 Windows 操作（访问受保护文件夹中的文件）将被授予对已解密方式的数据的访问权。由于文件不需要在每次使用时进行解密或者不需要在每次用它完成程序时重新加密，所以该功能使加密更方便。

FFE 文件夹加密状态

文件和文件夹加密实用程序使用户能够使用他们鼠标的右键单击按键保护敏感文件和文件夹。软件如何保护文件和文件夹根据文件或文件夹最初如何加密而不同。

文件夹可以处于以下任何一种状态：

- 不受保护的文件夹

  该文件夹，其子文件夹以及其任何父代文件夹都未指定为受保护。用户可选择保护此文件夹。

- 受保护的文件夹

  受保护的文件夹可处于三种状态之一：

  – 由当前用户保护

    当前用户已将此文件夹指定为受保护。所有文件已加密（包含所有子文件夹中的文件）。用户可选择取消保护此文件夹。

  – 由当前用户保护的文件夹的子文件夹

    当前用户已将此文件夹中的一个父代指定为受保护。所有文件已加密。当前用户没有右键单击选项。

  – 由不同的用户保护

    不同的用户已将此文件夹指定为受保护。所有文件已加密（包含所有子文件夹中的文件），并且对于当前用户不可用。当前用户没有右键单击选项。

- 受保护文件夹的父代文件夹

  受保护文件夹的父代文件夹可处于三种状态之一：

  – 它可包含当前用户所保护的一个或多个子文件夹

    当前用户已将一个或多个子文件夹指定为受保护。受保护子文件夹中的所有文件都已加密。用户可以选择保护父代文件夹。必须在取消对父文件夹中所有子文件夹的受保护之后，该父文件夹才能受保护。

  – 它可包含一个或多个不同用户所保护的一个或多个子文件夹

    一个或多个不同的用户已将一个或多个子文件夹指定为受保护。受保护的子文件夹中的所有文件已加密，并且对于当前用户不可用。当前用户没有右键单击选项。

– 它可包含当前用户，以及一个或多个不同用户所保护的子文件夹

当前用户和一个或多个不同的用户都已将子文件夹指定为受保护。当前用户没有右键单击选项。

- 关键文件夹

关键文件夹是在关键路径中的文件夹，因此不能受保护。以下是两个关键路径：Windows 路径和客户端安全路径。

通过右键单击保护文件夹选项分别处理每种状态。

文件和文件夹加密实用程序的技巧

在执行某些 FFE 实用程序功能时，以下信息可能会有用。

盘符保护

IBM FFE 实用程序只可用于加密驱动器 C 上的文件和文件夹。该实用程序不支持任何其它硬盘分区或物理驱动器上的加密。

删除受保护的文件和文件夹

要确保在 " 回收站 " 中没有敏感文件或文件夹设为未保护，您必须使用 Shift+Del 组合键删除受保护文件夹和文件。Shift+Del 按键顺序执行无条件删除操作，并且不会尝试将已删除文件放置到 " 回收站 " 中。

在从 **IBM FFE** 实用程序先前版本升级之前

在您从 IBM FFE 实用程序 V2.0 或更早版本进行升级之前，请从 IBM 安全 Web 站点下载并且使用访问控制列表（ACL）修复工具。在卸载早于 FFE V2.0 的任何版本*之前*，应该使用该修复实用程序。否则，卸载过程可能失败并导致受影响的文件不可访问。

卸载 **IBM FFE** 实用程序之前

卸载 IBM FFE 实用程序之前，请使用 IBM FFE 实用程序对当前受保护的文件或文件夹取消保护。

文件和文件夹加密（**FFE**）实用程序限制

IBM FFE 实用程序有以下限制：

移动受保护文件和文件夹时的限制

IBM FFE 实用程序不支持以下操作：

- 在受保护的文件夹中移动文件和文件夹
- 在受保护和不受保护的文件夹之间移动文件或文件夹

如果您试图执行这些不受支持的 " 移动 " 操作中的任何一种，操作系统将显示 " 拒绝访问 " 消息。该消息是正常的。它仅提供不支持 " 移动 " 操作的通知。作为使用 " 移动 " 操作的替代操作，请执行以下操作：

1. 将受保护文件或文件夹复制到新的位置。

2. 使用 Shift+Del 组合键删除原始文件或文件夹。

运行应用程序时的限制

IBM FFE 实用程序不支持从受保护文件夹运行应用程序。例如，如果您有一个名为 PROGRAM.EXE 的可执行文件，则您无法从受保护文件夹运行该应用程序。

路径名长度限制

当您试图使用 IBM FFE 实用程序保护一个文件夹或试图将未保护的文件夹中的文件或文件夹复制或移动至受保护的文件夹中，您可能会接收到操作系统发出的 “ 一个或多个路径名过长 ” 的消息。如果您接收到该消息，则有一个或多个的文件或文件夹的路径超出最大允许字符长度。要解决问题，请重新安排文件夹结构以缩短其深度，或者缩短一些文件夹名或文件名的长度。

保护文件夹的问题

如果您试图保护文件夹并接收到消息表明 “ 无法保护文件夹。一个或更多文件可能正在使用 ”，请检查以下内容：

- 验证当前未在使用文件夹中包含的文件。
- 如果 Windows 资源管理器显示您试图保护的文件夹的一个或多个子文件夹，请确保您试图保护的文件夹（而不是任一子文件夹）突出显示并处于活动状态。

第 3 章 CSS 安全证书漫游

IBM 客户端安全软件的安全证书漫游功能使 UVM 用户的安全证书能够在网络中支持 TCPA 的所有计算机上使用。该网络（称为漫游网络）使用户能够从网络中的任何计算机方便地进行工作，从而增强了用户的灵活性并提高了应用程序的可用性。

CSS 安全证书漫游网络要求

CSS 安全证书漫游网络由以下必要组件构成：

- 漫游服务器
- 漫游客户机
- 存储 UVM 用户存档的网络共享映射驱动器

注：漫游服务器和授权的漫游客户机只是支持 TCPA 的计算机，它们带有安装 IBM 客户端安全软件 5.1 或更高版本所使用的管理员密码（已建立）。

设置漫游服务器

要配置 CSS 安全证书漫游网络，必须指定一台 TCPA 计算机作为漫游*服务器*（称为系统 A）。其它计算机一旦向漫游服务器注册后即被授权为注册 CSS 的*客户机*。（第一个注册的客户机称为系统 B。）

您指定作为漫游服务器的计算机并无特殊之处。您可以使用将成为漫游网络一部分的任何一台计算机。漫游服务器就是一台普通的计算机，该计算机被指定用来确定哪些计算机已成为漫游网络 “ 可信 ” 的计算机。计算机向漫游服务器注册后即被网络中的所有计算机所信任。

配置漫游网络是一个包含两个步骤的过程：

1. 通过建立密钥、存档和漫游用户配置系统 A（服务器）。
2. 在 CSS 安全证书漫游网络中，将系统 B 和其它所有计算机注册为漫游客户机。

漫游服务器定义 CSS 安全证书漫游网络并且启动漫游客户机的注册，但是 CSS 安全证书漫游网络的重点是存储用户存档的已映射网络驱动器。该存档是存储用户安全证书的所有更新的位置。该存档不应该位于漫游服务器或任一漫游客户机上。初始化 CSS 客户机后，漫游服务器与任何其它 CSS 注册客户机一样运行。

配置漫游服务器

要配置漫游服务器，请完成以下过程：

1. 在指定的计算机上启动管理员控制台，然后单击配置安全证书漫游。或者如果已经把计算机配置成漫游，就选择将此系统重新配置为 **CSS** 漫游服务器，单击下一步，然后单击确定。
2. 在指定为漫游服务器的计算机上创建 `c:\roaming` 文件夹。
3. 启动管理员控制台并单击配置安全证书漫游。
4. 选择将此系统配置为 **CSS** 漫游服务器并单击下一步。

5. 单击配置。
6. 选择创建新的存档密钥并在“ 存档密钥文件夹 ”字段中输入新的密钥文件夹，其中存档密钥文件夹存储在 c:\roaming 文件夹中。
7. 选择使用现有的密钥对或创建新密钥对，然后单击下一步。
8. 输入存档文件夹，然后单击下一步。

   注：已注册漫游的其它计算机（漫游客户机）必须能够访问存档文件夹和密钥文件夹。c:\roaming 目录必须是映射的网络驱动器。

   如果当前存档中有文件，则向导的下一页会提示您如何处理这些文件。
9. 单击完成。

在漫游服务器上注册客户机

要在漫游服务器上注册漫游客户机，请完成以下过程：

1. 漫游服务器的配置完成后，将立即显示“ 安全证书漫游网络配置 ”屏幕。选择启用客户机注册，然后单击下一步。
2. 输入系统 B 上具有管理员权限的用户的名称，该用户将完成客户机注册。
3. 输入并确认该用户将使用的 8 个字符的密码。（不要将该过程与稍后发生的授权用户使用 UVM 混淆起来。）
4. 如果要使用用户配置实用程序注册客户机，则需要为该用户创建管理员配置文件。该过程会生成一个对该用户唯一的文件。在该用户以及系统 B 可以访问的位置存储该文件。

   注：使用管理员实用程序注册客户机时不需要生成该文件。
5. 输入系统 B 的管理员密码并单击下一步。
6. 如果您已创建管理员配置文件，请在该用户以及系统 B 可以访问的位置存储该文件。

完成先前的过程后，漫游服务器配置完毕。必须在每台漫游客户机上完成注册后漫游网络才可使用。

完成漫游客户机注册过程

在漫游服务器上注册了一系列可信系统后，必须在客户机系统上完成以下过程之一。漫游服务器必须正在运行并且已经连接到存档之后，您才能完成漫游客户机的注册过程。

使用管理员实用程序注册漫游客户机

要使用管理员实用程序注册漫游客户机，请完成以下过程：

1. 单击密钥配置。
2. 如果询问您是否要从存档复原密钥，请单击否。
3. 选择向 CSS 漫游服务器注册该系统，然后单击下一步。
4. 输入系统 A 创建的存档位置，输入在系统 A 上为该用户指定的系统注册密码，然后单击下一步。

   完成注册需要大约一分钟的时间。

使用用户配置实用程序注册漫游客户机

要使用用户配置实用程序注册漫游客户机，请完成以下过程：

1. 从“用户配置”选项卡单击向 **CSS** 漫游服务器注册。
2. 选择系统 A 上生成的管理员配置文件，输入为系统 A 上的该用户指定的系统注册密码，然后单击下一步。
3. 输入系统 A 创建的存档位置，然后单击下一步。

完成注册需要大约一分钟的时间。

使用大规模部署（静默）注册漫游客户机

要使用大规模部署静默地注册漫游客户机，请完成以下过程：

1. 创建 csec.ini 文件。有关如何创建 CSS .ini 文件的详细信息，请阅读《*客户端安全软件安装指南*》。
2. 在文件的 csssetup 节中，添加“enableroaming=1”。这表示该计算机应该注册为漫游客户机。
3. 在同一节中，添加“username=OPTION”条目。该值可能有三个选项：
   - 选项 **1**：字符串“**[promptcurrent]**” — 包含括号。如果在漫游服务器上生成了当前登录用户的一个 .dat 文件并且当前用户知道系统注册密码，就应该使用该指定。在部署之前，该选项将打开一个弹出窗口提示用户输入系统注册密码（sysregpwd）。
   - 选项 **2**：字符串“**[current]**” — 包含括号。如果在服务器上生成了当前登录用户的一个 .dat 文件，就应该使用该指定。sysregpwd 的操作如下一步中所述。
   - 选项 **3**：实际的用户名，例如“**joseph**”。如果使用了这样一个指定的用户名，漫游服务器必须已经生成“joseph.dat”。对于该情况，sysregpwd 的操作也如下一步中所述。
4. 如果使用了上述选项 2 或 3，则必须提供另一条目“sysregpwd=SYSREGPW”。这是一个八位数字的系统注册密码，或与当前的用户相关（如果实现选项 2），或与指定的用户相关（如果实现了选项 3）。
5. 要完成客户机注册，请将计算机连接至由漫游服务器设置的存档。csec.ini 文件中指定了该存档。csec.ini 文件中还指定了 CSS 安全证书漫游服务器上设置的密钥文件夹。
6. 使用管理员控制台加密 csec.ini 文件。

csec.ini 文件的示例

以下示例显示了一个 csec.ini 文件样本以及它是如何根据所选的安全证书漫游选项而发生变化的。这些选项如下：

- 无漫游值。 对于安全证书漫游不启用该基本文件。
- 漫游选项 **1**。 在客户机注册时使用选项 1 启用该文件进行漫游。当前用户必须在部署前提供系统注册密码。
- 漫游选项 **2**。 在客户机注册时使用选项 2 启用该文件进行漫游。当前用户必须提供在 .ini 文件中指定的用户标识和系统注册密码。
- 漫游选项 **3**。 在客户机注册时使用选项 3 启用该文件进行漫游。在 .ini 文件中指定了用户。必须在 .ini 文件中提供指定用户的系统注册密码。

