IBM® Client Security
解决方案

Client Security Software Version 4.0 管理员指南

IBM® Client Security
解决方案

Client Security Software Version 4.0 管理员指南

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 53 页的附录 A，『针对 Client Security Software 的美国出口法规』和第 59 页的附录 D，『**声明和商标**』。

目录

前言

本指南包含有关设置和使用 Client Security Software 提供的安全性功能的信息。

本指南组织如下:

“第 1 章, 『**介绍 IBM Client Security Software**』, ” 包含包含在软件中的软件概述, 以及可以帮助您决定如何使用 Client Security Software 的具体示例。

“第 2 章, 『如何使用 Client Security Software』, ” 包含使用 Client Security Software 提供的组件来设置 IBM 客户机用户要求的安全性功能的示例。

“第 3 章, 『将用户添加到 UVM』, ” 包含有关设置操作系统登录以及将新用户添加到 User Verification Manager（UVM）的 UVM 保护的指示信息。

“第 4 章, 『将用户添加到 UVM 后』, ” 包含有关编辑和保存 IBM 客户机的 UVM 策略的信息。

“第 5 章, 『处理 UVM 策略』, ” 包含有关设置对 Lotus Notes 用户标识的 UVM 保护的指示信息。

“第 6 章, 『使用 Administrator Utility 的其它功能』, ” 包含有关使用 Administrator Utility 功能的指示信息。

“第 7 章, 『针对客户机用户的指示信息』, ” 包含有关使用 Client Security Software 时客户机用户执行的不同任务的指示信息。本章还包含有关使用UVM 登录保护、Client Security 屏幕保护程序、安全电子邮件和 Client Utility 的指示信息。

“第 8 章, 『故障诊断』, ” 包含有关解决使用本指南提供的指示信息时可能遇到的已知限制和问题的有帮助的信息。

“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 UVM 密码短语和安全芯片密码的规则。

“附录 C, 『**对系统登录使用 UVM 保护的规则**』, ” 包含有关使用对操作系统登录的 UVM 保护的信息。

“附录 D, 『**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

本指南提供给将执行以下操作的安全性管理员:

- 设置 IBM 客户机的用户认证
- 设置并编辑 IBM 客户机的 UVM 安全性策略
- 使用 Administrator Utility 来管理安全性子系统（IBM 嵌入式安全芯片）和 IBM 客户机关联的设置

本指南也提供给将使用 IBM SecureWay Policy Director 来管理 UVM 策略中提供的认证对象的 Policy Director 管理员。Policy Director 管理员必须能够管理以下各项:

- Policy Director 对象空间
- 认证、授权和凭证获得过程
- 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

使用本指南以设置 IBM 客户机的用户认证和 UVM 安全性策略。本指南是*《Client Security Software 安装指南》*、*《将 Client Security 与 Policy Director 一起使用》*以及 *Client Security User's Guide* 的姊妹篇。本指南和所有 Client Security 的其它文档可以从 IBM Web 站点下载: http://www.pc.ibm.com/ww/security/secdownload.html。

对《*Client Security Software 安装指南*》的引用

本文档中提供了对*《Client Security Software 安装指南》*的引用。可以使用本指南前，必须在 IBM 客户机上安装 Client Security Software。有关安装该软件的指示信息提供在*《Client Security Software 安装指南》*上。

对《*将 Client Security 与 Policy Director 一起使用*》的引用

本文档中提供了对*《将 Client Security 与 Policy Director 一起使用》*的引用。将使用 Policy Director 来管理 UVM 策略的认证对象的安全性管理员必须阅读*《将 Client Security 与 Policy Director 一起使用》*。

对 *Client Security User's Guide* 的引用

本文档中提供了对 *Client Security User's Guide* 的引用。管理员可以使用本指南来设置和维护使用 Client Security Software 的 IBM 客户机上的 UVM 策略。管理员设置了用户认证和 UVM 安全性策略后，客户机用户可以阅读 *ClientSecurity User's Guide* 以了解如何使用 Client Security Software。

本用户指南包含有关执行 Client Security Software 任务（例如使用 UVM 登录保护、设置 Client Security 屏幕保护程序、创建数字证书和使用 Client Utility）的信息。

附加信息

可从 IBM Web 站点获取附加信息和安全性产品更新（当可用时）: http://www.pc.ibm.com/ww/security/index.html。

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 客户机能够在本地网络、企业或因特网范围内使用客户机安全性。

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元素以认证系统用户。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，这就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，并能够更新密钥压缩文档。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。

公用密钥基础结构（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，它是 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，基础级别硬件密钥用于在其上加密密钥，包括与每台客户机用户关联的用户密钥。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。这些应用程序包括 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 提供使您能够建立用于由 IBM 嵌入式安全芯片创建的密钥和数字证书的压缩文档的界面，并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简便地加密其文件。

第 2 章 如何使用 Client Security Software

管理员可以使用 Client Security Software 提供的多个组件来设置 IBM 客户机用户要求的安全性功能。当规划 Client Security 策略和配置时，请使用以下示例来指导您的思路。例如，Windows NT 用户可以设置对系统登录的 UVM 保护，禁止未经授权的用户登录到 IBM 客户机上。

示例 1 — 一个 Windows NT 4.0 客户机和一个 Windows XP 客户机，两者都使用 Outlook Express

在此示例中，一个 IBM 客户机（客户机 1）安装了 Windows NT 4.0 和 Outlook Express，另一个客户机（客户机 2）安装了 Windows XP 和 Outlook Express。有三个用户将要求客户机 1 上的 UVM 的认证设置；有一个客户机用户将要求客户机 2 上的 UVM 的认证设置。所有客户机用户将注册他们的指纹，以使其可用于认证。在本示例中将安装 UVM 感知指纹传感器。已经确定两个客户机都需要对 Windows 登录的 UVM 保护。管理员决定是否要在每个客户机上编辑并使用本地 UVM 策略。

要设置客户机安全性，请执行以下操作:

1. 在客户机 1 和客户机 2 上安装软件。有关详细信息请参考《*Client Security Software 安装指南*》。
2. 在每个客户机上安装 UVM 感知指纹传感器和任何关联的软件。

   有关 UVM 感知产品的信息，请转至万维网: http://www.pc.ibm.com/ww/security/secdownload.html。
3. 对每个客户机设置 UVM 的用户认证。有关详细信息，请参阅第 8 页的『将用户添加到 UVM』。请执行以下操作:
   a. 通过向用户指定 UVM 密码短语将用户添加到 UVM。由于客户机 1 有三个用户，因此必须重复向 UVM 添加用户的过程，直到添加完所有用户。
   b. 为每个客户机设置对 Windows 登录的 UVM 保护。
   c. 注册用户指纹。因为将设置策略表明三个用户将使用客户机 1，所以三个用户必须注册其指纹。

      注: 如果将指纹设置为认证要求，作为客户机的 UVM 策略的一部分，则每个用户必须注册他的或她的指纹。
4. 在对以下情况要求认证的每台客户机编辑并保存本地 UVM 策略:
   - 登录操作系统
   - 获取数字证书
   - 使用电子邮件消息的数字签名

   有关详细信息，请参阅第 17 页的『编辑本地 UVM 策略』。
5. 重新启动每台客户机以启用对 Windows 登录的 UVM 保护。
6. 通知用户您已为他们设置了 UVM 密码短语，并且已在 IBM 客户机的 UVM 策略中设置了认证要求。

现在用户可以执行以下操作:

- 使用 UVM 保护来锁定和解锁操作系统。

- 请求数字证书，并将嵌入式安全芯片选作与该证书关联的加密服务供应商。
- 使用数字证书来加密用 Outlook Express 创建的电子邮件消息。有关更多信息，请参阅第 31 页的第 7 章，『针对客户机用户的指示信息』。
- 阅读 *Client Security User's Guide* 以了解如何使用 Client Utility。

示例 2 — 使用 Lotus Notes 和 Client Security 屏幕保护程序的两个 Windows 2000 IBM 客户机

在本示例中，两个 IBM 客户机（客户机 1 和客户机 2）都安装了 Windows 2000 和 Lotus Notes。有两个用户将要求客户机 1 上的 UVM 的认证设置；有一个用户将要求客户机 2 上的 UVM 的认证设置。两个客户机都将要求对系统登录的 UVM 保护，且都要对 Lotus Notes 使用 Client Security 屏幕保护程序和 UVM 保护。管理员决定远程客户机的 UVM 策略将在客户机 1 上编辑，然后复制到客户机 2。

要设置客户机安全性，请执行以下操作:

1. 在客户机 1 和客户机 2 上安装软件。因为将使用远程客户机的 UVM 策略，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共密钥。有关软件安装的详细信息，请阅读《Client Security Software 安装指南》。
2. 对每台客户机设置 UVM 的用户认证。有关详细信息，请参阅第 8 页的『将用户添加到 UVM』。然后，执行以下操作:
   a. 通过向用户指定 UVM 密码短语将用户添加到 UVM。由于客户机 1 有两个用户，因此必须重复向 UVM 添加用户的过程，直到添加完两个用户。
   b. 在每台客户机上设置对 Windows 登录的 UVM 保护。
3. 在两台客户机上设置对 Lotus Notes 的 UVM 保护。有关更多信息，请参阅第 12 页的『使用对 Lotus Notes 的 UVM 保护』。
4. 在客户机 1 上编辑和保存远程客户机的 UVM 策略，然后将其复制给客户机 2。UVM 策略将要求用户认证来清除屏幕保护程序、登录到 Lotus Notes 以及登录操作系统。有关详细信息，请参阅第 19 页的『编辑和使用远程客户机的 UVM 策略』。
5. 重新启动对每台客户机启用系统登录的 UVM 保护。
6. 通知客户机用户已对每台客户机设置了 UVM 密码短语和策略。

现在用户可以阅读 Client Security User's Guide 以了解如何执行以下操作:

- 启用 Client Security 屏幕保护程序
- 使用对 Windows 2000 的 UVM 保护

示例 3 — 由 Policy Director 管理并将 Netscape 用于电子邮件的多台 Windows NT 4.0 IBM 客户机

以下示例面向的读者是打算使用 Policy Director 来管理由 UVM 策略设置的认证对象的企业管理员。在本示例中，多台 IBM 客户机都安装了 Windows NT 4.0 和 Netscape 两种软件。所有客户机都安装了 NetSEAT 客户机（一个 Policy Director 组件）。使用 LDAP 服务器的所有客户机都安装了 LDAP 客户机。远程客户机的 UVM 策略将安装在所有客户机上。UVM 策略将启用 Policy Director 来控制为客户机选择的认证对象。

注: 虽然可以在 Windows 98 客户机上安装 NetSEAT 客户机，但您只能在运行 Windows NT 4.0 的 IBM 客户机上将 Policy Director 与 Client Security 软件一起使用。

在本示例中，一个用户将要求每台客户机上的 UVM 的认证设置。所有用户都将注册他们的指纹以便可用于认证。在此示例中将安装 UVM 感知指纹传感器，而所有客户机要求对 Windows 登录的 UVM 保护。

要设置客户机安全性，请执行以下操作:

1. 在 Policy Director 服务器上安装 Client Security 组件。有关详细信息，请参阅《*将 Client Security 与 Policy Director 一起使用*》。
2. 在所有客户机上安装 Client Security Software。由于要使用远程客户机的 UVM 策略，因此当将软件安装在所有客户机上时必须使用相同的管理员公用密钥。有关软件安装的详细信息，请阅读《*Client Security Software 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关联的软件。有关可用的 UVM 感知产品的信息，请转至万维网: http://www.pc.ibm.com/ww/security/secdownload.html。
4. 在每台客户机上设置 UVM 的用户认证。有关详细信息，请参阅第 8 页的『将用户添加到 UVM』。然后，执行以下操作:
   a. 通过向用户指定 UVM 密码短语将用户添加到 UVM。
   b. 在每台客户机上设置对 Windows 登录的 UVM 保护。
   c. 注册每台客户机用户的指纹。如果在 IBM 客户机上要求进行指纹认证，则该客户机的所有用户必须注册其指纹。
5. 在每台客户机上配置 Policy Director 安装信息。有关详细信息，请参阅《*将 Client Security 与 Policy Director 一起使用*》.
6. 在其中一台客户机上编辑并保存远程客户机的 UVM 策略，然后将其复制给其它客户机。设置 UVM 策略，使 Policy Director 可以控制以下认证对象:
   - 登录操作系统
   - 获取数字证书
   - 使用电子邮件消息的数字签名

   有关详细信息，请参阅第 19 页的『编辑和使用远程客户机的 UVM 策略』。
7. 重新启动每台客户机以对启用 Windows 登录的 UVM 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。该模块在使用 Netscape 发送和接收电子邮件消息，并使用 IBM 嵌入式安全芯片获取数字证书的客户机上提供加密支持。有关更多信息，请参阅《*Client Security Software 安装指南*》。
9. 使用 Policy Director 来控制 Policy Director Management Console 中出现的 IBM Client Security Solution 对象。
10. 通知客户机用户已设置了 UVM 密码短语并对每台客户机设置了策略。
11. 建议客户机用户阅读 Client Security User's Guide 以了解如何执行以下操作:
    - 使用 UVM 保护以锁定和解锁操作系统
    - 使用 Client Utility
    - 将使用嵌入式安全芯片的数字证书应用为与证书关联的密码服务供应商
    - 使用数字证书加密用 Netscape 创建的电子邮件消息

第 3 章 将用户添加到 UVM

将用户添加到 UVM 时，以下信息是有用的。

客户机用户的认证

认证客户机级别的最终用户是计算机安全性关注的重要内容。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，它是 Client Security Software 的主要组件。

IBM 客户机的 UVM 安全性策略可以通过两种方式来管理:

- 在本地使用驻留在 IBM 客户机上的策略编辑器
- 在企业范围内使用 Policy Director

添加第一个用户时生成硬件加密密钥。

认证元素

认证元素（例如 UVM 密码短语或用户指纹）用于验证 IBM 客户机的用户。在将用户添加到 UVM 时，您将为该客户机用户指定一个 UVM 密码短语。UVM 密码短语可以长达 256 个字符，它是 UVM 使用的主要认证元素。在指定 UVM 密码短语时，会为该客户机用户创建用户加密密钥并存储在由 IBM 嵌入式安全芯片管理的单个文件中。如果 IBM 客户机为认证使用 UVM 感知设备，则必须用 UVM 注册认证元素（例如用户指纹）。

在用户认证设置过程中，可以选择 Client Security Software 提供的以下安全性功能:

- **对操作系统登录的 UVM 保护。**UVM 保护确保只有 UVM 识别的那些用户才能访问计算机。启用对系统登录的 UVM 保护前，请参阅第 11 页的『UVM 操作系统登录保护』获取重要信息。
- **Client Security 屏幕保护程序。**在添加客户机用户后，该用户可以设置和使用 Client Security 屏幕保护程序。在操作系统软件的“显示”选项设置 Client Security 屏幕保护程序。

将用户添加到 UVM 之前

当将客户机用户添加到 UVM 时，Administrator Utility 将向您提供可从中选择的用户名列表。列表中名称是通过使用操作系统来添加的用户帐户。在将客户机用户添加到 UVM 之前，请使用操作系统软件来创建用户帐户和那些用户的配置文件。Client Security Software 将结合由操作系统提供的安全性功能一起工作。以下列表描述了您可以用来对各个操作系统添加新用户的程序或过程。

- **Windows XP 和 Windows 2000。**请使用“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，请参阅操作系统文档。

  在 Windows XP 中，单击**创建新用户**按钮时不刷新“用户未在 UVM 中登记”字段。您必须退出并重新启动 Administrator Utility 以刷新此字段。
- **Windows NT Workstation 4.0。**请使用“用户管理器” 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，请参阅操作系统文档。

重要:

- 只将那些可以用来登录到操作系统的用户帐户登记到 UVM 中。如果某个用户帐户已登记到 UVM 中却无法用于登录到操作系统，则当启用了 UVM 登录保护时，**所有**用户都将被锁定在系统以外。
- 将新用户帐户登记到 UVM中时，请不要选中**用户下次登录时必须更改密码**复选框。

注:

1. 当您使用操作系统软件来添加新用户时，每个新用户的域密码必须是相同的。
2. 不要将先前更改过 Windows 用户名的用户登记到 UVM 中。UVM 将指向先前的用户名而 Windows 只能识别新用户名。
3. 从 Windows 中删除已登记到 UVM 中的用户帐户后，UVM 登录保护界面会错误地继续将该帐户作为可以用来登录到 Windows 的帐户来列出。此帐户无法用于登录到 Windows。
4. 在已将用户登记到 UVM 中后，请不要更改他的 Windows 用户名。否则，您将不得不把该新用户名重新登记到 UVM 中并请求所有新凭证。

将用户添加到 UVM

Windows XP、Windows 2000 Professional 和 Windows NT 用户必须以管理员权限登录以使用 Administrator Utility。

要将用户添加到 UVM，请完成以下过程:

1. 从 IBM 客户机的 Windows 桌面上单击**开始 > 程序 > IBM Client Security Software > Administrator Utility**。

   显示 Enter the IBM Security Chip password 消息。
2. 输入 IBM 安全芯片密码并单击 **OK**。

   Administrator Utility 窗口打开。
3. 在 **Windows Users Not Enrolled in UVM** 区域中，从列表中选择用户名。

   列表中的用户名是根据在操作系统或网络中创建的用户帐户来定义的。
4. 单击 **Enroll User**。

   显示一条 IBM Security Subsystem Administrator Utility 消息。
5. 单击 **OK**。
6. 输入 Key Storage Directory（Path）或单击 **Browse** 以指向该存储目录，并单击 **Next**。

