IBM® 客户端安全解决方案

客户端安全软件版本 5.4 安装指南

IBM® 客户端安全解决方案

客户端安全软件版本 5.4 安装指南

第一版（2004 年 10 月）

在使用该资料以及它支持的产品前，请确保阅读第 29 页的附录 A, 『客户端安全软件的美国出口条例』和第 35 页的附录 C, 『**声明与商标**』。对本手册所包含的内容，IBM 公司拥有最终解释权，如有变更，恕不另行通知。

© Copyright International Business Machines Corporation 2004. All rights reserved.

目录

© Copyright IBM Corp. 2004

前言

本节提供了有关如何使用本指南的信息。

关于本指南

本指南包含有关如何在 IBM 网络计算机（也称为 IBM 客户机，包含 IBM 嵌入式安全子系统）上安装 IBM 客户端安全软件的信息。本指南还包含有关如何启用 IBM 嵌入式安全子系统以及如何为安全子系统设置管理员密码的说明。

本指南的结构如下:

“第 1 章，『简介』”，包含基本安全概念的大纲、该软件中所包含的应用程序和组件的概述，以及公钥基础结构（PKI）功能的描述。

“第 2 章，『入门』”，包含计算机硬件和软件安装先决条件以及下载该软件的说明。

“第 3 章，『安装软件前』”，包含安装 IBM 客户端安全软件的先决条件说明。

“第 4 章，『下载、安装和配置软件』”，包含安装、更新和卸载软件的说明。

“第 5 章，『故障诊断』”包含解决问题的有用信息，您在使用本指南提供的说明时可能碰到这些问题。

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

“附录 B，『密码和口令信息』”包含口令标准，该标准适用于管理员密码的 UVM 口令和规则。

“附录 C，『**声明与商标**』”，包含法律声明和商标信息。

阅读本指南的对象

本指南适用于在 IBM 客户机上设置个人计算安全的网络或系统管理员。要求具备安全概念的知识（例如，网络环境中的公钥基础结构（PKI）和数字证书管理）。

如何使用本指南

使用本指南在 IBM 客户机上安装和设置个人计算安全。本指南是*《客户端安全软件管理员和用户指南》*配套指南。

本指南及有关客户端安全的所有其它文档可从 http://www.pc.ibm.com/us/security/secdownload.html IBM Web 站点下载。

© Copyright IBM Corp. 2004

对《*客户端安全软件管理员和用户指南*》的引用

本文档中提供对《*客户端安全软件管理员和用户指南*》的引用。《*管理员和用户指南*》包含有关使用用户验证管理工具（UVM）和处理 UVM 策略的信息，以及有关使用管理员实用程序和用户配置实用程序的信息。

安装软件后，使用《*管理员和用户指南*》中的说明来设置和维护每台客户机的安全策略。

附加信息

您可从 http://www.pc.ibm.com/us/security/index.html IBM Web 站点获得附加信息和安全产品更新（如果有的话）。

第 1 章 简介

无可挑剔的 ThinkPad™ 和 ThinkCentre™ 计算机装配有内置的加密硬件，它可以结合可下载的软件技术为客户机 PC 平台提供强大的安全级别。这些硬件和软件统称为 IBM 嵌入式安全子系统（ESS）。硬件组件是 IBM 嵌入式安全芯片而软件组件是 IBM 客户端安全软件（CSS）。

客户端安全软件是为 IBM 计算机设计的，该计算机使用 IBM 嵌入式安全芯片来加密文件和存储加密密钥。该软件由应用程序和组件组成，它们使 IBM 客户机系统能在整个本地网络、企业内部或因特网上使用客户端安全功能。

IBM 嵌入式安全子系统

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

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

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

IBM 嵌入式安全芯片

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

IBM 嵌入式安全子系统支持:

- RSA3 PKI 操作，例如对隐私的加密和对验证的数字签名
- RSA 密钥生成
- 伪随机数生成
- 200 毫秒内的 RSA 功能计算
- 用于 RSA 密钥对存储的 EEPROM 内存
- 在 TCG 主要规范 V1.1 中定义的所有可靠计算组织（TCG）功能
- 通过低针脚数量（LPC）总线与主处理器通信

IBM 客户端安全软件

IBM 客户端安全软件由以下软件应用程序和组件组成:

© Copyright IBM Corp. 2004

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

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

密码和密钥之间的关系

密码和密钥以及其它可选的验证设备协同工作以验证系统用户的身份。理解密码和密钥之间的关系对于理解 IBM 客户端安全软件如何运行至关重要。

管理员密码

管理员密码用于向 IBM 嵌入式安全子系统验证管理员。该密码在嵌入式安全子系统的安全硬件范围内维护和验证。一旦验证，管理员可以执行以下操作:

- 登记用户
- 启动策略界面
- 更改管理员密码

可以下列方式设置管理员密码:

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

具有创建并且维护管理员密码的策略很重要。如果已泄露或者忘记管理员密码，则可以更改它。

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

硬件公钥和私钥

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

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

在安全子系统的安全硬件范围内创建、存储和使用硬件私钥。硬件公钥可用于多种用途（因此称为公钥），但是它绝对不会暴露在安全子系统的安全硬件范围之外。硬件公钥和私钥是 IBM 密钥交换层次结构的关键部分，该层次结构在以后的部分中将有所描述。

硬件公钥和私钥的创建方式如下:

- 通过 IBM 客户端安全安装向导
- 通过管理员实用程序
- 使用脚本

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

管理员公钥和私钥

管理员公钥和私钥是 IBM 密钥交换层次结构整体的一部分。它们还允许在系统板或硬盘驱动器发生故障的情况下备份并复原特定于用户的数据。

管理员公钥和私钥对于所有系统可以是唯一的或者对于所有系统或系统组可以是公共的。值得注意的是这些管理员密钥必须是受管的，所以具有使用相对已知的密钥而言唯一的密钥的策略十分重要。

可以下列方式之一创建管理员公钥和私钥:

- 通过 IBM 客户端安全安装向导
- 通过管理员实用程序
- 使用脚本

ESS 存档

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

用户公钥和私钥

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

IBM 密钥交换层次结构

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

层次结构的下一个密钥“级别”（根以上）是管理员公钥和私钥或*管理员密钥对*。管理员密钥对可以在每台机器上都是唯一的，也可以在所有客户机或客户机子集上都相同。如何管理这一密钥对取决于您想如何管理网络。由于管理员私钥在客户机系统（通过硬件公钥受保护）和管理员定义的位置中驻留，所以它是唯一的。