四个不同的 CSEC.INI 文件示例如下：

[CSSSetup]	选项 **1**	选项 **2**	选项 3
	[CSSSetup]	[CSSSetup]	[CSSSetup]
suppw=bootup	suppw=bootup	suppw=bootup	suppw=bootup
hwpw=11111111	hwpw=11111111	hwpw=11111111	hwpw=11111111
newkp=1	newkp=1	newkp=1	newkp=1
keysplit=1	keysplit=1	keysplit=1	keysplit=1
kpl=c:\jgk	kpl=c:\\computer name\jgk，计算机在其中存储漫游服务器上的密钥对	kpl=c:\\computer name\jgk，计算机在其中存储漫游服务器上的密钥对	kpl=c:\\computer name\jgk，计算机在其中存储漫游服务器上的密钥对
kal=c:\jgk\archive	kal=c:\\computer name\archive，计算机在其中存储漫游服务器上的存档	kal=c:\\computer name\archive，计算机在其中存储漫游服务器上的存档	kal=c:\\computer name\archive，计算机在其中存储漫游服务器上的存档
pub= c:\jk\admin.key	pub= c:\jk\admin.key	pub= c:\jk\admin.key	pub= c:\jk\admin.key
pri= c:\jk\private1.key	pri= c:\jk\private1.key	pri= c:\jk\private1.key	pri= c:\jk\private1.key
wiz=0	wiz=0	wiz=0	wiz=0
clean=0	**enableroaming=1 username= [promptcurrent]**	**enableroaming=1 username= [current] sysregpwd=12345678**	**enableroaming=1 username= joseph sysregpwd=12345678**
	clean=0	clean=0	clean=0
[UVMEnrollment]	[UVMEnrollment]	[UVMEnrollment]	[UVMEnrollment]
enrollall=0	enrollall=0	enrollall=0	enrollall=0
enrollusers=1	enrollusers=1	enrollusers=1	enrollusers=1
user1=joseph	user1=joseph	user1=joseph	user1=joseph
user1uvmpw= q1234r	user1uvmpw=q1234r	user1uvmpw=q1234r	user1uvmpw=q1234r
user1winpw=	user1winpw=	user1winpw=	user1winpw=
user1domain=0	user1domain=0	user1domain=0	user1domain=0
user1ppchange=0	user1ppchange=0	user1ppchange=0	user1ppchange=0
user1ppexppolicy=0	user1ppexppolicy=0	user1ppexppolicy=0	user1ppexppolicy=0
user1ppexpdays= 184	user1ppexpdays=184	user1ppexpdays=184	user1ppexpdays=184
[UVMAppConfig]	[UVMAppConfig]	[UVMAppConfig]	[UVMAppConfig]
uvmlogon=0	uvmlogon=0	uvmlogon=0	uvmlogon=0
entrust=0	entrust=0	entrust=0	entrust=0
notes=0	notes=0	notes=0	notes=0
netscape=0	netscape=0	netscape=0	netscape=0
passman=0	passman=0	passman=0	passman=0
folderprotect=0	folderprotect=0	folderprotect=0	folderprotect=0
autoprotect=0	autoprotect=0	autoprotect=0	autoprotect=0

管理漫游网络

漫游网络的网络管理员必须授权用户并且管理用户和客户机对该网络的访问。这可能包括在 CSS 漫游网络上导入用户概要文件、同步用户数据或添加和删除用户及客户机既方便又快捷。这可能还包括复原漫游网络、更改管理员密钥对或更改存档位置。

授权用户

完成先前过程后，CSS 安全证书漫游网络配置完毕并且为漫游注册了漫游客户机。现在可以使用管理员实用程序来授权用户。

同步用户数据

每个用户的数据都存储在存档位置。在他所漫游的每台计算机本地也将存储一份该数据的副本。发生更改（例如获取证书或更改口令）时，本地数据也将得到更新。如果计算机连接到存档，则用户数据也将得到更新。当用户登录到另一台计算机时，更新将自动下载到该计算机（如果这台计算机也已连接到存档）。

然而与存档的连接无法得到完全保证，因此在计算机与存档之间用户数据有时可能不一致。如果在一台没有连接到存档的计算机上更改用户的数据，则更改不会反映在存档上，并且，由此也不会反映在其它计算机上。一旦将计算机连接到存档，更改就会更新到存档中并且在其它已连接计算机上的任何数据不一致也因此得到解决。然而，如果在包含更改的第一台计算机获取与存档的连接之前，在另一台连接到存档的计算机上进行了更改，则会发生不可更正的数据不一致问题。存档中的数据包含第一台计算机上未出现的更改，而该计算机包含存档中未出现的更改。如果出现这种情况，则将告知用户两种不同的配置并提示用户选择要保留的配置（本地配置还是存档的配置）。未选择的配置更改将丢失。因此，有一点很重要，即在任何其它计算机上进行更改之前确保对用户配置的任何更改都更新到存档。

恢复漫游环境中丢失的口令

当丢失或忘记了口令时，管理员可以在漫游服务器或任何注册的客户机中重新设置用户口令。除了启用安全 UVM 登录保护并导入了用户的系统以外，网络中的所有系统将更新此更改。在这些情况下，计算机中将不反映口令更新。要访问计算机，用户将需要密码重设文件并且需要完成密码重设过程。

导入用户概要文件

可以在漫游网络上使用管理员实用程序、管理员配置实用程序或 UVM GINA 将用户概要文件导入新的计算机。如果您希望在新计算机上导入不具有用户帐户的用户，则必须通过 Windows 控制面板创建 Windows 用户帐户。

注：要将用户导入漫游网络，用户必须在漫游网络中的另一台计算机上得到授权。

使用用户配置实用程序导入用户概要文件

要在漫游网络上使用用户配置实用程序将用户概要文件导入新的计算机，请以您希望导入的用户登录系统，单击开始 **>** 程序 **> Access IBM > IBM** 客户端安全软件 **>** 修改安全设置，然后在 “ 用户配置 ” 选项卡上单击从存档导入现有配置。

使用管理员实用程序导入用户概要文件

要在漫游网络上使用管理员实用程序将用户概要文件导入新的计算机，请选择该用户然后单击授权。当询问您是否要从存档导入该用户时，单击是。

使用 UVM GINA 导入用户概要文件

可以在漫游网络上使用 UVM GINA 将用户概要文件导入新的计算机。该过程从 UVM 登录屏幕开始。如果用户尚未获得在网络中给定系统上使用 UVM 的授权，则显示一个消息框，询问用户是否想要从存档导入。

注：

1. 如果希望在新计算机上导入不具有用户帐户的用户，则您必须在继续操作之前使用 Windows 控制面板创建 Windows 用户帐户。
2. 要在漫游服务器上访问存档，目录必须是映射网络驱动器。

要在漫游网络上使用运行 Windows 2000 的计算机上的 UVM GINA 将用户概要文件导入新的计算机，请完成以下过程：

1. 在登录时，输入您希望导入的用户的用户名和 UVM 口令。将显示消息询问您是否希望从存档导入用户概要文件。
2. 在提示时单击是导入用户，然后单击确定。
3. 如果存档位置在网络驱动器上，请在提示必须提供网络共享时单击是。
4. 在标准 Windows 登录屏幕输入 Windows 密码。显示存档路径的提示。
5. 输入存档网络路径。
6. 输入网络路径的用户名和密码。
7. 单击确定。如果操作正确完成，则将显示消息表明概要文件已成功导入。

要在漫游网络上使用运行 Windows XP 的计算机上的 UVM GINA 将用户概要文件导入新的计算机，请完成以下过程：

1. 在登录时，输入您希望导入的用户的用户名和 UVM 口令。将显示消息询问您是否希望从存档导入用户概要文件。
2. 在提示时单击是导入用户，然后单击确定。
3. 如果存档位置在网络驱动器上，请在提示必须提供网络共享时单击是。
4. 在出现标准 Windows 映射网络驱动器提示时，输入存档网络路径。
5. 单击完成。
6. 输入网络路径的用户名和密码，单击确定。如果操作正确完成，则将显示消息表明概要文件已成功导入。

注：要将用户导入漫游网络，用户必须在漫游网络中的另一台计算机上得到授权。

导入用户概要文件后，UVM 验证取决于该计算机的安全性策略。只有在满足该计算机的安全要求之后，用户才能登录。

在漫游网络中删除和恢复用户

要从漫游网络中删除用户，网络管理员必须完成以下管理员控制台过程：

1. 启动管理员控制台实用程序并输入管理员密码。
2. 单击配置安全证书漫游。

3. 选择从 **UVM** 和安全证书漫游网络删除用户，单击下一步。根据需要重复步骤。
4. 选择要删除的用户，单击删除。

   注：一旦用户从网络中删除，将永久丢失属于该用户的所有安全证书。

在网络管理员恢复删除的用户之前，这些用户不能被授权使用 UVM 和漫游网络。

要在漫游网络中恢复用户，网络管理员必须完成以下管理员控制台过程：

1. 启动控制台实用程序并输入管理员密码。
2. 单击配置安全证书漫游。
3. 选择恢复删除的用户，单击下一步。
4. 选择要恢复的用户，单击恢复。根据需要重复步骤。

   一旦用户得到恢复，可能重新授权他使用 UVM。恢复用户并不会自动授权他使用 UVM。

在漫游网络中删除和恢复注册的客户机

要从漫游网络中删除注册的客户机，网络管理员必须完成以下管理员控制台过程：

1. 启动控制台实用程序并输入管理员密码。
2. 单击配置安全证书漫游。
3. 选择从安全证书漫游网络删除注册的客户机并单击下一步。
4. 选择要删除的系统，单击删除。根据需要重复步骤。

   注：一旦客户机从网络中删除，将永久丢失属于该系统的所有基于机器的安全证书。

在网络管理员恢复删除的客户机之前，这些客户机不能向网络漫游服务器注册。

要将注册的客户机恢复到漫游网络，网络管理员必须完成以下管理员控制台过程：

1. 启动控制台实用程序并输入管理员密码。
2. 单击配置安全证书漫游。
3. 选择恢复删除的客户机并单击下一步。
4. 选择要恢复的客户机，单击恢复。根据需要重复步骤。

   一旦客户机得到恢复，它可以向漫游服务器重新注册。恢复客户机不会自动重新注册它。

注：删除客户机时在系统上出现安全证书的任何用户可能需要再次导入他们的安全证书。

在漫游网络中限定对注册客户机的访问

有时候，网络管理员可能希望让某些用户访问特定的注册客户机，而不允许其他用户进行访问。

要管理用户访问权，网络管理员必须完成以下管理员控制台过程：

1. 启动控制台实用程序并输入管理员密码。
2. 单击配置安全证书漫游。

3. 选择管理对注册客户机的用户访问并单击下一步。
4. 在选择 **CSS** 漫游网络中的系统框中选择要管理的注册客户机。将在两个列表框中列出具有访问权和没有访问权的用户。
5. 请执行以下操作之一：
   - 要限定用户的访问，请从具有访问权的用户列表中选择该用户并单击限制。根据需要重复步骤。
   - 要授权受限用户的访问，请从没有访问权的用户列表中选择该用户并单击允许。根据需要重复步骤。

漫游网络的访问管理功能需要在存档中创建新的文件夹。名为 Protected 的新文件夹对于网络管理员必须可写而对其它用户必须是只读的。如果用户对该文件夹具有写访问权，则他们可以手动恢复自己或他们的系统。

复原漫游网络

如果发生软件或硬件故障，则可能需要复原漫游网络。如果漫游服务器毁坏或者注册客户机中 CSS 使用的数据毁坏，请以与非漫游环境相同的方法使用管理员实用程序复原数据。如果注册客户机上的 IBM 嵌入式安全子系统发生故障或被清除，则必须向漫游服务器重新注册该客户机。不需要其它操作。

