IBM® Client Security 解决方案

Client Security Software Version 4.0 用户指南

IBM® Client Security 解决方案

Client Security Software Version 4.0 用户指南

第一版（2002 年 3 月）

在使用此信息及其支持的产品之前，请务必阅读第 29 页的附录 B, 『**声明和商标**』。

目录

前言

本指南包含有关在 IBM 网络计算机（也称为 IBM 客户机，包含有 IBM 嵌入式安全芯片）上使用 Client Security Software 的信息。

本指南的内容组织如下:

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

“第 2 章，『对系统登录使用 UVM 保护』，”包含有关对于 Windows XP、Windows NT、Windows 2000 用户使用 UVM 系统登录保护的说明。

“第 3 章，『客户机用户的说明』，”包含有关使用 Client Utility 和设置 Client Security 屏幕保护程序的说明，有关更改 UVM 密码短语和 Windows 密码的说明，以及有关在 Microsoft 和 Netscape 应用程序上使用 Client Security Software 加密功能的信息。

“第 4 章，『故障诊断』，”包含有关解决在使用本指南中提供的说明时可能遇到的问题的有帮助的信息。

“附录 A，『密码和密码短语规则』，”包含 UVM 密码短语和安全芯片密码的规则。

“附录 B，『**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

此指南专供 Client Security 最终用户（客户机用户）使用。在可以使用此指南中的信息之前，必须在您的计算机上安装和设置 Client Security Software。使用数字证书和使用登录以及屏幕保护程序的知识是必需的。

如何使用本指南

请使用此指南来设置 Client Security 屏幕保护程序、更改 UVM 密码短语和系统密码以及使用 Microsoft 和 Netscape 应用程序上的 Client Security 加密功能。本指南是 *《Client Security Software 安装指南》*、*《将 Client Security 与 Policy Director 一起使用》*和 *《Client Security Software 管理员指南》*的参考文档。

本指南中所提供的某些信息也提供在 *《Client Security Software 管理员指南》*中。该 *《管理员指南》*专供在 IBM 客户机上安装和设置 Client Security Software 的安全管理员使用。

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

附加信息

您可以在可用时从 IBM Web 站点 http://www.pc.ibm.com/ww/security/index.html 获取附加信息和安全性产品的更新。

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并存储加密密钥的 IBM 计算机设计的。此软件由应用程序和组件组成，这些应用程序和组件使 IBM 客户机能够通过本地网络、企业或因特网使用客户机安全性。

Client Security Software 应用程序和组件

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

- **Administrator Utility**: Administrator Utility 是管理员用于激活或取消激活嵌入式安全芯片，并用于创建、归档和重新生成加密密钥及密码短语的界面。此外，管理员可以使用此实用程序将用户添加到由 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部件以认证系统用户。例如，UVM 可以使用指纹阅读器进行登录认证。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，指定了客户机用户如何在系统上得到认证。
  - **UVM 系统登录保护**: UVM 软件使管理员能够通过登录界面控制计算机访问。UVM 保护确保只有经安全性策略识别的用户才可以访问操作系统。
  - **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 登录密码以让 UVM 识别，并可以更新密钥压缩文档。用户也可以用 IBM 嵌入式安全芯片创建数字证书的备份副本。

公共密钥基础结构（PKI）功能

Client Security Software 提供在商务中创建公用密钥基础结构（PKI）要求的所有组件，例如:

- **对客户机安全性策略的管理员控制。**认证客户机级别的最终用户是安全性策略的一个重要内容。Client Security Software 提供管理 IBM 客户机的安全性策略要求的界面。此界面是认证软件 User Verification Manager（UVM）的一部分，UVM 是 Client Security Software 的主要组件。
- **公用密钥密码术的加密密钥管理。**管理员用 Client Security Software 创建计算机硬件和客户机用户的加密密钥。创建了加密密钥后，它们通过密钥层绑定到 IBM 嵌入式安全芯片，其中基础级别的硬件密钥用来加密其上方的密钥，包含与每个客户机用户相关的用户密钥。IBM 嵌入式安全芯片上的加密和存储密钥添加客户机安全性的基本附加层，因为这些密钥已安全地绑定到计算机硬件上。
- **受 IBM 嵌入式安全芯片保护的数字证书创建和存储。**当您应用可以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 的应用程序的加密服务供应商。这些应用程序包含 Internet Explorer 和 Microsoft Outlook Express。这确保了数字证书的专用密钥存储在 IBM 嵌入式安全芯片上。Netscape 用户也可以选择 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。使用公用密钥密码术标准（PKCS）#11 的应用程序（例如 Netscape Messenger）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 功能是在原密钥一旦丢失或遭破坏时创建一个可以从其恢复密钥的密钥压缩文档。Client Security Software 提供一个界面，使您能够建立用 IBM 嵌入式安全芯片创建的用于密钥和数字证书的压缩文档，并使您能够在必要时恢复这些密钥和证书。
- **“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方便地加密其文件。

