IBM Client Security Solutions

Client Security, Version 5.1 Installationshandbuch

IBM Client Security Solutions

Client Security, Version 5.1 Installationshandbuch

Hinweis:
Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten Sie die Informationen in Anhang B, „Bemerkungen und Marken", auf Seite 53, lesen.

- Die IBM Homepage finden Sie im Internet unter: **ibm.com**
- IBM und das IBM Logo sind eingetragene Marken der International Business Machines Corporation.
- Das e-business-Symbol ist eine Marke der International Business Machines Corporation.
- Infoprint ist eine eingetragene Marke der IBM.
- ActionMedia, LANDesk, MMX, Pentium und ProShare sind Marken der Intel Corporation in den USA und/oder anderen Ländern.
- C-bus ist eine Marke der Corollary, Inc. in den USA und/oder anderen Ländern.
- Java und alle auf Java basierenden Marken und Logos sind Marken der Sun Microsystems, Inc. in den USA und/oder anderen Ländern.
- Microsoft Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.
- PC Direct ist eine Marke der Ziff Communications Company in den USA und/oder anderen Ländern.
- SET und das SET-Logo sind Marken der SET Secure Electronic Transaction LLC.
- UNIX ist eine eingetragene Marke der Open Group in den USA und/oder anderen Ländern.
- Marken anderer Unternehmen/Hersteller werden anerkannt.

Erste Ausgabe (April 2003)

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Client Security Solutions, Client Security Version 5.1 Installation Guide,
herausgegeben von International Business Machines Corporation, USA

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
SW TSC Germany
Kst. 2877
April 2003

Inhaltsverzeichnis

Vorwort

Dieser Abschnitt enthält Hinweise zur Verwendung dieses Handbuchs.

Inhalt dieses Handbuchs

Dieses Handbuch enthält Informationen zum Installieren von Client Security auf IBM Netzwerkcomputern, auch IBM Clients genannt, die integrierte IBM Security Chips enthalten. Außerdem enthält dieses Handbuch Anweisungen zur Aktivierung des integrierten IBM Security Chips und zur Festlegung eines Hardwarekennworts für den IBM Security Chip.

Das Handbuch umfasst folgende Inhalte:

Kapitel 1, „**Einführung in IBM Client Security**", enthält eine Übersicht über die in der Software enthaltenen Anwendungen und Komponenten sowie eine Beschreibung der PKI-Funkionen (Public Key Infrastructure).

Kapitel 2, „Erste Schritte", enthält Voraussetzungen für die Installation von Computerhardware und -software sowie Anweisungen zum Herunterladen der Software

Kapitel 3, „Vorbereitung der Software-Installation", enthält Anweisungen zu Voraussetzungen für die Installation von Client Security.

Kapitel 4, „Software installieren, aktualisieren und deinstallieren", enthält Anweisungen zum Installieren, Aktualisieren und Deinstallieren der Software.

Kapitel 5, „Fehlerbehebung", enthält nützliche Informationen zur Fehlerbehebung, die beim Befolgen der in diesem Handbuch enthaltenen Anweisungen auftreten können.

Anhang A, „Regeln für Kennwörter und Verschlüsselungstexte", enthält Kriterien für Kennwörter, die auf einen UVM-Verschlüsselungstext angewendet werden können, und Regeln für Kennwörter für den IBM Security Chip.

Anhang B, „Bemerkungen und Marken", enthält rechtliche Hinweise und Informationen zu Marken.

Zielgruppe

Dieses Handbuch ist für Netzwerk- und Systemadministratoren konzipiert, die für die Personal-Computing-Sicherheit auf IBM Clients sorgen. Vorausgesetzt werden Kenntnisse auf dem Gebiet der Sicherheitskonzepte, wie z. B. in PKI (Public Key Infrastructure) und in der Verwaltung von digitalen Zertifikaten in einer Netzwerkumgebung.

Benutzung des Handbuchs

Verwenden Sie dieses Handbuch, um die Personal-Computing-Sicherheit auf IBM Clients zu installieren und einzurichten. Dieses Handbuch dient als Ergänzung zu folgenden Handbüchern: *Client Security Administratorhandbuch*, *Client Security mit Tivoli Access Manager verwenden* und *Client Security Benutzerhandbuch*.

Dieses Handbuch und die gesamte weitere Dokumentation zu Client Security kann von der IBM Website unter
http://www.pc.ibm.com/ww/security/secdownload.html heruntergeladen werden.

Verweise auf das *Client Security Administratorhandbuch*

Dieses Handbuch enthält Verweise auf das *Client Security Administratorhandbuch*. Das *Administratorhandbuch* umfasst Informationen zur Verwendung von User Verification Manager (UVM) und zum Arbeiten mit der UVM-Policy sowie Informationen zur Verwendung des Administratordienstprogramms und des Benutzerkonfigurationsprogramm.

Wenn Sie die Software installiert haben, befolgen Sie die Anweisungen im *Administratorhandbuch* zum Einrichten und Verwalten der Security-Policy für die einzelnen Clients.

Verweise auf das *Client Security Benutzerhandbuch*

Das *Client Security Benutzerhandbuch*, das als Ergänzung zum *Client Security Administratorhandbuch* dient, enthält nützliche Informationen zur Ausführung von Benutzertasks mit Client Security, wie z. B. der Verwendung des UVM-Anmeldeschutzes, der Erstellung eines digitalen Zertifikats sowie der Verwendung des Benutzerkonfigurationsprogramms.

Zusätzliche Informationen

Zusätzliche Informationen sowie aktualisierte Fassungen der Sicherheitsprodukte erhalten Sie, sofern verfügbar, auf der IBM Website unter

http://www.pc.ibm.com/ww/security/index.html.

Kapitel 1. Einführung in IBM Client Security

Die Software "IBM Client Security" ist für IBM Computer konzipiert, die den integrierten IBM Security Chip zum Verschlüsseln von Dateien und Speichern von Chiffrierschlüsseln verwenden. Client Security besteht aus Anwendungen und Komponenten, mit denen IBM Kunden die Sicherheit von Clients im lokalen Netzwerk, im Unternehmen oder im Internet gewährleisten können.

Anwendungen und Komponenten von Client Security

Wenn Sie Client Security installieren, werden die folgenden Softwareanwendungen und -komponenten installiert:

- **Administratordienstprogramm:** Das Administratordienstprogramm ist die Schnittstelle, über die ein Administrator den integrierten IBM Security Chip aktiviert oder inaktiviert sowie Chiffrierschlüssel und Verschlüsselungstexte erstellt, archiviert und erneut generiert. Darüber hinaus kann ein Administrator mit diesem Dienstprogramm der Sicherheits-Policy, die von Client Security bereitgestellt wird, Benutzer hinzufügen.
- **User Verification Manager (UVM):** In Client Security werden mit UVM Verschlüsselungstexte und andere Elemente verwaltet, mit denen Systembenutzer authentifiziert werden. Mit einem Lesegerät für Fingerabdrücke kann UVM z. B. bei der Anmeldung Benutzer authentifizieren. UVM bietet folgende Möglichkeiten:
  - **Schutz durch UVM-Client-Policy:** Mit UVM kann ein Administrator die Sicherheits-Policy für Clients festlegen, die bestimmt, wie auf dem System die Authentifizierung eines Clientbenutzers erfolgt.

    Wenn die Policy festlegt, dass Fingerabdrücke für die Anmeldung erforderlich sind, und der Benutzer keine Fingerabdrücke registriert hat, hat er die Möglichkeit, Fingerabdrücke bei der Anmeldung zu registrieren. Wenn die Überprüfung von Fingerabdrücken erforderlich ist und kein Scanner angeschlossen ist, meldet UVM einen Fehler. Wenn das Windows-Kennwort nicht oder nicht richtig in UVM registriert ist, hat der Benutzer die Möglichkeit, das richtige Windows-Kennwort als Teil der Anmeldung anzugeben.
  - **UVM-Systemanmeldeschutz:** UVM ermöglicht es Administratoren, den Zugriff auf die Computer über eine Anmeldeschnittstelle zu steuern. Der UVM-Schutz stellt sicher, dass nur Benutzer, die von der Sicherheits-Policy erkannt werden, auf das Betriebssystem zugreifen können.
  - **UVM Client Security-Bildschirmschonerschutz:** Bei Einsatz von UVM können Benutzer den Zugriff auf den Computer über eine Schnittstelle für den Client Security-Bildschirmschoner steuern.
- **Administratorkonsole:** Die Administratorkonsole von Client Security ermöglicht es einem Sicherheitsadministrator, administratorspezifische Tasks über Fernzugriff auszuführen.
- **Benutzerkonfigurationsprogramm:** Mit dem Benutzerkonfigurationsprogramm können Clientbenutzer den UVM-Verschlüsselungstext ändern. Unter Windows 2000 und Windows XP können Benutzer mit dem Clientdienstprogramm Schlüsselarchive aktualisieren und Windows-Anmeldekennwörter ändern, so dass diese von UVM erkannt werden. Außerdem kann ein Benutzer Sicherungskopien der digitalen Zertifikate erstellen, die vom integrierten IBM Security Chip erzeugt wurden.

PKI-Funktionen

Client Security bietet alle erforderlichen Komponenten, um in Ihrem Unternehmen eine PKI (Public Key Infrastructure) aufzubauen, z. B.:

- **Steuerung der Client-Sicherheits-Policy durch Administratoren:** Die Authentifizierung von Endbenutzern auf Clientebene ist ein wichtiger Aspekt für Sicherheits-Policies. Client Security bietet die erforderliche Schnittstelle zur Verwaltung der Sicherheits-Policy eines IBM Clients. Diese Schnittstelle ist Teil der Authentifizierungssoftware UVM (User Verification Manager), der Hauptkomponente von Client Security.
- **Chiffrierschlüsselverwaltung für öffentliche Schlüssel:** Administratoren können mit Client Security Chiffrierschlüssel für die Computerhardware und für die Clientbenutzer erstellen. Bei der Erstellung von Chiffrierschlüsseln sind diese über eine Schlüsselhierarchie an den integrierten IBM Security Chip gebunden. In der Hierarchie wird ein Hardwareschlüssel der Basisebene verwendet, um die übergeordneten Schlüssel sowie die den einzelnen Clientbenutzern zugeordneten Benutzerschlüssel zu verschlüsseln. Die Verschlüsselung und Speicherung von Schlüsseln auf dem integrierten IBM Security Chip erweitert die Clientsicherheit um eine wesentliche zusätzliche Ebene, da die Schlüssel sicher an die Computerhardware gebunden sind.
- **Erstellung und Speicherung digitaler Signaturen, die durch den integrierten IBM Security Chip geschützt sind:** Wenn Sie ein digitales Zertifikat anfordern, das für die digitale Signatur und für die Verschlüsselung einer E-Mail verwendbar ist, können Sie mit Client Security den integrierten IBM Security Chip zur Bereitstellung der Verschlüsselung für Anwendungen einsetzen, die mit der Microsoft CryptoAPI funktionieren. Zu diesen Anwendungen gehören Internet Explorer und Microsoft Outlook Express. Dadurch ist sichergestellt, dass der private Schlüssel des digitalen Zertifikats auf dem integrierten IBM Security Chip gespeichert wird. Darüber hinaus können Netscape-Benutzer integrierte IBM Security Chips zum Generieren von privaten Schlüsseln für die zum Erhöhen der Systemsicherheit verwendeten digitalen Zertifikate auswählen. Anwendungen nach dem Standard PKCS #11 (Public-Key Cryptography Standard Nr. 11), wie z. B. Netscape Messenger, können sich über den integrierten IBM Security Chip schützen.
- **Digitale Zertifikate auf den integrierten IBM Security Chip übertragen:** Mit dem Tool zur Übertragung von Zertifikaten von Client Security können Sie Zertifikate, die mit dem Standard-Microsoft-CSP erstellt wurden, an das CSP-Modul des integrierten IBM Sicherheits-Subsystems übertragen. Dadurch wird der notwendige Schutz für private Schlüssel, die zu Zertifikaten gehören, beträchtlich erhöht, da die Schlüssel nun statt in gefährdeter Software im integrierten IBM Security Chip sicher gespeichert sind.
- **Funktion zur Schlüsselarchivierung und -wiederherstellung:** Eine wichtige PKI-Funktion ist das Erstellen eines Schlüsselarchivs, aus dem Schlüssel bei Verlust oder Beschädigung der Originalschlüssel wiederhergestellt werden können. Client Security bietet eine Schnittstelle, mit der Sie mit dem integrierten IBM Security Chip erstellte Archive für Schlüssel und digitale Zertifikate erstellen und diese Schlüssel und Zertifikate bei Bedarf wiederherstellen können.
- **Verschlüsselung von Dateien und Ordnern:** Die Verschlüsselung von Dateien und Ordnern ermöglicht dem Benutzer das schnelle und einfache Ver- und Entschlüsseln von Dateien und Ordnern. So wird eine höhere Stufe von Datensicherheit als erste der Sicherheitsmaßnahmen des CSS-Systems gewährleistet.