更改管理员密钥对

建议您不要在漫游网络中更改管理员密钥对。

要在漫游网络中更改管理员密钥对，必须完成以下步骤以使这些更改反映到网络中的所有计算机上。

1. 在漫游服务器上，使用管理员实用程序更改管理密钥对。
2. 重新注册网络中的所有客户机。
3. 对所有提示都保留现有文件。

更改存档文件夹

由于网络中的每台计算机访问的存档位置相同，所以在漫游网络中更改存档文件夹与在非漫游环境中更改文件夹稍有不同。

要在漫游网络上更改存档文件夹，请完成以下过程：

1. 采用以下过程将文件从旧的存档文件夹复制到新的存档文件夹中：
   a. 启动管理员实用程序并输入管理员密码。
   b. 单击密钥配置。
   c. 选择“更改存档位置”，然后单击下一步。
   d. 输入存档的新文件夹，然后单击下一步。
   e. 当提示将所有文件从旧的文件夹复制到新的文件夹时，单击是。
2. 采用以下过程更新网络上的所有其它计算机以使用新的存档文件夹：
   a. 启动管理员实用程序并且输入管理员密码。
   b. 单击密钥配置。
   c. 选择“更改存档位置”，然后单击下一步。
   d. 输入存档的新文件夹，然后单击下一步。

e. 当提示将所有文件从旧的文件夹复制到新的文件夹时，请单击否。

文件和文件夹加密（FFE）

文件和文件夹加密功能不受漫游环境的影响。然而受保护的文件夹是针对每台计算机分别进行管理的。因此如果一个文件夹受到系统 A 上用户 A 的保护，则系统 B 上具有相同名称的文件夹（如果有的话）不会受到保护，除非用户主动在系统 B 上保护该文件夹。

IBM 密码管理器

使用 IBM 密码管理器保护的所有密码在漫游网络中的所有计算机上都可用。

漫游术语和定义

在讨论有关设置漫游网络的概念和过程时以下术语将有助于理解：

漫游客户机注册
: 向漫游服务器注册计算机的过程。

漫游客户机
: 漫游网络中的所有可信 TCPA 计算机。

漫游服务器
: 用来启动漫游网络的 TCPA 计算机。

漫游客户机注册密码
: 用来向漫游服务器注册计算机的密码。

第 4 章 如何使用客户端安全软件

管理员可使用客户端安全软件提供的多个组件设置 IBM 客户机用户需要的安全功能。在您规划客户端安全策略和配置时，请使用下例作为参考。例如，Windows 2000 和 Windows XP 用户可以为系统登录设置 UVM 保护，从而禁止未授权用户登录到 IBM 客户机。

示例 1 — 使用 Outlook Express 的一台 Windows 2000 客户机和一台 Windows XP 客户机

在该示例中，一台 IBM 客户机（客户机 1）安装了 Windows 2000 和 Outlook Express，另一台客户机（客户机 2）安装了 Windows XP 和 Outlook Express。有三个用户需要在客户机 1 上进行 UVM 验证设置；一个客户机用户需要在客户机 2 上进行 UVM 验证设置。所有的客户机用户将注册他们的指纹以用于验证。在此示例期间将安装一个 UVM 感知指纹传感器。已经确定两台客户机都需要登录 Windows 的 UVM 保护。管理员决定将在每台客户机上编辑和使用 UVM 策略。

要设置客户端安全，请完成以下过程：

1. 在客户机 1 和客户机 2 上安装软件。有关详细信息，请参阅《*客户端安全软件安装指南*》。
2. 在每台客户机上安装 UVM 感知指纹传感器和任何相关联的软件。

   有关 UVM 感知产品的信息，请转至万维网的 http://www.pc.ibm.com/us/security/secdownload.html。
3. 对每个客户机使用 UVM 设置用户验证。请执行以下操作：
   a. 通过为用户分配 UVM 口令授权他们使用 UVM。因为客户机 1 有三个用户，所以您必须重复授权用户使用 UVM 的过程直到所有的用户都得到授权。
   b. 为每台客户机设置登录 Windows 的 UVM 保护。
   c. 注册用户指纹。因为将设置声明三个用户使用客户机 1 的策略，所以三个用户都必须在客户机 1 上注册他们的指纹。

      注：如果您将指纹作为客户机的 UVM 策略的一部分设置为验证要求，则每个用户都必须注册他或她的指纹。
4. 请需要对以下内容进行验证的每台客户机上编辑并保存本地 UVM 策略：
   - 登录 Windows
   - 获取数字证书
   - 为 Outlook Express 使用数字签名
5. 重新启动每台客户机来启用登录 Windows 的 UVM 登录保护。
6. 将您为用户设置的 UVM 口令以及在 UVM 策略中为 IBM 客户机设置的验证要求告知用户。

客户机用户现在能够执行以下任务：

- 使用 UVM 保护来锁定和解锁 Windows。

- 申请数字证书并选择嵌入式安全子系统作为与该证书关联的加密服务提供程序。
- 使用数字证书对 Outlook Express 创建的电子邮件消息进行加密。

Example 2 — 使用 Lotus Notes 的两台 Windows 2000 IBM 客户机

在此示例中，两台 IBM 客户机（客户机 1 和客户机 2）都安装了 Windows 2000 和 Lotus Notes。两个用户都需要在客户机 1 上进行 UVM 验证设置；一个用户需要在客户机 2 上进行验证设置；两台客户机都需要 Windows 登录的 UVM 登录保护。管理员决定在客户机 1 上编辑 UVM 策略并将它复制到客户机 2 上。

要设置客户端安全，请完成以下过程：

1. 在客户机 1 和客户机 2 上安装该软件。由于将使用相同的 UVM 策略文件，所以在客户机 1 和客户机 2 上安装软件时必须使用相同的管理员公钥。有关软件安装的详细信息，请阅读*《客户端安全软件安装指南》*。
2. 对每个客户机使用 UVM 设置用户验证。然后，执行以下任务：
   a. 通过给用户分配 UVM 口令向授权他们使用 UVM。因为客户机 1 有两个用户，所以您必须重复向 UVM 验证用户的过程直到所有用户得到授权。
   b. 在每台客户机上设置 Windows 登录的 UVM 登录保护。
3. 在两台客户机上都启用 UVM 保护的 Lotus Notes 支持。
4. 在客户机 1 上编辑并保存 UVM 策略，然后将它复制到客户机 2 上。UVM 策略需要通过用户验证来退出屏幕保护程序、登录到 Lotus Notes 和登录到 Windows。有关详细信息，请参阅第 38 页的『编辑和使用 UVM 策略』。
5. 重新启动每台客户机来启用登录 Windows 的 UVM 登录保护。
6. 通知客户机用户已为每个客户机所设置的 UVM 口令和策略。

示例 3 — 由 Tivoli Access Manager 管理并使用 Netscape 收发电子邮件的多台 Windows 2000 的 IBM 客户机

以下示例针对的读者是企业管理员，他计划使用 Tivoli Access Manager 管理 UVM 策略设置的验证对象。在此示例中，多台 IBM 客户机都安装了 Windows 2000 和 Netscape。所有客户机已安装 NetSEAT 客户机（一个 Tivoli Access Manager 组件）。使用 LDAP 服务器的所有客户机都已安装 LDAP 客户程序。 UVM 策略将允许 Tivoli Access Manager 控制客户机的选定验证对象。

在此示例中，一个用户在每台客户机都需要 UVM 进行验证设置。所有用户都将注册指纹以用于验证。该示例中将安装 UVM 感知指纹传感器，而且所有客户机都需要 Windows 登录的 UVM 登录保护。

要设置客户端安全，请完成以下过程：

1. 在 Tivoli Access Manager 服务器上安装客户端安全组件。要获取详细信息，请参阅*《结合客户端安全使用 Tivoli Access Manager》*。
2. 在所有客户机上安装客户端安全软件。因为要使用 UVM 策略，所以在所有客户机上安装软件时您必须使用相同的管理员公钥。有关软件安装的详细信息，请参阅*《客户端安全软件安装指南》*。
3. 在每台客户机上安装 UVM 感知指纹传感器和任何相关软件。有关可用的 UVM 感知产品的信息，请转至万维网的 http://www.pc.ibm.com/us/security/index.html。

4. 对每台客户机使用 UVM 设置用户验证。有关详细信息，请参阅第 27 页的『删除用户』。然后，执行以下任务：
   a. 通过为用户分配 UVM 口令向授权他们使用 UVM。
   b. 在每台客户机上设置登录 Windows 的 UVM 登录保护。
   c. 为每个客户机用户注册指纹。如果指纹验证在 IBM 客户机上是必需的，则该客户机所有的用户必须注册指纹。
5. 在每台客户机上配置 Tivoli Access Manager 安装信息。要获取详细信息，请参阅《*结合客户端安全使用 Tivoli Access Manager*》。
6. 编辑并保存其中一台客户机上的 UVM 策略，然后将它复制到其它客户机上。设置 UVM 策略，以便 Tivoli Access Manager 控制以下验证对象：
   - 登录 Windows
   - 获取数字证书
   - 为 Outlook Express 使用数字签名

   有关详细信息，请参阅第 38 页的『编辑和使用 UVM 策略』。
7. 重新启动每台客户机来启用登录 Windows 的 UVM 登录保护。
8. 将 IBM 嵌入式安全芯片 PKCS#11 模块安装到每台客户机上。此模块为使用 Netscape 收发电子邮件消息的客户机提供加密支持，并提供 IBM 嵌入式安全子系统来获取数字证书。有关更多信息，请参阅《*客户端安全软件安装指南*》。
9. 启用 Tivoli Access Manager 以控制出现在 Tivoli Access Manager 管理控制台中的 " IBM 客户端安全解决方案对象 "。
10. 客户机将您为用户设置的 UVM 口令和为每台客户机设置的策略告知用户。
11. 建议客户机用户阅读《*客户端安全软件用户指南*》以了解如何执行以下任务：
    - 使用 UVM 保护来锁定和解锁 Windows
    - 使用用户配置实用程序
    - 申请使用嵌入式安全子系统作为与数字证书关联的加密服务提供程序的数字证书
    - 使用数字证书加密 Netscape 创建的电子邮件消息

第 5 章 授权用户

授权 Windows 用户使用用户验证管理工具（UVM）时，以下信息将有所帮助。

客户机用户的验证

在客户机级别验证最终用户是计算机安全性的一个重要问题。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）（客户端安全软件的主要组件）的一部分。

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
- 在整个企业范围内使用 Tivoli Access Manager

当您添加第一个用户时，将生成硬件加密密钥。

验证元素

验证元素（如 UVM 口令或用户指纹）用于通过 IBM 客户机对用户进行授权。当您授权 Windows 用户使用 UVM 时，您为客户机用户指定 UVM 口令。UVM 口令（长度可达 256 个字符）是 UVM 使用的主要验证元素。当您指定 UVM 口令时，将为客户机用户创建用户加密密钥，这些密钥存储在由 IBM 嵌入式安全子系统管理的文件中。如果 IBM 客户机使用 UVM 感知设备验证，则验证元素（例如用户指纹或感应胸卡）也必须向 UVM 注册。

用户验证安装过程中，您可以选择客户端安全软件提供的以下功能：

- 操作系统登录的 **UVM** 保护。UVM 保护将确保只有 UVM 识别的那些用户才能访问计算机。在您启用操作系统登录的 UVM 保护之前，有关重要信息，请参阅『设置 UVM 登录保护』。
- 客户端安全屏幕保护程序。在添加了客户机用户之后，用户可以设置并使用客户端安全屏幕保护程序。客户端安全屏幕保护程序是通过 Windows 控制面板中的“显示”选项设置的。您必须启用系统登录的 UVM 保护以使用客户端安全屏幕保护程序。

授权用户前

要点：只授权可以用于登录到 Windows 的用户帐户。如果授权了*不能*用于登录到 Windows 的用户帐户，则在启用 UVM 登录保护时，所有用户都将被锁定在系统外。

要点：在安装过程中，必须至少授权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，则将不会应用安全设置并且信息将不受保护。

当您授权客户机用户时，管理员实用程序将为您提供可供选择的用户名列表。该列表中的名称是使用 Windows 添加的用户帐户。在您将客户机用户添加到 UVM 前，使用 Windows 为那些用户创建用户帐户和概要文件。客户端安全软件与 Windows 提供的安全功能一起工作。

使用 “ 用户和密码 ” 程序来创建新的用户帐户并管理用户帐户或组。有关更多信息，请参阅 Microsoft 文档。

注：

1. 使用 Windows 创建新用户时，每个新用户的域密码必须是相同的。
2. 不要对先前更改了 Windows 用户名的用户授权。UVM 将指向以前的用户名，而 Windows 将只识别新用户名。
3. 当从 Windows 中删除已授权的用户帐户时，UVM 登录保护界面继续不正确地列出可以用于登录到 Windows 的帐户。*不能*用该帐户登录到 Windows。
4. 用户授权后，不要更改其 Windows 用户名。如果您更改了用户名，则将不得不在 UVM 中重新授权新用户名并请求所有新的安全证书。

