IBM® Client Security
解决方案

Client Security Software Version 4.0 安装指南

IBM® Client Security
解决方案

Client Security Software Version 4.0 安装指南

第一版（2002 年 3 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，『针对 Client Security Software 的美国出口法规』和第 35 页的附录 C，『**声明和商标**』。

目录

前言

本部分提供如何使用本指南的信息。

关于本指南

本指南包含有关在 IBM 网络计算机（也称为 IBM 客户机，包括 IBM 嵌入式安全芯片）上安装 Client Security Software 的信息。本指南还包含有关启用 IBM 嵌入式安全芯片并为安全芯片设置硬件密码的信息。

本指南组织如下:

“第 1 章，『**介绍 IBM Client Security Software**』，”包含随 Client Security Software 提供的组件的概述。

“第 2 章，『入门』，”包含计算机硬件和软件安装的先决条件，以及有关下载软件的指示信息。

“第 3 章，『在安装软件之前』，”包含安装 Client Security Software 的先决条件指示信息。

“第 4 章，『安装、更新和卸载软件』，”包含安装、更新和卸载软件的指示信息。

“第 5 章，『故障诊断』，”包含帮助信息，以解决使用本指南中提供的指示信息时可能遇到的问题。

“附录 A，『针对 Client Security Software 的美国出口法规』，”包含有关软件的美国出口法规信息。

“附录 B，『密码和密码短语规则』，”包含有关设置密码和密码短语的规则。

“附录 C，『**声明和商标**』，”包含法律声明和商标信息。

应阅读本指南的人员

本指南旨在面向在 IBM 客户机上设置个人计算机安全性的网络或系统管理员。要求具有安全性概念的知识，例如网络环境中的公共密钥基础设施（PKI）和数字证书管理。

如何使用本指南

使用本指南以在 IBM 客户机上安装和设置个人计算机安全性。本指南是*《Client Security Software 管理员指南》*、*《将 Client Security 与 Policy Director 一起使用》*和*《Client Security 用户指南》*的姊妹篇。

本指南和所有关于 Client Security 的其它文档可从 IBM Web 站点 http://www.pc.ibm.com/ww/security/secdownload.html 下载。

对《*Client Security Software 管理员指南*》的引用

本文档中提供了对《*Client Security Software 管理员指南*》的引用。《*管理员指南*》包含有关使用 User Verification Manager（UVM）以及与 UVM 策略一起使用的信息，以及有关使用 Administrator Utility 和 Client Utility 的信息。

安装软件后，请使用《*管理员指南*》中的指示信息来设置和维护每台客户机的安全性策略。

对《*Client Security Software 用户指南*》的引用

《*Client Security 用户指南*》是《*Client Security Software 管理员指南*》的姊妹篇，它包含有关使用 Client Security Software（例如使用 UVM 登录保护、创建数字证书以及使用 Client Utility）执行用户任务的帮助信息。

附加信息

可以从 IBM Web 站点 http://www.pc.ibm.com/ww/security/index.html 获得附加信息和安全性产品更新（如果可用）。

第 1 章 介绍 IBM Client Security Software

Client Security Software 是为使用 IBM 嵌入式安全芯片加密和存储加密密钥的 IBM 计算机设计的。此软件由使 IBM 客户机能够使用本地网络、企业网或因特网中的客户机安全性的应用程序和组件组成。

Client Security Software 应用程序和组件

当安装 Client Security Software 时，将安装以下软件应用程序和组件:

- **Administrator Utility**: Administrator Utility 是管理员用来激活或取消激活嵌入式安全芯片并创建、归档和重新生成加密密钥和密码短语的界面。此外，管理员可以使用此实用程序将用户添加到 Client Security Software 提供的安全性策略。
- **User Verification Manager（UVM）**: Client Security Software 使用 UVM 来管理密码短语和其它元素以认证系统用户。例如，指纹阅读器可以由 UVM 使用来进行登录认证。UVM 软件启用以下功能:
  - **UVM 客户机策略保护**: UVM 软件使管理员能够设置客户机安全性策略，规定如何在系统上认证客户机用户。
  - **UVM 系统登录保护**: UVM 软件使管理员能够通过登录界面来控制计算机访问。UVM 保护确保只有被安全性策略识别的用户才能访问操作系统。
  - **UVM Client Security 屏幕保护程序保护**: UVM 软件使用户能够通过 Client Security 屏幕保护程序界面来控制对计算机的访问。
- **Client Utility**: Client Utility 使客户机用户能够更改 UVM 密码短语。在 Windows NT 上，Client Utility 使用户能够更改 Windows NT 登录密码以被 UVM 感知并更新密钥压缩文档。用户还可以创建使用 IBM 嵌入式安全芯片创建的数字证书的备份副本。

公共密钥基础设施（PKI）功能

Client Security Software 提供在您的业务中创建公共密钥基础设施（PKI）所要求的所有组件，例如:

- **通过客户机安全性策略的管理员控制。**客户机级别的认证最终用户是安全性策略包含的重要内容。Client Security Software 提供管理 IBM 客户机的安全性策略所要求的界面。此界面是认证软件 User Verification Manager（UVM）（它是 Client Security Software 的主要组件）的一部分。
- **公共密钥密码术的加密密钥管理。**管理员使用 Client Security Software 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，这些密钥通过密钥层绑定到 IBM 嵌入式安全芯片，其中基本级别的硬件密钥用来加密它上方的密钥，包括与每个客户机用户关联的用户密钥。由于密钥已安全绑定到计算机硬件，所以在 IBM 嵌入式安全芯片上加密和存储密钥添加了客户机安全性的基本额外层。
- **受 IBM 嵌入式安全芯片保护的数字证书创建和存储。**当应用可用于数字签名或加密电子邮件消息的数字证书时，Client Security Software 使您能够选择 IBM 嵌入式安全芯片作为使用 Microsoft CryptoAPI 的应用程序加密服务供应商。这些应用程序包括 Internet Explorer 和 Microsoft Outlook Express。这就确保了数字证书的专用密钥存储在 IBM 嵌入式安全芯片上。而且，Netscape 用户可以选择 IBM 嵌入式安全芯

片作为用于安全性的数字证书的专用密钥生成器。使用公共密钥密码术标准（PKCS）#11（例如 Netscape Messenger）应用程序可以利用由 IBM 嵌入式安全芯片提供的保护。

- **密钥压缩文档和恢复解决方案。**一个重要的 PKI 功能是创建一个密钥压缩文档，如果先前的密钥丢失或破坏，就可以从这个密钥压缩文档恢复密钥。Client Security Software 提供了一个界面，使您能够为使用 IBM 嵌入式安全芯片创建的密钥和数字证书建立压缩文档，以便在必要的时候对这些密钥和证书进行恢复。
- **右键单击加密。**“右键单击加密”使客户机用户能够通过单击鼠标右键简便地加密其文件。

第 2 章 入门

本部分包含与 Client Security Software 一起使用的硬件和软件兼容性要求。还提供有关下载 Client Security Software 的信息。

硬件要求

在下载并安装软件之前，请确保您的计算机硬件与 Client Security Software 兼容。

有关硬件和软件要求的最近信息，可在 IBM Web 站点 http://www.pc.ibm.com/ww/security/secdownload.html 获得。

IBM 嵌入式安全芯片

IBM 嵌入式安全芯片是嵌入在 IBM 客户机的系统板上的加密微处理器。这一基本的 IBM Client Security 组件将安全性策略功能从易受攻击的软件传送到安全硬件，从根本上增加了本地客户机的安全性。

只有 IBM 计算机和包含 IBM 嵌入式安全芯片的工作站才能支持 Client Security Software。如果尝试下载该软件并将其安装到不包含 IBM 嵌入式安全芯片的计算机上，该软件将不会正常安装或运行。

所支持的 IBM 型号

Client Security Software 经授权并支持许多 IBM 台式和笔记本计算机。有关所支持的型号的完整列表，请参考 http://www.pc.ibm.com/ww/resources/security/secdownload.html Web 页面。

软件要求

在下载并安装软件之前，请确保您的计算机软件和操作系统与 Client Security Software 兼容。

操作系统

Client Security Software 要求以下操作系统之一:

- Windows XP
- Windows 2000 Professional
- Windows NT 4.0，装有 Service Pack 5 或后续版本（仅限 NetVista 计算机。）