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

需要密钥时，密钥会交换到安全子系统中。加密的私钥会交换到安全子系统中，然后可以在芯片的受保护环境中使用。私钥从不在该硬件环境以外暴露或者使用。这样提供了几乎无限量通过 IBM 嵌入式安全芯片进行保护的数据。

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

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

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

CSS 公钥基础结构（PKI）功能

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

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

  注: 受 IBM 嵌入式安全子系统保护的数字证书无法导出到另一个 CSP。
- **密钥存档和恢复解决方案。**一项重要的 PKI 功能是创建密钥存档，在原始密钥丢失或损坏的情况下可以从该存档复原密钥。IBM 客户端安全软件提供界面，使您能够建立由 IBM 嵌入式安全子系统创建的密钥和数字证书的存档，并且在需要时复原这些密钥和证书。
- **文件和文件夹加密。**文件和文件夹加密使客户机用户能够加密或解密文件或文件夹。这样就在 CSS 系统安全性措施的基础上提供了数据安全的增强级别。
- **指纹验证。**IBM 客户端安全软件支持用于验证的 Targus PC 卡指纹阅读器和 Targus USB 指纹阅读器。为正常的运行，安装 Targus 指纹设备驱动程序之前，必须安装客户端安全软件。
- **智能卡验证。**IBM 客户端安全软件支持某些智能卡作为验证设备。客户端安全软件使智能卡能够作为单个用户的一次性验证标记使用。除非使用安全证书漫游，否则每个智能卡都绑定到系统。因为该智能卡必须与密码（可能会损坏）一起提供，所以需要智能卡使您的系统更安全。
- **安全证书漫游。**安全证书漫游使得到授权的网络用户能够使用网络上的任何计算机，就象是自己的工作站一样。用户得到授权在任意注册了客户端安全软件的客户机上使用 UVM 后，就能够将其个人数据导入到安全证书漫游网络中的其它任何注册的客户机中。其个人数据会在 CSS 存档以及任何曾经导入这些数据的计算机中得到自动更新和维护。对该个人数据的更新（诸如新的证书或口令更改）将立即在连接到漫游网络的所有其它计算机上可用。
- **FIPS 140-1 认证。**客户端安全软件支持 FIPS 140-1 认证的加密库。
- **口令失效。**当每个用户添加到 UVM 中时，客户端安全软件建立特定于用户的口令和口令失效策略。

第 2 章 入门

本节包含结合 IBM 客户端安全软件使用的硬件和软件兼容性要求。并提供有关下载 IBM 客户端安全软件的信息。

硬件要求

在您下载和安装软件前，请确保计算机硬件与 IBM 客户端安全软件兼容。

有关硬件和软件要求的最新信息可在 http://www.pc.ibm.com/us/security/index.html IBM Web 站点获取。

IBM 嵌入式安全子系统

IBM 嵌入式安全子系统是嵌入在 IBM 客户机系统板上的加密微处理器。该 IBM 客户端安全软件必不可少的组件将安全策略功能从易受攻击的软件转移到安全硬件，从根本上增加本地客户机的安全。

仅包含 IBM 嵌入式安全子系统的 IBM 计算机和工作站支持 IBM 客户端安全软件。如果您尝试下载该软件并将其安装到不包含 IBM 嵌入式安全子系统的计算机上，则该软件将不会正确安装或运行。

受支持的 IBM 型号

客户端安全软件已被许可并用于支持许多 IBM 台式机和笔记本计算机。有关受支持型号的完整列表，请参阅 http://www.pc.ibm.com/us/security/index.html Web 页面。

软件要求

在您下载和安装软件前，请确保计算机软件和操作系统与 IBM 客户端安全软件兼容。

操作系统

IBM 客户端安全软件需要以下操作系统之一:

- Windows XP
- Windows 2000 Professional

支持 UVM 的产品

IBM 客户端安全随附用户验证管理工具（UVM）软件，该软件使您能够为台式计算机定制验证。该基于策略的一级控件增加资产保护和密码管理的效率。与企业范围的安全策略程序兼容的 UVM，使您能够使用支持 UVM 的产品，包括以下内容:

- **生物测定学设备，例如指纹阅读器**

  UVM 为生物测定学设备提供即插即用接口。在安装支持 UVM 的传感器*前*，您必须安装 IBM 客户端安全软件。

© Copyright IBM Corp. 2004

要使用已经在 IBM 客户机上安装的支持 UVM 的传感器，您必须卸载支持 UVM 的传感器，安装 IBM 客户端安全软件，然后重新安装支持 UVM 的传感器。

- **Tivoli Access Manager V5.1**

  UVM 软件通过平稳地集成集中式、基于策略的访问控制解决方案（例如，Tivoli Access Manager）简化和改进策略管理。

  无论系统是在网络（台式机）上还是独立的，UVM 软件在本地强制执行策略，这样就创建了单个、统一的策略模型。

- **Lotus Notes V4.5 或更高版本**

  UVM 结合 IBM 客户端安全软件以改进 Lotus Notes 登录（Lotus Notes V4.5 或更高版本）的安全。

- **Entrust 桌面解决方案 5.1、6.0 或 6.1**

  Entrust 桌面解决方案增强因特网安全能力，以便关键的企业处理可以移至因特网。Entrust 智能提供了单个安全层，该安全层包含企业的整套增强安全需要（包含标识、私密性、验证和安全管理）。

- **RSA SecurID 软件令牌**

  RSA SecurID 软件令牌使在传统 RSA 硬件令牌中使用的相同子记录能够嵌入现有的用户平台。因此，用户可以通过访问嵌入的软件（而不是必须携带专用验证设备）对受保护资源进行验证。

- **Gemplus GemPC400 智能卡阅读器**

  Gemplus GemPC400 智能卡阅读器使安全策略包含了智能卡验证，为标准口令保护添加了额外的安全层。

Web 浏览器

IBM 客户端安全软件支持以下有关请求数字证书的 Web 浏览器:

- Internet Explorer 5.0 或更高版本
- Netscape 4.8 和 Netscape 7.1

浏览器加密长度信息

如果安装了强加密支持，则使用 128 位版本的 Web 浏览器。要检查 Web 浏览器的加密强度，请查看与浏览器一起提供的帮助系统。

加密服务

IBM 客户端安全软件支持以下加密服务:

- **Microsoft CryptoAPI**: CryptoAPI 是 Microsoft 操作系统和应用程序的缺省加密服务。通过内置的 CryptoAPI 支持，IBM 客户端安全软件使您能在为 Microsoft 应用程序创建数字证书时使用 IBM 嵌入式安全子系统的加密操作。
- **PKCS#11**: PKCS#11 是 Netscape、Entrust、RSA 及其它产品的加密标准。安装 IBM 嵌入式安全子系统 PKCS#11 模块后，您可以使用 IBM 嵌入式安全子系统为 Netscape、Entrust、RSA 及其它使用 PKCS#11 的应用程序生成数字证书。

电子邮件应用程序

IBM 客户端安全软件支持以下使用安全电子邮件的应用程序类型:

- 使用 Microsoft CryptoAPI 进行加密操作的电子邮件应用程序，例如 Outlook Express 和 Outlook（与受支持的 Internet Explorer 版本结合使用时）
- 使用公钥加密标准 #11（PKCS#11）进行加密操作的电子邮件应用程序，例如，Netscape Messenger（与受支持的 Netscape 版本结合使用时）
- 通过增强登录验证保护的 Lotus Notes 支持

第 3 章 安装软件前

本节包含在 IBM 客户机上运行安装程序和配置 IBM 客户端安全软件的先决条件说明。

有关客户端安全软件的安装所需的所有文件都在 http://www.pc.ibm.com/us/security/index.html IBM Web 站点中提供。该 Web 站点提供一些信息，将帮助确保您的系统包含 IBM 嵌入式安全子系统，并且使您能为系统选择相应的 IBM 客户端安全产品及服务。

安装软件前

安装程序在 IBM 客户机上安装 IBM 客户端安全软件并启用 IBM 嵌入式安全子系统；然而，安装细节根据许多因素而有所变化。

用户必须以管理员权限登录才能安装 IBM 客户端安全软件。

安装以与 Tivoli Access Manager 一起使用

如果您要使用 Tivoli Access Manager 为计算机控制验证要求，则在安装 IBM 客户端安全软件*前*必须安装某些 Tivoli Access Manager 组件。要获取详细信息，请参阅*《结合客户端安全使用 Tivoli Access Manager》*。

启动功能注意事项

两个 IBM 启动功能可能影响您启用 IBM 嵌入式安全子系统并生成加密密钥的方法。这些功能是 BIOS 管理员密码和增强的安全，并可从 IBM 计算机的 Configuration/Setup Utility 访问。IBM 客户端安全软件具有单独的管理员密码。为了避免混淆，在 Configuration/Setup Utility 中设置的管理员密码在客户端安全软件手册中称为 *BIOS 管理员密码*。

BIOS 管理员密码

BIOS 管理员密码阻止未经授权的人员更改 IBM 计算机的配置设置。该密码在 NetVista 或 ThinkCentre 计算机上使用 Configuration/Setup Utility 程序设置，或者在 ThinkPad 计算机上使用 IBM BIOS Setup Utility 程序设置。可以通过在计算机启动顺序过程中按 Enter 键或 F1 来访问相应的程序。该密码在 ThinkCentre Configuration/Setup Utility 中称为 *administrator password*，在 ThinkPad BIOS Setup Utility 中称为 *supervisor password*。

增强的安全

增强的安全为您的 BIOS 管理员密码以及启动顺序设置提供额外的保护。通过使用 Configuration/Setup Utility 程序（在计算机启动顺序期间通过按 F1 可以访问该程序），您可以确定是否已启用或禁用了增强的安全。

要获取有关密码和增强安全的更多信息，请参阅与您的计算机一起提供的文档。

© Copyright IBM Corp. 2004

在 NetVista 型号 6059、6569、6579、6649 和所有 NetVista Q1x 型号上的增强安全: 如果已经在这些 NetVista 型号（6059、6569、6579、6649、6646 和所有 Q1x 型号）上设置了管理员密码，则您必须打开管理员实用程序来启用 IBM 嵌入式安全子系统并生成加密密钥。

当增强的安全在这些型号上启用时，您必须使用管理员实用程序来启用 IBM 嵌入式安全子系统并在安装了 IBM 客户端安全软件后生成加密密钥。如果安装程序检测到启用了增强的安全，则将在安装过程结束时通知您。重新启动计算机并打开管理员实用程序来启用 IBM 嵌入式安全子系统并生成加密密钥。

所有其它 NetVista 型号（除型号 6059、6569、6579、6649 和所有 NetVista Q1x 型号外）上的增强安全: 如果已经在其它 NetVista 型号上设置了管理员密码，则在安装过程期间不需要您输入管理员密码。

当在这些 NetVista 型号上启用增强的安全时，您可以使用安装程序来安装该软件，但您必须使用 Configuration/Setup Utility 来启用 IBM 嵌入式安全子系统。在已启用 IBM 嵌入式安全子系统后，您可以使用管理员实用程序生成加密密钥。

BIOS 更新信息

安装软件前，您可能需要为计算机下载最新的基本输入／输出系统（BIOS）代码。要确定计算机使用的 BIOS 级别，重新启动计算机并按 F1 来启动 Configuration/Setup Utility。当 Configuration/Setup Utility 的主菜单打开时，选择 “Product Data” 来查看有关 BIOS 代码的信息。BIOS 代码级别也称为 EEPROM 修订级别。

要在 NetVista 型号（6059、6569、6579、6649）上运行 IBM 客户端安全软件 2.1 或更高版本，您必须使用 BIOS 级别 xxxx22axx 或更高级别；要在 NetVista 型号（6790、6792、6274、2283）上运行 IBM 客户端安全软件 2.1 或更高版本，您必须使用 BIOS 级别 xxxx20axx 或更高级别。要获取更多信息，请参阅与所下载的软件一起包含的自述文件。

要查找您的计算机的最新 BIOS 代码，请转至 http://www.pc.ibm.com/support IBM Web 站点，在搜索字段中输入 `bios` 并从下拉列表选择下载；然后按 Enter 键。会显示 BIOS 代码更新的列表。单击相应的型号并遵循 Web 页面上的说明。

对于密钥存档使用管理员密钥对

密钥对存档仅是您在外部介质上存储用于复原的管理员密钥对的副本。因为管理员实用程序用于创建密钥对存档，所以您必须在初始 IBM 客户机上安装 IBM 客户端安全软件，然后才可以创建管理员密钥对。

第 4 章 下载、安装和配置软件

本节包含在 IBM 客户机上下载、安装和配置 IBM 客户端安全软件的说明。本节还包含卸载该软件的说明。请确保在安装各种增强客户端安全功能的实用程序前先安装 IBM 客户端安全软件。