授权用户

用户必须以管理员权限登录才能使用管理员实用程序。

要使用 UVM 授权用户，请完成以下过程：

1. 从 IBM 客户机的 Windows 桌面，单击开始 **>** 设置 **>** 控制面板 **> IBM** 嵌入式安全子系统。

   显示 “ 输入管理员密码 ” 消息。
2. 输入管理员密码，然后单击确定。

   IBM 安全子系统的管理员实用程序主窗口打开。
3. 在 “ 选择要授权的 Windows 用户 ” 区域，从列表中选择一个用户名。

   注：列表中的用户名是由 Windows 中创建的用户帐户定义的。
4. 单击授权。

   显示 “ 用户验证设置 ” 屏幕。
5. 输入并确认新授权用户的用户验证管理工具初始口令，然后单击下一步。

   如果口令不符合安全策略要求，则屏幕显示输入的口令无效。如果发生这种情况，单击确定，然后单击查看口令要求以查看有效的口令必须满足的参数。

   一旦接受了口令，则显示消息表明操作成功完成。
6. 单击确定继续。

   显示 “ Windows 登录密码 ” 屏幕。如果启用了安全的 UVM 登录，则必须存储用户的当前 Windows 密码以使用户可以登录到系统。该屏幕使 “ 管理员 ” 能：

   - 让用户稍后使用用户配置实用程序存储其 **Windows** 密码。要让用户稍后使用用户配置实用程序存储其 Windows 密码，请选择相应的单选按钮，然后单击下一步。
   - 立即存储用户当前的 **Windows** 密码。要立即存储用户当前的 Windows 密码，请在提供的字段中输入和确认用户的密码，然后单击下一步。

     注：在此输入的密码必须与用户的当前 Windows 密码匹配。该设置不影响存储在 Windows 中的密码。

显示消息，表明操作成功完成。

7. 单击完成。

删除用户

用户必须以管理员权限登录才能使用管理员实用程序。

要使用 UVM 取消对用户的授权，请完成以下过程：

1. 从 IBM 客户机的 Windows 桌面，单击开始 **>** 设置 **>** 控制面板 **> IBM** 嵌入式安全子系统。

   显示“ 输入管理员密码 ”消息。

2. 输入管理员密码，然后单击确定。

   IBM 安全子系统的管理员实用程序主窗口打开。

3. 在“ 已授权使用 UVM 的 Windows 用户 ”区域中，从列表选择用户名。
4. 单击删除用户。

   显示一条消息警告将丢失所选用户的安全信息，包括用户所有现有的密钥、证书、注册指纹和存储的密码。

5. 单击是继续。

   显示消息询问您是否要删除用户的存档信息。如果您删除该信息，则用户就无法将先前保存的任何设置复原到任何系统上。

6. 单击是完成该操作。

创建新的用户

用户必须以管理员权限登录才能使用管理员实用程序。

要创建新的用户，请完成以下过程：

1. 从 IBM 客户机的 Windows 桌面，单击开始 **>** 设置 **>** 控制面板 **> IBM** 嵌入式安全子系统。

   显示“ 输入管理员密码 ”消息。

2. 输入管理员密码，然后单击确定。

   IBM 安全子系统的管理员实用程序主窗口打开。

3. 在“ 选择要授权的 Windows 用户 ”区域中，单击创建新的 **Windows** 用户。

   显示“ Windows 用户帐户 ”屏幕。

4. 单击创建新帐户。
5. 通过在提供的字段中输入名称来命名新帐户；然后单击下一步。
6. 通过选择相应的单选按钮，选取帐户类型。
7. 单击创建帐户。
8. 返回到 IBM 客户端安全子系统的管理员实用程序。

   在“ 选择要授权的 Windows 用户 ”区域中显示新的用户帐户。

第 6 章 使用 UVM 对用户授权后

对用户授权后，您可以利用其它的客户端安全功能，如下：

- 设置 **Windows** 的 **UVM** 登录保护。 有关更多信息，请参阅『设置 UVM 登录保护时的注意事项』。
- 存档用户加密密钥。有关更多信息，请参阅第 40 页的『更改密钥存档位置』。
- 设置客户端安全屏幕保护程序。有关更多信息，请参阅第 47 页的第 9 章，『客户机用户说明』。
- 使用 **UVM** 注册用户指纹。有关更多信息，请参阅第 30 页的『使用 UVM 注册用户指纹』。

  如果在向 UVM 添加用户前安装了 UVM 感知指纹传感器，则此时可进行指纹注册。

Windows 的 UVM 登录保护

UVM Windows 登录保护增强了与 Windows 一起提供的密码功能。UVM 登录界面替代了 Windows 登录，因此每次用户尝试登录系统时，将打开 UVM登录窗口。

设置 UVM 登录保护时的注意事项

设置和使用 Windows 登录的 UVM 保护前，请阅读以下信息：

- 如果 UVM 策略表明 Windows 登录需要指纹验证，而用户尚未注册指纹，则用户必须注册指纹后才能登录。

  同样，如果未使用 UVM 注册（或错误地注册了）用户 Windows 密码，则用户必须提供正确的 Windows 密码进行登录。
- 当启用 UVM 保护时，不要清除 IBM 嵌入式安全芯片。如果这样操作，您将完全地被锁定在系统之外。有关更多信息，请参阅第 53 页的第 10 章，『故障诊断』中的“管理员技巧”。
- 如果您管理员实用程序中清除了以 **UVM** 的安全登录替换标准 **Windows** 登录复选框，则系统将不使用 UVM 登录保护而返回到 Windows 登录进程。
- 如果您以 UVM 安全登录替换标准 Windows 登录并且启用 Cisco LEAP 功能，则您必须重新安装 Cisco Aironet Client 实用程序（ACU）。

设置 UVM 登录保护

要为 Windows 设置 UVM 登录保护，请完成以下过程：

1. 从 IBM 客户机的 Windows 桌面，单击开始 **>** 设置 **>** 控制面板 **> IBM** 嵌入式安全子系统。

   显示管理员实用程序主窗口。
2. 单击配置应用程序支持和策略。

   显示“UVM 应用程序和策略配置”屏幕。
3. 选择以 **UVM** 安全登录替换标准 **Windows** 登录复选框。

4. 单击确定。
5. 单击退出。
6. 关闭所有应用程序。
7. 重新启动计算机。

当计算机重新启动时，将提示您登录计算机。有关 UVM 保护的更多信息，请参阅第 29 页的『Windows 的 UVM 登录保护』。

恢复 UVM 口令

将为 IBM 客户机的安全策略授权的每个用户创建一个 UVM 口令。因为客户机用户可能丢失或忘记，或更改口令，所以管理员实用程序允许管理员恢复或更改丢失或忘记的口令。

要启动 UVM 口令恢复过程，请完成以下过程：

1. 从 IBM 客户机的 Windows 桌面，单击开始 **>** 设置 **>** 控制面板 **>** **IBM** 嵌入式安全子系统。

   显示管理员实用程序主窗口。
2. 在已授权使用 UVM 的 Windows 用户区域中选择一个用户。
3. 单击更改口令。

   显示 “ 更改口令 ” 屏幕。
4. 输入密钥存档的路径和目录名，或单击浏览找到该目录。
5. 在 “ 存档私钥文件 ” 字段中输入管理员私钥的路径和文件名，或单击浏览找到该文件。
6. 单击确定。

   如果管理员私钥被分割成多个文件，则显示消息要求您输入每个文件的位置和名称。当您在 “ 密钥文件 ” 字段中输入每个文件后，单击读取下一个。
7. 在 “ UVM 口令 ” 字段中，输入用户的 UVM 新口令并且在 “ 确认 UVM 口令 ” 字段中确认口令。单击查看口令要求查看 UVM 安全策略的强制规则列表。
8. 在 “ 口令到期 ” 区域中，选择并且设置可用的口令到期规则。
9. 单击下一步。将显示消息表明操作成功完成。
10. 单击完成。

使用 UVM 注册用户指纹

当 UVM 策略已被编辑以包含指纹验证时，每个用户必须使用 UVM 注册用户指纹。

要使用 UVM 注册用户指纹，请完成以下管理员实用程序过程：

1. 在 “ 已授权使用 UVM 的 Windows 用户 ” 区域中，从列表选择用户名。
2. 单击编辑用户。

   显示 “ 修改客户端安全用户配置 — 编辑 UVM 用户属性 ” 窗口。
3. 选中注册指纹和／或智能卡复选框，然后单击下一步。

   显示 “ 修改客户端安全用户配置 — 启用 UVM 的设备 ” 窗口。

4. 单击注册用户指纹。
5. 在“ 选择手 ”区域中，单击左或右。
6. 在“ 选择手指 ”区域中，单击选择您将识别获取指纹的手指，然后单击开始注册。
7. 将您的手指放在 UVM 感知指纹传感器上，并遵循屏幕上的指示信息操作。

   每个指纹可能需要识别四次，这取决于您的识别器型号。单击取消该手指取消指纹识别。
8. 指定另一个要注册的手指，或单击退出完成。

使用 **Lotus Notes** 的 **UVM** 登录保护

UVM 为 Lotus Notes 用户提供增强的安全保护。

启用和配置 **Lotus Notes** 用户标识的 **UVM** 登录保护

在可以启用 Lotus Notes 的 UVM 登录保护前，必须在 IBM 客户机上安装 Lotus Notes，必须为用户建立 Notes 用户标识和密码，并且必须授权 Lotus Notes 用户使用 UVM。

要设置 Lotus Notes 的 UVM 登录保护，请完成以下过程：

1. 从 IBM 客户机的 Windows 桌面，单击开始 **>** 设置 **>** 控制面板 **> IBM** 嵌入式安全子系统。

   显示管理员实用程序主窗口。
2. 单击配置应用程序支持和策略。

   显示“ UVM 应用程序和策略配置 ”屏幕。
3. 选择启用 **Lotus Notes** 支持复选框。

   现在已为 Lotus Notes 用户标识启用 UVM 保护。若有必要，请继续下列可选步骤配置 Lotus Notes 登录的策略。
4. 单击应用程序策略。

   显示“ 修改客户端安全策略配置 ”屏幕。
5. 请单击编辑策略。
6. 输入管理员密码，然后单击确定。显示“ IBM UVM 策略：Lotus Notes 登录 ”屏幕。
7. 在“ 对象选择 ”选项卡上，从“ 操作 ”下拉菜单中选择 **Lotus Notes** 登录。
8. 在“ 验证元素 ”选项卡上，为 Lotus Notes 登录选择所需的验证元素。
9. 单击应用保存选择。

   显示“ 必需的管理员私钥 ”屏幕。
10. 通过在所提供的字段中输入路径名，或单击浏览并选择相应的文件夹来指定私钥的位置。
11. 单击确定。

    “ IBM 用户验证管理工具：策略摘要 ”屏幕显示本地客户机策略控制的对象摘要。
12. 启动 Lotus Notes。

启动 Lotus Notes 时，完成 UVM 密码注册。

在 Lotus Notes 中使用 UVM 保护

在您能够使用 Lotus Notes 的 UVM 保护前，必须遵循『在 Lotus Notes 中设置 UVM 保护』中的步骤。

在 Lotus Notes 中设置 UVM 保护

要在 Lotus Notes 中设置 UVM 保护，请执行以下操作：

1. 登录到 Lotus Notes。

   显示“ IBM 用户验证管理工具 ”窗口。
2. 在可用的字段中输入并验证您的 Lotus Notes 密码。

   现在已向 UVM 注册您的 Lotus Notes 密码。

重新设置 Lotus Notes 密码

要重新设置 Lotus Notes 密码，请执行以下操作：

1. 登录到 Lotus Notes。
2. 从 Lotus Notes 菜单栏，单击文件 **>** 工具 **>** 用户安全。

   显示“ IBM 用户验证管理工具 ”窗口。
3. 输入 UVM 口令，然后单击确定。

   显示“ 用户安全 ”窗口。
4. 单击设置密码。

   显示“ IBM 用户验证管理工具 ”窗口。
5. 选择创建自己的密码单选按钮。
6. 在可用的字段中输入并验证新的 Lotus Notes 密码，然后单击确定。

注：在您将 Lotus Notes 中的密码更改为您以前使用的值时，Notes 将拒绝更改密码，但不会通知客户端安全软件。最终，UVM 将存储 Notes 拒绝的密码。

在 Lotus Notes 中更改密码时，如果您接收到消息表明该密码是以前使用过的，则您将需要退出 Lotus Notes，启动用户配置实用程序，然后将 Lotus Notes 密码复原为它先前的值。

如果 Lotus Notes 密码是随机生成的，在您收到此错误时，则您将无法得知原来的密码是什么，因此您无法手工重新设置密码。您必须从管理员那里请求新的标识文件或复原以前保存的标识文件的副本。