   显示一条消息表示操作已成功完成。
7. 单击 **OK**。

   Modify Client Security Key Configuration - ISS Key Setup/Archive 窗口打开。
8. 输入 Archive Location 路径或单击 **Browse** 以指向该压缩文档位置，并单击 **Next**。

   注: 如果在系统上启用了 BIOS Administrator Password，则显示一个密码字段。输入 BIOS 管理员密码并按下 **Enter** 键。

   显示一条消息表示操作已成功完成。
9. 单击 **OK**。

   Modify Client Security User Configuration - User Authentication Setup 窗口打开。

10. 输入并确认该用户的初始 UVM 密码短语，然后单击 **Next**。

    注: 在运行 Windows NT、Windows 2000 或 Windows XP 的系统上，**Next** 按钮可能不可用。如果发生此情况，则请单击“Windows 任务栏”上的 **Information** 一项并继续该过程。

    显示一条消息表示操作已成功完成。

11. 单击 **OK**。

    Modify Client Security User Configuration - Windows Logon Password 窗口打开。

12. 在 Windows Password 字段中，请输入与该用户关联的操作系统密码。

    重要: 系统将为用户提供相同的 Windows 密码而与域无关。请确保您输入的密码与用户的当前密码相匹配。不这样做将会导致该用户被系统拒绝访问。

13. 在 Confirm Windows Password 字段中，输入与用户关联的操作系统密码，然后单击 **Next**。

    在将当前已登录的用户登记到 UVM 中时，IBM User Verification Manager 窗口打开。

14. 将 UVM 密码短语输入密码短语字段。

    显示一条消息表示操作已成功完成。

15. 单击 **OK**。

    Modify Client Security User Configuration - UVM Enabled Devices 窗口打开。

    如果未安装指纹设备，则请进入步骤 20。

16. 单击 **Enroll Fingerprints**。

    Fingerprint Registration 窗口打开。

17. 通过单击相应的单选按钮来选择要注册的手和手指。

    Fingerprint Registration 窗口将反映您的选择。

18. 单击 **Start registration**。

19. 将手指放在 UVM 感知指纹传感器上并按屏幕上的指示信息进行操作。

    单击 **Cancel this finger** 来取消指纹扫描。成功注册指纹后将显示一个屏幕。

    注: 如果使用了 Digital Persona 或 OMRON 指纹设备，则必须四次扫描指纹。如果安装了 Targus DEFCON 适配器作为指纹设备，则只要扫描指纹一次。

20. 当完成注册指纹时请单击 **Exit**。

    Modify Client Security User Configuration - Operation Complete 窗口打开。

21. 单击 **Finish**。

    这让您返回 Administrator Utility 主窗口。您现在已经将用户添加到 UVM，创建了客户机的用户加密密钥并注册了用户指纹。要添加其他用户，请重复此过程。

22. 在将新用户添加到 UVM 后，请将为他们设置的 UVM 密码短语通知他们。用户可以通过使用 Client Utility 来更改他们的 UVM 密码短语。有关详细信息，请参阅第 31 页的第 7 章，『针对客户机用户的指示信息』。

第 4 章 将用户添加到 UVM 后

将用户添加到 UVM 后，可以完成额外的 Client Security 功能，如下所述:

- **设置对操作系统登录的 UVM 保护。**有关更多信息，请参阅『设置 UVM 操作系统登录保护』。
- **归档用户加密密钥。**有关更多信息，请参阅第 23 页的『更改密钥压缩文档位置』。
- **设置 Client Security 屏幕保护程序。**有关更多信息，请参阅第 31 页的第 7 章，『针对客户机用户的指示信息』。
- **通过 UVM 来注册用户指纹。**有关更多信息，请参阅第 12 页的『使用 UVM 注册用户指纹』。

  如果在将用户添加到 UVM 之前安装了 UVM 感知指纹传感器，则可以在那时进行指纹注册。

UVM 操作系统登录保护

Windows 操作系统包含提供登录保护的应用程序。UVM 保护设计成与那些 Windows 登录应用程序并行工作。UVM 系统登录保护增强了随操作系统提供的密码功能。对于 Windows XP Professional、Windows NT 和 Windows 2000，UVM 登录界面取代操作系统登录，使得用户每次尝试登录到系统上时都打开 UVM 登录窗口。

设置 UVM 操作系统登录保护

设置和使用对系统登录的 UVM 保护前，请阅读以下信息:

- 如果 UVM 策略指示 Windows NT、Windows 2000 或 Windows XP 系统登录要求指纹认证，而用户未注册指纹，则用户必须注册指纹以登录。如果要求指纹认证而没有连接扫描仪，则登录将失败并且系统将报告错误。

  此外，如果未用 UVM 注册（或注册不正确）用户 Windows 密码，那么用户必须提供正确的 Windows 密码以登录。
- 当启用了 UVM 保护时，不要清除 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。有关更多信息，请参阅第 37 页的第 8 章，『故障诊断』中的 “管理员技巧”。
- 如果清除了 Administrator Utility 中的 **Replace the standard Windows logon with UVM's secure logon** 复选框，则系统返回 Windows 登录过程而无需利用 UVM 登录保护。

设置 UVM 操作系统登录保护

要设置对操作系统的 UVM 保护，请完成以下过程:

1. 从 IBM 客户机的 Windows 桌面上单击**开始 > 程序 > IBM Client Security Software > Administrator Utility**。

   显示 Administrator Utility 主窗口。
2. 单击 **Configure Application Support and Policies**。

   显示 UVM Application and Policy Configuration 屏幕。
3. 选择 **Replace the standard Windows logon with UVM's secure logon** 复选框。

4. 单击 **OK**。
5. 重新启动计算机。

当计算机重新启动时，将提示您登录到计算机。有关 UVM 保护的更多信息，请参阅第 11 页的『UVM 操作系统登录保护』。

使用 UVM 注册用户指纹

当 UVM 策略已编辑成包括指纹认证时，每个用户必须用 UVM 注册指纹。

注: Windows XP 不支持 Digital Persona U.are.U Pro 指纹传感器。

要用 UVM 注册用户指纹，请完成以下 Administrator Utility 过程:

1. 在 UVM 的 Windows Users Enrolled 区域中，从列表中选择一个用户名。
2. 单击 **Edit User**。

   显示 Modify Client Security Key Configuration- Edit UVM User Attributes 窗口。
3. 选择 **Register with UVM-aware device** 并单击 **Next**。

   显示 Modify Client SecurityKey Configuration- UVM Enabled Devices 窗口。
4. 单击 **Register user fingerprints**。
5. 在 Select a hand 区域中，单击 **Left** 或 **Right**。
6. 在 Select a finger 区域中，单击以选择您想要扫描以获取其指纹的手指，然后单击 **Start registration**。
7. 将手指放在 UVM 感知指纹传感器上，并按照屏幕指示信息进行操作。

   取决于扫描仪型号，可能需要对每个指纹扫描四次。单击 **Cancel this finger** 来取消指纹扫描。
8. 指定另一个手指进行注册，或单击 **Exit** 完成。

使用对 Lotus Notes 的 UVM 保护

UVM 提供 Lotus Notes 用户的增强的安全性保护。

启用对 Lotus Notes 用户标识的 UVM 保护

在可启用对 Lotus Notes 的 UVM 保护之前，Notes 必须已安装在 IBM 客户机上，必须为用户建立了 Notes 用户标识和密码，并且此 Notes 用户必须已添加到 UVM。

要设置对 Lotus Notes 的 UVM 保护，请执行以下操作:

1. 从 IBM 客户机的 Windows 桌面上单击**开始 > 程序 > IBM Client Security Software > Administrator Utility**。

   显示 Administrator Utility 主窗口。
2. 单击 **Configure Application Support and Policies**。

   显示 UVM Application 和 Policy Configuration 屏幕。
3. 选择 **Enable Lotus Notes support** 复选框。
4. 单击 **Apply**。
5. 单击 **OK**。

显示 Application Support Actions 屏幕，并出现一条消息表示已启用了 Lotus Notes 支持。

6. 启动 Lotus Notes。

   当 Lotus Notes 启动时，UVM 密码注册完成。

使用 Lotus Notes 中的 UVM 保护

可以使用对 Lotus Notes 的 UVM 保护前，必须按“启用对 Lotus Notes 用户标识的 UVM 保护”中的步骤进行操作。

设置 Lotus Notes 中的 UVM 保护

要设置 Lotus Notes 中的 UVM 保护，请执行以下操作:

1. 登录到 Lotus Notes 中。

   显示 IBM User Verification Manager 窗口。

2. 在可用的字段输入并验证您的 Lotus Notes 密码。

   现在您的 Lotus Notes 密码已通过 UVM 进行了注册。

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 中。
2. 从 Lotus Notes 菜单栏中，单击 **File > Tools > User ID**。