第 2 章 对系统登录使用 UVM 保护

本章包含有关对系统登录使用 UVM 保护的信息。在可以使用 UVM 保护之前，必须对计算机启用该保护。有关对系统登录使用 UVM 保护的信息，请与您的安全管理员联系。

UVM 保护使您能够通过登录界面控制对操作系统的访问。登录过程可能会有所不同，这取决于所使用的操作系统，Windows 2000、Windows XP 或 Windows NT Workstation。

Windows XP、Windows NT 和 Windows 2000 用户

对于 Windows XP、Windows NT 和 Windows 2000，UVM 登录界面代替了 Windows 登录应用程序，这样，如果您尝试解锁计算机，则将打开 UVM 登录界面而不是 Windows 登录窗口。

访问 UVM 登录界面

要访问 UVM 登录界面，请按 **Ctrl + Alt + Delete**。从 UVM 登录界面，您可以进行以下操作:

- 单击 **Shut down** 以关闭计算机
- 单击 **Lock Workstation** 以锁定计算机（有关解锁计算机的信息，请参阅以下内容）
- 单击 **Task Manager** 以打开“任务管理器”
- 单击 **Logoff** 以注销当前用户

解锁客户机

要解锁运行 Windows XP、Windows NT 或 Windows 2000 的客户机（使用了 UVM 保护），请执行以下操作:

1. 按 **Ctrl + Alt + Delete** 来访问 UVM 登录界面。
2. 输入您的用户名和所登录的域，然后单击 **Unlock**。UVM 密码短语窗口打开。

   注: 虽然 UVM 能识别多个域，但您的用户密码对所有的域必须是相同的。
3. 输入您的 UVM 密码短语，然后单击 **OK** 以访问操作系统。
   - 如果 UVM 密码短语与已输入的用户名和域不匹配，则 UVM 登录窗口将再次打开。
   - 如果您对于已输入的用户名和域输入了正确的 UVM 密码短语，则登录成功。

您可能必须输入您的 UVM 密码短语并扫描您的指纹以解锁计算机，这取决于在该计算机的安全性策略中所设置的认证要求。有关更多信息，请与您的安全管理员联系。

第 3 章 客户机用户的说明

本节提供了信息以帮助客户机用户执行以下操作:

- 对系统登录使用 UVM 保护
- 设置 Client Security 屏幕保护程序
- 使用 Client Security Software 来加密文件和文件夹
- 使用 Client Utility
- 使用安全电子邮件和 Web 浏览
- 配置 UVM 声音首选项

本节中的信息也提供在 *Client Security User's Guide* 中。

对系统登录使用 UVM 保护

本节包含有关为 Windows XP、Windows NT 和 Windows 2000 Professional 系统使用 UVM 登录保护的信息。在您可以使用 UVM 保护之前，必须对计算机启用该保护。

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，这样，当用户解锁计算机时，打开的是 UVM 登录窗口，而非 Windows 登录窗口。在对计算机启用 UVM 保护后，每次启动计算机时都会打开 UVM 登录界面。

当计算机正在运行时，可以通过按下 **Ctrl + Alt + Delete** 以关闭或锁定计算机，或者打开“任务管理器”或注销当前用户来访问 UVM 登录界面。

要解锁使用 UVM 保护的 Windows XP、Windows NT 或 Windows 2000 Professional 客户机，请执行以下操作:

1. 按 **Ctrl + Alt + Delete** 来访问 UVM 登录界面。
2. 输入用户名和您所登录的域，然后单击 **Unlock**。

   UVM 密码短语窗口打开。

   注: 虽然 UVM 能识别多个域，但您的用户密码对所有的域必须是相同的。
3. 输入您的 UVM 密码短语，并单击 **OK** 以访问操作系统。如果 UVM 策略需要指纹认证，则显示一条消息提示您进行指纹扫描。