禁用 Lotus Notes 用户标识的 UVM 登录保护

如果您要禁用 Lotus Notes 用户标识的 UVM 登录保护，请执行以下操作：

1. 从 IBM 客户机的 Windows 桌面，单击开始 **>** 设置 **>** 控制面板 **> IBM** 嵌入式安全子系统。

   在输入管理员密码后，将显示管理员实用程序主窗口。
2. 单击配置应用程序支持和策略。

显示“ UVM 应用程序和策略配置 ”屏幕。

3. 取消选中启用 **Lotus Notes** 支持复选框。
4. 单击确定。

将显示“ 应用程序支持操作 ”屏幕，同时显示消息表明已禁用 Lotus Notes 支持。

设置切换的 Lotus Notes 用户标识的 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，请执行以下操作：

1. 退出 Lotus Notes。
2. 禁用当前用户标识的 UVM 保护。有关详细信息，请参阅第 32 页的『禁用 Lotus Notes 用户标识的 UVM 登录保护』。
3. 进入 Lotus Notes 并切换用户标识。有关切换用户标识的信息，请参阅 Lotus Notes 文档。
4. 要为您切换到的用户标识设置 UVM 保护，请进入 Lotus Notes 配置工具（由客户端安全软件提供）并设置 UVM 保护。请参阅第 32 页的『在 Lotus Notes 中使用 UVM 保护』。

使用 IBM 嵌入式安全芯片 PKCS#11 模块

由于客户端安全软件的使用通常与获取和使用带有支持 PKCS#11 的应用程序（例如 Netscape 应用程序或 RSA SecurID 软件令牌）的数字证书相关，所以该部分中提供的说明特定于客户端安全软件的使用。

有关如何使用 Netscape 应用程序的安全设置的详细信息，请参阅 Netscape 提供的文档。IBM 客户端安全软件仅支持 Netscape V4.7x。

注：要与客户端安全软件一起使用 128 位的浏览器，IBM 嵌入式安全芯片必须支持 256 位加密。通过单击芯片设置按钮，在管理员实用程序中可以找到客户端安全软件提供的加密长度。

安装 IBM 嵌入式安全芯片 PKCS#11 模块

在您能够使用数字证书前，您必须将 IBM 嵌入式安全芯片 PKCS#11 模块安装到计算机上。因为 IBM 嵌入式安全芯片 PKCS#11 模块的安装需要 UVM 口令，所以您必须至少将一个用户添加到计算机的安全策略中。

要使用 Netscape 安装 IBM 嵌入式安全芯片 PKCS#11 模块，请完成以下过程：

1. 打开 Netscape，然后单击文件 **>** 打开页面。
2. 找到 `ibmpkcsinstallt.html` 或 `ibmpkcsinstalls.html` 安装文件。

（如果您在安装软件时接受缺省目录，则文件位于 C:\Program Files\IBM\Security。）

3. 打开 Netscape 中的 `ibmpkcsinstallt.html` 或 `ibmpkcsinstalls.html` 安装文件。

显示消息，询问您是否确定要安装该安全性模块。

4. 单击确定。

UVM 口令窗口打开。

5. 输入 UVM 口令并单击确定。

显示消息，通知您模块安装完毕。

选择 IBM 嵌入式安全子系统生成数字证书

创建数字证书期间，将要求您选择要生成密钥的卡或数据库，请选择 **IBM** 嵌入式安全子系统增强的 **CSP**。

有关生成数字证书以及与 Netscape 一起使用的更多信息，请参阅 Netscape 提供的文档。

更新密钥存档

在您创建数字证书之后，请通过更新密钥存档备份证书。您可以使用用户配置实用程序更新密钥存档。

使用 PKCS#11 模块数字证书

请使用应用程序中的安全设置来查看、选择和使用数字证书。例如，在 Netscape Messenger 的安全设置中，您必须在选择数字证书后才能够使用它以数字方式签名或加密电子邮件消息。要获取更多的信息，请参阅由 Netscape 提供的文档。

在您安装 IBM 嵌入式安全芯片 PKCS#11 模块后，每次您使用数字证书时，UVM 将提示您满足验证要求。您可能必须输入 UVM 口令、识别您的指纹、或同时执行两个步骤来满足验证要求。在计算机的 UVM 策略中定义了验证要求。

如果您不能满足 UVM 策略设置的验证要求，则将显示错误消息。当您在该消息上单击确定时，将打开应用程序，但是直到重新启动应用程序并提供正确的 UVM 口令和／或指纹时，您才能使用 IBM 嵌入式安全芯片生成的数字证书。

第 7 章 处理 UVM 策略

注：尝试编辑本地客户机的 UVM 策略之前，请确保已经设置密钥。否则，当策略编辑器尝试打开本地策略文件时将显示错误消息。

在授权用户使用 UVM 后，您必须为每个 IBM 客户机编辑和保存安全策略。客户端安全软件提供的安全策略称为 UVM 策略，该策略结合了“授权用户”中提供的设置与客户机级别的验证要求。UVM 策略文件可以通过网络复制到客户机。

管理员实用程序具有可用于编辑和保存客户机 UVM 策略的内置 UVM 策略编辑器。在 IBM 客户机上执行的任务（如登录到 Windows 或解锁屏幕保护程序）称为验证对象，而且这些对象在 UVM 策略中具有指定给它们的验证要求。例如，您可将 UVM 策略设置为具备以下要求：

- 每个用户必须输入一个 UVM 口令并使用指纹验证以登录到 Windows。
- 每次获取数字证书时，每个用户必须输入 UVM 口令。

您也可使用 Tivoli Access Manager 控制特定验证对象，如 UVM 策略中所设置。

UVM 策略为 IBM 客户机，而不是个别用户设置验证对象的要求。因此，如果您将 UVM 策略设置为要求对象（例如 Windows 登录）的指纹验证，则授权为可使用 UVM 的每个用户都必须注册指纹以使用该对象。有关授权用户的详细信息，请参阅第 27 页的『删除用户』。

UVM 策略保存在名为 `globalpolicy.gvm` 的文件中。要通过网络使用 UVM，UVM 策略必须保存在一台 IBM 客户机上，然后复制到其它客户机上。将 UVM 策略文件复制到其它客户机可节省您在这些客户机上设置 UVM 策略的时间。

编辑 UVM 策略

编辑 UVM 策略，并仅在为其编辑策略的客户机上使用它。如果您在缺省位置安装了客户端安全，则 UVM 策略文件存储为 \Program Files\IBM\Security\UVM_Policy\globalpolicy.gvm。使用 UVM 策略编辑器编辑和保存 UVM 策略文件。管理员实用程序中提供 UVM 策略编辑器的界面。

验证的发生取决于您在策略编辑器中所作的选择。例如，如果您为 Lotus Notes 登录选择“第一次使用该方法后不要求口令”，则无论您何时登录到 Lotus Notes，它都会请求 UVM 验证。此后每次访问 Lotus Notes 时，都不需要口令，除非您重新引导或注销。

当您将 UVM 策略设置为对验证对象（例如 Windows 登录）要求指纹时，每个授权的 UVM 用户为了使用该对象必须注册他们的指纹。

编辑 UVM 策略时，您可用通过单击 **UVM** 策略摘要查看策略摘要信息。而且，您可单击应用保存您的更改。单击应用时，会显示一条消息提示您输入管理员私钥。输入管理员私钥，然后单击确定保存更改。如果您提供的管理员私钥不正确，则不会保存您的更改。

对象选择

UVM 策略对象使您能够为各种用户操作建立不同的安全策略。在管理员实用程序的“ IBM UVM 策略 ”屏幕的对象选择选项卡上指定有效的 UVM 对象。

有效 UVM 策略对象包含以下内容：

系统登录
: 该对象控制登录到系统所需的验证要求。

系统解锁
: 该对象控制退出客户端安全屏幕保护程序所需的验证要求。

Lotus Notes 登录
: 该对象控制登录到 Lotus Notes 所需的验证要求。

Lotus Notes 更改密码
: 该对象控制使用 UVM 生成随机 Lotus Notes 密码所需的验证要求。

数字签名（电子邮件）
: 该对象控制您在 Microsoft Outlook 或 Outlook Express 中单击“ 签名 ”按钮时所需的验证要求。

解密（电子邮件）
: 该对象控制您在 Microsoft Outlook 或 Outlook Express 中单击“ 解密 ”按钮时所需的验证要求。

文件和文件夹保护
: 该对象控制选择右击加密和解密时所需的验证要求。

密码管理器
: 当您使用 IBM 密码管理器（可从 IBM Web 站点获得）时，该对象控制必需的验证要求。激活它时，大多数用户应该保留“ 第一次使用该方法后不要求口令 ”上的设置。

Netscape — PKCS#11 登录
: 该对象控制在 PKCS#11 模块接收到 PKCS#11 C_OpenSession 调用时所必需的验证要求。大多数用户应该保留“ 第一次使用该方法后不需要口令 ”上的设置。

Entrust 登录
: 该对象控制当 Entrust 发出由 PKCS#11 模块接收的 PKCS#11 C_OpenSession 调用时所需的验证要求。大多数用户应该保留“ 第一次使用该方法后不需要口令 ”上的设置。

更改 **Entrust** 登录密码
: 该对象控制更改 Entrust 登录密码所需的验证要求。Entrust 通过发出由 PKCS#11 模块所接收的 PKCS#11 C_OpenSession 调用完成此操作。大多数用户应该保留“ 第一次使用该方法后不需要口令 ”上的设置。

验证元素

UVM 策略确定哪些可用的验证元素对于您启用的每个对象是必需的。这使您能为各种用户操作建立不同的安全策略。

可在管理员实用程序的“ IBM UVM 策略 ”屏幕的验证元素选项卡上选择验证元素，验证元素包含以下各项：

口令选择

此选择使管理员能建立 UVM 口令（口令用于以下列方式中的一种方式验证用户）：

- 每次需要的新口令。
- 第一次使用该方法后不需要口令。
- 如果在系统登录时给出，则不需要口令。

指纹选择

此选择使管理员能建立指纹识别（指纹识别用于以下列三种方式中的任意一种方式验证用户）：

- 每次需要的新指纹。
- 第一次使用该方法后不需要指纹。
- 如果在系统登录时给定，则不需要指纹。

全局指纹设置

此选择使管理员可确定在系统锁定用户前验证重试的最大数。此区域也能使管理员允许使用 UVM 口令覆盖指纹验证保护。

智能卡选择

该选择使管理员可请求提供智能卡作为附加的验证设备。

全局智能卡设置

该选择使管理员在提供 UVM 口令时，可把策略设置为允许覆盖。

使用 **UVM** 策略编辑器

要使用 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。

   显示 " UVM 应用程序和策略配置 " 屏幕。

2. 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。

3. 单击编辑策略按钮。

   显示 " 输入管理员密码 " 屏幕。

4. 输入管理员密码，然后单击确定。

   显示 " IBM UVM 策略 " 屏幕。

5. 在 " 对象选择 " 选项卡上，单击操作或对象类型，并选择您要指定验证要求的对象。

   操作包含系统登录、系统解锁和电子邮件解密；对象类型的示例为 " 获取数字证书 "。

6. 对于您选择的每个对象，执行以下操作之一：
   - 单击验证元素选项卡，并且编辑您要指定给对象的可用验证元素的设置。
   - 选择 **Access Manager** 控制所选对象启用 Tivoli Access Manager 来控制您选择的对象。仅当您要 Tivoli Access Manager 控制 IBM 客户机的验证元素时，才选择此选项。有关更多信息，请参阅《*结合客户端安全使用 Tivoli Access Manager*》。

要点：如果启用 Tivoli Access Manager 来控制对象，则您将控制授予 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。

- 选择拒绝对所选对象的所有访问以拒绝对所选对象的访问。

7. 单击确定保存更改并退出。

编辑和使用 UVM 策略

要跨越多个 IBM 客户机使用 UVM 策略，请编辑并保存 UVM 策略，然后将 UVM 策略文件复制到其它 IBM 客户机。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。

将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

如果您在缺省位置安装了客户端安全软件，则上述路径的根目录是 \Program Files。将这两个文件复制到客户机的 \IBM\Security\UVM_Policy\ 目录路径。

第 8 章 其它安全管理员功能

当您在 IBM 客户机上设置客户端安全软件时，您使用管理员实用程序启用 IBM 嵌入式安全芯片、设置安全芯片密码、生成硬件密钥并设置安全策略。本部分提供使用其它管理员实用程序功能的说明。