- **Authentifizierung über Fingerabdrücke:** IBM Client Security unterstützt das Lesegerät für Fingerabdrücke von Targus als PC-Karte oder über USB für die Authentifizierung. Die Client Security-Software muss installiert sein, bevor die Einheitentreiber für das Targus-Lesegerät für Fingerabdrücke installiert werden, damit ein ordnungsgemäßer Betrieb gewährleistet ist.
- **Smartcard-Authentifizierung:** IBM Client Security unterstützt jetzt auch Smartcards als Authentifizierungseinheiten. Client Security ermöglicht die Verwendung von Smartcards zur Authentifizierung als Token, d. h., es kann sich jeweils nur ein Benutzer authentifizieren. Jede Smartcard ist systemgebunden, wenn nicht der standortunabhängige Zugriff (Roaming) mit Berechtigungsnachweis verwendet wird. Wenn eine Smartcard erforderlich ist, sollte die Systemsicherheit erhöht werden, da diese Karte mit einem Kennwort geliefert werden muss, das möglicherweise ausspioniert werden kann.
- **Standortunabhängiger Zugriff mit Berechtigungsnachweis:** Der standortunabhängige Zugriff mit Berechtigungsnachweis ermöglicht es einem von UVM autorisierten Benutzer, jedes System im Netzwerk genau wie die eigene Workstation zu verwenden. Wenn ein Benutzer berechtigt ist, UVM auf irgendeinem bei CSS registrierten Client zu verwenden, kann er seine persönlichen Daten in alle anderen registrierten Clients im Netzwerk importieren. Die persönlichen Daten werden im CSS-Archiv und auf jedem System, in das sie importiert wurden, automatisch aktualisiert und gewartet. Aktualisierungen der persönlichen Daten, wie z. B. neue Zertifikate oder Änderungen am Verschlüsselungstext, sind sofort auf allen Systemen verfügbar.
- **FIPS 140-1-Zertifizierung:** Client Security unterstützt FIPS 140-1-zertifizierte, verschlüsselte Bibliotheken. FIPS-zertifizierte RSA-BSAFE-Bibliotheken werden auf TCPA-Systemen verwendet.
- **Ablauf des Verschlüsselungstexts:** Client Security legt jeweils beim Hinzufügen eines Benutzers einen benutzerspezifischen Verschlüsselungstext und eine Policy für das Ablaufen des Verschlüsselungstexts fest.
- **Automatischer Schutz für ausgewählte Ordner:** Die Funktion zum automatischen Schützen von Ordnern ermöglicht es einem Client-Security-Administrator, festzulegen, dass alle Ordner mit der Bezeichnung "Eigene Dateien" der von UVM autorisierten Benutzer automatisch geschützt werden, ohne dass seitens der Benutzer eine Aktivität ausgeführt werden muss.

Kapitel 2. Erste Schritte

In diesem Kapitel werden die Hard- und Softwarevoraussetzungen zur Verwendung von Client Security beschrieben. Außerdem werden Ihnen Informationen zum Herunterladen von Client Security bereitgestellt.

Hardwarevoraussetzungen

Bevor Sie die Software herunterladen und installieren, vergewissern Sie sich, dass Ihre Computerhardware mit Client Security kompatibel ist.

Die neusten Informationen zu den Hard- und Softwarevoraussetzungen finden Sie auf der IBM Website unter
http://www.pc.ibm.com/ww/security/secdownload.html.

Integrierter IBM Security Chip

Der integrierte IBM Security Chip ist ein verschlüsselter Mikroprozessor, der in der Systemplatine des IBM Clients integriert ist. Diese grundlegende Komponente von IBM Client Security wandelt die Funktionen der Security-Policy von ungeschützter Software in sichere Hardware um und trägt so dazu bei, die Sicherheit des lokalen Client wesentlich zu erhöhen.

Nur die IBM Computer und Workstations, die integrierte IBM Security Chips enthalten, unterstützen auch Client Security. Wenn Sie versuchen, die Software herunterzuladen und auf einem Computer zu installieren, der keinen integrierten IBM Security Chip enthält, hat dies zur Folge, dass die Software nicht ordnungsgemäß installiert und demzufolge auch nicht fehlerfrei ausgeführt wird.

Unterstützte IBM Modelle

Client Security ist für eine Vielzahl von IBM Desktopcomputern und Notebooks lizenziert, die es auch unterstützt. Eine vollständige Liste der unterstützten Modelle finden Sie auf der Webseite
http://www.pc.ibm.com/ww/resources/security/secdownload.html.

Softwarevoraussetzungen

Bevor Sie die Software herunterladen und installieren, vergewissern Sie sich, dass Ihre Computersoftware sowie das von Ihnen verwendete Betriebssystem mit Client Security kompatibel sind.

Betriebssysteme

Für die Ausführung von Client Security ist eines der folgenden Betriebssysteme erforderlich:

- Windows XP
- Windows 2000 Professional

UVM-sensitive Produkte

IBM Client Security wird mit der Software "User Verification Manager" (UVM) geliefert. Mit dieser Software können Sie die Authentifizierung für Ihren Desktopcomputer anpassen. Diese erste Stufe der Policy-basierten Steuerung erhöht den Investitionsschutz und die Effizienz der Kennwortverwaltung. UVM ist mit den unternehmensübergreifenden Security-Policy-Programmen kompatibel und ermöglicht es Ihnen, UVM-sensitive Produkte zu verwenden. Zu diesen Produkten gehören u. a. Folgende:

- **Biometrische Geräte, wie z. B. Lesegeräte für Fingerabdrücke**

  UVM bietet eine Plug-and-Play-Schnittstelle für biometrische Geräte. Sie müssen Client Security vor der Installation eines UVM-Sensors installieren.

  Um einen UVM-Sensor zu verwenden, der bereits auf einem IBM Client installiert wurde, müssen Sie zuerst den UVM-Sensor wieder deinstallieren, anschließend Client Security installieren und dann den UVM-Sensor erneut installieren.

- **Tivoli Access Manager Version 3.8 oder 3.9**

  UVM erleichtert und verbessert die Policy-Verwaltung durch eine reibungslose Integration in eine zentralisierte, Policy-basierte Zugriffssteuerungslösung, wie z. B. Tivoli Access Manager.

  UVM erzwingt eine lokale Policy, unabhängig davon, ob es sich bei dem System um ein in ein Netzwerk integriertes System (Desktop) oder ein Standalone-System handelt, und stellt somit ein einziges, einheitliches Policy-Modell bereit.

- **Lotus Notes ab Version 4.5**

  UVM erhöht zusammen mit Client Security die Sicherheit Ihrer Lotus Notes-Anmeldung (Lotus Notes ab Version 4.5).

- **Entrust Desktop Solutions 5.1, 6.0 oder 6.1**

  Die Unterstützung durch Entrust Desktop Solutions verbessert das Leistungsspektrum für die Internet-Sicherheit, so dass kritische Unternehmensprozesse über das Internet abgewickelt werden können. Entrust Entelligence stellt einen Single Security Layer zur Verfügung, der die gesamten Anforderungen eines Unternehmens hinsichtlich der erweiterten Sicherheitseinrichtungen (einschließlich Identifikation, Vertraulichkeit, Prüfung und Sicherheitsverwaltung) erfüllt.

- **RSA SecurID Software Token**

  Mit RSA SecurID Software Token kann der gleiche Datensatz für den Generierungswert für Zufallszahlen, der auch in herkömmlichen RSA Hardware Tokens verwendet wird, in bereits vorhandene Benutzerplattformen integriert werden. Demzufolge haben Benutzer die Möglichkeit, sich auf geschützten Ressourcen zu authentifizieren, indem sie auf die integrierte Software zugreifen, statt dedizierte Authentifizierungseinheiten verwenden zu müssen.

- **Targus-Lesegerät für Fingerabdrücke**

  Das Targus-Lesegerät für Fingerabdrücke ist eine benutzerfreundliche Schnittstelle, über die die Sicherheits-Policy für die Authentifizierung über Fingerabdrücke aktiviert werden kann.

- **Gemplus GemPC400-Smartcard-Leseeinheit**

  Die Gemplus GemPC400-Smartcard-Leseeinheit aktiviert die Sicherheitspolicy für die Smartcard-Authentifizierung und fügt so dem Standardschutz durch Verschlüsselungstext eine weitere Sicherheitsebene hinzu.

Webbrowser

Folgende Webbrowser werden von Client Security bei der Anforderung digitaler Zertifikate unterstützt:

- Internet Explorer 5.0 oder höher
- Netscape 4.51 bis Netscape 7

Informationen zum Webbrowser-Verschlüsselungsgrad

Wenn eine Unterstützung für hochgradige Verschlüsselung installiert ist, verwenden Sie die 128-Bit-Version Ihres Webbrowsers. Andernfalls verwenden Sie die 40-Bit-Version Ihres Webbrowsers. Weitere Informationen zur Feststellung des Verschlüsselungsgrades erhalten Sie über die Hilfefunktion des Browsers.

Verschlüsselungsdienste

Client Security unterstützt folgende Verschlüsselungsdienste:

- **Microsoft CryptoAPI:** CryptoAPI ist der Standardverschlüsselungsdienst für Betriebssysteme und Anwendungen von Microsoft. Mit der integrierten Unterstützung von CryptoAPI können Sie über Client Security die Verschlüsselungsvorgänge des integrierten IBM Security Chips beim Erstellen von digitalen Zertifikaten für Microsoft Anwendungen verwenden.
- **PKCS #11-Modul:** Beim PKCS #11-Modul handelt es sich um den Verschlüsselungsstandard für Netscape, Entrust, RSA und andere Produkte. Wenn Sie das PKCS #11-Modul für den integrierten IBM Security Chip installiert haben, können Sie mit dem integrierten IBM Security Chip digitale Zertifikate für Netscape, Entrust, RSA und andere Anwendungen, die das PKCS #11-Modul verwenden, erstellen.

E-Mail-Anwendungen

Client Security unterstützt folgende Anwendungstypen über gesicherte E-Mail:

- E-Mail-Anwendungen, die Microsoft CryptoAPI für Verschlüsselungsvorgänge verwenden, wie z. B. Outlook Express und Outlook (sofern eine unterstützte Version von Internet Explorer verwendet wird).
- E-Mail-Anwendungen, die das PKCS #11-Modul (Public Key Cryptographic Standard) für Verschlüsselungsvorgänge verwenden, wie z. B. Netscape Messenger (sofern eine unterstützte Version von Netscape verwendet wird).

Software herunterladen

Die Software "Client Security" kann von der IBM Website unter http://www.pc.ibm.com/ww/security/secdownload.html heruntergeladen werden.

Registrierungsformular

Wenn Sie die Software herunterladen, müssen Sie ein Registrierungsformular und einen Fragenkatalog ausfüllen und den Lizenzbedingungen zustimmen. Befolgen Sie die Anweisungen, die auf der Website zum Herunterladen der Software angezeigt werden.

Die Installationsdateien für Client Security sind in der sich selbst entpackenden Datei mit dem Namen "csec51.exe" enthalten.

Kapitel 3. Vorbereitung der Software-Installation

Dieses Kapitel enthält alle Vorbereitungen zum Ausführen des Installationsprogramms und zum Konfigurieren von Client Security auf IBM Clients. Alle für die Installation erforderlichen Dateien sind in der Datei "csec51.exe" enthalten, die Sie von der IBM Website herunterladen können.