   注: 可能还会需要进一步的认证过程，这取决于客户机的 UVM 策略认证要求。

Client Security 屏幕保护程序

Client Security 屏幕保护程序是计算机在空闲了指定的一段时间后，显示出一系列移动的图像。设置 Client Security 屏幕保护程序是控制通过屏幕保护应用程序来访问计算机的一种方法。一旦 Client Security 屏幕保护程序显示在桌面上，您就必须输入 UVM 密码短语以访问系统桌面。

设置 Client Security 屏幕保护程序

本节包含了有关设置 Client Security 屏幕保护程序的信息。在可以使用 Client Security 屏幕保护程序之前，至少有一个用户必须根据计算机的安全性策略进行注册。

要设置 Client Security 屏幕保护程序，请执行以下操作:

1. 单击**开始 > 设置 > 控制面板**。
2. 单击**显示**图标。
3. 单击**屏幕保护程序**选项卡。
4. 在“屏幕保护程序”下拉菜单中选择 **Client Security**。要更改屏幕保护程序的速度，请单击**设置**并选择希望的速度。
5. 单击**确定**。

Client Security 屏幕保护程序工作情况

Client Security 屏幕保护程序的工作情况根据 UVM Administrator Utility 和 Windows 屏幕保护程序的设置而有所不同。在 Windows XP、Windows NT 和 Windows 2000 下，系统首先检查 Windows 设置，然后检查 UVM Administrator Utility 设置。因此只有在 Windows 屏幕保护程序设置选项卡上选中了**密码保护**复选框，屏幕保护程序才会锁定。

如果选中了此复选框，则系统要求 Windows 密码或 UVM 密码短语，这取决于是否在 Administrator Utility 中选中了 **Use UVM Logon Protection** 复选框。如果已经选中，则系统要求 UVM 密码短语。如果未选中，则系统会要求 Windows 密码。

而且，可能已在计算机的安全性策略中设置了其它认证要求；因此，可能还会要求认证更多。例如，您可能不得不扫描您的指纹以解锁计算机。

注: 如果您禁用 IBM 嵌入式安全芯片或从安全性策略中除去所有用户，则 Client Security 屏幕保护程序将变为不可用。

Client Utility

Client Utility 能使客户机用户执行各种不需要管理员权限的安全性维护任务。

Client Utility 功能

Client Utility 能使客户机用户执行以下操作:

- **更改 UVM 密码短语。**要提高安全性，您可以定期更改 UVM 密码短语。
- **更新 Windows 登录设置。**当用 User Manager 程序更改某个客户机用户的 Windows XP 或 Windows NT 密码时，您也必须通过使用 Client Utility 来更改该密码。如果管理员使用 Administrator Utility 来更改某个用户的 Windows 登录密码，则那个用户以前创建的所有用户加密密钥都将被删除，并且相关联的数字证书也将变为无效。

  注: 更改 Windows 登录密码仅适用于 Windows XP、Windows NT 和 Windows 2000 的用户。
- **注册用户指纹。**如果要使用 UVM 感知指纹传感器（或扫描仪）来进行认证，则您可以通过 UVM 来注册您的指纹。

注: 在您可以通过 UVM 注册指纹之前，必须将指纹扫描仪连接到 IBM 客户机系统。有关如何连接和使用指纹扫描仪的说明，请参考硬件供应商所提供的文档。

- **更新密钥压缩文档。**如果您要创建数字证书并制作存储在 IBM 嵌入式安全芯片上的专用密钥的副本，或者要将密钥压缩文档移动到别的位置，则请更新该密钥压缩文档。
- 配置 UVM 声音首选项

Client Utility 的 Windows XP 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

在以上情况中，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

在以下任何情形中，Windows XP Home Limited User 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

使用 Client Utility

要使用 Client Utility，请执行以下操作:

1. 单击 **开始 > 程序 > IBM Client Security Software > Client Utility**。

   UVM 密码短语窗口打开。
2. 输入需要更改 UVM 密码短语或 Windows 密码的客户机用户的 UVM 密码短语，并单击 **OK**。

   下列窗口打开。
3. 在 **Required information** 区域中，输入为此用户设置的密钥压缩文档的路径。

   注: 在设置了密钥压缩文档后，Administrator Utility 将上次输入的路径植入 **Archive Directory (Path)** 字段。如果 **Archive Directory (Path)** 字段中的信息已删