要打开管理员实用程序，请完成以下过程：

1. 从 IBM 客户机的 Windows 桌面，单击开始 **>** 设置 **>** 控制面板 **> IBM** 嵌入式安全子系统。

   因为对管理员实用程序的访问受管理员密码的保护，所以将显示消息要求您输入管理员密码。该密码长度必须正好为八个字符。
2. 输入管理员密码，然后单击确定。

使用管理员控制台

客户端安全软件管理员控制台使安全管理员能从他的系统中远程执行特定于管理员的任务。

管理员控制台应用程序（console.exe）必须安装在 `\program files\ibm\security` 目录中并从该目录运行。

管理员控制台使安全管理员能够执行以下功能：

- 忽略或覆盖验证元素。管理员能够执行的忽略或覆盖功能包含的以下内容：
  - 忽略 **UVM** 口令。该功能使管理员能够忽略 UVM 口令。当使用该功能时，将创建一个随机的临时口令，同时创建一个密码文件。管理员将密码文件发送给用户，通过一些其它方法交流密码。这样确保了新口令的安全性。
  - 显示／更改指纹识别器／智能卡覆盖密码。该功能使管理员能够覆盖安全策略，即使该策略设置为“ 不 ”允许覆盖指纹识别器或智能卡的口令。如果用户的指纹阅读器损坏或智能卡不可用，这可能是必要的。管理员可以把覆盖密码读给用户听或通过电子邮件发送给用户。
- 访问存档密钥信息。管理员能够访问的信息包含以下内容：
  - 存档目录。该字段使管理员能够从远程位置找到存档密钥信息。
  - 存档公钥位置。该字段使管理员能够找到管理员公钥。
  - 存档私钥位置。该字段使管理员能够找到管理员私钥。
- 其它远程管理员功能。管理员控制台使安全管理员能够远程执行以下功能：
  - 创建管理员配置文件。 该功能使管理员能生成管理员配置文件，当用户要使用客户机实用程序登记或复位自身时需要它。管理员通常将该文件通过电子邮件发送给用户。
  - 加密／解密设置配置文件。该功能允许对设置配置文件进行加密以进一步提高安全性。它也可以解密文件，使其可被编辑。
  - 配置安全证书漫游。该功能将该系统注册为 CSS 漫游服务器。一旦注册，网络中的所有 UVM 授权用户将能够访问他们在该系统中的个人数据（口令和证书等）。

更改密钥存档位置

首次创建密钥存档时，请创建所有加密密钥的副本并保存到安装时指定的位置。

注：客户机用户还可使用用户配置实用程序更改密钥存档位置。有关更多信息，请参阅第 47 页的第 9 章，『客户机用户说明』。

要更改密钥存档位置，请完成以下管理员实用程序过程：

1. 单击密钥配置按钮。

   显示“ 修改客户机密钥配置 — 配置密钥 ”屏幕。
2. 单击更改存档位置单选按钮，然后单击下一步。

   显示“ 修改客户机密钥配置 — 新密钥存档位置 ”屏幕。
3. 输入新的路径或单击浏览来选择路径。
4. 单击确定。

   将显示消息，表明操作完成。
5. 单击完成。

更改存档密钥对

当您将管理员密钥保存到存档位置时，复制的密钥称为存档密钥对。这些密钥通常存储在软盘或网络目录上。

注：在更改存档密钥对前，请务必更新存档。

要更改存档密钥对，请完成以下管理员实用程序过程：

1. 单击密钥配置按钮。

   显示“ 修改客户机密钥配置 — 配置密钥 ”屏幕。
2. 单击更改存档密钥单选按钮，然后单击下一步。

   显示“ 修改密钥配置 — 公钥屏幕 ”屏幕。
3. 在“ 新存档密钥 ”区域中的“ 存档公钥文件 ”字段中输入新的存档公钥的文件名。您还可单击浏览搜索新文件，或单击创建生成新的存档公钥。

   注：请确保您在不包含旧存档密钥文件的位置中创建新的公钥。
4. 在“ 新存档密钥 ”区域中的“ 存档私钥文件 ”字段中输入新的存档私钥的文件名。您还可单击浏览搜索新的文件，或单击创建生成新的存档密钥对。

   注：请确保您在不包含旧存档密钥文件的位置中创建新的密钥对。
5. 在“ 旧存档密钥 ”区域中的“ 存档公钥 ”字段中输入旧的存档公钥的文件名，或单击浏览搜索文件。
6. 在“ 旧存档密钥 ”区域中的“ 存档私钥 ”字段中输入旧的存档私钥的文件名，或单击浏览搜索文件。
7. 在“ 存档位置 ”区域中，输入存储密钥存档的文件路径或单击浏览选择路径。
8. 单击下一步。

注：如果存档密钥对分割为多个文件，则将显示消息要求您输入每个文件的位置和名称。在字段中输入每个文件名后，单击读取下一个。

将显示消息，表明操作成功完成。

9. 单击确定。

将显示消息，表明操作完成。

10. 单击完成。

从存档复原密钥

如果更换系统板或硬盘驱动器故障危及用户密钥的完整性，则您将需要复原密钥。当您复原密钥时，是从密钥存档复制最近的用户密钥文件并将它们存储在 IBM 嵌入式安全系统上。复原密钥将覆盖当前存储在安全芯片上的任何密钥。

如果您使用包含 IBM 嵌入式安全子系统的新系统板更换您计算机中原有的系统板，并且加密密钥在您的硬盘驱动器中仍然有效，则可以通过使用新系统板上的 IBM 嵌入式安全子系统“ 重新加密 ”先前与计算机关联的加密密钥来复原这些密钥。在启用新芯片并设置管理员密码后，执行密钥复原。

有关启用新的安全子系统和设置管理员密码的详细信息，请参阅第 45 页的『启用 IBM 嵌入式安全子系统和设置管理员密码』。

注：密钥复原后，将自动启用 UVM 登录。因此，如果正在复原的系统上的 UVM 登录需要指纹验证，则您*必须*在复原之后、重新引导*之前*安装指纹软件，以防被锁定在系统之外。

下列说明假设硬盘驱动器故障未损坏管理员实用程序。如果硬盘驱动器故障损坏客户端安全文件，您可能需要重新安装客户端安全软件。

密钥复原要求

仅当满足以下条件时才能成功完成密钥复原操作。

- 复原的系统的计算机名必须与原有的系统计算机名相符。
- 复原的系统必须有可以访问原系统的 CSS 管理员密钥对和存档位置。
- 复原的系统必须具有已清除并已启用的 IBM 安全子系统。（使用 BIOS 启用和清除芯片。）
- 复原的系统必须与原系统具有相同的 IBM 安全子系统级别（即 TCPA 或非 TCPA）。

复原方案

以下是三种可用的 IBM 客户端安全复原方案：

- 更换系统板。如果需要更换原系统板或者如果要将硬盘驱动器移到新系统中，则需要使用与原系统的密钥存档一致的密钥重新建立 IBM 安全子系统。
- 更换整个系统。如果原系统丢失或被盗，则需要从存储在存档位置的信息重新建立 IBM 安全子系统和 IBM 客户端安全软件。
- 更换硬盘驱动器。如果在原系统上的硬盘驱动器发生故障并且新的硬盘驱动器已经安装到原系统上，则必须从存档位置复原 IBM 客户端安全软件。

更换系统板

要更换包含启用 IBM 嵌入式安全子系统的计算机的系统板，请完成以下过程：

1. 单击 Windows 控制面板中的 **IBM** 客户端安全子系统图标。
2. 输入并确认管理员密码；然后单击确定。
3. 在相应字段中，输入原系统的存档位置和管理员密钥位置；然后单击确定。
4. 单击确定。
5. 单击退出关闭管理员实用程序。

计算机现已完全复原。在继续之前，请重新引导计算机。

更换整个系统

在新系统上安装 IBM 客户端安全软件后，CSS 安装向导将在系统重新启动时自动运行。要开始更换整个系统并重新建立存储在存档位置中的信息，请完成以下过程：

1. 单击 CSS 安装向导的开始页面中的下一步。
2. 输入并确认新系统的管理员密码并单击下一步。
3. 选中使用现有的安全密钥单选按钮，并在相应字段中输入原系统的已存档管理员公钥和管理员私钥的位置。
4. 在 “ 备份安全信息 ” 区域中，输入临时的存档位置。

   注：

   a. 当系统在以后的步骤中从原系统存档完全复原后，删除该位置。

   b. 在复原原系统存档的过程中会覆盖信息的其余部分；因此，请使用缺省值。
5. 单击下一步。
6. 单击 “ 使用 IBM 客户端安全保护应用程序 ” 页面上的下一步。
7. 单击 “ 授权用户 ” 页面上的下一步。
8. 单击 “ 选择系统安全级别 ” 页面上的下一步。
9. 单击 “ 检查安全设置 ” 页面上的完成。
10. 单击确定。
11. 继续完成『更换硬盘驱动器』过程。

更换硬盘驱动器

要在更换硬盘驱动器后从存档位置复原 IBM 客户端安全软件，请完成以下过程：

1. 单击 Windows 控制面板中的 **IBM** 客户端安全子系统图标。
2. 输入在 CSS 安全向导中建立的管理员密码并单击确定。
3. 单击密钥配置。
4. 选中从存档复原 **IBM** 安全子系统密钥单选按钮并单击下一步。
5. 在相应字段中，输入原系统的存档位置和管理员密钥位置并单击下一步。
6. 单击确定。
7. 单击完成返回主配置页面。
8. 单击退出关闭管理员实用程序。

计算机现已完全复原。在继续之前，请重新引导计算机。

复位验证失败计数器

要复位用户的验证失败计数器，请完成以下管理员实用程序过程：

1. 在“ 已授权使用 UVM 的 Windows 用户 ”区域中，选择用户。
2. 单击复位失败计数。

   显示“ 复位用户的失败计数 ”屏幕。
3. 输入选定用户的 UVM 口令，然后单击确定。

   显示消息，通知您操作成功。
4. 单击确定。

更改 **Tivoli Access Manager** 设置信息

以下信息适合于安全管理员，他规划使用 Tivoli Access Manager 管理 UVM 安全策略的验证对象。有关更多信息，请参阅*《结合客户端安全使用 Tivoli Access Manager》*。

在客户机上配置 **Tivoli Access Manager** 安装信息

Tivoli Access Manager 安装到本地客户机之后，您可以使用管理员实用程序配置 Access Manager 安装信息。客户端安全软件使用配置文件在 IBM 客户机上配置 Tivoli Access Manager 安装信息。该配置文件用于链接 Tivoli Access Manager 和 UVM 策略放弃其控制的对象。

要在客户机上配置 Tivoli Access Manager 安装信息，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。

   显示“ UVM 应用程序和策略配置 ”屏幕。
2. 选择以 **UVM** 的安全登录替换标准 **Windows** 登录复选框。
3. 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. 在“ Tivoli Access Manager 安装信息 ”区域中，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，该区域才可用。您还可单击浏览搜索配置文件。
5. 单击编辑策略按钮并输入管理员密码。
6. 从“ 操作 ”下拉菜单中选择您要 Tivoli Access Manager 控制的操作。
7. 选择 **Access Manager** 控制所选对象复选框，该框中将显示勾选标记。
8. 单击应用按钮。在下次高速缓存刷新时发生更改。如果希望更改立即生效，请单击“ 修改客户端安全策略配置 ”屏幕上的刷新本地高速缓存按钮。

刷新本地高速缓存

将在 IBM 客户机上保留由 Tivoli Access Manager 管理的安全策略信息的本地副本。您可以设置本地高速缓存的刷新速率（以月和天为增量）或单击按钮立即更新本地高速缓存。

要设置或刷新本地高速缓存，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。

   显示“ UVM 应用程序和策略配置 ”屏幕。

2. 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。
3. 在 “ 本地高速缓存刷新间隔 ” 区域中，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。
   - 要设置刷新速率，请在提供的字段中输入月数和天数。月数和天数值表示已安排的刷新之间的时间数量。

更改管理员密码

您必须为客户机设置管理员密码以启用 IBM 嵌入式安全子系统。设置管理员密码之后，对管理员实用程序的访问受此密码的保护。为了提高安全性，您应该定期更改管理员密码。长期保持不变的密码可能更容易受到外部用户的攻击。请保护管理员密码以防止未授权的用户更改管理员实用程序中的设置。有关管理员密码规则的信息，请参阅第 71 页的附录 B, 『密码和口令信息』。

要更改管理员密码，请完成以下管理员实用程序步骤：

1. 单击芯片设置按钮。

   显示 “ 修改 IBM 安全芯片设置 ” 屏幕。
2. 单击更改芯片密码。

   显示 “ 更改 IBM 安全芯片密码 ” 屏幕。
3. 在 “ 新密码 ” 字段中，输入新密码。
4. 在 “ 确认 ” 字段中，再次输入该密码。
5. 单击确定。