UVM 感知产品

User Verification Manager（UVM）软件使您能够为您的桌面机器定制认证。这种基于策略的一级的控制增加了资产保护和密码管理的效率。与企业范围安全性策略程序兼容的 UVM 使您能够使用 UVM 感知产品，这些产品包括:

- **生物测量设备，例如指纹阅读器**

  UVM 为生物测量设备提供即插即用接口。在安装 UVM 感知传感器之前，必须安装 Client Security Software。

要使用已安装在 IBM 客户机上的 UVM 感知传感器，必须卸载 UVM 感知传感器，接着安装 Client Security Software，然后重新安装 UVM 感知传感器。

- **Tivoli SecureWay Policy Director 版本 3.7 或 3.8**

  UVM 软件通过使用集中的、基于策略的访问控制解决方案（例如 Policy Director）平滑地集成而简化并改善了策略管理。

  UVM 软件在本地强化了策略（无论系统在网络（桌面）上或是独立的），这就创建了单一的、统一的策略模型。

- **Lotus Notes 版本 4.5 或后续版本**

  UVM 与 Client Security Software 一起工作以改善 Lotus Notes 登录的安全性（Lotus Notes 版本 4.5 或后续版本）。

- **Entrust Entelligence**

  Entrust Entelligence 支持增强了因特网的安全性能力，这样，关键的企业过程就可以移到因特网上。Entrust Entelligence 提供了单一的安全层，它可以包含企业的整套增强安全性需求，包括识别、隐私、验证和安全性管理。

- **RSA SecurID Software Token**

  RSA SecurID Software Token 使与传统的 RSA 硬件令牌相同的种子记录嵌入到现有的用户平台上。因此，用户可以通过访问嵌入式软件认证受保护的资源，而无必携带专用的认证设备。

Web 浏览器

Client Security Software 支持以下 Web 浏览器来请求数字证书:

- Internet Explorer 5.0 或后续版本
- Netscape 4.51 或后续版本

Web 浏览器加密强度信息

如果安装了强加密的支持，请使用 128 位版本的 Web 浏览器。否则，请使用 40 位版本的 Web 浏览器。要检查您的 Web 浏览器的加密强度，请参阅随浏览器提供的帮助系统。

加密服务

Client Security Software 支持以下加密服务:

- **Microsoft CryptoAPI**: CryptoAPI 是 Microsoft 操作系统和应用程序的缺省加密服务。使用内置 CryptoAPI 支持，Client Security Software 使您能够在创建 Microsoft 应用程序的数字证书时使用 IBM 嵌入式安全芯片的加密操作。
- **PKCS#11**: PKCS#11 是 Netscape、Entrust、RSA 和其它产品的加密标准。安装 IBM 嵌入式安全芯片 PKCS#11 模块后，可以使用 IBM 嵌入式安全芯片来生成 Netscape、Entrust、RSA 和使用 PKCS#11 的其它应用程序的数字证书。

电子邮件应用程序

Client Security Software 支持使用安全电子邮件的以下应用程序类型:

- 使用加密操作的 Microsoft CryptoAPI 的电子邮件应用程序，例如 Outlook Express 和 Outlook（当与受支持版本的 Internet Explorer 一起使用时）
- 使用加密操作的公共密钥加密标准 #11（PKCS#11）的电子邮件应用程序，例如 Netscape Messenger（当与受支持版本的 Netscape 一起使用时）

下载软件

Client Security Software 可以从 IBM Web 站点 http://www.pc.ibm.com/ww/security/secdownload.html 下载。

注册表

当下载该软件时，必须填写注册表和调查问卷，并同意许可证条款。请按照 Web 站点提供的指示信息来下载软件。

Client Security Software 的安装文件包括在名为 csec4_0.exe 的自解压文件中。

出口法规

Client Security Software 包含可在北美洲以及世界各国下载的加密代码。如果您居住在一个禁止从美国的 Web 站点下载加密软件的国家或地区，则不能下载 Client Security Software。有关管理 Client Security Software 的出口法规的更多信息，请参阅第 31 页的附录 A，『针对 Client Security Software 的美国出口法规』。

第 3 章 在安装软件之前

本部分包含在 IBM 客户机上运行安装程序和配置 Client Security Software 的先决条件的指示信息。在从 IBM Web 站点下载的 csec4_0.exe 文件中提供了安装所要求的所有文件。

在安装软件之前

安装程序在 IBM 客户机上安装 Client Security Software，并启用 IBM 嵌入式安全芯片；然而，安装细节会因许多因素而不同。

在运行 Windows XP、Windows NT 和 Windows 2000 的客户机上安装

Windows XP、Windows NT 和 Windows 2000 用户必须使用管理员权限登录以安装 Client Security Software。

为与 Policy Director 使用安装

如果打算使用 Policy Director 来控制计算机的认证要求，则在安装 Client Security Software 之前必须安装某些 Policy Director 组件。有关详细信息，请参阅*《将 Client Security 与 Policy Director 一起使用》*.

启动功能注意事项

两个 IBM 启动功能会影响您启用安全性子系统（嵌入式安全芯片）并生成硬件加密密钥的方式。这两个功能是管理员密码和“增强安全性”。

管理员密码（NetVista）

管理员密码防止未经授权的人员更改 IBM 计算机的配置设置。使用 Configuration/Setup Utility 程序（通过在系统启动顺序过程中按下 F1 来访问该程序）来设置这些密码。

超级用户密码（ThinkPad）

超级用户密码防止未经授权的人员更改 IBM ThinkPad 计算机的配置设置。使用 IBM BIOS Setup Utility 程序（通过在系统启动顺序过程中按下 F1 来访问该程序）来设置这些密码。

增强安全性

“增强安全性”为您的管理员密码和启动顺序设置提供了额外的保护。通过使用 Configuration/Setup Utility 程序（通过在系统启动顺序过程中按下 F1 来访问该程序）可以查明是否启用或禁用了“增强安全性”。

有关管理员密码和“增强安全性”的更多信息，请参阅随计算机提供的文档。

NetVista 6059、6569、6579、6649 型以及所有 NetVista Q1x 型上的增强安全性:

如果已在 NetVista 型号（6059、6569、6579、6649、6646 和所有 Q1x 型号）上设置了管理员密码，则必须打开 Administrator Utility 以启用芯片并生成硬件密钥。

当在这些 NetVista 型号上启用了“增强安全性”时，则必须在安装 Client Security Software 后使用 Administrator Utility 来启用嵌入式安全芯片并生成硬件加密密钥。如

果安装程序检测到已启用了“增强安全性”，则您将在安装过程结束时得到通知。重新启动计算机并打开 Administrator Utility 以启用芯片并生成硬件密钥。

在所有其它 NetVista 型号（除了 6059、6569、6579、6649 型和所有 NetVista Q1x 型号）上的增强安全性: 如果已设置了其它 NetVista 型号上的管理员密码，则在安装过程中不会要求输入管理员密码。

当在这些 NetVista 型号上启用了“增强安全性”时，则可以使用安装程序来安装软件，但必须使用 Configuration/Setup Utility 来启用嵌入式安全芯片。启用芯片后，则可以使用 Administrator Utility 来生成硬件密钥。

BIOS 更新信息

在安装软件之前，可能需要为您的计算机下载最新的基本输入／输出系统（BIOS）代码。要确定您的计算机使用的 BIOS 级别，请重新启动计算机并按下 F1 来启动 Configuration/Setup Utility。当 Configuration/Setup Utility 的主菜单打开时，请选择 Product Data 来查看有关 BIOS 代码的信息。BIOS 代码级别还称为 EEPROM 修订级别。

要在 NetVista 型号（6059、6569、6579 和 6649）上运行 Client Security Software 2.1 或后续版本，则必须使用 BIOS 级别 xxxx22axx 或后续版本；要在 NetVista 型号（6790、6792、6274 和 2283）上运行 Client Security Software 2.1 或后续版本，则必须使用 BIOS 级别 xxxx20axx 或后续版本。有关更多新信息，请参阅随软件下载提供的自述文件。

要查找您的计算机的最新 BIOS 代码更新，请访问 IBM Web 站点 http://www.pc.ibm.com/support，在搜索字段中输入 bios，并从下拉列表中选择 downloads；然后按下 Enter 键。显示 BIOS 代码更新的列表。单击相应的 NetVista 型号，并按照 Web 页面上的指示信息操作。