除，或如果对于要添加的用户来说，该信息是不正确的，则请确保重新输入正确的信息。因为压缩文档目录是必需的信息。

4. 请执行以下操作之一:
   - 要更改 UVM 密码短语，在 **Change UVM Passphrase** 区域里，请在 **Enter new UVM passphrase** 字段中输入新的密码短语。接下来，在 **Confirm UVM passphrase** 字段中再次输入该密码短语，然后单击 **Change**。
   - 要更改 Windows XP、Windows NT 或 Windows 2000 登录密码，请单击 **Update Windows Password** 按钮并在 **Current Windows password** 字段中输入新的 Windows 密码。然后，在 **Confirm Windows password** 字段中再次确认该新密码，并单击 **Update**。有关 Windows NT 登录密码的规则，请参阅操作系统文档。

     注: 只能在“用户管理器”中更改当前已登录的用户的 Windows 登录信息。
   - 要更新密钥压缩文档，请单击 **Update Archive**；然后单击通知您操作已成功的窗口上的**确定**。
   - 要配置 UVM 声音文件，以在认证成功和失败时运行，请选择 **Configure UVM Sounds** 选项卡和 **Enable authentication event sounds** 复选框；然后单击 **Browse** 以选择声音文件以在认证成功和失败时运行。
5. 单击 **OK** 以退出。

使用安全电子邮件和 Web 浏览

如果在因特网上发送未受保护的事务，它们会遭到拦截和读取。您可以通过获取数字证书并使用它进行数字签名和加密电子邮件消息，或保护 Web 浏览器来禁止对您的因特网事务进行未经授权的访问。

数字证书，也称为数字标识或安全性证书，是由认证中心颁发并经过数字签名的电子凭证。当数字证书颁发给您时，认证中心会作为证书的所有者对您的身份进行验证。认证中心是可信的数字证书供应商并可以是第三方发行商，如 VeriSign，或者认证中心可以设置为您公司里的一台服务器。数字证书包含您的身份，例如您的姓名和电子邮件地址、证书到期日、公用密钥副本，以及认证中心的身份和其数字签名。

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

因为 Client Security Software 的使用通常是关于通过支持 Microsoft CryptoAPI 的应用程序（如 Outlook Express）来获取和使用数字证书的内容，所以本节提供的说明是特定于该软件的使用。

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

注: 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。由 Client Security Software 提供的加密强度可在 Administrator Utility 中找到。

获取 Microsoft 应用程序的数字证书

当使用认证中心来创建与 Microsoft 应用程序一起使用的数字证书时，将会提示您选择证书的加密服务供应商（CSP）。

要对 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 embedded Security Subsystem CSP** 做为您的加密服务供应商。这确保了数字证书的专用密钥存储在 IBM 安全芯片上。

此外，如果可用的话，则请选择强（或高）加密以获得更优良的安全性。因为 IBM 嵌入式安全芯片能够对数字证书的专用密钥进行高达 1024 位的加密，所以如果在认证中心界面中此选项是可用的，请选择该选项；1024 位加密也叫做强加密。

在选择了 **IBM embedded Security Subsystem CSP** 做为 CSP 之后，您可能必须输入 UVM 密码短语，扫描指纹或两个步骤都要进行以满足获取数字证书的认证要求。认证要求在计算机的 UVM 策略中定义。

从 Microsoft CSP 转移证书

IBM Client Security Software Certificate Transfer Tool 使您能将用缺省的 Microsoft CSP 创建的证书转移到 IBM 嵌入式安全系统 CSP。这就极大地增强了对于和证书关联的专用密钥提供的保护，因为这些专用密钥现在将安全地存储在 IBM 嵌入式安全芯片而不是脆弱的软件上。

要运行 Certificate Transfer Tool，请完成以下过程:

1. 从安全性软件的根目录（通常是 C:\Program Files\IBM\Security）运行 `xfercert.exe`。主对话框显示了与缺省 Microsoft 软件 CSP 关联的证书。

   注: 只有在创建时其专用密钥标记为 *exportable* 的证书才会显示在此列表中。
2. 选择要转移到 IBM 嵌入式安全系统 CSP 的证书。
3. 按下 **Transfer Certificates** 按钮。

现在证书与 IBM 嵌入式安全系统 CSP 关联并且专用密钥受到 IBM 嵌入式安全芯片的保护。任何使用这些专用密钥的操作（如，创建数字签名或解密电子邮件）都将在芯片保护的环境内执行。