Software-Installation einleiten

Das Installationsprogramm installiert Client Security auf dem IBM Client und aktiviert den integrierten IBM Security Chip. Die einzelnen Installationsschritte können in Abhängigkeit von verschiedenen Faktoren unterschiedlich ausfallen.

Auf Clients mit Windows XP oder Windows 2000 installieren

Die Benutzer von Windows XP und Windows 2000 müssen sich für die Installation von Client Security mit Administratorbenutzerberechtigung anmelden.

Für die Verwendung mit Tivoli Access Manager installieren

Wenn Sie Tivoli Access Manager zur Steuerung der Authentifizierungsbestimmungen für Ihren Computer verwenden möchten, müssen Sie vor der Installation von Client Security zuerst bestimmte Komponenten von Client Security Manager installieren. Weitere Informationen hierzu finden Sie im Handbuch *Client Security mit Tivoli Access Manager verwenden*.

Wichtige Hinweise zu den Funktionen beim Systemstart

Es gibt zwei IBM Funktionen beim Systemstart, die die Art und Weise, in der Sie das Sicherheits-Subsystem (integrierter IBM Security Chip) aktivieren und Chiffrierschlüssel für die Hardware erstellen, beeinflussen können. Bei diesen Funktionen handelt es sich um das Administratorkennwort und die erweiterten Sicherheitseinrichtungen.

Administratorkennwort (NetVista)

Administratorkennwörter verhindern, dass nicht autorisierte Personen die Konfigurationseinstellungen eines IBM Computers ändern. Diese Kennwörter werden im Programm "Configuration/Setup Utility" festgelegt. Dieses Programm können Sie während des Systemstarts mit F1 aufrufen.

Administratorkennwort (ThinkPad)

Administratorkennwörter verhindern, dass nicht autorisierte Personen die Konfigurationseinstellungen eines IBM ThinkPad Computers ändern. Diese Kennwörter werden im Programm "IBM BIOS Setup Utility" festgelegt. Dieses Programm können Sie während des Systemstarts mit F1 aufrufen.

Erweiterte Sicherheitseinrichtungen

Die erweiterten Sicherheitseinrichtungen bieten einen zusätzlichen Schutz für das Administratorkennwort und die Einstellungen während des Systemstarts. Im Programm "Configuration/Setup Utility" können Sie feststellen, ob die erweiterten Sicherheitseinrichtungen aktiviert sind oder nicht. Dieses Programm können Sie während des Systemstarts mit F1 aufrufen.

Weitere Informationen zu Kennwörtern und erweiterten Sicherheitseinrichtungen finden Sie in der Dokumentation zu Ihrem Computer.

Erweiterte Sicherheitseinrichtungen auf den NetVista-Modellen 6059, 6569, 6579, 6649 und auf allen NetVista Q1x-Modellen: Wenn auf den NetVista-Modellen 6059, 6569, 6579, 6649, 6646 und allen Q1x-Modellen ein Administratorkennwort festgelegt wurde, müssen Sie den Chip im Administratordienstprogramm aktivieren und die Schlüssel für die Hardware erstellen.

Wenn auf diesen NetVista-Modellen die erweiterten Sicherheitseinrichtungen aktiviert wurden, müssen Sie nach der Installation von Client Security im Administratordienstprogramm den integrierten IBM Security Chip aktivieren und die Chiffrierschlüssel für die Hardware erstellen. Wenn das Installationsprogramm feststellt, dass die erweiterten Sicherheitseinrichtungen aktiviert sind, erhalten Sie am Ende des Installationsprozesses eine entsprechende Nachricht. Starten Sie den Computer erneut, und öffnen Sie das Administratordienstprogramm, um den Chip zu aktivieren und die Schlüssel für die Hardware zu erstellen.

Erweiterte Sicherheitseinrichtungen auf allen anderen NetVista-Modellen (mit Ausnahme von 6059, 6569, 6579, 6649 und allen NetVista Q1x-Modellen): Wenn für ein anderes Modell ein Administratorkennwort festgelegt wurde, müssen Sie während des Installationsprozesses kein Administratorkennwort eingeben.

Wenn auf diesen NetVista-Modellen die erweiterten Sicherheitseinrichtungen aktiviert wurden, können Sie die Software mit Hilfe des Installationsprogramms installieren, müssen jedoch den integrierten IBM Security Chip über das Programm "Configuration/Setup Utility" aktivieren. Wenn Sie den Chip aktiviert haben, können Sie im Administratordienstprogramm die Schlüssel für die Hardware erstellen.

Informationen zur BIOS-Aktualisierung

Bevor Sie die Software installieren, müssen Sie möglicherweise den neuesten BIOS-Code (Basic Input/Output System) für Ihren Computer herunterladen. Um die auf Ihrem Computer verwendete BIOS-Stufe festzustellen, müssen Sie den Computer erneut starten und mit F1 das Programm "Configuration/Setup Utility" aufrufen. Wenn das Hauptmenü des Programms "Configuration/Setup Utility" angezeigt wird, wählen Sie "Product Data" aus, um weitere Informationen zum BIOS-Code zu erhalten. Die BIOS-Codestufe wird auch als EEPROM-Änderungsstufe bezeichnet.

Um Client Security 2.1 oder höher auf den NetVista-Modellen 6059, 6569, 6579, 6649 auszuführen, müssen Sie die BIOS-Stufe xxxx22axx oder höher verwenden. Um Client Security 2.1 oder höher auf den NetVista-Modellen 6790, 6792, 6274, 2283 auszuführen, müssen Sie die BIOS-Stufe xxxx20axx oder höher verwenden. Weitere Informationen hierzu finden Sie in der README-Datei, die im Software-Download enthalten ist.

Die neusten BIOS-Code-Aktualisierungen für Ihren Computer finden Sie auf der IBM Website unter http://www.pc.ibm.com/support, indem Sie dort in das Suchfeld "BIOS" eingeben, die entsprechenden Downloads aus der Dropdown-Liste auswählen und die Eingabetaste drücken. Daraufhin Ihnen wird eine Liste mit allen BIOS-Code-Aktualisierungen angezeigt. Klicken Sie auf die zutreffende NetVista-Modellnummer, und befolgen Sie die auf der Webseite angezeigten Anweisungen.

Archivschlüsselpaar verwenden

Mit dem Archivschlüsselpaar, das sich aus dem öffentlichen Schlüssel für Administratoren und dem privaten Schlüssel für Administratoren zusammensetzt, können Sie Chiffrierschlüssel für die Hardware für einen IBM Client erstellen und Kopien der Schlüsseldaten an einer beliebigen Stelle für Wiederherstellungszwecke aufbewahren.

Da Sie das Administratordienstprogramm von Client Security zum Erstellen des Archivschlüsselpaars verwenden, müssen Sie Client Security auf einem ersten IBM Client installieren und anschließend das Archivschlüsselpaar erstellen. Weitere Anweisungen zum Installieren und zum Konfigurieren der Software auf dem ersten IBM Client finden Sie auf den folgenden Seiten.

Anmerkung: Wenn Sie eine UVM-Policy verwenden möchten, die auf fernen Clients verwendet werden kann, müssen Sie beim Installieren der Software auf diesen Clients das gleiche Archivschlüsselpaar verwenden.

Kapitel 4. Software installieren, aktualisieren und deinstallieren

Dieses Kapitel enthält Anweisungen zum Herunterladen, Installieren und Konfigurieren von Client Security auf IBM Clients. Außerdem enthält dieses Kapitel Anweisungen zum Deinstallieren der Software. Installieren Sie IBM Client Security, bevor Sie eines der Dienstprogramme für Client Security installieren.

Wichtig: Wenn Sie von einer Version von Client Security aufrüsten, die älter als Version 5.0 ist, müssen Sie alle verschlüsselten Dateien entschlüsseln, bevor Sie Client Security 5.1 installieren. Client Security 5.1 kann aufgrund von Änderungen bei der Dateiverschlüsselungsimplementierung keine Dateien entschlüsseln, die mit älteren Versionen von Client Security als Version 5.0 verschlüsselt wurden.

Software herunterladen und installieren

Alle für die Installation von Client Security erforderlichen Dateien sind in der Datei "csec51.exe" enthalten, die Sie von der IBM Website unter http://www.pc.ibm.com/ww/security/secdownload.html herunterladen können. Auf der Website finden Sie Informationen, mit deren Hilfe Sie sicherstellen können, dass Sie über den integrierten IBM Security Chip verfügen und die Ihnen die Auswahl des passenden Client Security-Angebots für Ihr System ermöglichen.

Gehen Sie wie folgt vor, um die entsprechenden Dateien für Ihr System herunterzuladen:

1. Geben Sie in einem Webbrowser den URL für folgende IBM Website ein: http://www.pc.ibm.com/ww/security/secdownload.html.
2. Vergewissern Sie sich anhand der Informationen auf der Website, dass Ihr System über den integrierten IBM Security Chip verfügt, indem Sie Ihre Modellnummer mit den Angaben in der Tabelle mit den Systemvoraussetzungen vergleichen. Klicken Sie anschließend auf **Continue**.
3. Wählen Sie den Radioknopf für Ihren Maschinentyp, und klicken Sie auf **Continue**.
4. Erstellen Sie eine Benutzer-ID, füllen Sie das Onlineformular zur Registrierung aus, und lesen Sie die Lizenzvereinbarung. Klicken Sie dann auf **Accept Licence**.

   Sie werden danach automatisch zur Download-Seite für Client Security geführt.
5. Befolgen Sie die angezeigten Anweisungsschritte, um die erforderlichen Einheitentreiber, Readme-Dateien, Software, Referenzdokumente und zusätzliche Dienstprogramme von IBM Client Security herunterzuladen. Gehen Sie anhand der auf der Website angegebenen Download-Reihenfolge vor.
6. Klicken Sie auf dem Windows-Desktop auf **Start > Ausführen**.
7. Geben Sie in das Feld "Ausführen" `d:\directory\csec51.exe` ein. Hierbei gibt d:\directory\ den Laufwerkbuchstaben und das Verzeichnis an, in dem die Datei gespeichert ist.
8. Klicken Sie auf **OK**.

   Das Begrüßungsfenster des InstallShield-Assistenten von IBM Client Security wird angezeigt.

9. Klicken Sie auf **Weiter**.

   Der Assistent extrahiert die Dateien und installiert die Software. Nach Abschluss der Installation werden Sie gefragt, ob der erforderliche Neustart sofort oder zu einem späteren Zeitpunkt durchgeführt werden soll.

10. Klicken Sie zur Bestätigung auf **OK**.

    Nach dem Neustart des Computers wird der Konfigurationsassistent von IBM Client Security aufgerufen.

Konfigurationsassistenten für die Installation von IBM Client Security verwenden

Der Konfigurationsassistent für die Installation von IBM Client Security stellt eine Schnittstelle zur Verfügung, die Sie beim Installieren von Client Security und beim Aktivieren des integrierten IBM Security Chips unterstützt. Der Konfigurationsassistent von IBM Client Security führt Sie auch durch die Tasks zum Konfigurieren einer Sicherheits-Policy auf einem IBM Client.

Dies umfasst folgende Schritte:

- **Kennwort des Sicherheitsadministrators definieren**

  Mit dem Kennwort des Sicherheitsadministrators wird der Zugriff auf das Administratordienstprogramm von IBM Client Security gesteuert, mit dem die Sicherheitseinstellungen für diesen Computer geändert werden.

- **Sicherheitsschlüssel für Administratoren erstellen**

  Bei Sicherheitsschlüsseln für Administratoren handelt es sich um eine Gruppe digitaler Schlüssel, die in einer Computerdatei gespeichert sind. Es empfiehlt sich, diese Sicherheitsschlüssel auf einem austauschbaren Datenträger oder Laufwerk zu speichern. Wenn im Administratordienstprogramm des IBM Sicherheits-Subsystems eine Änderung an der Sicherheits-Policy vorgenommen wird, erfolgt eine Systemanfrage nach dieser Datei als Nachweis dafür, dass die Berechtigung zur Änderung der Sicherheits-Policy vorliegt.