使用压缩文档密钥对

压缩文档密钥对（包括管理员公共密钥和管理员专用密钥）使您能够生成 IBM 客户机的硬件加密密钥，并在其它处保存密钥数据的副本以进行恢复。

由于使用 Administrator Utility 来创建压缩文档密钥对，所以必须在初始 IBM 客户机上安装 Client Security Software，然后使用 Administrator Utility 来生成压缩文档密钥对。下面提供了在第一台 IBM 客户机上安装和配置软件的指示信息。

创建压缩文档密钥对后，可以使用安装程序来快速在其它 IBM 客户机上安装和配置软件，而无需使用 Administrator Utility。有关更多信息，请参阅第 10 页的『当管理员公共密钥可用时在其它 IBM 客户机上安装软件 — 仅限无人照管安装』。

注: 如果打算使用可在远程客户机上使用的 UVM 策略，则必须使用与在那些客户机上安装软件时相同的压缩文档密钥对。

第 4 章 安装、更新和卸载软件

本部分包含在 IBM 客户机上安装和配置 Client Security Software 的指示信息。在从 IBM Web 站点 http://www.pc.ibm.com/ww/security/secdownload.html 下载的 csec4_0.exe 文件中提供了安装所要求的所有文件。本部分还包含卸载软件的指示信息。

重要: 在安装 lient Security Software 3.0 或后续版本之*前*，必须解密使用前一版本的 Client Security Software 加密的所有文件。由于软件的文件加密实现中的更改，Client Security Software 3.0 或后续版本不能加密使用前一版本的 Client Security Software 加密的文件。

在第一台 IBM 客户机上安装软件

在启动安装过程之前，请关闭所有打开的程序，并重新启动计算机（如果还没有这样做）；然后完成以下过程以在第一台 IBM 客户机上安装 Client Security Software。

使用 IBM Client Security Software - InstallShield Wizard

IBM Client Security Software - InstallShield Wizard 提供帮助您安装 Client Security Software 并启用 IBM 嵌入式安全芯片的界面。

要使用 IBM Client Security Software - InstallShield Wizard，请完成以下过程:

1. 从 Windows 桌面，单击**开始 > 运行**。
2. 在“运行”字段中，输入 `d:\directory\csec4_0.exe`，其中 d:\directory\ 是文件所在的驱动器盘符和目录。
3. 单击 **Setup** 继续。

   IBM Client Security Software - InstallShield Wizard 打开。
4. 单击 **Next**。

   License Agreement 窗口打开。
5. 单击 **Yes** 以接受 License Agreement。

   必须同意 License Agreement 的条款以安装 Client Security Software。如果单击 **No**，安装程序将关闭，而不安装 Client Security Software。

   单击 **Yes** 后，Choose Destination Location 窗口打开。

   如果您的系统不具有相应的 SMBus 设备驱动程序，则会显示一条消息，表示此时要安装 SMBus 设备驱动程序。在某些系统上，该操作将要求在完成安装之前重新启动系统。
6. 单击 **Next** 以接受缺省目录 c:\Program Files\IBM\Security，或单击 **Browse** 以选择不同的目录；然后单击 **Next**。

   Select Program Folder 窗口打开。
7. 单击 **Next** 以接受缺省程序文件夹 IBM Client Security Software，然后单击 **Next**。
8. 单击 **Finish**。

   已成功安装 Client Security Software，并且已启用 IBM 嵌入式安全芯片。计算机将重新启动。

注: 如果已启用“增强安全性”，“安装向导”将提示您重新启动计算机以通过 F11 安装实用程序来启用 IBM 嵌入式安全芯片。

当管理员公共密钥可用时在其它 IBM 客户机上安装软件 — 仅限无人照管安装

如果已在第一台 IBM 客户机上安装了软件，并创建了管理员密钥对，则可以通过使用安装程序在其它 IBM 客户机上安装软件并启用安全性子系统。

在安装过程中，必须选择管理员公共密钥和密钥压缩文档的位置。如果要使用驻留在共享目录上的管理员公共密钥或将密钥压缩文档保存到共享目录，则在使用安装程序之前，必须首先将驱动器盘符映射到目标目录。有关将驱动器盘符映射到共享网络资源的信息，请参阅 Windows 操作系统文档。

执行无人照管安装

在开始无人照管安装之前，请阅读第 7 页的第 3 章，『在安装软件之前』。在无人照管安装过程中，不显示错误消息。如果无人照管安装过早结束，请执行照管安装以查看可能显示的任何错误消息。

无人照管安装使管理员能够在远程 IBM 客户机上安装 Client Security Software，而不必物理地转至客户机计算机。

注:

1. Windows NT 或 Windows 2000 用户必须使用管理员用户权限来登录以安装 Client Security Software。
2. 必须安装 SMBus 设备驱动程序来执行无人照管安装。
3. 如果要在 NetVista 6059、6569、6579、6649 或 6646 Q1x 型号上安装 Client Security Software，并且已为计算机设置了管理员密码，则必须编辑 szAdminPassword 字段。

要执行无人照管安装，请完成以下过程:

1. 使用压缩程序将所有文件从 csec30.exe 解压缩到公共文件夹。请注意 setup.exe 和 setup.iss 文件存储在指定的文件夹中。
2. 将 admin.key 文件复制到 IBM 客户机的硬盘或共享网络目录，以便该文件可用于无人照管安装。
3. 编辑并保存 setup.iss 文件。该文件中可能需要编辑的参数以粗体显示如下。

```
[InstallShield Silent]
Version=v6.00.000
File=Response File
szAdminPassword=11111111
szHWPassword=password
szKeyFile=C:\MyKeyFile
szArchivePath=C:\MyArchive
[File Transfer]
OverwrittenReadOnly=NoToAll
[{355B3C24-68B7-11D4-B3EC-000629B04E58}-DlgOrder]
Dlg0={355B3C24-68B7-11D4-B3EC-000629B04E58}-SdWelcome-0
Count=6
Dlg1={355B3C24-68B7-11D4-B3EC-000629B04E58}-SdLicense-0
Dlg2={355B3C24-68B7-11D4-B3EC-000629B04E58}-SdAskDestPath-0
Dlg3={355B3C24-68B7-11D4-B3EC-000629B04E58}-SdSelectFolder-0
Dlg4={355B3C24-68B7-11D4-B3EC-000629B04E58}-MessageBox-0
Dlg5={355B3C24-68B7-11D4-B3EC-000629B04E58}-SdFinishReboot-0
[{355B3C24-68B7-11D4-B3EC-000629B04E58}-SdWelcome-0]
Result=1
[{355B3C24-68B7-11D4-B3EC-000629B04E58}-SdLicense-0]
Result=1
[{355B3C24-68B7-11D4-B3EC-000629B04E58}-SdAskDestPath-0]
szDir=C:\Program Files\IBM\Security
Result=1
[{355B3C24-68B7-11D4-B3EC-000629B04E58}-SdSelectFolder-0]
szFolder=IBM Client Security Software
Result=1
[Application]
Name=IBM Client Security Software
Version=2.01.001a
Company=IBM
Lang=0009
[{355B3C24-68B7-11D4-B3EC-000629B04E58}-MessageBox-0]
Result=1
[{355B3C24-68B7-11D4-B3EC-000629B04E58}-SdFinishReboot-0]
Result=1
BootOption=3
```

setup.iss 文件的这些参数指定以下功能:

- **szDir=C:\Program Files\IBM\Security** 指定 Client Security Software 将要安装到的目录。
- **szFolder=IBM Client Security Software** 指定 Client Security Software 将要安装到的文件夹。
- **szHWPassword=password** 指定 IBM 嵌入式安全芯片的硬件密码为 “password”。可以指定想要的任何硬件密码，只要它符合硬件密码的规则。有关硬件密码规则的信息，请参阅第 33 页的附录 B, 『密码和密码短语规则』。

- **szKeyFile=C:\MyKeyFile** 指定至 admin.key 文件的路径。要使无人照管安装正常运行，admin.key 必须在客户机硬盘上或共享网络目录上的指定路径中。如果使用的 admin.key 文件存储在软盘上，请将其复制到客户机硬盘或共享网络目录，以便该文件可用于无人照管安装。
- **szArchivePath=C:\MyArchive** 指定归档密钥的路径。要使无人照管安装正常运行，请不要将密钥压缩文档存储在软盘上。如果想要将密钥压缩文档存储在软盘上，请在无人照管安装过程中将密钥压缩文档存储在客户机硬盘上或共享网络目录上，然后在安装完成后将其复制到软盘。
- **（仅对某些系统）szAdminPassword=11111111** 指定已为计算机设置的管理员密码。如果您正在下面的一台计算机上安装 Client Security Software:
  - NetVista 6059、6569、6579 或 6649
  - NetVista 6646 所有 Q1x 型号