   显示 IBM User Verification Manager 窗口。

3. 输入 UVM 密码短语并单击 **OK**。

   显示 User ID 窗口。

4. 单击 **Set Password**。

   显示 IBM User Verification Manager 窗口。

5. 选择 **Create your own password** 单选按钮。
6. 在可用的字段中输入并验证您的新 Lotus Notes 密码，并单击 **OK**。

注: 将 Lotus Notes 中的密码更改到先前曾经使用的值时，Notes 拒绝密码更改，但是不通知 Client Security Software。因此，UVM 存储 Notes 拒绝的密码。

如果当您在 Lotus Notes 中更改密码时接收到一条消息表示该密码以前已使用过，则您将需要退出 Lotus Notes，启动 Client Utility，并将 Lotus Notes 密码恢复到以前的值。

如果您的 Lotus Notes 密码是随机生成的，而您收到了此错误消息，但您没办法知道该密码是什么，因此无法手工将其重新设置。您必须向管理员请求一个新的标识文件或恢复以前保存过的标识文件的副本。

禁用对 Lotus Notes 用户标识的 UVM 保护

如果想禁用对 Lotus Notes 用户标识的 UVM 保护，请执行以下操作:

1. 从 IBM 客户机的 Windows 桌面上单击**开始 > 程序 > IBM Client Security Software > Administrator Utility**。

   显示 Administrator Utility 主窗口。

2. 单击 **Configure Application Support and Policies**。

显示 UVM Application and Policy Configuration 屏幕。

3. 不选择 **Enable Lotus Notes support** 复选框。
4. 单击 **OK**。

   显示 Application Support Action 屏幕，并有消息指示禁用了 Lotus Notes 支持。

设置对切换的 Lotus Notes 用户标识的 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 Lotus Notes。
2. 禁用对当前用户标识的 UVM 保护。有关详细信息，请参阅第 13 页的『禁用对 Lotus Notes 用户标识的 UVM 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. 要为已转换到的用户标识设置 UVM 保护，请进入 Lotus Notes Configuration 工具（由 Client Security Software 提供），并设置 UVM 保护。请参阅第 13 页的『使用 Lotus Notes 中的 UVM 保护』。

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

由于 Client Security Software 的使用通常是关于使用支持 PKCS#11 的应用程序（特别是 Netscape 应用程序）来获取和使用数字证书，因此本部分中提供的指示信息特定于 Client Security Software 的使用。

有关如何使用 Netscape 应用程序的安全性设置的详细信息，请参阅 Netscape 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。可以在 Administrator Utility 中通过单击 **Chip Settings** 按钮查找 Client Security Software 提供的加密强度。

安装 Netscape 应用程序的 IBM 嵌入式安全芯片 PKCS#11 模块

可以使用数字证书前，必须将 IBM 嵌入式安全芯片 PKCS#11 模块安装到计算机上。因为安装 IBM 嵌入式安全芯片 PKCS#11 模块要求 UVM 密码短语，所以必须至少将一个用户添加到计算机的安全性策略。

要安装 IBM 嵌入式安全芯片 PKCS#11 模块，请完成以下步骤:

1. 从 IBM 客户机的 Windows 桌面上单击**开始 > 程序 > IBM Client Security Software > Administrator Utility**。

   显示 Administrator Utility 主窗口。
2. 单击 **Configure Application Support and Policies**。

   显示 UVM Application and Policy Configuration 屏幕。
3. 选中 **Enable Netscape support** 复选框。
4. 单击 **Apply**。

   显示 Application Support Action 屏幕，并有消息指示启用了 Entrust 支持。
5. 单击 **OK**。

使用 Netscape 应用程序的 PKCS#11 登录保护

当设置了计算机的 PKCS#11 登录保护时，每次登录到 Netscape 时必须要符合认证要求。可能必须输入 UVM 密码短语和／或扫描指纹以符合认证要求。认证要求在计算机的 UVM 策略中定义。

选择 IBM 嵌入式安全芯片以生成 Netscape 应用程序的数字证书

在 Netscape 内生成数字证书时，请选择 IBM 嵌入式安全芯片作为与证书关联的专用密钥的生成器。

在数字证书创建过程中，会被要求选择希望在其中生成密钥的卡或数据库，请选择 **IBM embedded Security Subsystem**。

有关生成数字证书和将证书与 Netscape 一起使用的更多信息，请参阅 Netscape 提供的文档。

更新 Netscape 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。可以使用 Client Utility 更新密钥压缩文档。

使用 Netscape 应用程序的数字证书

使用 Netscape 应用程序中的安全性设置来查看、选择和使用数字证书。例如，在 Netscape Messenger 的安全性设置中，必须在可以使用它对电子邮件消息进行数字签名或加密之前选择证书。有关更多信息，请参阅由 Netscape 提供的文档。

安装了 IBM 嵌入式安全芯片 PKCS#11 模块之后，每次使用数字证书时 UVM 都会提示需要认证要求。可能必须输入 UVM 密码短语和／或扫描指纹以符合认证要求。认证要求在计算机的 UVM 策略中定义。

如果不符合 UVM 策略设置的认证要求，则显示一条错误消息。如果单击此消息上的 **OK** 时，将打开 Netscape，但是重新启动 Netscape 并提供正确的 UVM 密码短语和／或指纹前不能使用由 IBM 嵌入式安全芯片生成的数字证书。

第 5 章 处理 UVM 策略

尝试编辑本地客户机的 UVM 策略前，请确保 UVM 中至少登记了一个用户。否则，当策略编辑器尝试打开本地策略文件时，将显示一条错误消息。

将用户添加到 UVM 后，必须编辑并保存每个 IBM 客户机的安全性策略。Client Security Software 提供的安全性策略称为 UVM 策略，它结合了 “将用户添加到 UVM” 中提供的设置和客户机级别的认证要求。UVM 策略可用于本地或跨多个客户机远程控制客户机的安全性策略。

Administrator Utility 具有一个内置 UVM 策略编辑器，可以用来编辑并保存本地客户机或远程客户机的 UVM 策略。IBM 客户机执行的任务（例如登录到操作系统或清除屏幕保护程序），称为认证对象，并且这些对象必须已在 UVM 策略内将认证要求分配给它们。例如，可以设置 UVM 策略以要求以下操作:

- 每个用户必须输入 UVM 密码短语，并使用近似徽标认证以登录到操作系统。
- 每次获得数字证书时，每个用户必须输入 UVM 密码短语。

当在 UVM 策略中进行设置时，Policy Director 将控制特殊的认证对象。

UVM 策略为 IBM 客户机（而非个别用户）设置认证对象的要求。因此，如果您设置 UVM 策略以要求认证对象（例如操作系统登录）的指纹时，则添加到 UVM 的每个用户必须注册指纹以使用该对象。有关添加用户的详细信息，请参阅第 8 页的『将用户添加到 UVM』。

保存在文件中的 UVM 策略命名为 globalpolicy.gvm。要在远程客户机上使用 UVM，UVM 策略必须存储在一个 IBM 客户机上，然后复制到其它客户机。使用远程客户机上的 UVM 策略可以节省在其它客户机上设置 UVM 策略的时间。

编辑本地 UVM 策略

编辑本地 UVM 策略并将它仅用于对其进行编辑的客户机上。如果将 Client Security 安装在其缺省位置，则本地 UVM 策略存储为 \Program Files\IBM\Security\UVM_Policy\globalpolicy.gvm。请使用 UVM 策略的编辑器来编辑和保存本地 UVM 策略。只有已添加到 UVM 的用户可以使用 UVM 策略编辑器。Administrator Utility 中提供了 UVM 策略编辑器的界面。

当保存对 UVM 策略的更改时，会显示一条要求管理员专用密钥的消息。输入管理员专用密钥并单击 **OK** 以保存更改。如果提供的管理员专用密钥不正确，则不会保存更改。

认证基于您在策略编辑器中选择的内容而发生。例如，如果选择 Lotus Notes 登录的 “No passphrase required after 1st used this way”，然后无论何时登录到 Lotus Notes 时，它将要求 UVM 认证。直至您重新引导或注销，此后每次访问 Lotus Notes，将不要求该密码短语。

当设置 UVM 策略以要求对认证对象（例如操作系统登录）提供指纹时，添加给 UVM 的每个用户必须已注册其指纹以使用该对象。

编辑 UVM 策略时，可以通过单击 UVM Policy Summary 来查看策略摘要信息。同时还可以单击 **Apply** 以保存更改。在单击 **Apply** 后，会显示一条消息提示您需要管理员专用密钥。输入管理员专用密钥并单击 **OK** 以保存更改。如果提供的管理员专用密钥不正确，则不会保存更改。

UVM 策略对象

UVM 策略对象使您能够建立不同用户操作的不同的安全性策略。

有效的 UVM 策略对象包含以下各项:

System Logon
此对象控制登录到系统所必需的认证要求。

System Unlock
此对象控制清除 Client Security 屏幕保护程序所必需的认证要求。

Netscape - PKCS#11 Logon
此对象控制 PKCS#11 模块接收到 PKCS#11 C_OpenSession 呼叫时所必需的认证要求。大多数用户必须将此设置保留为 “No passphrase required after 1st used this way.”。