要点: 如果您从 IBM 客户端安全软件 5.0 先前的版本升级，则*必须*在安装客户端安全软件 5.1 或更高版本*前*解密所有已加密的文件。由于在 IBM 客户端安全软件 5.1 或更高版本的文件加密实现中的更改，因此，IBM 客户端安全软件 5.1 或更高版本无法解密使用客户端安全软件 5.0 先前版本加密的文件。

下载软件

有关客户端安全软件的安装所需的所有文件都在 http://www.pc.ibm.com/us/security/index.html IBM Web 站点中提供。该 Web 站点提供一些信息，将帮助确保您的系统包含 IBM 嵌入式安全子系统，并且使您能为系统选择相应的 IBM 客户端安全产品及服务。

要为系统下载相应的文件，请完成以下过程:

1. 使用 Web 浏览器，转至 http://www.pc.ibm.com/us/security/index.html IBM Web 站点。
2. 在 “Resources” 框中，单击 **Support and downloads**。
3. 在 Web 页面的嵌入式安全子系统和 IBM 客户端安全软件部分，单击 **Software download**。
4. 在 “Select a system” 框中，单击 **Detect my system & continue** 或在提供的字段中输入您的七位机器型号数字。
5. 在提供的字段中输入您的电子邮件地址并从下拉菜单中选择您的国家或地区。
6. 选择有关您是否想发送关于其它产品及服务的信息的相应复选框。
7. 通过单击 **View Licence** 查看许可证协议；然后单击 **Accept Licence**。

   您将被自动重定向到 IBM 客户端安全下载页面。
8. 找到客户端安全软件 5.4 的相关链接，并单击 **Download Now**。

   注: 有关特定升级和限制信息，请参阅 `css54readme.html` 文件。
9. 单击**保存**以在您的硬盘驱动器上保存安装可执行文件的副本。
10. 指定 “另存为” 的位置并单击**保存**。要开始安装该软件，当下载完成时单击**打开**，或者双击可执行文件图标。

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

© Copyright IBM Corp. 2004

安装软件

要为系统安装相应的文件，请完成以下过程:

1. 双击可执行文件。

   打开“欢迎使用 IBM 客户端安全软件 InstallShield 向导”窗口。
2. 单击**下一步**。

   显示 IBM 客户端安全软件许可证协议。
3. 阅读许可证协议的条款，选择**我接受许可证协议中的条款**单选按钮，然后单击**下一步**。

   显示“产品选择”屏幕。
4. 选择以下单选按钮之一，并单击**下一步**。
   - **IBM 客户端安全软件和 IBM 密码管理器。**该选择将安装或升级 IBM 客户端安全软件、IBM 密码管理器和所有必要的设备驱动程序。
   - **仅 IBM 客户端安全软件。**该选择将安装或升级 IBM 客户端安全软件和所有必要的设备驱动程序。

   显示“目标文件夹”屏幕。
5. 单击**下一步**接受缺省安装位置，或单击**更改**以浏览至希望的目标文件夹。

   显示“安装程序准备就绪”屏幕。
6. 单击**安装**开始安装，或单击**上一步**查看或更改您的任何安装设置。

   状态栏显示安装进度，之后“InstallShield 向导已完成”屏幕将显示。
7. 单击**完成**退出向导。

您必须重新启动计算机以使对于计算机所进行的安装更改生效。

选择配置选项

IBM 客户端安全安装向导的第一个屏幕使您能够选择配置选项。选择相应的配置选项非常重要。请在选择配置选项前仔细查看以下信息。安全用户新手应该选择*典型配置*选项。

典型配置

当使用客户端安全安装向导选择 IBM 客户端安全软件的典型配置时，您将配置以下客户端安全功能:

- IBM 密码管理器（如果在安装时已选定）
- 右键单击文件加密
- 口令和指纹验证
- 数字签名支持

在客户端安全安装向导中使用推荐的*典型配置*选项使配置过程变得更为简单。然而，当选择该配置时客户端安全软件的某些高级功能已禁用，导致某些 CSS 功能不可用。

典型配置缺省设置

典型配置硬编码缺省设置如下:

- **存档位置**: C:\documents and settings\all users\application data\ibm\security\archive
- **管理员密钥对位置**: C:\documents and settings\all users\application data\ibm\security\keys

  管理员私钥不分割，且由 CSS 管理员口令加密。

其它设置包含以下内容:

- 已启用 IBM 密码管理器支持
- 安全策略是中级: 每种可用的验证方法将仅在首次使用 CSS 功能时需要。
- 始终需要口令验证。
- 当在设置时检测集成的指纹阅读器时，将需要指纹验证。
- 设置 CSS 的用户的 UVM 口令也是 CSS *管理员密码*。更改 UVM 口令还将更改 CSS 管理员密码。CSS 管理员口令永不失效。

典型配置组件限制

当选定了典型配置时，客户端安全软件在高级配置之后启用的某些功能将禁用。这些功能无法在 CSS 的典型配置下使用。要启用这些功能，您必须将配置转换为高级配置。在典型配置之后的功能差异如下:

- **管理员实用程序**

  以下操作在典型配置下是不允许的:

  – 重新设置用户
  – 删除用户
  – 使用芯片设置按钮更改管理员密码
  – 密钥配置功能

  如果用户尝试以上操作之一，将提示他转换为 CSS 高级配置。该转换过程解密管理员私钥，且将管理员密钥对移至由用户指定的位置。

- **管理员控制台**

  以下用法差异应用在典型配置下:

  – 存档目录、私钥位置和公钥位置为硬编码且无法更改。该存档仅可以在本地计算机上编辑。
  – 配置安全证书漫游的选项在典型配置下不可用。如果您选择典型配置，随后想要设置安全证书漫游网络，则必须首先将典型配置转换为高级配置。
  – 对于 CSS 管理员 UVM 口令忽略操作无法执行。

- **用户配置实用程序**

  以下用法差异应用在典型配置下:

  – 设置 CSS 的用户的 UVM 口令也是管理员密码。更改 UVM 口令还将更改管理员密码。
  – 无法重新设置 CSS 管理员用户。
  – 配置安全证书漫游的选项在典型配置下不可用。

将典型配置转换为高级配置

要将客户端安全软件典型配置转换为高级配置，请完成以下过程:

1. 启动管理员实用程序。
2. 输入 CSS 管理员密码。
3. 单击**密钥配置**按钮。
4. 单击**确定**继续。
5. 输入您想要存储解密的管理员密钥对的位置。解密的密钥对不应该存储在本地硬盘驱动器上。转换过程现在已完成。
6. 更改存档位置。该存档不应该存储在本地硬盘驱动器上。