  Eine Backup-Version der Sicherheitsdaten wird auch für den Fall gespeichert, dass die Systemplatine oder ein Festplattenlaufwerk des Computers ausgetauscht werden muss. Diese Backup-Version sollte nicht auf dem System gespeichert werden.

- **Anwendungen mit IBM Client Security schützen**

  Wählen Sie die Anwendungen aus, die mit IBM Client Security gegen unzulässige Zugriffe geschützt werden sollen. Einige Optionen sind nur verfügbar, wenn hierfür erforderliche Anwendungen installiert sind.

- **Benutzer autorisieren**

  Benutzer müssen, bevor Sie auf den Computer zugreifen können, für den Zugriff autorisiert werden. Beim Autorisieren eines Benutzers müssen Sie den Verschlüsselungstext des betreffenden Benutzers angeben. Nicht autorisierte Benutzer haben keinen Zugriff auf den Computer.

- **Sicherheitsstufe des Systems auswählen**

  Durch Auswahl einer Systemsicherheitsstufe können Sie auf schnelle und einfache Weise eine grundlegende Sicherheits-Policy einrichten. Sie können zu einem späteren Zeitpunkt im Administratordienstprogramm von IBM Client Security eine angepasste Sicherheits-Policy definieren.

Gehen Sie wie folgt vor, um den Konfigurationsassistenten für die Installation von IBM Client Security zu verwenden:

1. Falls der Assistent nicht bereits geöffnet ist, klicken Sie auf **Start > Programme > Access IBM > IBM Client Security > Konfigurationsassistent von IBM Client Security**.

   Im Fenster "Willkommen beim Konfigurationsassistenten von IBM Client Security" wird eine Übersicht über die Konfigurationsprozedur angezeigt.

   Anmerkung: Falls Sie die Authentifizierung über Fingerabdruck nutzen wollen, müssen Sie das Lesegerät für Fingerabdrücke und die zugehörige Software installieren, bevor Sie fortfahren.

2. Klicken Sie auf **Weiter**, um die Konfigurationsprozedur über den Assistenten zu beginnen.

   Die Anzeige "Sicherheitsadministratorkennwort angeben" erscheint.

3. Geben Sie in das Feld "Geben Sie das Administratorkennwort ein" das Kennwort des Sicherheitsadministrators ein, und klicken Sie auf **Weiter**.

   Anmerkung: Bei der Erstinstallation oder nach dem Löschen des Inhalts des integrierten IBM Security Chip müssen Sie das Kennwort des Sicherheitsadministrators im Feld "Bestätigen Sie das Administratorkennwort" bestätigen. Gegebenenfalls müssen Sie auch Ihr Administratorkennwort eingeben.

   Die Anzeige "Sicherheitsschlüssel für Administratoren erstellen" erscheint.

4. Führen Sie einen der folgenden Schritte aus:

   - **Neue Sicherheitsschlüssel erstellen**

     Gehen Sie wie folgt vor, um neue Sicherheitsschlüssel zu erstellen;

     a. Klicken Sie auf den Radioknopf **Neue Sicherheitsschlüssel erstellen**.
     b. Geben Sie die Speicherposition für die Sicherheitsschlüssel der Administratoren an, indem Sie entweder den Pfadnamen in das dafür dafür vorgesehene Feld eingeben oder auf **Durchsuchen** klicken und den entsprechenden Ordner auswählen.
     c. Wenn Sie den Sicherheitsschlüssel für einen erhöhten Schutz teilen möchten, klicken Sie auf das Markierungsfeld **Backup-Version des Sicherheitsschlüssels für erhöhte Sicherheit teilen**, so dass ein Haken in dem Feld angezeigt wird. Mit Hilfe der Pfeiltasten können Sie anschließend im Auswahlfeld **Anzahl der Teilungen** die gewünschte Anzahl auswählen.

   - **Einen vorhandenen Sicherheitsschlüssel verwenden**

     Gehen Sie wie folgt vor, um einen vorhandenen Sicherheitsschlüssel zu verwenden:

     a. Klicken Sie auf den Radioknopf **Einen vorhandenen Sicherheitsschlüssel verwenden**.
     b. Geben Sie entweder durch Eingabe des Pfadnamens in das entsprechende Feld oder durch Klicken auf **Durchsuchen** und Auswählen den entsprechenden Ordners die Speicherposition des öffentlichen Schlüssels an.
     c. Geben Sie entweder durch Eingabe des Pfadnamens in das entsprechende Feld oder durch Klicken auf **Durchsuchen** und Auswählen den entsprechenden Ordners die Speicherposition des privaten Schlüssels an.

5. Geben Sie die Speicherposition der Backup-Version der Sicherheitsdaten an, indem Sie entweder den Pfadnamen in das dafür dafür vorgesehene Feld eingeben oder auf **Durchsuchen** klicken und den entsprechenden Ordner auswählen.
6. Klicken Sie auf **Weiter**.

   Die Anzeige "Anwendungen mit IBM Client Security schützen" erscheint.
7. Aktivieren Sie den Schutz für IBM Client Security, indem Sie die entsprechenden Markierungsfelder auswählen, so dass darin ein Haken angezeigt wird, und auf **Weiter** klicken. Folgende Auswahlmöglichkeiten von Client Security stehen Ihnen jetzt zur Verfügung:
   - **Sicherer Zugriff durch Ersetzen der normalen Windows-Anmeldung durch die gesicherte Client Security-Anmeldung**

     Wählen Sie dieses Feld aus, um die normale Windows-Anmeldung durch die sichere Client-Security-Anmeldung zu ersetzen. Dadurch wird die Systemsicherheit erhöht. Bei der Anmeldung ist dann jeweils eine Authentifizierung mit dem integrierten IBM Sicherheitschip und optionalen Einheiten, wie z. B. Lesegeräten für Fingerabdrücke, erforderlich.
   - **Datei- und Ordnerverschlüsselung aktivieren**

     Wählen Sie dieses Feld aus, wenn Sie Dateien auf Ihrem Festplattenlaufwerk mit dem integrierten IBM Security Chip sichern möchten. (Hierzu muss das Dienstprogramm zur Verschlüsselung von Dateien und Ordnern von IBM Client Security heruntergeladen werden.)
   - **Unterstützung für IBM Client Security Password Manager aktivieren**

     Wählen Sie dieses Feld aus, wenn Sie IBM Passwort Manager verwenden möchten, um die Kennwörter für Ihre Website-Anmeldungen und -Anwendungen zweckmäßig und sicher zu speichern. (Hierfür müssen Sie die Anwendung "IBM Client Security Password Manager" herunterladen.)
   - **Lotus Notes-Anmeldung durch IBM Client Security-Anmeldung ersetzen**

     Wählen Sie dieses Feld aus, wenn Benutzer von Lotus Notes in Client Security über den integrierten IBM Security Chip automatisch authentifiziert werden sollen.
   - **Unterstützung für Entrust aktivieren**

     Wählen Sie dieses Feld aus, wenn Sie die Integration in Entrust-Sicherheitssoftwareprodukte aktivieren möchten.
   - **Microsoft Internet Explorer schützen**

     Mit diesem Schutz können Sie Ihre E-Mail-Kommunikation und die Suche im Web mit Microsoft Internet Explorer (erfordert ein digitales Zertifikat) schützen. Standardmäßig ist die Unterstützung für Microsoft Internet Explorer aktiviert.

   Nach Auswahl der entsprechenden Markierungsfelder wird das Fenster "Benutzer autorisieren" angezeigt.
8. Geben Sie die erforderlichen Angaben in die Anzeige "Benutzer autorisieren" ein. Verwenden Sie dafür eine der folgenden Prozeduren:
   - Gehen Sie wie folgt vor, um Benutzer zum Ausführen der Funktionen von IBM Client Security zu autorisieren:
     a. Wählen Sie im Bereich "Nicht autorisierte Benutzer" einen Benutzer aus.
     b. Klicken Sie auf **Benutzer autorisieren**.
     c. Geben Sie den Verschlüsselungstext für IBM Client Security in die dafür vorgesehenen Felder ein, bestätigen Sie diese Eingaben, und klicken Sie auf **Fertig stellen**.

d. Klicken Sie auf **Weiter**.

- Gehen Sie wie folgt vor, um die Autorisierung von Benutzern zur Ausführung der Funktionen von IBM Client Security aufzuheben:
  a. Wählen Sie im Bereich "Autorisierte Benutzer" einen Benutzer aus.
  b. Klicken Sie auf **Benutzerberechtigung widerrufen**.
  c. Geben Sie den Verschlüsselungstext für IBM Client Security in die dafür vorgesehenen Felder ein, bestätigen Sie diese Eingaben, und klicken Sie auf **Fertig stellen**.
  d. Klicken Sie auf **Weiter**.

Das Fenster "Sicherheitsstufe des Systems auswählen" wird angezeigt.

9. Gehen Sie wie folgt vor, um eine Systemsicherheitsstufe auszuwählen:
   a. Wählen Sie die von Ihnen gestellten Anforderungen für eine Authentifizierung durch Anklicken der entsprechenden Markierungsfelder aus. Sie können mehrere Anforderungen für die Authentifizierung auswählen.
   b. Wählen Sie eine Systemsicherheitsstufe aus, indem Sie die Auswahlleiste auf die gewünschte Sicherheitsstufe ziehen und auf **Weiter** klicken.

   Anmerkung: Sie können zu einem späteren Zeitpunkt mit dem Policy-Editor von IBM Client Security eine angepasste Security-Policy definieren.
10. Überprüfen Sie die Sicherheitseinstellungen, und wählen Sie einen der folgenden Schritte aus:
    - Klicken Sie auf **Fertig stellen**, um die Einstellungen zu akzeptieren.
    - Gehen Sie zum Ändern der Einstellungen wie folgt vor: Klicken Sie auf **Zurück**, nehmen Sie gewünschten Änderungen vor, und kehren Sie zu dieser Anzeige zurück. Klicken Sie dann auf **Fertig stellen**.

    Ihre Einstellungen werden über den integrierten IBM Security Chip in IBM Client Security konfiguriert. Es wird eine Nachricht angezeigt, die bestätigt, dass Ihr Computer jetzt durch IBM Client Security geschützt ist.
11. Klicken Sie auf **OK**.

    Sie können jetzt "IBM Client Security Password Manager" und die Dienstprogramme zur Verschlüsselung von Dateien und Ordnern installieren und konfigurieren.

IBM Security Chip aktivieren

Zur Verwendung von IBM Client Security muss der IBM Security Chip aktiviert sein. Falls der Chip nicht aktiviert ist, können Sie ihn mit Hilfe des Administratordienstprogramms aktivieren. Anweisungen zur Verwendung des Konfigurationsassistenten finden Sie im vorhergehenden Abschnitt.

Gehen Sie wie folgt vor, um den IBM Security Chip mit dem Administratordienstprogramm zu aktivieren:

1. Klicken Sie auf **Start > Einstellungen > Systemsteuerung > Subsystem von IBM Client Security**.

   Es erscheint eine Anzeige mit der Mitteilung, dass der IBM Security Chip nicht aktiviert ist, und der Frage, ob der Chip aktiviert werden soll.

2. Klicken Sie auf **Ja**.

   Es wird eine Nachricht angezeigt, die darauf hinweist, dass vor dem Fortfahren das Administratorkennwort über das BIOS inaktiviert werden muss, falls ein entsprechenden definiert ist.
3. Führen Sie einen der folgenden Schritte aus:
   - Wenn ein Administratorkennwort definiert ist, klicken Sie auf **Abbrechen**, inaktivieren Sie das Kennwort, und führen Sie dann diese Prozedur aus.
   - Ist kein Administratorkennwort definiert, klicken Sie auf **OK**, um fortzufahren.
4. Schließen Sie alle geöffneten Anwendungen, und klicken Sie auf **OK**, um einen Neustart des Computers durchzuführen.
5. Klicken Sie nach dem Neustart zum Öffnen des Administratordienstprogramms auf **Start > Einstellungen > Systemsteuerung > Subsystem von IBM Client Security**.