Lotus Notes Logon
此对象控制登录到 Lotus Notes 所必需的认证要求。

Lotus Notes Change Password
此对象控制使用 UVM 以生成随机 Lotus Notes 密码所必需的认证要求。

Digital Signature（e-mail）
此对象控制单击 Microsoft Outlook 或 Outlook Express 中的 “签名” 按钮时所必需的认证要求。

Decryption（e-mail）
此对象控制单击 Microsoft Outlook 或 Outlook Express 中的 “解密” 按钮时所必需的认证要求。

Acquire Digital Certificate
此对象控制获取数字证书所必需的认证要求。

File and Folder Protection
此对象控制右键单击选择的加密和解密时所必需的认证要求。

Entrust Logon
此对象控制 Entrust 造成 PKCS#11 模块接收到 PKCS#11 C_OpenSession 呼叫时所必需的认证要求。大多数用户必须将此设置保留为 “No passphrase required after 1st used this way.”。

Change Entrust Logon Password
此对象控制更改 Entrust 登录密码所必需的认证要求。Entrust 通过造成 PKCS#11 模块接收到 PKCS#11 C_OpenSession 呼叫来执行此操作。大多数用户必须将此设置保留为 “No passphrase required after 1st used this way.”。

启动 UVM 策略编辑器

要启动 UVM 策略编辑器，请完成以下 Administrator Utility 过程:

1. 单击 **Configure Application Support and Policy** 按钮。

2. 单击 **Policy Configuration** 按钮。
3. 在 UVM Policy 区域中，选择 **Local Client**，然后单击 **Edit UVM Policy**。

   Global Policy Access Password 窗口打开。
4. 输入 password 然后按下 Enter 键。

   UVM 策略文件的缺省访问密码是单词 password。在编辑 UVM 策略后，可以更改访问密码。有关更多信息，请参阅第 21 页的『更改 UVM 策略文件的密码』。
5. 在 Policy Selection 页面上，从下拉菜单中选择 UVM 策略文件（globalpolicy.gvm）。
6. 单击 **Object Selection** 选项卡，然后单击 **Action** 或 **Object Type**，并选择您想要为其指定认证要求的对象。

   操作包含 System Logon、System Unlock 和 E-mail Decryption; 对象类型的一个示例是 Acquire Digital Certificate。
7. 对于选择的每个对象，请执行以下操作:
   - 单击 **Authentication Elements** 选项卡，然后编辑想要指定给对象的可用认证元素的设置。
   - 选择 **Policy Director controls selected object** 以使 Policy Director 能够控制所选择的对象。仅在您想让 Policy Director 控制 IBM 客户机的认证元素时才选择该选项。有关更多信息，请参阅*《将 Client Security 与 Policy Director 一起使用》*。

     重要: 如果使 Policy Director 能够控制对象，则您要将控制权交给 Policy Director 对象空间。如果这样做，您必须重新安装 Client Security Software 以重新建立对该对象的本地控制。
   - 选择 **Deny all access to selected object** 以拒绝访问所选择的对象。
8. 单击 **Information** 选项卡并输入系统名称、用户详细信息，以及系统和企业管理员详细信息的信息。
9. 单击 **Policy Selection** 选项卡并单击 **UVM Policy** 按钮。

   Save 和 **Save as** 按钮变成可用的。
10. 执行以下操作之一:
    - 单击 **Save** 以保存策略文件并按照屏幕上的指示信息进行操作。
    - 单击 **Save as** 以新密码保存文件。有关更改密码的更多信息，请参阅第 21 页的『更改 UVM 策略文件的密码』。

      保存更改后，会显示一条要求管理员专用密钥的消息。输入管理员专用密钥并单击 **OK** 以继续。如果提供的管理员专用密钥不正确，则不会保存更改。
11. 单击 **OK** 以保存更改并退出。

编辑和使用远程客户机的 UVM 策略

要使用跨多台 IBM 客户机的 UVM 策略，请编辑并保存远程客户机的 UVM 策略，然后将 UVM 策略文件复制到其它 IBM 客户机。如果将 Client Security 安装在其缺省位置，则远程 UVM 策略文件将存储为 \Program Files\IBM\Security\UVM_Policy\remote\globalpolicy.gvm。必须在创建 \remote 子目录及其内容前保存 UVM 策略文件。

请使用 UVM 策略编辑器来编辑和保存远程客户机的 UVM 策略。Administrator Utility 中提供了 UVM 策略编辑器的界面。只有已添加到 UVM 的用户可以使用 UVM 策略编辑器。

当保存对 UVM 策略的更改时，会显示一条消息，请求管理员专用密钥。输入管理员专用密钥并单击 OK 以保存更改。如果提供的管理员专用密钥不正确，则不会保存更改。

当设置 UVM 策略要求远程客户机以提供要求认证对象（如操作系统登录）的指纹时，每个用户必须具有注册的指纹以使用该对象。所有使用策略的远程客户机都必须安装了 UVM 感知指纹传感器。

在编辑 UVM 策略文件的同时，通过单击 **UVM Policy Summary** 可以查看策略摘要信息。同时还可以单击 **Apply** 以保存更改。如果单击 **Apply**，会显示一条消息，提示您需要管理员专用密钥。输入管理员专用密钥并单击 **OK** 以保存更改。如果提供的管理员专用密钥不正确，则不会保存更改。

要启动 UVM 策略编辑器，请完成以下 Administrator Utility 过程:

1. 单击 **Configure Application Support and Policy** 按钮。
2. 单击 **Policy Configuration** 按钮。
3. 在 UVM Policy 区域，请选择 **Remote Clients**，然后单击 **Edit UVM Policy**。

   Global Policy Access Password 窗口打开。
4. 输入 `password` 然后按下 Enter 键。

   UVM 策略文件的缺省访问密码是单词 password。在编辑 UVM 策略后，可以更改访问密码。有关更多信息，请参阅第 21 页的『更改 UVM 策略文件的密码』。
5. 在 Policy Selection 页面上，从下拉菜单中选择 UVM 策略文件（globalpolicy.gvm）。
6. 单击 **Object Selection** 选项卡，单击 **Action** 或 **Object Type**，然后选择想要指定认证要求的对象。

   操作包含 System Logon、System Unlock 和 E-mail Decryption; 对象类型的一个示例是 Acquire Digital Certificate。
7. 对于选择的每个对象，请执行以下操作之一:
   - 单击 **Authentication Elements** 选项卡，然后编辑想要指定给对象的可用认证元素的设置。
   - 选择 **Policy Director controls selected object** 以使 Policy Director 能够控制所选择的对象。仅在您想让 Policy Director 控制 IBM 客户机的认证元素时才选择该选项。有关更多信息，请参阅*《将 Client Security 与 Policy Director 一起使用》*。

     重要: 如果使 Policy Director 能够控制对象，则您要将控制权交给 Policy Director 对象空间。如果这样做，您必须重新安装 Client Security Software 以重新建立对该对象的本地控制。
   - 选择 **Deny all access to selected object** 以拒绝访问选择的对象。
8. 单击 **Information** 选项卡并输入系统名称、用户详细信息，以及系统和企业管理员详细信息的信息。
9. 单击 **Remote Configuration** 选项卡。选择在将使用此 UVM 策略的远程客户机上可用的认证元素。

   对于 Policy Director 管理员: 如果 Policy Director 启用了远程客户机，请选择 **Policy Director enabled client** 复选框。

10. 单击 **Policy Selection** 选项卡并单击 **UVM Policy** 按钮。

    Save 和 **Save as** 按钮变成可用的。

11. 执行以下操作之一:
    - 单击 **Save** 以保存策略文件。
    - 单击 **Save as** 以新密码保存文件。有关更改密码的信息，请参阅『更改 UVM 策略文件的密码』。

    保存更改后，会显示一条要求管理员专用密钥的消息。

12. 输入管理员专用密钥并单击 **OK** 以继续。

    如果提供的管理员专用密钥不正确，则不会保存更改。

13. 单击 **OK** 以保存更改并退出。
14. 将以下文件复制到将使用此 UVM 策略的其它远程 IBM 客户机上:
    - \IBM\Security\UVM_Policy\remote\globalpolicy.gvm
    - \IBM\Security\UVM_Policy\remote\globalpolicy.gvm.sig

如果已将 Client Security Software 安装在其缺省位置，则前面的根目录为 \Program Files。将这两个文件都复制到远程客户机上的 \IBM\Security\UVM_Policy\ 目录路径。

更改 UVM 策略文件的密码

要保护 UVM 策略设置，您可以更改 UVM 策略文件的访问密码。每次进入 UVM 策略编辑器时，必须输入访问密码。

以下指示信息假定您已进入 UVM 策略编辑器并且已准备好保存 UVM 策略文件。

要更改 UVM 策略文件的密码，请完成以下过程:

1. 选择 UVM 策略文件（globalpolicy.gvm）并单击 **UVM Policy** 按钮。
2. 单击 **Save as** 以新密码保存文件。

   Save as 窗口打开。在保存了文件以后，将显示一条消息要求您验证是否要用新的名称来保存该文件。

   要更改 UVM 策略概要文件的当前密码，请指定当前的 UVM 策略文件（...\IBM\Security\UVM_Policy\globalpolicy.gvm）。

3. 单击 **OK**。
4. 在 Access Password 字段中，输入 UVM 策略文件的当前密码并单击 **Change Password**。

   如果没有在 Access Password 字段中输入当前密码，则显示一条错误消息。Access Password 窗口再次打开。

5. 在 New Password 字段中，输入新密码。

   策略密码可以是长度最多为 255 个字符的字母数字字符的任意组合。

6. 在 Verify Password 字段中，再次输入新密码并按下 Enter 键。

第 6 章 使用 Administrator Utility 的其它功能

当在 IBM 客户机上设置 Client Security Software 时，请使用 Administrator Utility 来启用 IBM 嵌入式安全芯片，设置安全芯片密码，生成硬件密钥，以及设置安全性策略。本部分提供有关使用其它 Administrator Utility 功能的指示信息。

要打开 Administrator Utility，请完成以下步骤:

1. 从 IBM 客户机的 Windows 桌面上单击**开始 > 程序 > IBM Client Security Software > Administrator Utility**。

   由于对 Administrator Utility 的访问受安全芯片密码的保护，因此显示一条消息要求您输入安全芯片密码。
2. 输入安全密码，然后单击 **OK**。

更改密钥压缩文档位置

当第一次创建了密钥压缩文档时，就创建了所有密钥的副本并将它们保存到在安装时指定的位置。

注: 客户机用户还可以使用 Client Utility 来更改密钥压缩文档位置。有关更多信息，请参阅第 31 页的第 7 章，『针对客户机用户的指示信息』。

要更改密钥压缩文档位置，请完成以下 Administrator Utility 过程:

1. 单击 **Key Configuration** 按钮。
2. 单击 **Change the archive location** 单选按钮。

   显示 Modify Client Key Configuration- New Key Archive Location 屏幕。
3. 输入新路径，或单击 **Browse** 以选择路径。
4. 单击 **Next**。
5. 单击 **Finish**。

更改压缩文档密钥对

当第一次创建了压缩文档密钥对时，它通常存储在软盘上或可以让多个用户访问的共享目录中。如果该压缩文档密钥对损坏了，则您可以更改成不同的压缩文档密钥对。

注: 在更改压缩文档密钥对之前，务必更新压缩文档。

要更改压缩文档密钥对，请完成以下 Administrator Utility 过程:

1. 单击 **Key Configuration** 按钮。

   显示 Modify Client Security Key Configuration 屏幕。
2. 单击 **Change IBM Security Subsystem Archive keypair** 单选按钮。

   Modify Client Security Key Configuration - New UVM Administrator Public Key File 窗口打开。
3. 在 New ISS Archive Public Key File 字段中，输入新的压缩文档密钥对的文件名。还可以单击 **Browse** 来搜索文件，或单击 **Create** 来生成新的压缩文档密钥对。

注: 请确保在不包含 Old ISS Archive Private Key 文件的位置创建新的管理员公用密钥。

4. 在 Old ISS Archive Private Key File 字段中，输入压缩文档密钥对的文件名，或单击 **Browse** 以搜索文件。
5. 在 Archive Directory (Path) 字段中，输入密钥压缩文档所存储的路径，或单击 **Browse** 以选择路径。
6. 单击 **Next**。

   注: 如果压缩文档密钥对分割为多个文件，则显示一条消息，要求您输入每个文件的位置和名称。在 Key File 字段中输入每个文件名之后，请单击 **Read Next**。
7. 单击 **OK**。

恢复密钥

如果已更换系统板或硬盘驱动器出故障，您可能需要恢复密钥。在恢复密钥时，您要从密钥压缩文档复制最新的用户密钥文件并将其存储在 IBM 嵌入式安全芯片上。这些复制的用户密钥文件出现在它们先前在计算机上所存储的目录中，例如网络目录或软盘。

从压缩文档恢复加密密钥

如果将计算机中的系统板更换为包含 IBM 嵌入式安全芯片的系统板，并且加密密钥在硬盘驱动器上仍然有效，则可以通过使用 IBM 嵌入式安全芯片“重新加密”先前与计算机关联的加密密钥来在新的系统板上恢复这些加密密钥。

在启用新的芯片并设置安全芯片密码后可执行密钥恢复。有关详细信息，请参阅第 28 页的『启用 IBM 嵌入式安全芯片和设置安全芯片密码』。

要在更换系统板后恢复密钥，请完成以下 Administrator Utility 过程:

1. 单击 **Key Configuration** 按钮。
2. 单击 **Restore IBM Security Subsystem keys from archive**，然后单击 **Next**。
3. 在 Archive Directory (Path) 字段中，输入管理员公用密钥的路径和文件名，或单击 **Browse** 来搜索文件。
4. 在 ISS Archive Private Key File 字段中，输入管理员专用密钥的路径和文件名，或单击 **Browse** 以搜索文件。
5. 单击 **Next**。

   显示一条消息表明操作已成功完成。

   注: 如果管理员专用密钥分割成多个文件，则显示一条消息，要求您输入每个文件的位置和名称。在 Key File 字段中输入每个文件后，单击 **Read Next**。
6. 单击 **OK**。
7. 单击 **Finish**。

注: 如果在恢复压缩文档后更改管理员密钥对，则显示错误消息。如果发生这种情况，则必须将用户添加到 UVM，然后请求新证书。

从密钥压缩文档恢复用户密钥

如果计算机的硬盘驱动器故障破坏了用户密钥的完整性，则可以从密钥压缩文档恢复密钥。恢复密钥将覆盖已存储的任何密钥。

注: 密钥恢复后，UVM 登录自动启用。因此，如果要求 UVM 登录的指纹认证，则在恢复之后的重新引导前“必须”安装指纹软件，以避免锁定在系统之外。

下列指示信息假定 Administrator Utility 未受硬盘驱动器故障的损坏。如果硬盘驱动器故障破坏了客户机安全性文件，则可能需要重新安装 Client Security Software。

要从密钥压缩文档恢复用户密钥，请完成以下 Administrator Utility 过程:

1. 单击 **Key Configuration** 按钮。
2. 单击 **Restore IBM Security Subsystem keys from archive** 单选按钮。

   Modify Client Security Key Configuration - Restore All IBM Security Subsystem Keys 窗口打开。
3. 在 Archive Directory (Path) 字段中，输入管理员公用密钥的路径，或单击 **Browse** 以定位文件。
4. 在 ISS Archive Private Key File 字段中，输入管理员专用密钥的路径和文件名，或单击 **Browse** 以定位文件。
5. 单击 **Next**。

   显示一条消息，表明操作已成功完成。

   注: 如果管理员专用密钥分割为多个文件，则显示一条消息，要求您输入每个文件的位置和名称。在 Key File 字段中输入每个文件后，单击 **Read Next**。
6. 单击 **OK**。
7. 单击 **Finish**。

复位认证故障计数器

要为某个用户复位认证失败计数器，请完成以下 Administrator Utility 过程:

1. 在 UVM 区域登记的 Windows 用户中，选择用户。
2. 单击 **Reset Fail Count**。
3. 输入所选择用户的 UVM 密码短语，并单击 **OK**。

   显示一条消息，通知您操作成功。
4. 单击 **OK**。

更改 Policy Director 安装信息

以下信息旨在面向计划使用 Policy Director 来管理 UVM 安全性策略的认证对象的安全性管理员。有关更多信息，请参阅*《将 Client Security 与 Policy Director 一起使用》*。

编辑 Policy Director 安装信息

要在 IBM 客户机上配置 Policy Director 安装信息，请完成以下 Administrator Utility 过程:

1. 单击 **Configure Application Support and Policy** 按钮。
2. 单击 **Policy Configuration** 按钮。
3. 选择您将使用的服务器注册表的 DCE 或 LDAP。
4. 对与所选择的服务器注册表相关的每个字段，输入适当的信息。

刷新本地高速缓存

由 Policy Director 管理的安全性策略信息的本地副本保留在 IBM 客户机上。可以按月份和天数的增量设置本地高速缓存的刷新率，或者可以单击按钮来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 Administrator Utility 过程:

1. 单击 **Configure Application Support and Policy** 按钮。
2. 单击 **Policy Configuration** 按钮。
3. 执行以下操作之一:
   - 要刷新本地高速缓存，请单击 **Refresh NOW**。
   - 要设置刷新率，请在提供的字段中输入月数和天数。月数和天数的值代表已调度的刷新之间的时间量。