  并且已为计算机设置了管理员密码，则必须在 `szAdminPassword =` 的旁边输入管理员密码。如果您正在其上安装软件的计算机未在上面列出，则不必编辑 szAdminPassword 项。

  注: 如果提供不错误的管理员密码，软件也会安装，但不会启用嵌入式安全芯片，并不会生成硬件密钥。有关更多信息，请参阅第 7 页的『启动功能注意事项』。

4. 从 Windows 桌面，单击**开始 > 运行**。
5. 输入至 setup.exe 的路径，并将 [space]-s 添加到路径（例如，`C:\Security\setup.exe -s`）。

   所有文件都将安装到为 szDir 指定的目录，并且计算机将重新启动。

升级 Client Security Software 的版本

安装了先前版本的 Client Security Software 的客户机可能需要更新以利用新的 Client Security Software 功能。

从先前版本的软件更新

要从先前版本的 Client Security Software 更新系统，请完成以下过程:

1. 卸载先前的软件。
2. 安装新的软件。

   注: 要使用与为 IBM 嵌入式安全芯片设置的相同的硬件密码，请不要清除 IBM 嵌入式安全芯片。
3. 创建新的用户加密密钥。
4. 设置用户认证。
5. 获取用于电子邮件的新的数字证书。

有关更多信息，请参阅*《Client Security Software 管理员指南》*。

清除 IBM 嵌入式安全芯片（NetVista）

要从 IBM 嵌入式安全芯片擦除所有用户加密密钥，并清除芯片的硬件密码，则必须清除芯片。在清除 IBM 嵌入式安全芯片之前，请阅读下面的信息。

注意:

- 如果清除了 IBM 嵌入式安全芯片，则存储在芯片上的所有加密密钥和证书都将丢失，并且硬盘上的内容可能变为不可使用。
- 在 Windows XP、Windows NT 和 Windows 2000 中，当 UVM 登录保护已启用时不要清除或禁用 IBM 嵌入式安全芯片。如果这样做，硬盘上的内容将变为不可使用，并且必须重新格式化硬盘驱动器并重新安装所有软件。

  要禁用 UVM 保护，请打开 Administrator Utility 并清除 **Use UVM Logon Protection for this Workstation instead of using Windows Logon Protection** 复选框。在禁用 UVM 保护之前，必须重新启动计算机。

要清除 IBM 嵌入式安全芯片，请完成以下过程:

1. 关闭并重新启动计算机。
2. 当在屏幕上出现 Configuration/Setup Utility 提示时，按下 F1。

   显示 Configuration/Setup Utility 的主菜单。
3. 选择 **System Security**。
4. 选择 **IBM embedded Security Chip**。
5. 选择 **Clear IBM Security Chip**。
6. 选择 **Yes**。
7. 按下 Esc 继续。
8. 按下 Esc 退出并保存设置。

清除 IBM 嵌入式安全芯片（ThinkPad）

要从 IBM 嵌入式安全芯片擦除所有用户加密密钥，并清除芯片的硬件密码，必须清除芯片。在清除 IBM 嵌入式安全芯片之前，请阅读下面的信息。

注意:

- 如果清除了 IBM 嵌入式安全芯片，则存储在芯片上的所有加密密钥和证书都将丢失，并且硬盘上的内容可能变为不可使用。
- 在 Windows XP、Windows NT 和 Windows 2000 中，当 UVM 登录保护已启用时不要清除或禁用 IBM 嵌入式安全芯片。如果这样做，硬盘上的内容将变为不可使用，并且必须重新格式化硬盘驱动器并重新安装所有软件。

  要禁用 UVM 保护，请打开 Administrator Utility 并清除 **Use UVM Logon Protection for this Workstation instead of using Windows Logon Protection** 复选框。在禁用 UVM 保护之前，必须重新启动计算机。

要清除 IBM 嵌入式安全芯片，请完成以下过程:

1. 关闭并重新启动计算机。
2. 当在屏幕上出现 IBM BIOS Setup Utility 提示时，按下 F1。

   显示 IBM BIOS Setup Utility 主菜单。
3. 选择 **Config**。
4. 选择 **IBM Security Chip**。
5. 选择 **Clear IBM Security Chip** 并按下 Enter 键。
6. 选择 **Yes** 以确认。
7. 按下 F10 以保存并退出。

卸载 Client Security Software

Windows NT、Windows 2000 和 Windows XP 用户必须使用管理员权限登录以卸载 Client Security Software。如果非管理员用户试图卸载 Client Security Software，将显示错误消息。

注: 在卸载 IBM Client Security Software 之前，必须卸载所有 UVM 感知传感器软件。

要卸载 Client Security Software，请完成以下过程:

1. 关闭所有 Windows 程序。
2. 从 Windows 桌面，单击**开始 > 设置 > 控制面板**。
3. 单击**添加／删除程序**图标。
4. 在可以自动除去的软件的列表中，选择 **IBM Client Security**。
5. 单击**添加／删除**。
6. 单击 **Yes** 以卸载软件。
7. 执行以下操作之一:
   - 如果为 Netscape 安装了 IBM 嵌入式安全芯片 PKCS#11 模块，会显示一条信息，要求您启动该过程以禁用 IBM 嵌入式安全芯片 PKCS#11 模块。单击 **Yes** 以继续进行。

     显示一系列消息。对于每条消息，请单击 **OK**，直到除去 IBM 嵌入式安全芯片 PKCS#11 模块。

     除去 PKCS#11 模块不会除去或删除系统中的数字证书。它取消了 Netscape 和 IBM 嵌入式安全芯片之间的通信。
   - 如果没有为 Netscape 安装 IBM PKCS#11 模块，会显示一条消息，询问您是否想要删除与 Client Security Software 一起安装的共享 DLL 文件。

     单击 **Yes** 以卸载这些文件，或单击 **No** 以保留这些文件为安装状态。保留这些文件为安装状态不影响计算机的正常操作。
8. 除去软件后，单击 **OK**。

   卸载 Client Security Software 后必须重新启动计算机。

当卸载 Client Security Software 时，仅除去安装的软件组件。任何创建的加密密钥仍然存储在 IBM 嵌入式安全芯片上。当卸载 Client Security Software 时，密钥压缩文档不受影响；然而，所有通过 IBM 嵌入式安全芯片获取的数字证书都将删除。

第 5 章 故障诊断

以下部分提供对防止或识别和纠正使用 Client Security Software 时可能产生的问题有帮助的信息。

管理员功能

本部分包含设置和使用 Client Security Software 时管理员可能发现的有帮助的信息。

设置管理员密码（NetVista）

在 Configuration/Setup Utility 中可用的安全性设置使管理员能够执行以下操作:

- 更改 IBM 嵌入式安全芯片的硬件密码
- 启用或禁用 IBM 嵌入式安全芯片
- 清除 IBM 嵌入式安全芯片

注意:

- 在 Windows XP、Windows NT 和 Windows 2000 中，当 UVM 登录保护已启用时不要清除或禁用 IBM 嵌入式安全芯片。如果这样做，硬盘的内容会变为不可使用，而您必须重新格式化硬盘驱动器并重新安装所有软件。

  要禁用 UVM 保护，请打开 Administrator Utility 并清除 **Replace the standard Windows logon with UVM's secure logon** 复选框。在禁用 UVM 保护之前，必须重新启动计算机。
- 如果 UVM 保护已启用，请不要清除或禁用 IBM 嵌入式安全芯片。如果这样做，硬盘的内容会变为不可使用，而您必须重新格式化硬盘驱动器并重新安装所有软件。
- 清除了 IBM 嵌入式安全芯片后，存储在芯片上的所有加密密钥和证书将丢失。

因为这些安全性设置可以通过计算机的 Configuration/Setup Utility 访问，所以请设置管理员密码以阻止未经授权的用户更改这些设置。

要设置管理员密码:

1. 关闭并重新启动计算机。
2. 当在屏幕上出现 Configuration/Setup Utility 提示时，请按下 **F1**。

   Configuration/Setup Utility 的主菜单打开。
3. 选择 **System Security**。
4. 选择 **Administrator Password**。
5. 输入密码并按下键盘上的向下箭头。
6. 再次输入密码并按下向下箭头。
7. 选择 **Change Administrator password** 并按下 Enter 键；然后再次按下 Enter 键。
8. 按下 **Esc** 退出并保存设置。

设置了管理员密码后，每次尝试访问 Configuration/Setup Utility 时都会出现一个提示。

重要: 请将管理员密码记录在安全的地方。如果丢失或忘记管理员密码，则不能访问 Configuration/Setup Utility，也不能更改或删除密码，除非卸下计算机外盖并移动系统板上的跳线。有关更多信息，请参阅随计算机提供的硬件文档。

设置超级用户密码（ThinkPad）

在 IBM BIOS Setup Utility 中可用的安全性设置使管理员能够执行以下操作:

- 启用或禁用 IBM 嵌入式安全芯片
- 清除 IBM 嵌入式安全芯片

注意:

- 在 Windows XP、Windows NT 和 Windows 2000 中，UVM 登录保护启用时不要清除或禁用 IBM 嵌入式安全芯片。如果这样做，硬盘的内容会变为不可使用，而您必须重新格式化硬盘驱动器并重新安装所有软件。

  要禁用 UVM 保护，请打开 Administrator Utility 并清除 **Replace the standard Windows logon with UVM's secure logon** 复选框。在禁用 UVM 保护之前，必须重新启动计算机。
- 如果启用了 UVM 保护，请不要清除或禁用 IBM 嵌入式安全芯片。如果这样做，硬盘的内容会变为不可使用，而您必须重新格式化硬盘驱动器并重新安装所有软件。
- 清除了 IBM 嵌入式安全芯片后，存储在芯片上的所有加密密钥和证书将丢失。

设置 Client Security Software 后，请设置超级用户密码以阻止未经授权的用户更改这些设置。

要设置超级用户密码，请完成以下过程:

1. 关闭并重新启动计算机。
2. 当在屏幕上出现 IBM BIOS Setup Utility 提示时，请按下 **F1**。

   IBM BIOS Setup Utility 的主菜单打开。
3. 选择 **Password**。
4. 选择 **Supervisor Password**。
5. 输入密码并按下 Enter 键。
6. 再次输入密码并按下 Enter 键。
7. 单击 **Continue**。
8. 按下 F10 保存并退出。

设置了超级用户密码后，每次试图访问 IBM BIOS Setup Utility 时都会出现一个提示。

重要: 请将超级用户密码记录存在安全的地方。如果丢失或忘记了超级用户密码，则不能访问 IBM BIOS Setup Utility，也不能更改或删除密码。有关更多信息，请参阅随计算机提供的硬件文档。

保护硬件密码

设置安全芯片密码以启用客户机的 IBM 嵌入式安全芯片。设置了安全芯片密码后，对 Administrator Utility 的访问受密码保护。应该保护安全芯片密码以禁止未经授权的用户更改 Administrator Utility 中的设置。

清除 IBM 嵌入式安全芯片（NetVista）

如果要从 IBM 嵌入式安全芯片擦除所有用户加密密钥并清除芯片的硬件密码，则必须清除该芯片。清除 IBM 嵌入式安全芯片前请阅读下面“注意”框中的信息。

注意:

- 如果启用了 UVM 保护，请不要清除或禁用 IBM 嵌入式安全芯片。如果这样做，硬盘的内容会变为不可使用，而您必须重新格式化硬盘驱动器并重新安装所有软件。

  要清除 UVM 保护，请打开 Administrator Utility 并清楚 **Replace the standard Windows logon with UVM's secure logon** 复选框。在禁用 UVM 保护之前，必须重新启动计算机。
- 清除了 IBM 嵌入式安全芯片后，存储在芯片上的所有加密密钥和证书将丢失。

要清除 IBM 嵌入式安全芯片，请执行以下操作:

1. 关闭并重新启动计算机。
2. 当在屏幕上出现 Configuration/Setup Utility 提示时，请按下 F1。

   Configuration/Setup Utility 的主菜单打开。
3. 选择 **System Security**。
4. 选择 **IBM Embedded Security Chip**。
5. 选择 **Clear IBM Security Chip**。
6. 选择 **Yes**。
7. 按下 Esc 继续。
8. 按下 Esc 退出并保存设置。

清除 IBM 嵌入式安全芯片（ThinkPad）

如果要从 IBM 嵌入式安全芯片擦除所有用户加密密钥并清除芯片的硬件密码，则必须清除该芯片。清除 IBM 嵌入式安全芯片前请阅读下面“注意”框中的信息。

注意:

- 如果启用了 UVM 保护，请不要清除或禁用 IBM 嵌入式安全芯片。如果这样做，硬盘的内容会变为不可使用，而您必须重新格式化硬盘驱动器并重新安装所有软件。

  要清除 UVM 保护，请打开 Administrator Utility 并清除 **Replace the standard Windows logon with UVM's secure logon** 复选框。在禁用 UVM 保护之前，必须重新启动计算机。
- 清除了 IBM 嵌入式安全芯片后，存储在芯片上的所有加密密钥和证书将丢失。

要清除 IBM 嵌入式安全芯片，请执行以下操作:

1. 关闭并重新启动计算机。
2. 当在屏幕上出现 IBM BIOS Setup Utility 提示时，请按下 Fn。

   注: 在某些 ThinkPad 型号上，您可能需要在电源打开时按下 F1 键以清除安全芯片。有关详细信息，请参考 IBM BIOS Setup Utility 的帮助消息。

   IBM BIOS Setup Utility 的主菜单打开。
3. 选择 **Security**。
4. 选择 **IBM TCPA Feature Setup**。

5. 选择 **Clear IBM TCPA Security Feature**。
6. 选择 **Yes**。
7. 按下 Enter 键继续。
8. 按下 F10 保存并退出。

Administrator Utility

以下部分包含使用 Administrator Utility 时要记住的信息。

删除用户

从 Windows XP、Windows NT 和 Windows 2000 删除用户时，将从 Administrator Utility 的用户列表中删除用户名。

使用 Policy Director 控件拒绝访问所选择的对象

当选择了 Policy Director 控件时，将禁用 **Deny all access to selected object** 复选框。在 UVM 策略编辑器中，如果选择 **Policy Director controls selected object** 以启用 Policy Director 来控制认证对象，将不禁用 **Deny all access to selected object** 复选框。虽然 **Deny all access to selected object** 复选框保持为活动的，但不能选择它来覆盖 Policy Director 控件。

已知限制

本部分包含有关与 Client Security Software 相关的已知限制的信息。

将 Client Security Software 与 Windows 操作系统一起使用

所有 Windows 操作系统有以下已知限制：如果在 UVM 中登记的客户机用户更改了其 Windows 用户名，则所有 Client Security 功能都将丢失。该用户必须在 UVM 中重新登记新用户名并请求所有新凭证。

Windows XP 操作系统有以下已知限制：在 UVM 中登记的用户如果先前已经更改了其 Windows 用户名，则无法被 UVM 认出。UVM 将指向先前的用户名而 Windows 只能认出新用户名。即使在安装 Client Security Software 前已经更改了 Windows 用户名，此限制仍然会发生。

将 Client Security Software 与 Netscape 应用程序一起使用

权限故障后 Netscape 打开：如果 UVM 密码短语窗口打开，则继续前必须输入 UVM 密码短语并单击 **OK**。如果输入错误的 UVM 密码短语（或对指纹扫描提供了错误的指纹），则会显示错误消息。如果单击 **OK**，将打开 Netscape，但是将不能使用由 IBM 嵌入式安全芯片生成的数字证书。必须退出并重新进入 Netscape，然后在可以使用 IBM 嵌入式安全芯片证书前输入正确的 UVM 密码短语。

不显示算法：如果在 Netscape 中查看了 IBM 嵌入式安全芯片 PKCS#11 模块，则不选择该模块支持的所有散列算法。以下算法由 IBM 嵌入式安全芯片 PKCS#11 模块支持，但在 Netscape 中查看时不会识别为受支持的：

- SHA-1
- MD5

IBM 嵌入式安全芯片证书和加密算法

提供以下信息以帮助识别有关可与 IBM 嵌入式安全芯片证书一起使用的加密算法的问题。有关可与其电子邮件应用程序一起使用的加密算法相关的当前信息，请参阅 Microsoft 或 Netscape。