更新 Microsoft 应用程序的密钥压缩文档

创建数字证书之后，请通过更新密钥压缩文档来备份证书。您可以使用 Administrator Utility 来更新密钥压缩文档。

使用 Microsoft 应用程序的数字证书

使用 Microsoft 应用程序中的安全性设置以查看和使用数字证书。有关更多信息，请参阅由 Microsoft 提供的文档。

在创建了数字证书并使用其对电子邮件消息进行签名之后，UVM 将在您第一次对电子邮件消息进行数字签名时提示您需要认证要求。您可能必须输入 UVM 密码短语，扫描指纹或两个步骤都要进行以满足使用数字证书的要求。认证要求在计算机的 UVM 策略中定义。

第 4 章 故障诊断

以下部分提供对防止或识别并纠正使用 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，启用 UVM 登录保护时不要清除或禁用 IBM 嵌入式安全芯片。否则，硬盘的内容将变得不可使用，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。您必须在禁用 UVM 保护以前重新启动计算机。
- 如果启用了 UVM 保护，请不要清除或禁用 IBM 嵌入式安全芯片。否则，硬盘的内容将变得不可使用，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 嵌入式安全芯片时，存储在该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. 输入您的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，每次试图访问 Configuration/Setup Utility 时都会出现一个提示。

重要的: 请将管理员密码记录在安全的地方。如果丢失或忘记了管理员密码，您就不能访问 Configuration/Setup Utility，也不能更改或删除密码，除非卸下计算机机箱盖并移动系统板上的跳线。有关更多信息，请参阅计算机随附的硬件文档。

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，启用 UVM 登录保护时不要清除或禁用 IBM 嵌入式安全芯片。否则，硬盘的内容将变得不可使用，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。您必须在禁用 UVM 保护以前重新启动计算机。
- 如果启用了 UVM 保护，请不要清除或禁用 IBM 嵌入式安全芯片。否则，硬盘的内容将变得不可使用，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 嵌入式安全芯片时，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. 当屏幕上出现 IBM BIOS Setup Utility 提示符时，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。

重要的: 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，您就不能访问 IBM BIOS Setup Utility，也不能更改或删除密码。有关更多信息，请参阅计算机随附的硬件文档。

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 的访问由此密码保护。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以下“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。否则，硬盘的内容将变得不可使用，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。您必须在禁用 UVM 保护以前重新启动计算机。
- 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. 当屏幕上出现 Configuration/Setup Utility 提示出现时，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以下“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。否则，硬盘的内容将变得不可使用，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。您必须在禁用 UVM 保护以前重新启动计算机。
- 清除了 IBM 嵌入式安全芯片时，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 IBM BIOS Setup Utility 提示出现在屏幕上后，请按下 Fn。

   注: 在某些 ThinkPad 机型上，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 的帮助信息。

   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，该用户名将从 Administrator Utility 的用户列表中删除。

使用 Policy Director 控件来拒绝访问所选择的对象

当选择了 Policy Director 控件时，未禁用 **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，则不禁用 **Deny all access to selected object** 复选框。虽然 **Deny all access to selected object** 复选框保持活动，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，所有 Client Security 功能性将丢失。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，则可以继续前必须输入 UVM 密码短语并单击 **OK**。如果输入不正确的 UVM 密码短语（或对指纹扫描提供了不正确的指纹），则会显示错误消息。如果单击 **OK**，将打开 Netscape，但是您不能使用由 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的最新信息，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 与具有 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）的算法的 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: 某些 RC2 算法和其它算法可能不能与 IBM 嵌入式安全芯片证书一起使用，这取决于您的 Outlook Express（128 位）版本是如何配置或更新的。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，则 UVM 保护无法运行: 您可以仅对于 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. 禁用对当前用户标识的 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。

   如果要设置对切换到的用户标识的 UVM 保护，则请继续步骤 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

在以上情况中，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 策略设置为拒绝对认证对象（例如电子邮件解密）的访问，则声明访问被拒绝的消息将根据所使用的软件而有所不同。例如，来自 Outlook Express 的声明对认证对象的访问被拒绝的错误消息，与来自 Netscape 的声明访问被拒绝的错误消息不同。