在将客户端安全软件已转换为高级配置之后，它将无法转换回典型配置。

高级配置

IBM 客户端安全软件的*高级配置*配置以下*其它*客户端安全功能:

- **UVM 登录保护**
- **密钥存储位置选择**
- **应用程序支持**: Entrust、文件和文件夹加密、Lotus Notes

使用 IBM 客户端安全安装向导

IBM 客户端安全安装向导提供了一个界面，该界面帮助您安装客户端安全软件并启用 IBM 嵌入式安全芯片。请完成以下过程以使 IBM 客户端安全安装向导能够指导您逐步完成有关在 IBM 客户机上设置安全策略所涉及的必需的任务。

IBM 客户端安全安装向导指导您逐步完成的一般步骤如下: 特定步骤的不同取决于您选择的配置选项。

- **设置安全管理员密码**

  安全管理员密码（在这些手册中称为管理员密码）用于控制对 IBM 客户端安全管理员实用程序的访问，该实用程序用于更改该计算机的安全设置。

- **创建管理员安全密钥**

  管理员安全密钥是一组存储在计算机文件中的数字密钥。这些密钥文件也称为管理员密钥、管理员密钥对或密钥对存档。建议您在可移动磁盘或驱动器上保存这些重要的安全密钥。当管理员实用程序中对安全策略进行更改时，将提示您提供管理员密钥来证明策略更改是经过授权的。

  还保存了备份安全信息，以防您需要替换计算机的系统板或硬盘驱动器。在远离本地系统的某处存储该备份信息。

- **用 IBM 客户端安全保护应用程序**

  选择您要用 IBM 客户端安全保护的应用程序。如果您尚未安装其它必需的应用程序，则一些选项可能不可用。

- **授权用户**

  用户可以访问计算机前，需要经过授权。授权用户时，您必须指定用户的口令。不允许未经授权的用户使用计算机。

- **选择系统安全级别**

  选择系统安全级别使您能既快又方便地建立基本安全策略。稍后，您可以在“IBM 客户端安全管理员实用程序”中定制安全策略。

使用安装向导完成典型配置

要使用 IBM 客户端安全安装向导完成典型配置，请完成以下过程:

1. 单击**开始 > 程序 > Access IBM > IBM 客户端安全软件 > IBM 客户端安全安装向导**。

   “欢迎使用 IBM 客户端安全安装向导”屏幕使您能够选择配置选项。
2. 选择“典型配置”（推荐）单选按钮并单击**下一步**。

   该选择启用 IBM 密码管理器且只需要输入一些参数。当您选择典型配置时，CSS 将您的备份信息和安全密钥存储在您的硬盘驱动器上。安全用户新手应该使用典型配置选项。此为缺省设置。

   显示“口令输入”屏幕。
3. 请完成以下任务:
   a. 在“输入口令”字段中输入口令。如果需要，单击**查看口令要求**按钮以帮助建立有效口令。

      注: 在初始安装的基础上或清除了 IBM 嵌入式安全芯片后，将要求您在“确认口令”字段中确认您的口令。还可能要求您提供超级用户密码（如果适用）。
   b. 在“口令提示”字段中输入词或短语。
   c. 单击**下一步**。

   如果在您的计算机上已检测到指纹阅读器，则将显示“指纹存储”屏幕。缺省情况下将选中**是，我想立即存储指纹**复选框。
4. 请执行以下操作之一:
   - 清除**是，我想立即存储指纹**复选框，然后单击**下一步**。
   - 单击**下一步**并按照屏幕上的指示信息开始立即注册您的指纹。

   显示“授权其他用户”屏幕。
5. 请执行以下操作之一:
   - 选中**选择要立即授权的其他用户（可选）**复选框然后单击**下一步**。
   - 单击**跳过**跳过该任务。

   显示“您的安全设置和功能的摘要”屏幕。
6. 单击**完成**以实现您已选定的安全设置。该过程可能需要几分钟。显示一条消息，表明您的计算机现在受 IBM 客户端安全的保护。
7. 单击**确定**。

使用安装向导完成高级配置

要使用 IBM 客户端安全安装向导完成典型配置，请完成以下过程:

1. 单击**开始 > 程序 > Access IBM > IBM 客户端安全软件 > IBM 客户端安全安装向导**。

   “欢迎使用 IBM 客户端安全安装向导”屏幕使您能够选择配置选项。
2. 选择**高级配置**单选按钮并单击**下一步**。

   该选择需要您指定配置信息（例如，密钥存储位置和安全级别），并允许您启用 CSS 登录保护、Lotus Notes 保护以及 IBM 密码管理器。

   显示“设置安全管理员密码”屏幕。
3. 在“输入管理员密码”字段中输入安全管理员密码并单击**下一步**。

   注: 首次安装时或清除了 IBM 嵌入式安全芯片后，将要求您在“确认管理员密码”字段确认安全管理员密码。还可能要求您提供超级用户密码（如果适用）。

   显示“创建管理员安全密钥”屏幕。
4. 请执行以下操作之一:
   - **创建新的安全密钥**

     要创建新的安全密钥，使用以下过程:
     a. 单击**新建密钥**单选按钮。
     b. 通过在所提供的字段中输入路径名，或通过单击**浏览**并选择相应的文件夹来指定您要在哪里保存管理员安全密钥。
     c. 如果您要分割安全密钥以增强保护，则单击**分割密钥存档以增强安全**复选框，以便在框中显示复选标记，然后使用箭头在**分割数**滚动框中选择期望的数值。
   - **使用现有的安全密钥**

     要使用现有的安全密钥，使用以下过程:
     a. 单击**使用现有的安全密钥**单选按钮。
     b. 通过在所提供的字段中输入路径名，或通过单击**浏览**并选择相应的文件夹来指定公钥的位置。
     c. 通过在所提供的字段中输入路径名，或单击**浏览**并选择相应的文件夹来指定私钥的位置。
5. 通过在所提供的字段中输入路径名，或通过单击**浏览**并选择相应的文件夹来指定其中您要保存安全信息的备份副本的密钥存档位置。
6. 单击**下一步**。

   显示“用 IBM 客户端安全保护应用程序”屏幕。
7. 通过选择相应的复选框（以便在每个所选框中显示复选标记）启用 IBM 客户端安全保护，并单击**下一步**。可用的客户端安全选择如下所示:
   - **通过用客户端安全安全登录替换常规的 Windows 登录来保护对系统的访问。**

     选择该框，以客户端安全安全登录替换常规的 Windows 登录。这将增加您系统的安全性，经过 IBM 嵌入式安全芯片和可选设备（如指纹阅读器或智能卡）验证后，才允许登录。
   - **启用文件和文件夹加密**