   显示消息，通知您操作成功。

   注意：不要按 Enter 键或 Tab 键 > Enter 键保存更改。如果您这样做，则将显示 “ 禁用芯片 ” 屏幕。如果 “ 禁用芯片 ” 窗口打开，请不要禁用芯片；退出该屏幕。
6. 单击确定。

查看有关客户端安全软件的信息

通过单击管理员实用程序的芯片设置按钮，您可以获取关于 IBM 嵌入式安全子系统和客户端安全软件的以下信息：

- 与客户端安全软件一起使用的固件的版本号
- 嵌入式安全芯片的加密状态
- 硬件加密密钥的有效性
- IBM 嵌入式安全芯片的状态

禁用 IBM 嵌入式安全子系统

管理员实用程序提供了禁用 IBM 嵌入式安全子系统的方法。因为启动管理员实用程序和禁用安全子系统都需要管理员密码，所以请保护管理员密码，以防止未授权用户禁用子系统。

要点：在启用 UVM 保护时，请勿清除 IBM 嵌入式安全子系统。如果您这样做，将被完全锁定在系统之外。要清除 UVM 保护，请打开管理员实用程序并清除以 **UVM** 安全登录替换标准 **Windows** 登录复选框。在禁用系统登录的 UVM 保护之前，您必须重新启动计算机。

要禁用嵌入式安全子系统，请完成以下管理员实用程序过程：

1. 单击芯片设置按钮。
2. 单击禁用芯片按钮，然后遵循屏幕上的指示信息操作。
3. 如果您的计算机启用了增强的安全，您可能必须输入 Configuration/Setup Utility 中设置的 BIOS 管理员密码以禁用芯片。

要在禁用子系统后使用 IBM 嵌入式安全子系统及其加密密钥，必须重新启用安全子系统。

启用 **IBM** 嵌入式安全子系统和设置管理员密码

如果在安装 IBM 嵌入式子系统后需要启用该软件，则可以使用管理员实用程序重新设置管理员密码并设置新的加密密钥。

在更换系统板之后或是已禁用 IBM 嵌入式安全子系统时，您可能需要启用该子系统来复原密钥存档。

要启用安全子系统并设置管理员密码，请完成下列过程：

1. 从 IBM 客户机的 Windows 桌面，单击开始 **>** 设置 **>** 控制面板 **> IBM** 嵌入式安全子系统。

   显示消息，要求您为 IBM 客户机启用 IBM 嵌入式安全子系统。
2. 单击是。

   显示一条消息要求您重新启动计算机。在启用 IBM 嵌入式安全子系统之前，您必须重新启动计算机。如果计算机已启用增强的安全，则您可能需要输入 Configuration/Setup Utility 中设置的 BIOS 管理员密码或超级用户密码来启用芯片。
3. 单击确定重新启动计算机。
4. 从 Windows 桌面，单击开始 **>** 设置 **>** 控制面板 **> IBM** 嵌入式安全子系统。

   因为对管理员实用程序的访问受管理员密码的保护，所以将显示消息要求您输入管理员密码。
5. 在 “ 新密码 ” 字段中输入新的管理员密码，然后在 “ 确认 ” 字段中再次输入它。
6. 单击确定。

启用 **Entrust** 支持

IBM 嵌入式安全芯片使用客户端安全软件以增强 Entrust 安全功能。使用客户端安全软件在计算机上启用 Entrust 支持将把 Entrust 软件安全功能传送到 IBM 安全芯片。

客户端安全软件将自动查找 entrust.ini 文件以启用 Entrust 支持；然而，如果 entrust.ini 文件不在通常的路径中，则将为用户打开对话框找到 entrust.ini 文件。用户找到并选择文件后，客户端安全即可启用 Entrust 支持。单击启用 **Entrust** 支持复选框后，在 Entrust 可以使用 IBM 嵌入式安全芯片之前，需要进行重新引导。

要启用 Entrust 支持，请完成以下过程：

1. 从 IBM 客户机的 Windows 桌面，单击开始 **>** 设置 **>** 控制面板 **> IBM** 嵌入式安全子系统。

   显示管理员实用程序主窗口。
2. 单击配置应用程序支持和策略。

   显示“ UVM 应用程序和策略配置 ”屏幕。
3. 选择启用 **Entrust** 支持复选框。
4. 单击应用。

   将显示“ IBM 客户端安全 Entrust 支持 ”屏幕，并显示表明 Entrust 支持已启用的消息。

注：您必须重新启动计算机，使更改生效。

第 9 章 客户机用户说明

本部分提供信息帮助客户机用户执行以下任务:

- 为系统登录使用 UVM 保护
- 使用用户配置实用程序
- 使用安全的电子邮件和 Web 浏览
- 配置 UVM 声音首选项

为系统登录使用 UVM 保护

本部分包含关于为系统登录使用 UVM 登录保护的信息。在您可以使用 UVM 保护之前，必须在计算机上启用它。

UVM 保护使您能够通过登录界面控制对操作系统的访问。UVM 登录保护替换 Windows 登录应用程序，因此，当用户对计算机解锁时，将打开 UVM 登录窗口而不是 Windows 登录窗口。在计算机上启用 UVM 保护之后，在您启动计算机时，将打开 UVM 登录界面。

计算机运行时，您可以通过按 **Ctrl + Alt + Delete** 访问 UVM 登录界面以关闭或锁定计算机、打开 " 任务管理器 " 或注销当前用户。

解锁客户机

要解锁使用 UVM 保护的 Windows 客户机，请完成以下过程：

1. 按 **Ctrl + Alt + Delete** 以访问 UVM 登录界面。
2. 输入您的用户名以及您要登录的域，然后单击解锁。

   UVM 口令窗口打开。

   注：尽管 UVM 识别多个域，但您的用户密码必须在所有域中保持一致。
3. 输入 UVM 口令，然后单击确定访问操作系统。

注：

1. 如果 UVM 口令与输入的用户名和域不匹配，UVM 登录窗口会再次打开。
2. 根据客户机的 UVM 策略验证要求，可能还需要进行进一步的验证过程。

用户配置实用程序

用户配置实用程序使客户机用户能执行各种不需要管理员访问权的安全维护任务。

用户配置实用程序功能

用户配置实用程序使客户机用户能够执行以下操作：

- 更新密码和存档。该选项卡使您能够执行以下功能：
  - 更改 **UVM** 口令。要提高安全性，您可以定期更改 UVM 口令。

- 更新 **Windows** 密码。当您使用 " Windows 用户管理器 " 程序更改 UVM 授权的客户机用户的 Windows 密码时，还必须使用 IBM 客户端安全软件用户配置实用程序更改密码。如果管理员使用管理员实用程序更改用户的 Windows 登录密码，将删除所有先前为该用户创建的用户加密密钥，同时与之相关的数字证书也将无效。
- 重新设置 **Lotus Notes** 密码。要提高安全性，Lotus Notes 用户可以更改他们的 Lotus Notes 密码。
- 更新密钥存档。如果您创建了数字证书并要为存储在 IBM 嵌入式安全芯片上的私钥制作副本，或如果要将密钥存档移动到另一个位置，请更新密钥存档。

- 配置 **UVM** 声音首选项。用户配置实用程序使您能选择在验证成功和失败时播放的声音文件。
- 用户配置。该选项卡使您能够执行以下功能：
-

  - 重新设置用户。此功能使您能重新设置您的安全配置。当重新设置安全配置时，所有先前的密钥、证书、指纹等都将被擦除。
  - 从存档复原用户安全配置。此功能使您能从存档复原设置。如果文件已损坏或要恢复到先前的一个配置，这是个有效的方法。
  - 向 **CSS** 漫游服务器注册。该功能使您能够向 CSS 漫游服务器注册此系统。一旦注册了该系统，您就能够将当前配置导入系统。

用户配置实用程序 **Windows XP** 限制

Windows XP 强制规定了一些访问限制，以限定某些功能只对特定环境下的客户机用户可用。

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

在以上情形中，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

管理员启动并退出管理员实用程序后，将清除这些限制。

Windows XP Home

Windows XP Home 的受限用户在以下任何一种情形中都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

使用用户配置实用程序

要使用用户配置实用程序，请完成以下过程：

1. 单击开始 **>** 程序 **> Access IBM > IBM** 客户端安全软件 **>** 修改安全设置。

   显示 IBM 客户端安全软件用户配置实用程序主屏幕。
2. 选择以下选项卡之一：
   - 更新密码和存档。此选项卡使您能更改 UVM 口令、更新 UVM 中的 Windows 密码、重新设置 UVM 中的 Lotus Notes 密码并更新您的加密存档。
   - 配置 **UVM** 声音。此选项卡使您能选择在验证成功和失败时播放的声音文件。
   - 用户配置。此选项卡使用户能够从存档中复原其用户配置、重新设置其安全配置或向漫游服务器注册（如果该计算机可以用作漫游客户机）。
3. 单击确定退出。

使用安全的电子邮件和 **Web** 浏览

如果您通过因特网发送了未受保护的事务，它们有可能被拦截和读取。您可以通过获取数字证书并使用它来进行数字签名和加密电子邮件消息或保护您的 Web 浏览器，来防止对您的因特网事务的未授权访问。

数字证书（又称为数字标识或安全证书）是一个由认证中心发出和数字签名的电子安全证书。当向您发出一个数字证书时，认证中心确认您的身份为证书所有者。认证中心是一个可信数字证书的供应商，并可以是第三方签发者（如 VeriSign），或者认证中心也可以设置为公司内部的服务器。数字证书包含您的身份（如您的名字和电子邮件地址）、证书的到期日期、您的公钥副本以及认证中心的身份及其数字签名。

结合 **Microsoft** 应用程序使用客户端安全软件

本部分中提供的说明专指客户端安全软件的使用，而客户端安全软件通常与使用支持 Microsoft CryptoAPI 的应用程序（如 Outlook Express）获取和使用数字证书有关。

有关如何创建安全设置和使用电子邮件应用程序（例如，Outlook Express 和 Outlook）的详细信息，请参阅那些应用程序提供的文档。

获取 **Microsoft** 应用程序的数字证书

当您使用认证中心创建一个与 Microsoft 应用程序一起使用的数字证书时，将提示您为证书选择一个加密服务提供程序（CSP）。

要为您的 Microsoft 应用程序使用 IBM 嵌入式安全芯片的加密功能，请确保在您获取数字证书时选择 **IBM** 嵌入式安全子系统 **CSP** 作为加密服务提供程序。这将确保数字证书的私钥存储在 IBM 安全芯片上。

同样，如果可用，请选择强（或高）加密以获取额外的安全性。由于 IBM 嵌入式安全芯片有能力将数字证书的私钥加密提高到 1024 位，如果在认证中心界面中提供该选项，请选择它；1024 位加密又称为强加密。

选择 **IBM** 嵌入式安全子系统 **CSP** 作为 CSP 之后，您或许要输入 UVM 口令和／或识别指纹以满足获取数字证书的验证要求。计算机的 UVM 策略中定义了验证要求。

转移来自 **Microsoft CSP** 的证书

IBM CSS 证书转移向导使您能够将使用缺省 Microsoft CSP 创建的证书转移到 IBM 嵌入式安全系统 CSP。转移证书极大地增加了为与证书相关联的私钥提供的保护，因为它们将安全地存储在 IBM 嵌入式安全子系统上，而不是在易受攻击的软件上。

可以转移两种类型的安全证书：

- 用户证书：用户证书的目的是对给定的用户进行授权。从认证中心（CA）（例如 cssdesk）获取用户证书是常见的做法。认证中心是存储、颁发和发布证书的可信机构。您可能需要用户证书对电子邮件、加密的电子邮件进行签名或登录到特定服务器。
- 机器证书：机器证书的目的是用来唯一地标识特定计算机。使用机器证书时，验证是基于使用的计算机而不是其使用者。

CSS 证书转移向导应用程序只转移标记为 " 可导出 " 的 Microsoft 证书，并且仅限于密钥大小不超过 1024 位的证书。

如果用户需要转移机器证书但是没有系统的管理员权限，则管理员可以发送管理员配置文件，这样使用户能够转移证书而不需要提供管理员密码。使用位于 `c:\\program files\ibm\security` 文件夹中的管理员控制台实用程序来创建管理员配置文件。

要使用 CSS 证书转移向导，请完成以下过程：

1. 单击开始 **> Access IBM > IBM** 客户端安全软件 **> CSS** 证书转移向导。

   显示 " IBM CSS 证书转移向导 " 欢迎屏幕。
2. 单击下一步开始。
3. 选择要转移的证书类型并单击下一步。 CSS 证书转移向导只能转移 Microsoft 证书库中标记为 " 可导出 " 的证书。
4. 通过单击界面的 " 颁发到 " 区域中显示的证书名选择要转移的证书，然后单击下一步。显示消息表明证书转移成功。