故障诊断图表

如果 Client Security Software 遇到问题，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 **确定** 退出该窗口。再次开始安装过程以安装 Client Security Software 的新版本。
安装过程中显示一条消息，声明已经安装了 Client Security Software 的先前版本。	单击 **确定** 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。
安装访问由于未知硬件密码被拒绝	**操作**
当用启用的 IBM 嵌入式安全芯片在 IBM 客户机上安装软件时，IBM 嵌入式安全芯片的硬件密码未知。	清除该芯片以继续安装。
无人照管安装不开始	**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开始安装。
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 文件响应不正确	**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。
更改管理员公用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，如果更改管理员公用密钥，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**
更改了管理员公用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 并请求新的证书（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 策略文件以执行更改，然后保存该文件。
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）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 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某些 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
UVM 中登记的用户的 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 识别。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进行解密。 **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。
从具有多个与之相关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相关的证书，这些证书中的一些可能变为无效。如果与证书相关的专用密钥不再存在于生成证书的发送方计算机的 IBM 嵌入式安全芯片上，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**
如果电子邮件消息的作者不具有与其电子邮件帐户相关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相关的证书。有关更多信息，请参阅 Outlook Express 提供的文档。
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）算法进行加密。	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，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 没有更新与证书相关的加密强度	**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 的通讯簿中删除相关的证书。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 中显示解密错误消息	**操作**
可以通过在 Outlook Express 中双击消息来打开该消息。在某些情况下，当过快地双击加密的消息时，会出现解密错误消息。	关闭该消息，然后再次打开加密的电子邮件消息。
当选择加密的消息时也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中单击“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，声明消息不能发送。	关闭错误消息，然后单击**发送**按钮一次。
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进行解密。 **注**: 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 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 嵌入式安全芯片证书，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**。有关更多信息，请参阅由 Netscape 提供的文档。
电子邮件消息将不同的算法返回客户机	**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）算法进行加密。	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。如果输入不正确的 UVM 密码短语，会显示一条错误消息，声明认证故障。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，则与电子邮件相关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 嵌入式安全芯片相关的所有证书的副本。
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，Netscape 延迟	**操作**
如果添加 IBM 嵌入式安全芯片 PKCS#11 模块后打开 Netscape，则在 Netscape 打开之前会发生短时间的延迟。	不要求操作。这仅适用于信息的用途。

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，多次显示 UVM 密码短语窗口或指纹认证窗口	**操作**
UVM 安全性策略指定用户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不止一次显示。	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，会显示与 VBScript 或 JavaScript 相关的错误消息。	重新启动计算机，再次获得证书。

Policy Director 故障诊断信息

如果将 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 不可用。
对于用户和组来说，用户控制都是有效的。	**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
启用 Lotus Notes 的 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。
当试图更改 Notes 密码时显示错误消息	**操作**
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**
执行以下操作时可能会显示错误消息: • 使用 Lotus Notes Configuration 工具来设置对 Notes 标识的 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 **确定** 以关闭该错误消息。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 Notes 标识由随机生成的密码来加密，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 Client Security Software 3.0 或更高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进行解密	**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 或更高版本后不进行解密。	这是一个已知的限制。 在安装 Client Security Software 3.0 或更高版本*之前*，必须解密所有使用先前版本的 Client Security Software 加密的文件。由于其文件加密执行中的更改，Client Security Software 3.0 不能解密使用先前版本的 Client Security Software 加密过的文件。

UVM 感知设备故障诊断信息

如果使用 UVM 感知设备时遇到问题，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，然后将该设备重新连接到 USB 端口，该设备可能不正常工作。	在设备重新连接到 USB 端口后，请重新启动计算机。

附录 A. 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。

不正确尝试

如果十次输入不正确密码，则计算机将锁定 1 小时 17 分钟。这段时间过后，如果您又十次输入不正确密码，则计算机将锁定 2 小时 34 分钟。每回您十次输入不正确密码后，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并且更独特。

以下规则适合于 UVM 密码短语:

长度 密码短语可以最多为 256 个字符长度。

字符 密码短语可以包含键盘产生的任何字符组合，包含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操作系统的密码不同。UVM 密码短语可以与其它鉴别设备（如 UVM 感知指纹传感器）一起使用。

不正确尝试

如果您在会话期间多次输入了不正确的 UVM 密码短语，则计算机将不会锁定。对不正确尝试的次数没有限制。

附录 B. 声明和商标

本附录提供 IBM 产品的法律声明和商标信息。

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，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（无论明示的，还是默示的）保证，包括（但不限于）非侵权性、适销性或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（包含本程序）之间进行信息交换，以及 (ii) 允许对已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。

部件号: 01R2758

中国印刷

(1P) P/N: 01R2758