如果您要用 IBM 嵌入式安全芯片保护硬盘上的文件，则选择该框。（需要您下载 IBM 客户端安全文件和文件夹加密实用程序）。

- **启用 IBM 客户端安全密码管理器支持**

  如果您需要使用 IBM 密码管理器方便安全地存储 Web 站点登录和应用程序的密码，请选择该框。

- **用 IBM 客户端安全登录替换 Lotus Notes 登录**

  如果您想使客户端安全通过 IBM 嵌入式安全芯片对 Lotus Notes 用户进行验证，则选择该框。

- **启用 Entrust 支持**

  如果您想启用与 Entrust 安全软件产品的集成，则选择该框。

- **保护 Microsoft Internet Explorer**

  该保护使您能够保护电子邮件通信和通过 Microsoft Internet Explorer 进行的 Web 浏览（要求数字证书）。缺省情况下启用对 Microsoft Internet Explorer 的支持。

在您选择相应的复选框后，显示“授权用户”屏幕。

8. 通过完成以下过程之一来完成“授权用户”屏幕:
   - 要授权用户执行 IBM 客户端安全功能，请执行以下操作:
     a. 在“未授权用户”区域中选择一个用户。
     b. 单击**授权用户**。
     c. 在所提供的字段中输入并确认 IBM 客户端安全口令，并单击**下一步**。

        显示“UVM 口令失效”屏幕。
     d. 设置用户口令失效并单击**完成**。
     e. 单击**下一步**。
   - 要取消用户执行 IBM 客户端安全功能的授权，请执行以下操作:
     a. 在“已授权用户”区域中选择一个用户。
     b. 单击**取消对用户的授权**。

        显示消息“您是否确定要取消授权？”。
     c. 单击**是**。
     d. 单击**下一步**。

显示“选择系统安全级别”屏幕。

9. 通过单击相应的复选框选择希望的验证要求。您可以选择多个验证要求。
   - **使用 UVM 口令**复选框作为缺省选定。
   - 必须先安装指纹阅读器设备驱动程序和智能卡阅读器设备驱动程序，然后才可以启动 IBM 客户端安全安装向导以使这些设备对于安装向导可用。
   - 通过拖动滑动选择器到所期望的安全级别来选择系统安全级别，并单击**下一步**。

     注: 稍后，您可以使用管理员实用程序中的策略编辑器定义定制安全策略。

显示“安装完成 – 查看安全设置”屏幕。

10. 复查您的安全设置并采用以下操作之一:
    - 要接受设置，单击**完成**。
    - 要更改设置，单击**上一页**，做相应的更改；然后返回到该屏幕，并单击**完成**。

    IBM 客户端安全软件通过 IBM 嵌入式安全芯片配置设置。显示一条消息，确认您的计算机现在受 IBM 客户端安全的保护。
11. 单击**确定**。

启用 IBM 安全子系统

在您可以使用客户端安全软件前，必须启用 IBM 安全子系统。如果尚未启用芯片，则您可以使用管理员实用程序来启用它。先前部分中包含了使用“安装向导”的说明。

要使用管理员实用程序启用 IBM 安全子系统，请完成以下过程:

1. 单击**开始 > 设置 > 控制面板 > IBM 嵌入式安全子系统**。

   屏幕显示一条消息，表明尚未启用 IBM 安全子系统，并且询问您是否要立即启用它。
2. 单击**是**。

   显示一条消息，表明您是否已经启用了超级用户密码或 BIOS 管理员密码，继续操作前您必须在 BIOS Setup Utility 中禁用它。
3. 请执行以下操作之一:
   - 如果您启用了超级用户密码，单击**取消**，禁用超级用户密码，然后完成该过程。
   - 如果您没有启用超级用户密码，则单击**确定**继续。
4. 关闭所有打开的应用程序并单击**确定**以重新启动计算机。
5. 系统重新启动后，单击**开始 > 设置 > 控制面板 > IBM 嵌入式安全子系统**以打开管理员实用程序。

   显示一条消息，表明尚未配置或已经清除了 IBM 安全子系统。这时需要一个新密码。
6. 在相应的字段中输入并确认新的管理员密码，然后单击**确定**。

   操作完成并显示管理员实用程序主屏幕。

升级您的客户端安全软件版本

已安装客户端安全软件的先前版本的客户机应该将其软件更新至该版本，以利用客户端安全的新功能。

要点: 在安装该版本的 IBM 客户端安全软件之前，已安装了 IBM 客户端安全软件 V4.0x 的系统必须卸载 IBM 客户端安全软件 V4.0x 并清除芯片。如果不这样做，可能会导致安装失败，或没有响应的软件。

使用新的安全数据升级

如果您要完全除去客户端安全软件并重新开始，请完成以下过程:

1. 使用控制面板的“添加/删除程序” applet 卸载客户端安全软件的先前版本。

2. 重新引导系统。
3. 在 BIOS Setup Utility 中清除 IBM 嵌入式安全芯片。
4. 重新引导您的系统。
5. 安装客户端安全软件的最新版本并使用 IBM 客户端安全安装向导进行配置。

使用现有的安全数据从 CSS 5.0 或更高版本升级

如果您要使用现用的安全数据从客户端安全软件 V5.0 或更高版本升级，请完成以下过程:

1. 通过完成以下步骤更新您的存档:
   a. 请单击**开始 > 程序 > Access IBM > IBM 客户端安全软件 > 修改安全设置**。
   b. 单击**更新密钥存档**按钮以确保您的备份信息已更新。

      记录存档目录。
   c. 退出 IBM 客户端安全软件用户配置实用程序。
2. 通过完成以下步骤升级客户端安全软件的现有版本:
   a. 从 Windows 桌面，单击**开始 > 运行**。
   b. 在“运行”字段中，输入 `d:\directory\csec5xxus_00yy.exe`，其中 `d:\directory\` 是可执行文件所在的盘符和目录。`xx` 和 `yy` 是字母数字。
   c. 选择**升级**。
   d. 重新引导系统。

卸载客户端安全软件

在您卸载 IBM 客户端安全软件之前，请确保您卸载了各种实用程序（IBM 客户端安全密码管理器、IBM 客户端安全文件和文件夹加密（FFE）实用程序），这些实用程序增强客户端安全功能，例如 IBM。用户必须使用管理员权限登录才能卸载客户端安全软件。