   Es wird eine Nachricht angezeigt, die darauf hinweist, dass der IBM Security Chip nicht konfiguriert wurde oder sein Inhalt gelöscht wurde. An dieser Stelle muss ein neues Kennwort eingegeben werden.
6. Geben Sie in das entsprechende Feld ein neues Kennwort für den IBM Security Chip ein, und bestätigen Sie das Kennwort. Klicken Sie anschließend auf **OK**.

   Anmerkung: Das Kennwort muss 8 Zeichen lang sein.

   Daraufhin kehrt das Programme zur Hauptanzeige des Administratordienstprogramms zurück.

Software auf anderen IBM Clients installieren, wenn der öffentliche Schlüssel für Administratoren verfügbar ist (nur für nicht überwachte Installationen)

Wenn Sie die Software auf dem ersten IBM Client installiert und ein Schlüsselpaar für Administratoren erstellt haben, können Sie mit Hilfe des Installationsprogramms die Software installieren und das Sicherheits-Subsystem auf anderen IBM Clients aktivieren.

Während der Installation müssen Sie eine Speicherposition für den öffentlichen Schlüssel für Administratoren, den privaten Schlüssel für Administratoren und das Schlüsselarchiv auswählen. Wenn Sie einen öffentlichen Schlüssel für Administratoren verwenden möchten, der in einem gemeinsam benutzten Verzeichnis gespeichert ist, oder das Schlüsselarchiv in einem gemeinsam benutzten Verzeichnis speichern möchten, müssen Sie erst dem Zielverzeichnis einen Laufwerkbuchstaben zuordnen, bevor Sie das Installationsprogramm verwenden können. Weitere Informationen zum Zuordnen eines Laufwerkbuchstabens zu einer gemeinsam benutzten Netzwerkressource finden Sie in der Dokumentation zu Ihrem Windows-Betriebssystem.

Nicht überwachte Installation ausführen

Durch eine nicht überwachte Installation kann Client Security von einem Administrator auf einem fernen IBM Client installiert werden, ohne dass der Administrator direkten (physischen) Zugriff auf den Clientcomputer haben muss.

Bevor Sie mit einer nicht überwachten Installation beginnen, lesen Sie Kapitel 3, „Vorbereitung der Software-Installation", auf Seite 9. Bei nicht überwachten Instal-

lationen werden keine Fehlernachrichten angezeigt. Wenn eine nicht überwachte Installation vorzeitig beendet wird, führen Sie eine überwachte Installation aus, um alle Fehlernachrichten anzuzeigen.

Anmerkung: Zum Installieren von Client Security müssen Benutzer mit Administratorbenutzerrechten angemeldet sein.

Ausführliche Informationen zur Durchführung einer nicht überwachten Installation enthält die Readme-Datei "css51readme" auf der IBM Website unter http://www.pc.ibm.com/ww/security/secdownload.html.

Massenimplementierung

Mit Hilfe einer Massenimplementierung können Sicherheitsadministratoren gleichzeitig auf mehreren Computern eine Sicherheits-Policy einrichten. Auf diese Weise kann die Verwaltung und Implementierung von Sicherheits-Policies vereinfacht werden, und die Implementierung der richtigen Sicherheits-Policies kann leichter sichergestellt werden.

Für die Durchführung einer Massenimplementierung müssen folgende Einheitentreiber installiert sein:

- SM-Buseinheitentreiber
- LPC-Buseinheitentreiber (für TCPA-Systeme)

Eine Massenimplementierung umfasst im Wesentlichen zwei Schritte:

- Masseninstallation
- Massenkonfiguration

Masseninstallation

Zur gleichzeitigen Installation von IBM Client Security auf einer Vielzahl von Clients muss eine nicht überwachte Installation durchgeführt werden. Beim Einleiten einer Massenimplementierung muss der Parameter für nicht überwachte Installation verwendet werden.

Gehen Sie wie folgt vor, um eine Masseninstallation einzuleiten:

1. Erstellen Sie die Datei CSS.ini.

   Dieser Schritt ist nur erforderlich, wenn Sie beabsichtigen, eine Massenkonfiguration durchzuführen.
2. Extrahieren Sie mit Hilfe von Winzip den Inhalt des CSS-Installationspakets mit Ordnernamen.
3. Bearbeiten Sie in der Datei "setup.iss" die Einträge `szIniPath` und `szDir`, die für eine Massenkonfiguration erforderlich sind.

   Der vollständige Inhalt dieser Datei ist nachfolgend aufgeführt. Der Parameter `szIniPath` ist nur erforderlich, wenn eine Massenkonfiguration durchgeführt werden soll.
4. Kopieren Sie die Dateien auf das Zielsystem.
5. Erstellen Sie die Befehlszeilenanweisung `\setup -s`.

   Diese Befehlszeilenanweisung sollte vom Desktop eines Benutzers mit Administratorberechtigung ausgeführt werden. Ein geeigneter Ort hierfür ist die Programmgruppe "Autostart" oder das Fenster "Ausführen".
6. Löschen Sie die Befehlszeilenanweisung nach dem nächsten Systemstart.

Nachfolgend ist der vollständige Inhalt der Datei ″setup.iss″ mit einigen Beschreibungen aufgeführt: [InstallShield Silent] Version=v6.00.000 File=Response File szIniPath=d:\csssetup.ini (Über diesen Parameter werden der Name und die Speicherposition der für die Massenkonfiguration erforderlichen .ini-Datei angegeben. Handelt es sich hierbei um ein Netzlaufwerk, muss das Laufwerk verbunden sein. Soll keine Massenkonfiguration in Verbindung mit einer Installation im Hintergrund durchgeführt werden, entfernen Sie diesen Eintrag.) [File Transfer] OverwrittenReadOnly=NoToAll [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-DlgOrder] Dlg0={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdLicense-0 Count=4 Dlg1={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdAskDestPath-0 Dlg2={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdSelectFolder-0 Dlg3={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdFinishReboot-0 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdLicense-0] Result=1 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdAskDestPath-0] szDir=C:\Program Files\IBM\Security (Über diesen Parameter wird das Installationsverzeichnis für Client Security angegeben. Hierbei muss es sich um ein lokales Laufwerk des Computers handeln.) Result=1 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdSelectFolder-0] szFolder=IBM Client Security Software (Über diesen Parameter wird die Programmgruppe für Client Security angegeben.) Result=1 [Application] Name=Client Security Version=5.00.002f Company=IBM Lang=0009 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdFinishReboot-0] Result=6 BootOption=3

Massenkonfiguration

Die folgende Datei wird zum Einleiten einer Massenkonfiguration benötigt. Der Name der Datei ist beliebig, die Datei muss jedoch über die Erweiterung .ini verfügen. Nachfolgend ist ein Beispiel für die Datei aufgeführt. Die seitlich angegebene Beschreibung ist nicht Bestandteil der Datei. Mit Hilfe des folgenden Befehls kann die Datei über die Befehlszeile ausgeführt werden, falls die Massenkonfiguration nicht in Verbindung mit einer Masseninstallation ausgeführt wird.

```
<CSS_Installationsordner>\acamucli /ccf:c:\csec.ini
```

Anmerkung: Falls Dateien oder Pfade auf einem Netzlaufwerk liegen, muss dem Netzlaufwerk ein Laufwerkbuchstabe zugeordnet sein.

[CSSSetup]	Abschnittsüberschrift für CSS-Konfiguration.
suppw=bootup	Administrator-/Supervisorkennwort. Keine Angabe, falls nicht erforderlich.
hwpw=11111111	CSS-Hardwarekennwort. Muss 8 Zeichen lang sein. Angabe immer erforderlich. Richtige Angabe erforderlich, falls Hardwarekennwort bereits definiert wurde.
newkp=1	1: neues Administratorschlüsselpaar generieren. 0: vorhandenes Administratorschlüsselpaar verwenden.
keysplit=1	Wenn newkp = 1, wird hiermit die Anzahl der privaten Schlüsselkomponenten angegeben. **Anmerkung:** Enthält das vorhandene Schlüsselpaar mehrere private Schlüsselkomponenten, müssen alle privaten Schlüsselkomponenten im selben Verzeichnis gespeichert werden.
kpl=c:\jgk	Speicherposition des Administratorschlüsselpaars, wenn newkp = 1. Falls es sich um ein Netzlaufwerk handelt, muss dieses verbunden sein.
kal=c:\jgk\archive	Speicherposition des Benutzerschlüsselarchivs. Falls es sich um ein Netzlaufwerk handelt, muss dieses verbunden sein.
pub=c:\jk\admin.key	Speicherposition des öffentlichen Schlüssels für Administratoren, falls ein vorhandenes Administratorschlüsselpaar verwendet wird. Falls es sich um ein Netzlaufwerk handelt, muss dieses verbunden sein.

pri=c:\jk\private1.key	Speicherposition des privaten Schlüssels für Administratoren, falls ein vorhandenes Administratorschlüsselpaar verwendet wird. Falls es sich um ein Netzlaufwerk handelt, muss dieses verbunden sein.
clean=0	1: .ini-Datei nach Initialisierung löschen. 0: .ini-Datei nach Initialisierung nicht löschen.
[UVMEnrollment]	Abschnittsüberschrift für Benutzerregistrierung.
enrollall=0	1: Alle lokalen Benutzeraccounts in UVM registrieren. 0: Bestimmte Benutzeraccounts in UVM registrieren.
defaultuvmpw=top	Wenn enrollall = 1, gilt dieser UVM-Verschlüsselungstext für alle Benutzer.
defaultwinpw=down	Wenn enrollall = 1, wird dieses Windows-Kennwort bei UVM für alle Benutzer registriert.
enrollusers=2	Wenn enrollall = 0, wird hiermit die Anzahl der Benutzer angegeben, die in UVM registriert werden.
user1=joseph	Anzahl der zu registrierenden Benutzer mit 1 beginnend aufzählen. Die Benutzernamen müssen die Accountnamen sein. Gehen Sie wie folgt vor, um unter XP den Accountnamen herauszufinden. 1. Rufen Sie das Fenster ″Computerverwaltung″ auf. 2. Klicken Sie auf den Eintrag ″Lokale Benutzer und Gruppen″. 3. Öffnen Sie den Ordner ″Benutzer″. Bei den in der Spalte ″Name″ enthaltenen Einträgen handelt es sich um die Accountnamen.
user1uvmpw=chrome	Anzahl der zu registrierenden Benutzer mit UVM-Verschlüsselungstext mit 1 beginnend aufzählen.
user1winpw=spinning	Anzahl der zu registrierenden Benutzer, die bei UVM mit Windows-Verschlüsselungstext registriert sind, mit 1 beginnend aufzählen.
user1domain=0	0: Angabe, dass es sich hierbei um einen lokalen Account handelt. 1: Angabe, dass es sich hierbei um einen Domänenaccount handelt.
user2=hallie user2uvmpw=left user2winpw=right user2domain=0	
[UVMAppConfig]	Abschnittsüberschrift für Installation von UVM-sensitiven Anwendungen und Modulen.
uvmlogon=0	1: UVM-Anmeldeschutz verwenden. 0: Windows-Anmeldung verwenden.
entrust=0	1: UVM für Entrust-Authentifizierung verwenden. 0: Entrust-Authentifizierung verwenden.
notes=0	1: UVM-Schutz für Lotus Notes verwenden. 0: Kennwortschutz von Lotus Notes verwenden.
passman=0	1: Password Manager verwenden. 0: Password Manager nicht verwenden.
folderprotect=0	1: Verschlüsselung von Dateien und Ordnern verwenden. 0: Verschlüsselung von Dateien und Ordnern nicht verwenden.

Softwareversion von Client Security aktualisieren

Damit Clients, auf denen eine Version von Client Security vor Version 5.0 installiert ist, die neuen Funktionen von Client Security nutzen können, muss die auf den Clients installierte Software auf Version 5.1 aktualisiert werden.

Wichtig: Bei TCPA-Systemen, auf denen IBM Client Security Version 4.0x installiert ist, muss vor der Installation von IBM Client Security Version 5.1 der Inhalt des Chips gelöscht werden. Andernfalls besteht die Möglichkeit, dass die Installation fehlschlägt oder die Software nicht reagiert.