当将电子邮件从一个 Outlook Express（128 位）客户机发送到另一个 Outlook Express（128 位）客户机时: 如果将 Outlook Express 与 128 位版本的 Internet Explorer 4.0 或 5.0 一起使用以将加密的电子邮件发送到使用 Outlook Express（128 位）的其它客户机，则使用 IBM 嵌入式安全芯片证书加密的电子邮件消息只能使用 3DES 算法。

在 Outlook Express（128 位）客户机和 Netscape 客户机之间发送电子邮件时: 从 Netscape 客户机到 Outlook Express（128 位）客户机的 RC2(40)、RC2(64) 或 RC2(128) 加密请求始终返回到使用 RC2(40) 算法的 Netscape 客户机。

对于在 Outlook Express（128 位）客户机中的选择，某些算法可能不可用: 取决于您的 Outlook Express（128 位）版本是如何配置或更新的，某些 RC2 算法和其它算法可能不可与 IBM 嵌入式安全芯片证书一起使用。有关与 Outlook Express 的版本一起使用的加密算法的当前信息，请参阅 Microsoft。

对 Lotus Notes 用户标识使用 UVM 保护

如果在 Notes 会话中切换用户标识，UVM 保护将不运行: 您可以只对 Notes 会话的当前用户标识设置 UVM 保护。要从一个启用了 UVM 保护的用户标识切换到另一个用户标识，请执行以下操作:

1. 退出 Notes。
2. 对当前用户标识禁用 UVM 保护。
3. 进入 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。

   如果要对切换到的用户标识设置 UVM 保护，请继续步骤 4。
4. 进入由 Client Security Software 提供的 Lotus Notes Configuration 工具并设置 UVM 保护。

Client Utility 限制

Windows XP 强制访问限制，这些访问限制对某些环境下的客户机用户的可用功能进行限制。

Windows XP Professional

在 Windows XP Professional 中，客户机用户限制可能应用于以下情形:

- Client Security Software 安装在稍后转换为 NTFS 格式的分区中
- Windows 文件夹位于稍后转换为 NTFS 格式的分区中
- 压缩文档文件夹位于稍后转换为 NTFS 格式的分区中

在以上情况下，Windows XP Professional Limited User 可能不能执行以下 Client Utility 任务:

- 更改其 UVM 密码短语
- 更新用 UVM 注册的 Windows 密码
- 更新密钥压缩文档

管理员启动并退出 Administrator Utility 后，这些限制被清除。

Windows XP Home

Windows XP Home Limited User 不能使用以下任何情形中的 Client Utility:

- Client Security Software 安装在 NTFS 格式的分区中
- Windows 文件夹位于 NTFS 格式的分区中
- 压缩文档文件夹位于 NTFS 格式的分区中

错误消息

与 Client Security Software 相关的错误消息在事件日志中生成: Client Security Software 使用可能在事件日志中生成错误消息的设备驱动程序。与这些消息相关的错误不影响计算机的正常运行。

如果对认证对象的访问被拒绝，则 UVM 调用由相关程序生成的错误消息: 如果 UVM 策略设置为拒绝访问认证对象（例如电子邮件解密），则表明访问被拒绝的消息将根据使用的软件而不同。例如，来自 Outlook Express 的表明对认证对象的访问被拒绝的错误消息，与来自 Netscape 的表明访问被拒绝的错误消息不同。

故障诊断图表

如果遇到 Client Security Software 的问题，则以下部分包含的故障诊断图表可能有帮助。

安装故障诊断信息

如果安装 Client Security Software 时遇到问题，则以下故障诊断信息可能有帮助。

问题症状	可能的解决方案
软件安装过程中显示一条错误消息	**操作**
安装软件时显示一条消息，询问您是否想要除去选择的应用程序及其所有组件。	单击 **OK** 退出该窗口。再次开始安装过程以安装新版本的 Client Security Software。
安装过程中显示一条消息，表明已经安装了先前版本的 Client Security Software。	单击 **OK** 从该窗口退出。请执行以下操作: 1. 卸载该软件。 2. 重新安装该软件。 **注**: 如果您计划使用相同的硬件密码来保护 IBM 嵌入式安全芯片，则不必清除该芯片和重新设置密码。
安装访问由于未知的硬件密码被拒绝	**操作**
当在具有 IBM 嵌入式安全芯片的 IBM 客户机上安装软件时，IBM 嵌入式安全芯片的硬件密码是未知的。	清除该芯片以继续安装。
无人照管安装不启动	**操作**
必须安装 SMBus 设备驱动程序以执行无人照管安装。	安装 SMBus 设备驱动程序并重新启动安装。
无人照管安装过早结束	**操作**
在无人照管安装过程中，不显示错误消息。	执行照管安装以查看可能显示的任何错误消息。
setup.exe 文件不正常响应	**操作**
如果从 csec4_0.exe 文件将所有文件解压缩到公共目录中，则 setup.exe 文件将不正常工作。	运行 smbus.exe 文件以安装 SMBus 设备驱动程序，然后运行 csec4_0.exe 文件以安装 Client Security Software 代码。
安装 UVM 感知指纹传感器时显示一条错误消息	**操作**
在 DigitalPersona U.are.UPro 指纹传感器安装过程中，显示一条消息要求您执行以下操作: 1. 连接指纹传感器。 2. 等待传感器上的红灯闪亮。 3. 单击 **OK**。 4. 选择 **Yes, I want to restart my computer now**，然后单击 **Finish**。 系统将重新启动。	不要求更多操作。指纹传感器将正确安装。

Administrator Utility 故障诊断信息

如果使用 Administrator Utility 时遇到问题，则以下故障诊断信息可能有帮助。

问题症状	可能的解决方案
在 Administrator Utility 中输入并确认您的 UVM 密码短语后，Next 按钮不可用。	**操作**

问题症状	可能的解决方案
在运行 Windows NT、Windows 2000、或 Windows XP 的系统上，当您将用户添加到 UVM 时，在 Administrator Utility 中输入并确认 UVM 密码短语后 **Next** 按钮可能不可用。	单击 Windows “任务栏” 上的 **Information** 项并继续该过程。
试图编辑本地 UVM 策略时显示一条错误消息	**操作**
编辑本地 UVM 策略时，如果 UVM 中没有用户登记，则可能显示一条错误消息。	在试图编辑策略文件前将用户添加到 UVM。
更改管理员公共密钥时显示一条错误消息	**操作**
清除嵌入式安全芯片然后恢复密钥压缩文档后，如果更改管理员公共密钥，可能显示一条错误消息。	可能的话，请将用户添加到 UVM 并请求新的证书。
试图恢复 UVM 密码短语时显示一条错误消息	**操作**
更改了管理员公共密钥然后试图恢复用户的 UVM 密码短语时可能显示一条错误消息。	请执行以下操作之一: • 如果不需要用户的 UVM 密码短语，则不需要任何操作。 • 如果需要用户的 UVM 密码短语，则必须将用户添加到 UVM，请求一个新的证书（可能的话）。
试图保存 UVM 策略文件时显示一条错误消息	**操作**
当您试图通过单击 **Apply** 或 **Save** 来保存 UVM 策略文件（globalpolicy.gvm）时，可能显示一条错误消息。	退出该错误消息，再次编辑 UVM 策略文件以进行更改，然后保存文件。
试图打开 UVM 策略编辑器时显示一条错误消息	**操作**
当前用户（已登录到操作系统上的用户）没有添加到 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。
使用 Administrator Utility 时显示一条错误消息	**操作**
使用 Administrator Utility 时，可能显示以下错误消息: 试图访问 Client Security 芯片时发生一个缓冲区 I/O 错误。这可以通过重新引导来纠正。	退出错误消息并重新启动计算机。
更改安全芯片密码时显示一条禁用的芯片消息	**操作**
试图更改安全芯片密码时，如果输入确认密码后按下了 Enter 键或 Tab > Enter，则启用 Disable 芯片按钮并显示禁用的芯片确认消息。	请执行以下操作: 1. 从禁用的芯片确认窗口退出。 2. 要更改安全芯片密码，请输入新密码，输入确认密码，然后单击 **Change**。输入确认密码后不要按下 Enter 键或 Tab > Enter。