   注：转移机器证书将需要管理员密码或管理员配置文件。
5. 单击确定返回到 CSS 证书转移向导。

证书在转移后将与 IBM 嵌入式安全子系统 CSP 相关联，并且私钥受 IBM 嵌入式安全子系统的保护。任何使用这些私钥的操作（例如，创建数字签名或解密电子邮件）将在 IBM 嵌入式安全子系统保护的环境内完成。

更新 **Microsoft** 应用程序的密钥存档

在您创建数字证书之后，通过更新密钥存档来备份证书。可以使用管理员实用程序来更新密钥存档。

使用 **Microsoft** 应用程序的数字证书

使用 Microsoft 应用程序中的安全设置查看和使用数字证书。要获取更多的信息，请参阅 Microsoft 提供的文档。

在您创建数字证书并使用它签名电子邮件消息后，UVM 将在您第一次对电子邮件消息进行数字签名时提示输入验证要求。您可能需要输入 UVM 口令和／或识别指纹以满足使用数字证书的验证要求。计算机的 UVM 策略中定义了验证要求。

配置 **UVM** 声音首选项

用户配置实用程序使您能使用提供的界面来配置声音首选项。要更改缺省声音首选项，请完成以下过程：

1. 单击开始 **>** 程序 **> Access IBM > IBM** 客户端安全软件 **>** 修改安全设置。

   显示 IBM 客户端安全软件用户配置实用程序屏幕。
2. 选择配置 **UVM** 声音选项卡。
3. 在“ UVM 验证声音 ”区域的“ 验证成功 ”字段中输入想要与成功验证关联的声音文件的文件路径，或单击浏览选择文件。
4. 在“ UVM 验证声音 ”区域的“ 验证失败 ”字段中输入与失败验证关联的声音文件的文件路径，或单击浏览选择文件。
5. 单击确定完成过程。

第 10 章 故障诊断

以下部分的信息有助于防止、识别和更正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有所帮助的信息。

IBM 客户端安全软件只能在具有 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，它们使 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

必须首先在客户机上安装 IBM 客户端安全软件，并且必须授权用户使用该软件才能保护客户机用户信息。一个易于使用的安装向导将指导您逐步完成整个安装过程。

要点：在安装过程中，必须至少授权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，则不会应用您的安全设置并且您的信息将不受保护。

如果完成了安装向导而没有授权任何用户，请关闭和重新启动计算机；然后从 Windows 开始菜单运行客户端安全安装向导并授权一个 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敏感信息。

删除用户

当您删除用户时，将从管理员实用程序中的用户列表中删除用户名。

设置 BIOS 管理员密码（ThinkCentre）

在 Configuration/Setup Utility 中提供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防止未授权用户更改这些设置。

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. 输入您的密码并按您键盘上的向下箭头。
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 BIOS 管理员密码后，每次您试图访问 Configuration/Setup Utility 时都会出现提示。

要点：请妥善保存您的 BIOS 管理员密码的记录。如果您丢失或遗忘了 BIOS 管理员密码，则无法访问 Configuration/Setup Utility，且您在不卸下计算机外盖和移动系统板上的跳线的情况下无法更改或删除 BIOS 管理员密码。请参阅随计算机附带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 提供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防止未授权的用户对这些设置进行更改。

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. 当屏幕上出现 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 区域打开。

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，每次尝试访问 BIOS Setup Utility 时会出现提示。

要点：请妥善保存超级用户密码。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。请参阅随计算机附带的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。保护管理员密码以防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 嵌入式安全子系统中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. 当屏幕上出现 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 嵌入式安全子系统中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. 在重新启动计算机时按住 Fn 键。
3. 当屏幕上出现 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。

有关 CSS V5.2 的已知问题或限制

以下信息在使用客户端安全软件 V5.2 时可能会有所帮助。

漫游限制

使用 CSS 漫游服务器

在任何人试图登录到 CSS 漫游服务器时将显示 CSS 管理员密码提示。然而，不输入该密码也能正常使用计算机。

在漫游环境中使用 IBM 安全密码管理器

存储在使用 IBM 客户端安全密码管理器的一个系统上的密码可以在漫游环境中的其它系统上使用。当用户登录到漫游网络的其它系统中时将自动从存档中检索新的条目（如果该存档可用）。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之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。当漫游用户生成新的 Internet Explorer 证书时，该用户必须至少等待 20 秒才能在另一个系统导入、复原或更改其 CSS 配置。在这 20 秒刷新时间间隔之前尝试这些操作中的任何操作都将导致证书丢失。同样，如果在生成证书时用户没有连接到存档中，则在连接到存档之后用户应等待 20 秒以确保证书在存档中得到更新。

Lotus Notes 密码和安全证书漫游

如果启用了 Lotus Notes 支持，用户的 Lotus Notes 密码将用 UVM 存储。用户将不必输入他们的 Notes 密码以登录 Lotus Notes。将要求他们提供 UVM 口令、指纹和智能卡等（取决于安全策略设置）以访问 Lotus Notes。

如果用户从 Lotus Notes 中更改其 Notes 密码，则将使用新密码更新 Lotus Notes 标识文件并更新新 Notes 密码的 UVM 副本。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。如果带有更新密码的 Notes 标识文件在其它系统上不可用，则 Notes 密码的 UVM 副本就可能与漫游网络的其它系统上标识文件的 Notes 密码不匹配。如果这样，则用户无法访问 Lotus Notes。

如果用户带有更新密码的 Notes 标识文件在另一个系统上也不可用，则应该将该更新的 Notes 标识文件复制到漫游网络的其它系统上以便该标识文件中的密码与 UVM 存储的副本匹配。或者，用户可以从“开始”菜单运行“修改安全设置”并将 Notes 密码更改回原来的值。然后 Notes 密码就能通过 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中时，一旦用户有权访问该存档，则将从该存档中下载最新的用户安全证书集。最初登录时，用户无法访问网络共享资源，因此只有在系统登录完成后才可以下载最新的安全证书。例如，如果更改了漫游网络中另一个系统上的 UVM 口令或在另一个系统上注册了新的指纹，则那些更新将不可用，直至登录过程完成。如果更新的用户安全证书不可用，则用户应该尝试先前的口令或其它注册的指纹来登录系统。在完成登录后，用户更新的安全证书将可用并且新的口令和指纹将用 UVM 注册。

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。

本地用户名和域用户名

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。如果不这样做，则当启用了 IBM UVM 安全 Windows 登录替换后在本地和域登录间切换时将提示他们更新 IBM UVM Windows 密码。

CSS 不提供使用同一帐户名登记单独的域和本地用户的功能。如果尝试用同一个标识登记本地和域用户，则显示以下消息：已配置选定的用户标识。CSS 不允许在一个系统中单独登记公共域和本地用户标识，这样公共用户标识将有权访问同一套安全证书，如证书、存储的指纹等。

重新安装 **Targus** 指纹软件

如果卸下并重新安装了 Targus 指纹软件，则为了启用指纹支持，必须在客户端安全软件中手动添加启用指纹支持所需的注册表条目。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。必须重新引导系统以便客户端安全软件识别更改并启用指纹支持。

注：为了添加这些注册表条目，您在系统上必须具有管理员权限。

BIOS 超级用户口令

IBM 客户端安全软件 5.2 和更早版本不支持某些 ThinkPad 系统上可用的 BIOS 超级用户口令功能。如果您启用 BIOS 超级用户口令，则必须从 BIOS Setup 完成对安全子系统所做的任何启用和禁用。

使用 **Netscape 7.x**

Netscape 7.x 与 Netscape 4.x 的工作方式不同。一旦启动 Netscape 后不会出现口令提示。或更确切地说，PKCS#11 模块只在需要时装入，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。某些其它介质，例如网络共享或 USB 存储钥匙，可能是良好的存档位置。

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用 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，智能卡应该只注册一个用户帐户。

验证智能卡

如果智能卡需要验证，则 UVM 将显示请求该智能卡的对话框。当将智能卡插入阅读器时，将显示请求智能卡 PIN 的对话框。如果用户输入不正确的 PIN，UVM 将再次请求智能卡。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 口令和 Windows 密码，或使用用户配置实用程序更新其密钥存档。

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更改了 Windows 用户名，也会有此限制。

结合 Netscape 应用程序使用客户端安全软件

授权失败后打开 **Netscape**：如果 UVM 口令窗口打开，则在继续以前必须输入 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），则显示一条错误消息。如果您单击确定，则将打开 Netscape，但您将无法使用由 IBM 嵌入式安全子系统生成的数字证书。您必须退出后重新进入 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，则该模块支持的所有散列算法都没有被选中。以下算法受 IBM 嵌入式安全子系统 PKCS#11 模块的支持，但在 Netscape 中查看时不标识为受支持：

- 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与 IBM 嵌入式安全子系统证书一起使用的加密算法的问题。请参阅 Microsoft 或 Netscape 的资料，以获取有关与它们的电子邮件应用程序一起使用的加密算法的当前信息。

当从一台 **Outlook Express**（**128** 位）客户机将电子邮件发送至另一台 **Outlook Express**（**128** 位）客户机时：如果您使用带 128 位的 Internet Explorer 4.0 或 5.0 版本的 Outlook Express 将加密的电子邮件发送至其它使用 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只能使用 3DES 算法。

当在一台 **Outlook Express**（**128** 位）客户机与一台 **Netscape** 客户机间发送电子邮件时：从一台 Netscape 客户机至一台 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）客户机中不可以选择某些算法：某些 RC2 算法以及其它算法也许不能与 IBM 嵌入式安全子系统证书一起使用，这取决于如何配置或更新您的 Outlook Express（128 位）版本。请参阅 Microsoft 的资料以获取有关与您的 Outlook Express 版本一起使用的加密算法的当前信息。

对于 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。

   如果要设置已切换至的用户标识的 UVM 保护，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

在以上情形中，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形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您计算机的正常操作。

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，声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 的声明拒绝访问验证对象的错误消息与来自 Netscape 的声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
软件安装期间显示一条错误消息	操作
安装软件时显示一条消息，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。

问题症状	可能的解决方案
安装期间显示消息，表明您必须升级或删除该程序。	请执行下列操作之一： • 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所帮助。

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
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）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您的计算机。
当更改管理员密码时显示禁用芯片的消息	操作

问题症状	可能的解决方案
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。不要在输入确认密码后按 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。
受限用户在 **Windows XP Home** 中无法使用用户配置实用程序	操作
Windows XP Home 的受限用户在以下任何一种情形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

问题症状	可能的解决方案
IBM ThinkPad 计算机不支持多个 UVM 感知指纹传感器的交换。	不要切换指纹传感器型号。对远程工作以及扩展坞中的工作使用相同的型号。

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性。	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更改了 Windows 用户名，也会有此限制。	
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相关联的证书）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。	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。
尝试对电子邮件消息进行数字签名时产生故障消息	操作
如果电子邮件消息的撰写者尝试对电子邮件消息进行数字签名，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用户帐户关联的证书。要获取更多的信息，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
在使用 Outlook Express（带有 128 位版本的 Internet Explorer 4.0 或 5.0）的客户机之间发送加密的电子邮件时，仅可使用 3DES 算法。	有关与 Outlook Express 一起使用的加密算法的当前信息，请参阅 Microsoft 的文档。

问题症状	可能的解决方案
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 的资料以获取有关与您的 Outlook Express 版本一起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 中的加密长度并使用带有 Internet Explorer 4.0（128 位）的 Outlook Express 将签名的电子邮件消息发送到客户机时，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
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
读加密的电子邮件时发生问题	操作

问题症状	可能的解决方案
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。
尝试对电子邮件消息进行数字签名时产生故障消息	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。要获取更多的信息，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 的资料以获取有关与您的 Outlook Express 版本一起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
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
当同一发送方多次接收数字签名的电子邮件时，不覆盖与电子邮件关联的第一个数字证书。	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，创建了与 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。

问题症状	可能的解决方案
打开 **Netscape** 代理程序并导致 **Netscape** 失败	操作
打开 Netscape 代理程序并关闭 Netscape。	关闭 Netscape 代理程序。
如果您尝试打开它，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的延迟。	不需要操作。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
在数字证书请求期间 **UVM** 口令窗口或指纹验证窗口显示多次	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

以下故障诊断信息可以在您结合客户端安全软件使用 Tivoli Access Manager 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
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** 无法完成它的设置	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
将不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

问题症状	可能的解决方案
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不同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翻倍。

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 口令可以比传统的密码更长并且更具唯一性。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，包含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。可结合其它验证设备使用 UVM 口令，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（假定用户可以获取对该系统的访问权）。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是否匹配后，授权用户访问权。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，请阅读以下提示：

- 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 UVM 口令允许输入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，包括某些情形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