Upgrade mit neuen Sicherheitsdaten durchführen

Gehen Sie wie folgt vor, um Client Security vollständig zu entfernen und eine Neuinstallation durchzuführen:

1. Deinstallieren Sie die vorhandene Version von Client Security (Systemsteuerung -> Software).
2. Führen Sie einen Neustart des Systems durch.
3. Löschen Sie den Inhalt des integrierten IBM Security Chip über das BIOS-Dienstprogramm.
4. Führen Sie einen Neustart des Systems durch.
5. Installieren Sie Client Security Release 5.1 und konfigurieren Sie die Software mit dem Konfigurationsassistenten von IBM Client Security.

Upgrade auf Client Security Version 5.1 mit vorhandenen Sicherheitsdaten durchführen

Gehen Sie wie folgt vor, um ein Upgrade von einem Release von Client Security vor Version 5.0 unter Verwendung der vorhandenen Sicherheitsdaten durchzuführen:

1. Gehen Sie wie folgt vor, um Ihr Archiv zu aktualisieren:
   a. Klicken Sie auf **Start > Programme > Access IBM > IBM Client Security > Client-Dienstprogramm**.
   b. Klicken Sie auf die Schaltfläche **Archiv aktualisieren**, um Ihre Backup-Daten zu aktualisieren.

      Notieren Sie sich das Archivverzeichnis.
   c. Beenden Sie das Client-Dienstprogramm von IBM Client Security.
2. Gehen Sie wie folgt vor, um die vorhandene Version von Client Security zu entfernen:
   a. Suchen Sie die öffentlichen und privaten Schlüssel für Administratoren, die bei der Konfiguration der vorherigen Version von Client Security erstellt wurden.
   b. Klicken Sie auf **Start > Einstellungen > Systemsteuerung > Software**, und entfernen Sie IBM Client Security.
   c. Wählen Sie bei der Frage, ob ein Neustart durchgeführt werden soll, **Nein** aus.
   d. Fahren Sie das System herunter.

3. Gehen Sie wie folgt vor, um den Inhalt des integrierten IBM Security Chip zu löschen:
   a. Schalten Sie das System ein.
   b. Drücken Sie F1, um das Programm "IBM BIOS Setup Utility" aufzurufen.
   c. Setzen Sie den Cursor auf das Feld mit den Einstellungen für den IBM Security Chip, und löschen Sie den Inhalt des Chips.
   d. Verlassen Sie das Programm "IBM BIOS Setup Utility".

      Der Startvorgang wird anschließend fortgesetzt.
4. Führen Sie das Installationsprogramm von Client Security Version 5.0 aus.
5. Führen Sie bei entsprechender Aufforderung einen Neustart durch.

   Nach dem Neustart wird der Konfigurationsassistent von IBM Client Security automatisch aufgerufen. Führen Sie den Konfigurationsassistenten NICHT aus.
6. Klicken Sie auf **Abbrechen**, um den Konfigurationsassistenten zu beenden.
7. Gehen Sie wie folgt vor, um die Standard-Sicherheits-Policy temporär zu sichern.
   a. Wechseln Sie im Windows Explorer in das Installationsverzeichnis von IBM Client Security (Standardverzeichnis: c:\program files\ibm\security).
   b. Klicken Sie mit der rechten Maustaste auf den Ordner UVM_Policy, und wählen Sie **Kopieren**.
   c. Klicken Sie mit der rechten Maustaste auf den Windows-Desktop, und wählen Sie **Einfügen**.

      Auf diese Weise wird eine temporäre Sicherung auf dem Windows-Desktop erstellt.

      Anmerkung: Die Einstellungen Ihrer vorhandenen Sicherheits-Policy werden durch neue Standardeinstellungen ersetzt.
8. Gehen Sie wie folgt vor, um die Einstellungen von IBM Client Security Version 4.0x wiederherzustellen:
   a. Klicken Sie auf **Start > Einstellungen > Systemsteuerung > Subsystem von IBM Client Security**.

      Die Hauptanzeige des Administratordienstprogramms von IBM Client Security wird angezeigt.
   b. Klicken Sie auf die Schaltfläche **Schlüsselkonfiguration**.
   c. Wählen Sie **Ja** aus, um die Schlüssel aus dem Archiv wiederherzustellen.
9. Geben Sie die Speicherposition des vorherigen Archivverzeichnisses an.
10. Geben Sie die Speicherposition der öffentlichen und privaten Schlüsseldateien für Administratoren aus dem vorherigem Release an.

    Die Mitteilung, dass Ihr Archiv für das neue Release aktualisiert wird, wird angezeigt.
11. Klicken Sie auf **OK**.
12. Geben Sie die Speicherposition für die neuen Schlüssel für Administratoren an. Achten Sie darauf, dass die Schlüssel an einer anderen Speicherposition als die vorhandenen Schlüssel für Administratoren erstellt werden. Falls Sie bereits Schlüssel für Administratoren für Release 5.0 auf einem anderen System erstellt haben, können Sie den Eintrag **Vorhandenes CSS-Archivschlüsselpaar verwenden** auswählen und die Speicherposition der vorhandenen Schlüssel angeben.

13. Klicken Sie auf **Weiter**.

    Ihr Archiv wird konvertiert und wiederhergestellt.
14. Beenden Sie die Anwendung.
15. Gehen Sie wie folgt vor, um die Policy-Einstellungen wiederherzustellen:
    a. Wechseln Sie im Windows Explorer in das Installationsverzeichnis von IBM Client Security (Standardverzeichnis: c:\program files\ibm\security).
    b. Ziehen Sie den Ordner "UVM_Policy" mit Hilfe der linken Taste vom Desktop in das Installationsverzeichnis von IBM Client Security.
    c. Klicken Sie zur Bestätigung der angezeigten Warnungen jeweils auf **Ja**.

    Die Migration Ihrer Sicherheitsdaten zu Client Security Software Release 5.0 ist damit abgeschlossen.

Anmerkung: Falls Sie in Client Security Version 4.0x Änderungen an der Sicherheits-Policy vorgenommen hatten, können Sie diese Änderungen wiederholen. Gehen Sie dazu wie folgt vor:

1. Klicken Sie auf **Start > Einstellungen > Systemsteuerung > Subsystem von IBM Client Security**.
2. Klicken Sie auf die Schaltfläche **Anwendungsunterstützung und Policies konfigurieren**.
3. Klicken Sie auf die Schaltfläche **Anwendungs-Policy**.
4. Klicken Sie auf die Schaltfläche **Policy bearbeiten**.

Upgrade von Release 5.1 auf aktuellere Versionen mit vorhandenen Sicherheitsdaten durchführen

Gehen Sie wie folgt vor, um ein Upgrade von Client Security Version 5.0 auf aktuellere Versionen der Software unter Verwendung der vorhandenen Sicherheitsdaten durchzuführen:

1. Gehen Sie wie folgt vor, um Ihr Archiv zu aktualisieren:
   a. Klicken Sie auf **Start > Programme > Access IBM > IBM Client Security > Sicherheitseinstellungen ändern**.
   b. Klicken Sie auf die Schaltfläche **Archiv aktualisieren**, um Ihre Backup-Daten zu aktualisieren.

      Notieren Sie sich das Archivverzeichnis.
   c. Beenden Sie das Benutzerkonfigurationsprogramm von IBM Client Security.
2. Gehen Sie wie folgt vor, um die vorhandene Version von Client Security zu entfernen:
   a. Suchen Sie die öffentlichen und privaten Schlüssel für Administratoren, die bei der Konfiguration der vorherigen Version von Client Security erstellt wurden.
   b. Führen Sie die Datei "csec51.exe" aus.
   c. Wählen Sie die Option **Sicherheit** aus.
   d. Führen Sie einen Neustart des Systems durch.

Client Security deinstallieren

Vor dem Deinstallieren von IBM Client Security müssen die diversen Dienstprogramme von IBM Client Security deinstalliert werden. Zum Deinstallieren von Client Security müssen Benutzer mit Administratorbenutzerrechten angemeldet sein.

Anmerkung: Vor dem Deinstallieren von IBM Client Security müssen Sie alle Dienstprogramme von IBM Client Security und die gesamte UVM-Sensorsoftware deinstallieren.

Gehen Sie wie folgt vor, um Client Security zu deinstallieren:

1. Schließen Sie alle Windows-Programme.
2. Klicken Sie auf dem Windows-Desktop auf **Start > Einstellungen > Systemsteuerung**.
3. Klicken Sie auf das Symbol **Software**.
4. Wählen Sie in der Liste der Software, die automatisch entfernt werden kann, den Eintrag **IBM Client Security** aus.
5. Klicken Sie auf **Ändern/Entfernen**.
6. Wählen Sie den Radioknopf **Entfernen** aus.
7. Klicken Sie zum Deinstallieren der Software auf **Ja**.
8. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie das PKCS #11-Modul des integrierten IBM Security Chips für Netscape installiert haben, wird eine Nachricht angezeigt, die Sie zum Starten des Inaktivierungsprozesses des PKCS #11-Moduls des integrierten IBM Security Chips auffordert. Klicken Sie auf **Ja**, um fortzufahren.

     Daraufhin wird Ihnen eine Reihe von Nachrichten angezeigt. Klicken Sie bei jeder einzelnen Nachricht so lange immer wieder auf **OK**, bis das PKCS #11-Modul des integrierten IBM Security Chips entfernt ist.
   - Wenn Sie das PKCS #11-Modul des integrierten IBM Security Chips für Netscape nicht installiert haben, wird eine Nachricht angezeigt, in der Sie gefragt werden, ob Sie die gemeinsam benutzten DLL-Dateien, die mit Client Security installiert wurden, löschen möchten.

     Klicken Sie auf **Ja**, um diese Dateien zu deinstallieren, oder klicken Sie auf **Nein**, wenn die installierten Dateien weiterhin installiert bleiben sollen. Wenn Sie die installierten Dateien beibehalten möchten, hat dies keinen Einfluss auf die normale Funktion des Computers.
9. Klicken Sie nach dem Entfernen der Software auf **OK**.

   Nach dem Deinstallieren von Client Security müssen Sie den Computer erneut starten.

Beim Deinstallieren von Client Security werden alle installierten Softwarekomponenten von Client Security mit allen Benutzerschlüsseln, digitalen Zertifikaten, registrierten Fingerabdrücken und gespeicherten Kennwörtern entfernt. Das Schlüsselarchiv bleibt beim Deinstallieren von Client Security jedoch erhalten.

Kapitel 5. Fehlerbehebung

Im Folgenden finden Sie Informationen zur Vermeidung, Erkennung und Behebung von Fehlern, die bei der Verwendung von Client Security auftreten können.

Administratorfunktionen

Dieser Abschnitt enthält Informationen für Administratoren zur Konfiguration und zur Verwendung von Client Security.

Administratorkennwort festlegen (ThinkCentre)

Über die Sicherheitseinstellungen im Programm "Configuration/Setup Utility" können Administratoren folgende Vorgänge durchführen:

- Das Hardwarekennwort für den integrierten IBM Security Chip ändern
- Den integrierten IBM Security Chip aktivieren oder inaktivieren
- Den Inhalt des integrierten IBM Security Chips löschen

Achtung:

- Löschen oder inaktivieren Sie den integrierten IBM Security Chip nicht bei aktivierter gesicherter UVM-Anmeldung. Andernfalls wird der Inhalt der Festplatte unbrauchbar, und Sie müssen die Festplatte neu formatieren und die gesamte Software neu installieren.

  Um den UVM-Schutz zu inaktivieren, öffnen Sie das Administratordienstprogramm, klicken Sie auf **Anwendungsunterstützung und Policies konfigurieren**, und inaktivieren Sie das Markierungsfeld **Die Windows-Standardanmeldung durch eine gesicherte UVM-Anmeldung ersetzen**. Sie müssen den Computer erneut starten, damit der UVM-Schutz inaktiviert wird.
- Löschen oder inaktivieren Sie den integrierten IBM Security Chip nicht bei aktiviertem UVM-Schutz. Andernfalls haben Sie keinen Zugriff mehr auf das System.
- Wenn Sie den Inhalt des integrierten IBM Security Chips löschen, gehen alle Chiffrierschlüssel und Zertifikate verloren, die auf dem Chip gespeichert sind.