Client Utility 故障诊断信息

如果使用 Client Utility 时遇到问题，则以下故障诊断信息可能有帮助。

问题症状	可能的解决方案
Limited User 无法执行 Windows XP Professional 中某些 Client Utility 功能	**操作**
Windows XP Professional Limited User 可能不能执行以下 Client Utility 任务: • 更改其 UVM 密码短语 • 更新使用 UVM 注册的 Windows 密码 • 更新密钥压缩文档	管理员启动并退出 Administrator Utility 后，这些限制被清除。
Limited User 不能使用 Windows XP Home 中的 Client Utility	**操作**
在以下任何情形中，Windows XP Home Limited User 均不能使用 Client Utility: • Client Security Software 安装在 NTFS 格式的分区中 • Windows 文件夹位于 NTFS 格式的分区中 • 压缩文档文件夹位于 NTFS 格式的分区中	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 Client Security Software 时遇到问题，则以下故障诊断信息可能有帮助。

问题症状	可能的解决方案
尝试 Client Security 管理员功能时显示一条错误消息	**操作**
尝试执行 Client Security 管理员功能后显示以下错误消息: ERROR 0197: Invalid Remote change requested.Press <F1> to Setup	必须禁用 ThinkPad 超级用户密码以执行特定的 Client Security 管理员功能。 要禁用超级用户密码，请执行以下操作: 1. 按下 F1 访问 IBM BIOS Setup Utility。 2. 输入当前超级用户密码。 3. 输入空的新超级用户密码，然后确认空密码。 4. 按下 Enter 键。 5. 按下 F10 保存并退出。
不同的 UVM 感知指纹传感器不正常工作	**操作**
IBM ThinkPad 计算机不支持多个 UVM 感知指纹传感器的相互交换。	不要切换指纹传感器型号。远程工作时使用与从扩展坞工作时同样的型号。

Microsoft 故障诊断信息

以下故障诊断图表包含在将 Client Security Software 与 Microsoft 应用程序或操作系统一起使用遇到问题时可能会有帮助的信息。

问题症状	可能的解决方案
对于在 UVM 中登记的用户，Client Security 不能正常工作	**操作**
登记的客户机用户可能已更改了其 Windows 用户名。如果发生了这种情况，所有 Client Security 功能都将丢失。	在 UVM 中重新登记新用户名并请求所有新凭证。
注: 在 Windows XP 中，在 UVM 中登记的用户如果先前已经更改了其 Windows 用户名，则不会被 UVM 感知。即使在安装 Client Security Software 前已经更改了 Windows 用户名，此限制仍然会发生。	
使用 Outlook Express 读取加密的电子邮件的问题	**操作**
由于发送方和接收方使用的 Web 浏览器的加密强度的差异，所以不能对加密过的电子邮件解密。 **注**: 要将 128 位 Web 浏览器与 Client Security Software 一起使用，IBM 嵌入式安全芯片必须支持 256 位加密。如果 IBM 嵌入式安全芯片支持 56 位加密，则必须使用 40 位 Web 浏览器。可以在 Administrator Utility 中找到 Client Security Software 提供的加密强度。	请验证以下情况: 1. 发送方使用的 Web 浏览器的加密强度与接收方使用的 Web 浏览器的加密强度兼容。 2. Web 浏览器的加密强度与 Client Security Software 的固件提供的加密强度兼容。
从具有多个与之关联的证书的地址使用证书的问题	**操作**
Outlook Express 可以列出多个与单一电子邮件地址关联的证书，这些证书中的一些可能变为无效。如果与证书关联的专用密钥不再存在于生成证书的发送方计算机的 IBM 嵌入式安全芯片，则证书可能变为无效。	请求接收方重新发送其数字证书；然后在 Outlook Express 的通讯簿中选择证书。
当尝试数字签名电子邮件消息时出现失败消息	**操作**
如果在电子邮件消息的作者不具有与其电子邮件帐户关联的证书时尝试数字签名电子邮件消息，则显示错误消息。	使用 Outlook Express 中的安全性设置来指定要与用户帐户关联的证书。请参阅 Outlook Express 提供的文档，以获取更多信息。
Outlook Express（128 位）只使用 3DES 算法加密电子邮件消息	**操作**
当在将 Outlook Express 与 128 位版本的 Internet Explorer 4.0 或 5.0 一起使用的客户机之间发送加密的电子邮件时，只能使用 3DES 算法。	要将 128 位浏览器与 Client Security Software 一起使用，IBM 嵌入式安全芯片必须支持 256 位加密。如果 IBM 嵌入式安全芯片支持 56 位加密，则必须使用 40 位 Web 浏览器。可以在 Administrator Utility 中找到 Client Security Software 提供的加密强度。 请参阅 Microsoft 以获取有关与 Outlook Express 一起使用的加密算法的当前信息。
Outlook Express 客户机返回使用不同算法的电子邮件消息	**操作**

问题症状	可能的解决方案
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使用 RC2（40）算法加密。	不要求操作。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 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使用 Outlook Express 中的证书时出现错误消息	**操作**
通过在 Administrator Utility 中使用密钥恢复功能可以恢复证书。某些证书，例如 VeriSign 提供的免费证书，在密钥恢复后可能不会恢复。	恢复密钥后，请执行以下操作之一: • 获取新证书 • 在 Outlook Express 中的认证中心再次注册
Outlook Express 没有更新与证书关联的加密强度	**操作**
当发送方在 Netscape 中选择加密强度并将签名的电子邮件消息发送到将 Outlook Express 与 Internet Explorer 4.0（128 位）一起使用的客户机时，返回的电子邮件的加密强度可能不匹配。	从 Outlook Express 的通讯簿中删除关联的证书。再次打开签名的电子邮件，并将证书添加到 Outlook Express 的通讯簿中。
在 Outlook Express 中显示错误解密消息	**操作**
通过在 Outlook Express 中双击消息可以打开该消息。在某些情况下，当过快地双击加密的消息时，会出现加密错误消息。	关闭该消息，然后再次打开加密的电子邮件消息。
而且，当选择加密的消息时，会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，则不要求操作。
当在加密的电子邮件上单击“发送”按钮两次时，显示错误消息。	**操作**
当使用 Outlook Express 时，如果单击发送按钮两次来发送加密的电子邮件消息，则会显示一条错误消息，表明消息不能发送。	关闭错误消息，然后单击一次**发送**按钮。
当请求证书时显示错误消息	**操作**
使用 Internet Explorer 时，如果请求使用 IBM 嵌入式安全芯片 CSP 的证书，则会接收到错误消息。	再次请求数字证书。

Netscape 应用程序故障诊断信息

以下故障诊断图表包含在将 Client Security Software 与 Netscape 应用程序一起使用遇到问题时可能会有帮助的信息。

问题症状	可能的解决方案
读取加密的电子邮件时的问题	**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 浏览器的加密强度的差异，所以不能对加密过的电子邮件解密。 **注**: 要将 128 位浏览器与 Client Security Software 一起使用，则 IBM 嵌入式安全芯片必须支持 256 位加密。如果 IBM 嵌入式安全芯片支持 256 位加密，则必须使用 40 位 Web 浏览器。可以在 Administrator Utility 中找到 Client Security Software 提供的加密强度。	请验证以下功能: 1. 发送方使用的 Web 浏览器的加密强度与接收方使用的 Web 浏览器的加密强度兼容。 2. Web 浏览器的加密强度与 Client Security Software 的固件提供的加密强度兼容。
当尝试数字签名电子邮件消息时出现失败消息	**操作**
当没有在 Netscape Messenger 中选择 IBM embedded Security Chip certificate，并且电子邮件消息的作者尝试使用证书签名时，会显示错误消息。	使用 Netscape Messenger 中的安全性设置来选择证书。当 Netscape Messenger 打开时，单击任务栏上的安全性图标。Security Info 窗口打开。在左面板中单击 **Messenger**，然后选择 **IBM embedded Security Chip certificate**。请参阅由 Netscape 提供的文档以获取更多信息。
电子邮件消息使用不同算法返回到客户机	**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使用 RC2（40）算法加密。	不要求操作。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 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。
不能使用由 IBM 嵌入式安全芯片生成的数字证书	**操作**
由 IBM 嵌入式安全芯片生成的数字证书不可使用。	验证当打开了 Netscape 时，已输入了正确的 UVM 密码短语。如果输入错误的 UVM 密码短语，会显示一条错误消息，表明认证失败。如果单击 **OK**，将打开 Netscape，但您将不能使用由 IBM 嵌入式安全芯片生成的证书。必须退出并重新打开 Netscape，然后输入正确的 UVM 密码短语。
来自同一个发送方的新数字证书不能在 Netscape 中被替换	**操作**
当数字签名的电子邮件不止一次被同一个发送方接收到时，则与电子邮件关联的第一个数字证书不会被覆盖。	如果接收到多个电子邮件证书，则只有一个证书是缺省证书。请使用 Netscape 中的安全性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。
不能导出 IBM 嵌入式安全芯片证书	**操作**
不能在 Netscape 中导出 IBM 嵌入式安全芯片证书。Netscape 中的导出功能可以用于备份证书。	请转至 Administrator Utility 或 Client Utility 以更新密钥压缩文档。当更新密钥压缩文档时，将创建与 IBM 嵌入式安全芯片关联的所有证书的副本。
当在硬盘驱动器发生故障后尝试使用恢复的证书时出现的错误消息	**操作**