注: 在卸载 IBM 客户端安全软件前，您必须卸载所有 IBM 客户端安全软件实用程序和所有支持 UVM 的传感器软件。卸载客户端安全软件需要管理员密码。

要卸载客户端安全软件，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. 在可以自动删除的软件列表中，选择 **IBM 客户端安全软件**。
5. 单击**添加/删除**。
6. 选择**删除**单选按钮。
7. 单击**下一步**卸载软件。
8. 单击**确定**确认该操作。
9. 在提供的界面中输入管理员密码并单击**确定**。
10. 请执行以下操作之一:

- 如果您为 Netscape 安装了 IBM 嵌入式安全芯片 PKCS#11 模块，则显示一条消息，要求您启动禁用 IBM 嵌入式安全芯片 PKCS#11 模块的进程。单击**是**以继续。

  将显示一系列消息。对每条消息单击**确定**，直至除去了 IBM 嵌入式安全芯片 PKCS#11 模块为止。
- 如果您没有为 Netscape 安装 IBM 嵌入式安全芯片 PKCS#11 模块，则显示一条消息，询问您是否要删除与客户端安全软件一起安装的共享 DLL 文件。

  单击**是**卸载这些文件，或单击**否**保留这些已安装的文件。保留这些已安装的文件不会影响计算机的正常运作。

显示消息“您是否要从存档中删除该系统的信息？”。如果您选择**否**，则当重新安装 IBM 客户端安全软件的更新版本时可以复原该信息。

11. 删除该软件后，单击**完成**。

    您必须在卸载客户端安全软件后重新启动计算机。

卸载客户端安全软件时，您全部除去已安装的客户端安全软件组件以及所有用户密钥、数字证书、已注册的指纹和存储的密码。

出口条例

IBM 客户端安全软件包含可以在北美和全球范围内下载的加密代码。如果您住在禁止从美国的 Web 站点中下载加密软件的国家或地区，则无法下载 IBM 客户端安全软件。有关管理 IBM 客户端安全软件的出口条例的更多信息，请参阅第 29 页的附录 A, 『客户端安全软件的美国出口条例』。

第 5 章 故障诊断

以下部分的信息有助于防止或识别以及更正安装或配置客户端安全软件时可能会遇到的问题。

管理员功能

授权用户

必须首先在客户机上安装 IBM 客户端安全软件，并且**必须**授权用户使用该软件才能保护客户机用户信息。易于使用的“安装向导”会指导您完成整个安装过程。

要点: 在安装过程中，**必须**至少授权一个客户机用户使用 UVM。如果在最初安装客户端安全软件时没有授权任何用户使用 UVM，则**不**会应用您的安全设置并且您的信息将**不**受保护。

如果完成了安装向导而没有授权任何用户，请关闭和重新启动计算机；然后从 Windows 开始菜单运行客户端安全安装向导并授权一个 Windows 用户使用 UVM。这将使 IBM 客户端安全软件能够应用您的安全设置并且保护您的敏感信息。

设置 BIOS 管理员密码（ThinkCentre）

在 Configuration/Setup Utility 中提供的安全设置使管理员能执行以下操作:

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

注意:

- 清除 IBM 嵌入式安全子系统时，所有存储在该子系统上的加密密钥和证书都将丢失。

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

设置 BIOS 管理员密码:

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

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

© Copyright IBM Corp. 2004

在您设置 BIOS 管理员密码后，每次您试图访问 Configuration/Setup Utility 时都会出现提示。

要点: 请妥善保存您的 BIOS 管理员密码的记录。如果您丢失或遗忘了 BIOS 管理员密码，则无法访问 Configuration/Setup Utility，且您在不卸下计算机外盖和移动系统板上的跳线的情况下无法更改或删除 BIOS 管理员密码。请参阅随计算机附带的硬件文档以获取更多的信息。

设置超级用户密码（ThinkPad）

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

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

注意:

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

在设置了客户端安全软件后，请设置一个超级用户密码以防止未授权的用户对这些设置进行更改。

要设置超级用户密码，请完成以下过程之一:

示例 1

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

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

示例 2

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

   Access IBM predesktop 区域打开。
3. 双击 **Start setup utility**。
4. 使用方向键浏览菜单以选择 **Security**。
5. 选择 **Password**。
6. 选择 **Supervisor Password**。
7. 输入您的密码并按 Enter 键。

8. 再次输入您的密码并按 Enter 键。
9. 单击 **Continue**。
10. 按 F10 保存并退出。

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

要点: 请妥善保存超级用户密码。如果您丢失或忘记了超级用户密码，则无法访问 IBM BIOS Setup Utility，而且无法更改或删除密码。请参阅随计算机附带的硬件文档以获取更多的信息。

清除 IBM 嵌入式安全子系统（ThinkCentre）

如果您想从 IBM 嵌入式安全子系统中擦除所有的用户加密密钥并清除此子系统的管理员密码，则必须清除芯片。在清除 IBM 嵌入式安全子系统前，请阅读下面的信息。

注意:

- 清除 IBM 嵌入式安全子系统时，所有存储在该子系统上的加密密钥和证书都将丢失。

要清除 IBM 嵌入式安全子系统，请完成以下过程:

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

   Setup Utility 主菜单打开。
3. 选择 **Security**。
4. 选择 **IBM TCPA Security Feature** 并按 Enter 键。
5. 选择 **Yes**。
6. 按 Enter 键确认您的选择。
7. 按 F10 保存更改并退出 Setup Utility。
8. 选择 **Yes** 并按 Enter 键。计算机将重新启动。

清除 IBM 嵌入式安全子系统（ThinkPad）

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

注意:

- 清除 IBM 嵌入式安全子系统时，所有存储在该子系统上的加密密钥和证书都将丢失。

要清除 IBM 嵌入式安全子系统，请完成以下过程:

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

   Setup Utility 主菜单打开。
3. 选择 **Security**。
4. 选择 **IBM Security Chip** 并按 Enter 键。
5. 按 Enter 键并选择 **Disabled**。
6. 按 Enter 键确认您的选择。
7. 按 Enter 键继续。

8. 按 F10 保存更改并退出 Setup Utility。
9. 选择 **Yes** 并按 Enter 键。计算机将重新启动。

有关 CSS V5.4 的已知问题或限制

以下信息在安装或配置客户端安全软件 V5.4 时可能会有所帮助。

重新安装 Targus 指纹软件

如果 Targus 指纹软件被除去并且重新安装，则必须手动添加启用客户端安全软件中的指纹支持所需要的注册表项以启用指纹支持。下载包含所需条目的注册表文件（atplugin.reg）并双击它将注册表条目合并到该注册表中。在提示时，单击“确定”以确认该操作。必须重新引导系统以使客户端安全软件能够识别更改并启用指纹支持。