Da auf Ihre Sicherheitseinstellungen über das Programm "Configuration/Setup Utility" des Computers zugegriffen werden kann, legen Sie ein Administratorkennwort fest, um zu verhindern, dass diese Einstellungen durch nicht autorisierte Benutzer geändert werden.

Gehen Sie wie folgt vor, um ein Administratorkennwort festzulegen:

1. Fahren Sie das System herunter, und starten Sie es erneut.
2. Drücken Sie während der Eingabeaufforderung des Programms "Configuration/Setup Utility" die Taste **F1**.

   Das Hauptmenü des Programms "Configuration/Setup Utility" wird geöffnet.
3. Wählen Sie die Option **System Security** aus.
4. Wählen Sie die Option **Administrator Password** aus.
5. Geben Sie das Kennwort ein, und drücken Sie auf der Tastatur die Taste mit dem Abwärtspfeil.
6. Geben Sie das Kennwort erneut ein, und drücken Sie auf der Tastatur die Taste mit dem Abwärtspfeil.

7. Wählen Sie **Change Administrator password** aus, und drücken Sie die Eingabetaste. Drücken Sie danach erneut die Eingabetaste.
8. Drücken Sie die Taste **Esc**, um die Einstellungen zu speichern und das Programm zu verlassen.

Nach dem Festlegen eines Administratorkennworts wird bei jedem Zugriff auf das Programm "Configuration/Setup Utility" eine Eingabeaufforderung angezeigt.

Wichtig: Bewahren Sie Ihr Administratorkennwort an einem sicheren Ort auf. Sollten Sie das Administratorkennwort verlieren oder vergessen, können Sie nicht auf das Programm "Configuration/Setup Utility" zugreifen und das Kennwort nicht ändern oder löschen, ohne die Computerabdeckung zu entfernen und auf der Systemplatine eine Brücke zu versetzen. Weitere Informationen hierzu finden Sie in der Hardwaredokumentation, die mit Ihrem Computer geliefert wurde.

Administratorkennwort festlegen (ThinkPad)

Mit den Sicherheitseinstellungen im Programm "IBM BIOS Setup Utility" können Administratoren folgende Vorgänge durchführen:

- Den integrierten IBM Security Chip aktivieren oder inaktivieren
- Den Inhalt des integrierten IBM Security Chips löschen

Achtung:

- Löschen oder inaktivieren Sie den integrierten IBM Security Chip nicht bei aktivierter gesicherter UVM-Anmeldung. Andernfalls haben Sie keinen Zugriff mehr auf das System.

  Um den UVM-Schutz zu inaktivieren, öffnen Sie das Administratordienstprogramm, klicken Sie auf **Anwendungsunterstützung und Policies konfigurieren**, und inaktivieren Sie das Markierungsfeld **Die Windows-Standardanmeldung durch eine gesicherte UVM-Anmeldung ersetzen**. Sie müssen den Computer erneut starten, damit der UVM-Schutz inaktiviert wird.

  Wenn Sie den Inhalt des integrierten IBM Security Chips löschen, gehen alle Chiffrierschlüssel und Zertifikate verloren, die auf dem Chip gespeichert sind.
- Bei einigen ThinkPad-Modellen ist es vor der Installation oder dem Upgrade von Client Security notwendig, das Administratorkennwort vorübergehend zu inaktivieren.

Nach der Konfiguration von Client Security legen Sie ein Administratorkennwort fest, um nicht berechtigte Benutzer daran zu hindern, diese Einstellungen ändern.

Gehen Sie wie folgt vor, um ein Administratorkennwort festzulegen:

1. Fahren Sie das System herunter, und starten Sie es erneut.
2. Drücken Sie während der Eingabeaufforderung des Programms "IBM BIOS Setup Utility" die Taste **F1**.

   Das Hauptmenü des Programms "IBM BIOS Setup Utility" wird geöffnet.
3. Wählen Sie die Option **Password** aus.
4. Wählen Sie die Option **Supervisor Password** aus.
5. Geben Sie das Kennwort ein, und drücken Sie die Eingabetaste.
6. Geben Sie das Kennwort erneut ein, und drücken Sie die Eingabetaste.
7. Klicken Sie auf **Continue**.
8. Drücken Sie die Taste F10, um die Einstellungen zu speichern und das Programm zu beenden.

Nach dem Festlegen eines Administratorkennworts wird bei jedem Zugriff auf das Programm "IBM BIOS Setup Utility" eine Eingabeaufforderung angezeigt.

Wichtig: Bewahren Sie Ihr Administratorkennwort an einem sicheren Ort auf. Sollten Sie das Administratorkennwort verlieren oder vergessen, können Sie nicht auf das Programm "IBM BIOS Setup Utility" zugreifen und das Kennwort nicht ändern oder löschen. Weitere Informationen hierzu finden Sie in der Hardwaredokumentation, die mit Ihrem Computer geliefert wurde.

Hardwarekennwort schützen

Sie können ein Kennwort für den IBM Security Chip festlegen, um den integrierten IBM Security Chip für einen Client zu aktivieren. Nachdem Sie das Kennwort für den IBM Security Chip festgelegt haben, ist der Zugriff auf das Administratordienstprogramm durch dieses Kennwort geschützt. Sie müssen das Kennwort für den IBM Security Chip vor unberechtigtem Zugriff schützen, damit nicht berechtigte Benutzer die Einstellungen im Administratordienstprogramm nicht ändern können.

Inhalt des integrierten IBM Security Chips löschen (ThinkCentre)

Wenn Sie alle Chiffrierschlüssel für Benutzer aus dem integrierten IBM Security Chip sowie das Hardwarekennwort für den Chip löschen möchten, müssen Sie den Inhalt des Chips löschen. Lesen Sie die nachfolgend unter "Achtung" aufgeführten Informationen, bevor Sie den Inhalt des integrierten IBM Security Chips löschen.

Achtung:

- Löschen oder inaktivieren Sie den integrierten IBM Security Chip nicht bei aktiviertem UVM-Schutz. Andernfalls haben Sie keinen Zugriff mehr auf das System.

  Um den UVM-Schutz zu inaktivieren, öffnen Sie das Administratordienstprogramm, klicken Sie auf **Anwendungsunterstützung und Policies konfigurieren**, und inaktivieren Sie das Markierungsfeld **Die Windows-Standardanmeldung durch eine gesicherte UVM-Anmeldung ersetzen**. Sie müssen den Computer erneut starten, damit der UVM-Schutz inaktiviert wird.
- Wenn Sie den Inhalt des integrierten IBM Security Chips löschen, gehen alle Chiffrierschlüssel und Zertifikate verloren, die auf dem Chip gespeichert sind.

Gehen Sie wie folgt vor, um den Inhalt des integrierten IBM Security Chips zu löschen:

1. Fahren Sie das System herunter, und starten Sie es erneut.
2. Drücken Sie während der Eingabeaufforderung des Programms "Configuration/Setup Utility" die Taste **F1**.

   Das Hauptmenü des Programms "Configuration/Setup Utility" wird geöffnet.
3. Wählen Sie die Option **Security** aus.
4. Wählen Sie **IBM TCPA Feature Setup** aus.
5. Wählen Sie **Clear IBM TCPA Security Feature** aus.
6. Wählen Sie **Yes** aus.
7. Drücken Sie die Taste "Esc", um fortzufahren.
8. Drücken Sie Taste "Esc", um das Programm zu verlassen und die Einstellungen zu speichern.

Inhalt des integrierten IBM Security Chips löschen (ThinkPad)

Wenn Sie alle Chiffrierschlüssel für Benutzer aus dem integrierten IBM Security Chip und das Hardwarekennwort für den Chip löschen möchten, müssen Sie den Inhalt des Chips löschen. Lesen Sie die nachfolgend unter ″Achtung″ aufgeführten Informationen, bevor Sie den Inhalt des integrierten IBM Security Chips löschen.

Achtung:

- Löschen oder inaktivieren Sie bei aktiviertem UVM-Schutz den integrierten IBM Security Chip nicht. Andernfalls wird der Inhalt der Festplatte unbrauchbar, und Sie müssen die Festplatte neu formatieren und die gesamte Software neu installieren.

  Um den UVM-Schutz zu inaktivieren, öffnen Sie das Administratordienstprogramm, klicken Sie auf **Anwendungsunterstützung und Policies konfigurieren**, und inaktivieren Sie das Markierungsfeld **Die Windows-Standardanmeldung durch eine gesicherte UVM-Anmeldung ersetzen**. Sie müssen den Computer erneut starten, damit der UVM-Schutz inaktiviert wird.
- Wenn Sie den Inhalt des integrierten IBM Security Chips löschen, gehen alle Chiffrierschlüssel und Zertifikate verloren, die auf dem Chip gespeichert sind.

Gehen Sie wie folgt vor, um den Inhalt des integrierten IBM Security Chips zu löschen:

1. Fahren Sie das System herunter, und starten Sie es erneut.
2. Drücken Sie während der Eingabeaufforderung des Programms ″IBM BIOS Setup Utility″ die Taste ″Fn″.

   Anmerkung: Auf einigen ThinkPad-Modellen müssen Sie möglicherweise beim Einschalten die Taste F1 drücken, um auf das Programm ″IBM BIOS Setup Utility″ zuzugreifen. Weitere Informationen hierzu finden Sie in der Hilfenachricht des Programms ″IBM BIOS Setup Utility″.

   Das Hauptmenü des Programms ″IBM BIOS Setup Utility″ wird geöffnet.
3. Wählen Sie **Config** aus.
4. Wählen Sie **IBM Security Chip** aus.
5. Wählen Sie **Clear IBM Security Chip** aus.
6. Wählen Sie **Yes** aus.
7. Drücken Sie die Eingabetaste, um fortzufahren.
8. Drücken Sie die Taste F10, um die Einstellungen zu speichern und das Programm zu beenden.

Administratordienstprogramm

Der folgende Abschnitt enthält Informationen, die Sie bei der Verwendung des Administratordienstprogramms beachten müssen.

Benutzer löschen

Wenn Sie einen Benutzer löschen, wird der Benutzername in der Benutzerliste des Administratordienstprogramms gelöscht.

Keinen Zugriff auf ausgewählte Objekte mit der Tivoli Access Manager-Steuerung zulassen

Das Markierungsfeld **Keinen Zugriff auf ausgewähltes Objekt zulassen** ist nicht inaktiviert, wenn die Tivoli Access Manager-Steuerung ausgewählt wurde. Wenn Sie im UVM-Policy-Editor die Option **Access Manager steuert ausgewähltes Objekt** auswählen, um ein Authentifizierungsobjekt über Tivoli Access Manager zu steuern, wird das Markierungsfeld **Keinen Zugriff auf ausgewähltes Objekt zulassen** nicht inaktiviert. Auch wenn das Markierungsfeld **Keinen Zugriff auf ausgewähltes Objekt zulassen** weiterhin aktiviert ist, kann die Tivoli Access Manager-Steuerung nicht über dieses Markierungsfeld außer Kraft gesetzt werden.

Bekannte Einschränkungen

Dieser Abschnitt enthält Informationen zu bekannten Einschränkungen in Bezug auf Client Security.

Client Security mit Windows-Betriebssystemen einsetzen

Alle Windows-Betriebssysteme weisen die folgende bekannte Einschränkung auf: Wenn ein in UVM registrierter Clientbenutzer seinen Windows-Benutzernamen ändert, geht die gesamte Funktionalität von Client Security verloren. Der Benutzer muss den neuen Benutzernamen erneut in UVM registrieren und alle neuen Berechtigungsnachweise anfordern.

Windows XP-Betriebssysteme weisen die folgende bekannte Einschränkung auf: In UVM registrierte Benutzer, deren Windows-Benutzername zuvor geändert wurde, werden von UVM nicht erkannt. UVM verweist auf den früheren Benutzernamen, während Windows nur den neuen Benutzernamen erkennt. Diese Einschränkung gilt selbst dann, wenn der Windows-Benutzername vor der Installation von Client Security geändert wurde.