问题症状	可能的解决方案
通过在 Administrator Utility 中使用密钥恢复功能可以恢复证书。某些证书，例如 VeriSign 提供的免费证书，在密钥恢复后可能不会恢复。	恢复密钥后，将获取新证书。
Netscape 代理程序打开并导致 Netscape 失败	**操作**
Netscape 代理程序打开并关闭 Netscape。	关闭 Netscape 代理程序。
尝试打开 Netscape 时，显示 Netscape	**操作**
如果添加 IBM 嵌入式安全芯片 PKCS#11 模块，然后打开 Netscape，则在 Netscape 打开之前会发生短时间的延迟。	不要求操作。这仅适用于信息用途。

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 密码短语窗口或指纹认证窗口显示多次	**操作**
UVM 安全性策略指定用户在可以获得数字证书之前提供 UVM 密码短语或指纹认证。如果用户尝试获得证书，则请求 UVM 密码短语或指纹扫描的认证窗口将显示不止一次。	每次认证窗口打开时，请输入 UVM 密码短语或扫描您的指纹。
显示 VBScript 或 JavaScript 错误消息	**操作**
当请求数字证书时，会显示一条与 VBScript 或 JavaScript 相关的错误消息。	重新启动计算机，然后再次获得证书。

Policy Director 故障诊断信息

如果在将 Policy Director 与 Client Security Software 一起使用时遇到问题，则以下故障诊断信息可能有帮助。

问题症状	可能的解决方案
本地策略设置与服务器上的设置不一致	**操作**
Policy Director 允许不受 UVM 支持的某些位配置。因此，配置 PD 服务器时，本地策略要求可以覆盖管理员进行的设置。	这是一个已知限制。
Policy Director 安装设置不可访问	**操作**
Policy Director 设置和本地高速缓存安装设置在 Administrator Utility 的 Policy Setup 页面中不可访问。	安装 Policy Director Runtime Environment。如果 Runtime Environment 没有安装在 IBM 客户机上，则 Policy Setup 页面上的 Policy Director 将不可用。
用户控制对于用户和组都是有效的。	**操作**
配置 Policy Director 服务器时，如果将用户定义到组，且 **Traverse bit** 打开时，则用户控制对于用户和组都是有效的。	不要求操作。

Lotus Notes 故障诊断信息

如果在将 Lotus Notes 与 Client Security Software 一起使用时遇到问题，则以下故障诊断信息可能有帮助。

问题症状	可能的解决方案
对 Lotus Notes 启用 UVM 保护后，Notes 不能完成其安装	**操作**
使用 Administrator Utility 启用 UVM 保护后，Lotus Notes 不能完成安装。	这是一个已知限制。 在 Administrator Utility 中启用 Lotus Notes 支持前，Lotus Notes 必须已配置并处于运行状态。
当尝试更改 Notes 密码时显示错误消息	**操作**
当使用 Client Security Software 时更改 Notes 密码会显示一条错误消息。	重试密码更改。如果这不起作用，请重新启动客户机。
随机生成密码后显示错误消息	**操作**
执行以下操作时会显示一条错误消息: • 使用 Lotus Notes Configuration 工具对 Notes 标识设置 UVM 保护 • 打开 Notes 并使用由 Notes 提供的功能来更改 Notes 标识文件的密码 • 更改密码后立即关闭 Notes	单击 **OK** 以关闭错误消息。不要求其它操作。 与错误消息相反，已更改密码。新密码是由 Client Security Software 创建的随机生成的密码。现在使用随机生成的密码来加密 Notes 标识文件，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 Client Security Software 3.0 或后续版本加密文件时遇到问题，则以下故障诊断信息可能有帮助。

问题症状	可能的解决方案
先前加密的文件将不会解密	**操作**
使用先前版本的 Client Security Software 加密的文件在升级到 Client Security Software 3.0 或后续版本后不解密。	这是一个已知的限制。 在安装 Client Security Software 3.0 或后续版本*之前*，必须解密所有使用前一版本的 Client Security Software 加密的文件。由于其文件加密实现中的更改，Client Security Software 3.0 不能解密使用前一版本的 Client Security Software 加密过的文件。

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，则以下故障诊断信息可能有帮助。

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
当从通用串行总线（USB）端口断开连接 UVM 感知设备，然后将该设备与 USB 端口重新连接时，该设备不会正常工作。	在设备与 USB 端口重新连接后，重新启动计算机。

附录 A. 针对 Client Security Software 的美国出口法规

IBM Client Security Software 软件包已经过 IBM 出口法规办公室（ERO）审核，并按照美国政府出口法规的要求，IBM 已提交合适的文档，并从美国商务部获得针对国际分发（除了美国政府禁运的那些国家或地区）的不超过 256 位加密支持的零售分类许可。美国和其它国家或地区的法规随各个国家或地区政府的不同而更改。

如果不能下载 Client Security Software 软件包，请联系当地的 IBM 销售部，以与 IBM 国家出口法规合作伙伴（ERC）协商。

附录 B. 密码和密码短语规则

本附录包含有关适合于不同系统密码的规则的信息。

硬件密码规则

以下规则适合于硬件密码:

长度 该密码长度必须恰好为八个字符。

字符 该密码必须仅包含字母数字字符。允许字母和数字的组合。不允许特殊字符，如空格、!、?、%。

属性 设置安全芯片密码以启用计算机中的 IBM 嵌入式安全芯片。每次访问 Administrator Utility 时必须输入此密码。

错误尝试

如果十次输入错误的密码，则计算机将锁定 1 小时 17 分钟。这段时间过后，如果您再有十次输入错误的密码，则计算机将锁定 2 小时 34 分钟。每当有十次输入错误的密码后，计算机禁用的时间将加倍。

UVM 密码短语规则

为了提高安全性，UVM 密码短语可以比传统密码更长些且更独特。。

以下规则适合于 UVM 密码短语:

长度 密码短语可以最多长达 256 个字符。

字符 密码短语可以包含键盘产生的任何字符组合，包括空格和非字母数字字符。

属性 UVM 密码短语与您可能用于登录到操作系统的密码不同。UVM 密码短语可以用于与其它认证设备（例如 UVM 感知指纹传感器）联合。

错误尝试

如果您在会话期间多次输入了错误的 UVM 密码短语，则计算机不锁定。对错误尝试的次数没有限制。

附录 C. 声明和商标

本附录给出 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 可能在其它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可用产品和服务的信息，请向您当地的 IBM 代理咨询。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、程序或服务的操作，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中描述的内容有关的各项专利。提供本文档并未授予用户使用这些专利的任何许可证。您可以用书面方式将许可证查询寄往:

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

本条款不适用联合王国或任何这样的条款与当地法律不一致的国家或地区: 国际商业机器公司以“仅此状态”的基础提供本出版物，不附有任何形式的（无论是明示的，还是默示的）保证，包括（但不限于）对非侵权性、适销性和适用于某特定用途的默示保证。某些国家或地区在某些交易中不允许免除明示或默示的保证。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；这些更改将编入本资料的新版本中。IBM 可以随时对本出版物中描述的产品和／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它程序（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，请与以下地址联系: IBM Corporation, Department 80D, P.O. Box 12195, 3039 Cornwallis, Research Triangle Park, NC 27709, U.S.A. 只要遵守适当的条款和条件，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材料均由 IBM 依据 IBM 客户协议、IBM 国际程序许可证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／或其它国家或地区的商标。

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

Microsoft、Windows 和 Windows NT 是 Microsoft Corporation 在美国和／或其它或家或地区的商标。

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。

部件号: 01R2759

中国印刷

(1P) P/N: 01R2759