恢复 UVM 密码短语

UVM 密码短语为添加到 IBM 客户机的安全性策略中的每个用户而创建。由于密码短语可能会丢失或忘记，或者可能由客户机用户更改，因此 Administrator Utility 提供了一种恢复密码短语的方式。

要恢复密码短语，请完成以下 Administrator Utility 过程:

1. 从 Windows Users Enrolled in UVM 字段中选择一个用户。
2. 单击 **Recover Passphrase** 按钮。

   Recover Passphrase 窗口打开。
3. 在 IBM Security Subsystem Key Archive 字段中，输入管理员公用密钥的路径和文件名，或单击 **Browse** 以定位文件。
4. 在 IBM Security Subsystem Archive Private Key file 字段中，输入管理员专用密钥的路径和文件名。
5. 单击 **OK**。

   显示一条消息，向您显示用户的 UVM 密码短语。

如果将管理员专用密钥分割成多个文件，则显示一条消息，要求您输入每个文件的位置和名称。在 Key File 字段中输入每个文件后，单击 **Read Next**。

更改 IBM 安全芯片密码

您必须设置安全芯片密码以启用 IBM 嵌入式安全芯片。对 Administrator Utility 的访问也受安全芯片密码的保护。为了提高安全性，请定期更改安全芯片密码。长时间保持不变的密码可能更容易被外部攻击。有关安全芯片密码规则的信息，请参阅第 55 页的附录 B, 『密码和密码短语规则』。

要更改 Security Chip 密码，请完成以下 Administrator Utility 过程:

1. 单击 **Chip Settings** 按钮。

   显示 Modify IBM Security Chip Settings 屏幕。

2. 单击 **Change chip password**。

   Change IBM Security Chip password 窗口打开。

3. 在 New password 字段中，输入新密码。
4. 在 the Confirmation 字段中，再次输入密码。
5. 单击 **OK**。

   显示一条消息，通知您操作成功。

   注意: 不要按 Enter 键或 Tab > Enter 以保存更改。如果这样做，则 Disable chip 窗口会打开。如果 Disable chip 窗口打开，请不要禁用该芯片；而是退出该窗口。

6. 单击 **OK**。

查看关于 Client Security Software 的信息

有关 IBM 嵌入式安全芯片和 Client Security Software 的以下信息，可以通过 Chip Setup 屏幕获得:

- 嵌入式安全芯片的加密状态
- IBM 嵌入式安全芯片的状态
- 与 Client Security Software 一起使用的固件的版本号
- 硬件加密密钥的有效性

要查看客户机安全性信息，请完成以下 Administrator Utility 过程:

1. 单击 **Chip Settings** 按钮。

   Modify IBM Security Chip Settings 窗口打开，它包含有关软件和 IBM 安全芯片状态的信息。

2. 单击 **Refresh** 以验证状态。
3. 单击 **close** 以退出。

禁用 IBM 嵌入式安全芯片

Administrator Utility 提供禁用 IBM 嵌入式安全芯片的方法。因为要求安全芯片密码来启动 Administrator Utility 和禁用芯片，所以请保护安全芯片密码以禁止未经授权的用户禁用芯片。

重要: 如果已对系统登录启用了 UVM 保护，则不要禁用芯片。如果这样做，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，然后单击 **Replace the standard Windows logon with UVM's secure logon** 复选框。必须重新启动计算机，才能对系统登录禁用 UVM 保护。

要禁用嵌入式安全芯片，请完成以下 Administrator Utility 过程:

1. 单击 **Chip Settings** 按钮。
2. 单击 **Disable Chip** 按钮，并按照屏幕上的指示信息操作。
3. 如果计算机启用了“增强安全性”，则您可能必须输入在 Configuration/Setup Utility 中设置的管理员密码以禁用该芯片。

要在芯片禁用后使用 IBM 嵌入式安全芯片和硬件加密密钥，必须重新启用芯片。

启用 IBM 嵌入式安全芯片和设置安全芯片密码

在安装软件之后，如果需要启用 IBM 嵌入式安全芯片，则可以使用 Administrator Utility 来重新设置安全芯片的密码并设置新的加密密钥。

在系统板更换后或者如果禁用了 IBM 嵌入式安全芯片，则可能需要启用该芯片以恢复密钥压缩文档。

要启用芯片并设置安全芯片密码，请完成以下过程:

1. 从 IBM 客户机的 Windows 桌面上单击**开始 > 程序 > IBM Client Security Software > Administrator Utility**。

   显示一条消息，要求启用 IBM 客户机的 IBM 嵌入式安全芯片。
2. 单击 **Yes**。

   显示一条消息要求重新启动计算机。在 IBM 嵌入式安全芯片将要启用之前，必须重新启动计算机。如果您的计算机已启用“增强安全性”，则可能需要输入在 Configuration/Setup Utility 中设置的管理员密码以启用芯片。
3. 单击 **OK** 以重新启动计算机。
4. 从 Windows 桌面，单击**开始 > 程序 > IBM Client Security Software > Administrator Utility**。

   由于对 Administrator Utility 的访问受安全芯片密码的保护，因此显示一条消息，要求您输入安全芯片密码。
5. 在 New password 字段中，输入新的安全芯片密码，然后在 Confirmation 字段中再次输入该密码。
6. 单击 **OK**。

启用 Entrust 支持

IBM 嵌入式安全芯片与 Client Security Software 配合使用以增强 Entrust 安全性功能。在装有 Client Security Software 的计算机上启用 Entrust 支持可将 Entrust 软件安全性功能转移给 IBM 安全芯片。

Client Security Software 将自动启用 Entrust 支持; 但是，如果 entrust.ini 文件不在常规路径中，则为用户打开一个对话框以浏览 entrust.ini 文件。在用户定位并选择该文件后，Client Security 便可以启用 Entrust 支持。单击 Enable Entrust Support 按钮后，在 Entrust 使用 IBM 嵌入式安全芯片之前，必须重新引导。

要启用 Entrust 支持，请完成以下过程:

1. 从 IBM 客户机的 Windows 桌面上单击**开始 > 程序 > IBM Client Security Software > Administrator Utility**。

   显示 Administrator Utility 主窗口。
2. 单击 **Configure Application Support and Policies**。

   显示 UVM Application and Policy Configuration 屏幕。
3. 选择 **Enable Entrust support** 复选框。
4. 单击 **Apply**。

显示 IBM Client Security Entrust Support 屏幕，并出现一条消息，表示已启用 Entrust 支持。

注: 必须重新启动计算机以使更改有效。

第 7 章 针对客户机用户的指示信息

本部分提供的信息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 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

本部分中的信息也在 *Client Security User's Guide* 中提供。

对系统登录使用 UVM 保护

本节包含有关对 Windows XP、Windows NT 和 Windows 2000 Professional 系统使用 UVM 登录保护的信息。必须对计算机启用 UVM 保护，才能使用该保护。

UVM 保护使您能够通过登录界面控制对操作系统的访问。UVM 登录保护代替 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** 访问 UVM 登录界面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。

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 识别多个域，但对于所有域，用户密码必须是相同的。
3. 输入您的 UVM 密码短语，并单击 **OK** 以访问操作系统。如果 UVM 策略要求指纹认证，则显示一条消息，提示您进行指纹扫描。

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

Client Security 屏幕保护程序

Client Security 屏幕保护程序是当计算机处于空闲状态指定的时间段后显示的一系列移动图像。设置 Client Security 屏幕保护程序是通过屏幕保护程序控制访问计算机的一种方式。一旦在桌面上显示 Client Security 屏幕保护程序，则必须输入 UVM 密码短语以访问系统桌面。

设置 Client Security 屏幕保护程序

本部分包含有关设置 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，在您的计算机的安全性策略上必须至少注册了一个用户。

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**并选择期望的速度。
5. 单击 **OK**。

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，仅当已在 Windows 屏幕保护程序设置选项卡上选择了**密码保护**复选框时，屏幕保护程序才锁定。

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。如果已经选中它，则系统要求 UVM 密码短语。如果没有选中它，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，可能还会要求进一步认证。例如，可能必须扫描您的指纹以解锁计算机。

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

Client Utility

Client Utility 使客户机用户能够执行不要求管理员访问的各种安全性维护。

Client Utility 功能

Client Utility 使客户机用户能够执行以下操作:

- **更改 UVM 密码短语。**要提高安全性，可以定期更改 UVM 密码短语。
- **更新 Windows 登录设置。**当使用“用户管理器”程序更改某台客户机用户的 Windows XP 或 Windows NT 密码时，也必须通过使用 Client Utility 来更改该密码。如果管理员使用 Administrator Utility 来更改用户的 Windows 登录密码，则先前为该用户创建的所有用户加密密钥都将删除，并且关联的数字证书将变为无效。

  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。**如果想要使用 UVM 感知指纹传感器（或扫描仪）进行认证，则可以使用 UVM 注册您的指纹。