注: 为了添加这些注册表条目，您在系统上必须具有管理员权限。

BIOS 超级用户口令

IBM 客户端安全软件 5.4 及更早版本不支持某些 ThinkPad 系统上可用的 BIOS 超级用户口令功能。如果您启用 BIOS 超级用户口令，则必须从 BIOS Setup 完成对安全子系统所做的任何启用和禁用。

智能卡限制

注册智能卡

在用户可以成功地使用智能卡进行验证之前，必须向 UVM 注册该智能卡。如果某智能卡分配给多个用户，则只有最后注册该卡的用户才能使用该卡。所以智能卡应该只注册给一个用户帐户。

故障诊断图表

以下部分提供的故障诊断图表可在您使用客户端安全软件遇到问题时提供帮助。

安装故障诊断信息

以下故障诊断信息可能在您安装客户端安全软件过程中遇到问题时向您提供帮助。

问题症状	可能的解决方案
软件安装期间显示一条错误消息	**操作**
安装软件时显示一条消息，询问您是否要除去所选应用程序及其全部组件。	单击**确定**退出窗口。再次开始安装过程来安装客户端安全软件的新版本。
安装期间显示消息，表明您必须升级或删除该程序。	执行下列操作之一: • 如果已安装客户端安全软件 5.0 之前的版本，则选择**删除**以将其删除。然后，重新启动计算机并使用 IBM BIOS Setup Utility 清除安全子系统。 • 否则，选择**升级**并继续安装。
由于未知管理员密码的原因，拒绝安装访问	**操作**

问题症状	可能的解决方案
在启用 IBM 嵌入式安全子系统的 IBM 客户机上安装软件时，IBM 嵌入式安全子系统的管理员密码未知。	清除安全子系统以继续安装。
当尝试某些客户端安全管理员功能时显示错误消息	**操作**
在尝试执行客户端安全管理员功能后会显示错误消息。	必须禁用 ThinkPad 超级用户密码或 ThinkCentre BIOS 管理员密码以在加密器 1（非 TCG）系统上生成硬件密钥对。CSS 安装过程直到相应的密码已禁用才可以启用 IBM 嵌入式安全子系统。

附录 A. 客户端安全软件的美国出口条例

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

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

© Copyright IBM Corp. 2004

附录 B. 密码和口令信息

本附录包含有关密码和口令的信息。

密码和口令规则

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

管理员密码规则

管理员实用程序中的界面使安全管理员能够通过简单界面控制管理员密码标准。该界面使管理员能够建立以下管理员密码规则:

注: 以下括号中提供了每个口令标准的缺省设置。管理员密码永不失效。

- 确定是否设置允许的最小字母数字字符数（是，6）

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

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

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

  例如，缺省情况下，1password 是无效密码。
- 确定是否使口令能以数字结束（否）

  例如，缺省情况下，password8 是无效密码。

以下一般规则适合于管理员密码:

长度 该密码最长可为 256 个字符。

字符 该密码可以包含键盘输入字符的任何组合，包括空格和非字母数字字符。

属性 管理员密码不同于您可能用于登录操作系统的密码。管理员密码可以结合其它验证设备使用，例如支持 UVM 的指纹传感器。

不正确的尝试

如果在会话过程中多次输入不正确的管理员密码，则计算机将实行一系列反攻击延迟。

UVM 口令规则

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

© Copyright IBM Corp. 2004

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

注: 以下括号中提供了每个口令标准的缺省设置。

- 确定是否设置允许的最小字母数字字符数（是，6）

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

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

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

  例如，缺省情况下，1password 是无效密码。
- 确定是否使口令能以数字结束（否）

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

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

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

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

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

- 确定是否在一定天数后，使口令失效（是，184）

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

  如果选择了该选项，口令将永不失效。

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

以下一般规则是关于 UVM 口令的:

长度 口令最多可以是 256 个字符。

字符 口令可包含键盘输入字符的任何组合，包含空格和非字母数字字符。

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

不正确的尝试

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

在系统上使用 National TPM 的失败计数

下表显示了 National TPM 系统的反攻击延迟设置:

尝试次数	下次失败时的延迟
7-13	每次 4 秒
14-20	每次 8 秒
21-27	每次 16 秒
28-34	每次 32 秒
35-41	每次 64 秒（每次 1.07 分）
42-48	每次 128 秒（每次 2.13 分）
49-55	每次 256 秒（每次 4.27 分）
56-62	每次 512 秒（每次 8.53 分）
63-69	每次 1,024 秒（每次 17.07 分）
70-76	每次 2,048 秒（每次 34.13 分）
77-83	每次 68.26 分（每次 1.14 小时）
84-90	每次 136.52 分（每次 2.28 小时）
91-97	每次 273.04 分（每次 4.55 小时）
98-104	每次 546.08 分（每次 9.1 小时）
105-111	每次 1,092.16 分（每次 18.2 小时）
112-118	每次 2,184.32 分（每次 36.4 小时）

National TPM 系统不区分用户口令和管理员密码。任何使用 IBM 嵌入式安全芯片的验证遵守相同的策略。没有最大超时。每次失败的尝试触发以上显示的延迟。反攻击延迟在第 118 次尝试时并未结束；或更确切地说，它们按以上说明的方式无限次继续。

在系统上使用 Atmel TPM 的失败计数

下表显示了 Atmel TPM 系统的反攻击延迟设置:

尝试次数	下次失败时的延迟
15	1.1 分钟
31	2.2 分钟
47	4.4 分钟
63	8.8 分钟
79	17.6 分钟
95	35.2 分钟
111	1.2 小时

尝试次数	下次失败时的延迟
127	2.3 小时
143	4.7 小时

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

重新设置口令

如果用户忘记其口令，则管理员可以使用户能够重新设置其口令。

远程重新设置口令

要远程重新设置密码，请完成以下过程:

- **管理员**

  远程管理员必须执行以下操作:

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

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

- **用户**

  用户必须执行以下操作:

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

     UVM 验证文件中的信息与所提供的密码是否匹配后，授权用户访问权。然后直接提示用户更改口令。

这是所建议的重新设置已丢失口令的方式。

手动重新设置口令

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

附录 C. 声明与商标

该附录提供 IBM 产品的法律声明以及商标信息。

声明

本信息是为在美国提供的产品和服务编写的。

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

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

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

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

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

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

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

商标

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

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

© Copyright IBM Corp. 2004

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

其它公司、产品和服务名称可能是其它公司的商标或服务标记。

中国印刷