注: 在可以使用 UVM 注册指纹之前，指纹扫描仪必须与 IBM 客户机系统连接。有关如何连接和使用指纹扫描仪的指示信息，请参考硬件供应商所提供的文档。

- **更新密钥压缩文档。**如果创建数字证书并要制作存储在 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 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. 输入要求 UVM 密码短语或 Windows 密码更改的客户机用户的 UVM 密码短语，然后单击 **OK**。

   以下窗口打开。
3. 在 **Required information** 区域，输入至为此用户设置的密钥压缩文档的路径。

   注: 设置密钥压缩文档后，Administrator Utility 将上次输入的路径填充到 **Archive Directory (Path)** 字段中。如果 **Archive Directory (Path)** 字段中的信息已删除，或者如果该信息对于想要添加的用户来说是不正确的，则请确保重新输入正确的信息（因为压缩文档目录是所要求的信息）。

4. 请执行以下操作之一:
   - 要在 **Change UVM Passphrase** 区域中更改 UVM 密码短语，请在 **Enter new UVM passphrase** 字段中输入新密码短语。接下来，请在 **Confirm UVM passphrase** 字段中再次输入密码短语，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，然后在 **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: 只更改“用户管理器”中的 Windows 登录信息以使用户正确登录。
   - 要更新密钥压缩文档，请单击 **Update Archive**；然后在通知您操作成功的窗口上单击 **OK**。
   - 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** 来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，它们会遭受拦截和读取。通过获取数字证书并使用它来数字签名并加密电子邮件消息或保护 Web 浏览器，可以禁止对您的因特网事务的未经授权的访问。

数字证书（也称为数字标识或安全性证书）是认证中心颁发并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。认证中心是数字证书的受信任的供应商，它可能是第三方发行商，如 VeriSign，或者认证中心可能在您的公司内作为服务器设置。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

由于 Client Security Software 的使用通常是关于使用支持 Microsoft CryptoAPI 的应用程序（例如 Outlook Express）来获取和使用数字证书，因此本部分中提供的指示信息特定于 Client Security Software 的使用。

有关如何创建安全性设置和电子邮件应用程序（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。可在 Administrator Utility 中查找 Client Security Software 提供的加密强度。

获取 Microsoft 应用程序的数字证书

使用认证中心创建与 Microsoft 应用程序一起使用的数字证书时，您会得到提示选择证书的加密服务供应商（CSP）。

要为 Microsoft 应用程序使用 IBM 嵌入式安全芯片的加密能力，请确保当获取数字证书时选择 **IBM embedded Security Subsystem CSP** 作为加密服务供应商。这确保了数字证书的专用密钥存储在 IBM 安全芯片上。

而且，如果可用，请选择强（或高）加密以获取优良的安全性。因为 IBM 嵌入式安全芯片能够对数字证书专用密钥进行多达 1024 位的加密，所以如果在认证中心界面内该选项可用，请选择该选项；1024 位加密也被称作强加密。

选择 **IBM embedded Security Subsystem CSP** 作为 CSP 后，可能必须输入 UVM 密码短语，和／或扫描指纹以满足获取数字证书的要求。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 使您能够将用缺省 Microsoft CSP 创建的证书转移给 IBM 嵌入式安全系统 CSP。这将大大增强提供给与证书关联的专用密钥的保护，因为它们现在将安全存储在 IBM 嵌入式安全芯片上，而不是存储在脆弱的软件上。

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` 程序。主对话框显示了与缺省 Microsoft 软件 CSP 关联的证书。

   注: 只有在创建时专用密钥标记为 *exportable* 的证书才会显示在该列表中。
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 IBM 嵌入式安全芯片的保护。任何使用这些专用密钥的操作（例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。可以使用 Administrator Utility 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查看和使用数字证书。请参阅由 Microsoft 提供的文档以获取更多信息。

创建数字证书并使用证书对电子邮件消息签名之后，UVM 将在您第一次对电子邮件消息数字签名时提示您需要认证要求。可能必须输入 UVM 密码短语和／或扫描指纹以满足使用数字证书的认证要求。认证要求在计算机的 UVM 策略中定义。

第 8 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。如果这样做，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。必须重新启动计算机，才能禁用 UVM 保护。
- 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 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。如果丢失或忘记了管理员密码，您就不能访问 Configuration/Setup Utility，并且只有卸下计算机箱盖并移动系统板上的跳线才能更改或删除密码。有关更多信息，请参阅计算机随附的硬件文档。

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。如果这样做，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。必须重新启动计算机，才能禁用 UVM 保护机。
- 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 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，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 的访问受此密码保护。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 嵌入式安全芯片之前请阅读以下“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。如果这样做，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。重新启动计算机，才能禁用 UVM 保护。
- 清除 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 嵌入式安全芯片之前请阅读以下“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。如果这样做，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。必须重新启动计算机，才能禁用 UVM 保护。
- 清除 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，则所有 Client Security 功能将丢失。该用户将必须在 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 识别。UVM 将指向先前的用户名而 Windows 只能识别新用户名。即使在安装 Client Security Software 之前已经更改了 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，则在可以继续之前必须输入 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之前输入正确的 UVM 密码短语。

不显示算法：如果在 Netscape 中查看 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。

当电子邮件从一个 Outlook Express（128 位）客户机被发送到另一个 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）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: 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能与 IBM 嵌入式安全芯片证书一起使用。有关与您的 Outlook Express 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 保护不运行: 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

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。与这些消息关联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 调用由关联的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，则表明被拒绝访问的消息将根据使用的软件而不同。例如，来自 Outlook Express 的一条错误消息表明对认证对象的访问被拒绝，这与来自 Netscape 的错误消息不同，来自 Netscape 的错误消息表明访问被拒绝。

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
在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 Client Security Software 的新版本。
安装过程中显示一条消息，表明已经安装了 Client Security Software 的先前版本。	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，则不必清除该芯片并重新设置密码。
安装访问由于未知的硬件密码被拒绝	**操作**
当在启用 IBM 嵌入式安全芯片的 IBM 客户机上安装软件时，则 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。
无人照管安装不开始	**操作**
必须安装 SMBus 设备驱动程序来执行无人照管安装。	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。	不要求进一步操作。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: A buffer I/O error occurred while trying to access the Client Security chip. This might be corrected by a reboot.	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芯片的消息	**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 将不能使用 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 之前已经更改了 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。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。有关与您的 Outlook Express 版本一起使用的加密算法的当前信息，请参阅 Microsoft。
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 不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**
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，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如果在将 Client Security Software 与 Netscape 应用程序一起使用遇到问题时可能有帮助的信息。

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，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，单击工具栏上的安全性图标。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，表明认证故障。如果单击 **OK**，将打开 Netscape，但您将不能使用由 IBM 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 中被更换	**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。
在硬盘驱动器发生故障后尝试使用恢复的证书时出现错误消息	**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，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 出现延迟	**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 安装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
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 标识文件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 或后续版本后不进行解密。	这是一个已知的限制。 在安装 Client Security Software 3.0 或后续版本*之前*，必须使用先前版本的 Client Security Software 解密所有已加密的文件。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 端口时，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. 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 已经提交适合的文档，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。

如果您不能下载 Client Security Software 软件包，请联系本地 IBM 营业部，以与 IBM 国家或地区出口法规合作伙伴（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。

不正确尝试

如果十次输入不正确的密码，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不正确的密码，则计算机将锁定 2 小时 34 分钟。每当有十次输入不正确的密码后，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 密码短语更长些并且可以比传统密码更特别。

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。

不正确尝试

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

附录 C. 对系统登录使用 UVM 保护的规则

UVM 保护确保只有已经添加到特定 IBM 客户机的 UVM 的那些用户才能访问操作系统。Windows 操作系统包含提供登录保护的应用程序。虽然 UVM 保护设计为与那些 Windows 登录应用程序并行工作，但是 UVM 保护与操作系统不同。

对于 Windows XP、Windows NT 和 Windows 2000，UVM 登录界面代替操作系统登录界面，因此每次用户尝试登录到系统时 UVM 登录窗口打开。

对系统登录设置和使用 UVM 保护之前请阅读以下技巧:

- 当启用了 UVM 保护时，不要清除 IBM 嵌入式安全芯片。如果这样做，硬盘上的内容将变为不可用，并且必须重新格式化硬盘驱动器并重新安装所有软件。
- 如果清除 Administrator Utility 中的 **Use UVM Logon Protection for this Workstation instead of using Windows Logon Protection** 复选框，则系统返回 Windows 登录过程，而无需 UVM 登录保护。
- 在 Windows XP、Windows NT 和 Windows 2000 中，有选项让您指定输入 Windows NT 登录应用程序的正确密码所允许的最大尝试次数。此选项不应用于 UVM 登录保护。您可以设置输入 UVM 密码短语所允许的尝试次数没有限制。

附录 D. 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用于 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（无论明示的，还是默示的）保证，包括（但不限于）对非侵权性、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；这些更改将编入本出版物的新版本中。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: 01R2761

中国印刷

(1P) P/N: 01R2761