Client Security mit Netscape-Anwendungen einsetzen

Netscape wird nach einem Berechtigungsfehler geöffnet: Wenn das Fenster "UVM-Verschlüsselungstext" geöffnet wird, müssen Sie den UVM-Verschlüsselungstext eingeben und auf **OK** klicken, bevor Sie fortfahren können. Wenn Sie einen falschen UVM-Verschlüsselungstext eingeben (oder bei einer Scannerabtastung von Fingerabdrücken einen falschen Fingerabdruck liefern), wird eine Fehlernachricht angezeigt. Wenn Sie auf **OK** klicken, wird Netscape geöffnet, Sie können aber das vom integrierten IBM Security Chip generierte digitale Zertifikat nicht verwenden. Sie müssen Netscape verlassen, erneut aufrufen und den richtigen UVM-Verschlüsselungstext eingeben, bevor Sie das Zertifikat für den integrierten IBM Security Chip verwenden können.

Algorithmen werden nicht angezeigt: Beim Anzeigen des Moduls in Netscape ist keiner der vom PKCS #11-Modul des integrierten IBM Security Chips unterstützten Hashverfahren-Algorithmen ausgewählt. Die folgenden Algorithmen werden vom PKCS #11-Modul des integrierten IBM Security Chips unterstützt, jedoch nicht als unterstützt erkannt, wenn sie in Netscape angezeigt werden:

- SHA-1
- MD5

Zertifikat des integrierten IBM Security Chips und Verschlüsselungsalgorithmen

Im Folgenden finden Sie Informationen zu Verschlüsselungsalgorithmen, die Sie mit dem Zertifikat des integrierten IBM Security Chips verwenden können. Aktuelle Informationen zu Verschlüsselungsalgorithmen für die jeweilige E-Mail-Anwendung erhalten Sie von Microsoft oder Netscape.

Beim Senden von E-Mails von einem Outlook Express-Client (128 Bit) an einen anderen Outlook Express-Client (128 Bit): Wenn Sie Outlook Express mit der 128-Bit-Version von Internet Explorer 4.0 oder 5.0 verwenden, um verschlüsselte E-Mails an andere Clients mit Outlook Express (128 Bit) zu senden, können mit dem Zertifikat des integrierten IBM Security Chips verschlüsselte E-Mails nur mit dem 3DES-Algorithmus verschlüsselt werden.

Beim Senden von E-Mails zwischen einem Outlook Express-Client (128 Bit) und einem Netscape-Client: Eine Verschlüsselungsanforderung gemäß RC2(40), RC2(64) oder RC2(128) von einem Netscape-Client an einen Outlook Express-Client (128 Bit) wird an den Netscape-Client immer mit dem RC2(40)-Algorithmus zurückgesendet.

Möglicherweise stehen einige Algorithmen im Outlook Express-Client (128 Bit) nicht zur Auswahl: Je nachdem, wie die Version von Outlook Express (128 Bit) konfiguriert oder aktualisiert wurde, sind möglicherweise einige RC2-Algorithmen und andere Algorithmen für die Verwendung mit dem Zertifikat des integrierten IBM Security Chips nicht verfügbar. Aktuelle Informationen zu den Verschlüsselungsalgorithmen, die mit den verschiedenen Versionen von Outlook Express verwendet werden, erhalten Sie von Microsoft.

UVM-Schutz für eine Lotus Notes-Benutzer-ID verwenden

Der UVM-Schutz funktioniert nicht, wenn Sie innerhalb einer Notes-Sitzung die Benutzer-ID wechseln: Sie können den UVM-Schutz nur für die aktuelle Benutzer-ID einer Notes-Sitzung konfigurieren. Gehen Sie wie folgt vor, um von einer Benutzer-ID, für die UVM-Schutz aktiviert wurde, zu einer anderen Benutzer-ID zu wechseln:

1. Verlassen Sie Lotus Notes.
2. Inaktivieren Sie den UVM-Schutz für die aktuelle Benutzer-ID.
3. Rufen Sie Lotus Notes auf, und wechseln Sie die Benutzer-ID. Weitere Informationen zum Wechseln von Benutzer-IDs finden Sie in der Dokumentation zu Lotus Notes.

   Wenn Sie den UVM-Schutz für die Benutzer-ID, zu der Sie gewechselt haben, konfigurieren möchten, fahren Sie mit Schritt 4 fort.
4. Rufen Sie das von Client Security bereitgestellte Tool zur Lotus Notes-Konfiguration auf, und konfigurieren Sie den UVM-Schutz.

Einschränkungen für das Benutzerkonfigurationsprogramm

Unter Windows XP gibt es für einen Clientbenutzer unter bestimmten Umständen Zugriffseinschränkungen für die verfügbaren Funktionen.

Windows XP Professional

Unter Windows XP Professional können die Einschränkungen für Clientbenutzer in den folgenden Situationen auftreten:

- Client Security ist auf einer Partition installiert, die später in das NTFS-Format konvertiert wird.
- Der Windows-Ordner befindet sich auf einer Partition, die später in das NTFS-Format konvertiert wird.
- Der Archivordner befindet sich auf einer Partition, die später in das NTFS-Format konvertiert wird.

In den vorgenannten Fällen können Benutzer von Windows XP Professional mit eingeschränkter Berechtigung möglicherweise folgende Tasks im Benutzerkonfigurationsprogramm nicht ausführen:

- Den UVM-Verschlüsselungstext ändern
- Das mit UVM registrierte Windows-Kennwort aktualisieren
- Das Schlüsselarchiv aktualisieren

Diese Einschränkungen gelten nicht mehr, nachdem ein Administrator das Administratordienstprogramm gestartet und beendet hat.

Windows XP Home

Benutzer von Windows XP Home mit eingeschränkter Berechtigung können in den folgenden Fällen das Benutzerkonfigurationsprogramm nicht verwenden:

- Client Security ist auf einer Partition im NTFS-Format installiert.
- Der Windows-Ordner befindet sich auf einer Partition im NTFS-Format.
- Der Archivordner befindet sich auf einer Partition im NTFS-Format.

Fehlernachrichten

Fehlernachrichten für Client Security werden in Ereignisprotokoll geschrieben: Client Security verwendet einen Einheitentreiber, der möglicherweise Fehlernachrichten in das Ereignisprotokoll schreibt. Die Fehler, auf denen diese Nachrichten basieren, wirken sich auf den normalen Betrieb des Computers nicht aus.

UVM ruft Fehlernachrichten auf, die vom zugeordneten Programm generiert werden, wenn für ein Authifizierungsobjekt der Zugriff verweigert wird: Wenn in der UVM-Policy die Verweigerung des Zugriffs für ein Authentifizierungsobjekt, z. B. für die E-Mail-Verschlüsselung festgelegt ist, variiert die Nachricht über den verweigerten Zugriff je nach verwendeter Software. Eine Fehlernachricht von Outlook Express über die Verweigerung des Zugriffs auf ein Authentifizierungsobjekt unterscheidet sich somit von einer Netscape-Fehlernachricht über verweigerten Zugriff.

Fehlerbehebungstabellen

Im folgenden Abschnitt finden Sie Tabellen, die Ihnen bei der Behebung von Fehlern in Verbindung mit Client Security weiterhelfen können.

Fehlerbehebungsinformationen zur Installation

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Installation von Client Security weiterhelfen können.

Fehlersymptom	**Mögliche Lösung**
Während der Softwareinstallation wird eine Fehlernachricht angezeigt.	**Maßnahme**
Bei der Softwareinstallation werden Sie in einer Nachricht gefragt, ob Sie die ausgewählte Anwendung und alle zugehörigen Komponenten entfernen möchten.	Klicken Sie auf **OK**, um das Fenster zu verlassen. Beginnen Sie erneut mit dem Installationsprozess, um die neue Version von Client Security zu installieren.
Während der Installation wird eine Nachricht angezeigt, die besagt, dass bereits eine vorherige Version von Client Security installiert ist.	Klicken Sie auf **OK**, um das Fenster zu verlassen. Gehen Sie wie folgt vor: 1. Deinstallieren Sie die Software. 2. Installieren Sie die Software erneut. **Anmerkung:** Wenn Sie dasselbe Hardwarekennwort zum Schutz des integrierten IBM Security Chips verwenden möchten, müssen Sie den Inhalt des Chips nicht löschen und kein neues Kennwort festlegen.
Der Installationszugriff wird verweigert, da das Hardwarekennwort unbekannt ist	**Maßnahme**
Wenn Sie die Software auf einem IBM Client mit aktiviertem integrierten IBM Security Chip installieren, ist das Hardwarekennwort für den integrierten IBM Security Chip unbekannt.	Löschen Sie den Inhalt des Chips, um mit der Installation fortzufahren.
Die Datei ″setup.exe″ reagiert nicht ordnungsgemäß (CSS Version 4.0x)	**Maßnahme**
Wenn Sie alle Dateien aus ″csec4_0.exe″ in ein gemeinsames Verzeichnis extrahieren, funktioniert die Datei ″setup.exe″ nicht ordnungsgemäß.	Führen Sie die Datei ″smbus.exe″ aus, um den SMBus-Einheitentreiber zu installieren, und führen Sie anschließend die Datei ″csec4_0.exe″ aus, um den Softwarecode von Client Security zu installieren.

Fehlerbehebungsinformationen zum Administratordienstprogramm

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Verwendung des Administratordienstprogramms weiterhelfen können.

Fehlersymptom	Mögliche Lösung
Policy für UVM-Verschlüsselungstext nicht erzwungen	**Maßnahme**
Das Markierungsfeld **Mehr als 2 wiederkehrende Zeichen nicht zulassen** funktioniert nicht in IBM Client Security Version 5.0	Dies ist eine bekannte Einschränkung bei IBM Client Security Version 5.0.
Die Schaltfläche ″Weiter″ ist nicht verfügbar, nachdem Sie im Administratordienstprogramm den UVM-Verschlüsselungstext eingegeben und bestätigt haben.	**Maßnahme**
Wenn Sie neue Benutzer in UVM aufnehmen, ist die Schaltfläche **Weiter** möglicherweise nicht mehr verfügbar, nachdem Sie Ihren UVM-Verschlüsselungstext im Administratordienstprogramm eingegeben und bestätigt haben.	Klicken Sie in der Windows-Taskleiste auf **Informationen**, und fahren Sie mit dem Vorgang fort.
Beim Versuch, eine lokale UVM-Policy zu bearbeiten, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Beim Bearbeiten der lokalen UVM-Policy wird möglicherweise eine Fehlernachricht angezeigt, wenn in UVM keine Benutzer registriert sind.	Fügen Sie in UVM einen Benutzer hinzu, bevor Sie versuchen, die Policy-Datei zu bearbeiten.
Beim Ändern des öffentlichen Schlüssels für Administratoren wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie den Inhalt des integrierten Security Chips löschen und anschließend das Schlüsselarchiv wiederherstellen, wird bei der Änderung des öffentlichen Schlüssels für Administratoren möglicherweise eine Fehlernachricht angezeigt.	Fügen Sie in UVM die Benutzer hinzu, und fordern Sie ggf. neue Zertifikate an.
Beim Versuch, einen UVM-Verschlüsselungstext wiederherzustellen, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie einen öffentlichen Schlüssel für Administratoren ändern und anschließend versuchen, einen UVM-Verschlüsselungstext für einen Benutzer wiederherzustellen, wird möglicherweise eine Fehlernachricht angezeigt.	Führen Sie einen der folgenden Schritte aus: • Sollte für den Benutzer der UVM-Verschlüsselungstext nicht benötigt werden, ist keine Maßnahme erforderlich. • Wenn der UVM-Verschlüsselungstext für den Benutzer erforderlich ist, müssen Sie ihn in UVM aufnehmen und ggf. neue Zertifikate anfordern.

Fehlersymptom	Mögliche Lösung
Beim Versuch, die UVM-Policy-Datei zu speichern, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie versuchen, eine UVM-Policy-Datei (globalpolicy.gvm) durch Klicken auf **Übernehmen** oder **Speichern** zu speichern, wird eine Fehlernachricht angezeigt.	Schließen Sie die Fehlernachricht, bearbeiten Sie die UVM-Policy-Datei erneut, und speichern Sie die Datei.
Beim Versuch, den UVM-Policy-Editor zu öffnen, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn der aktuelle Benutzer, der am Betriebssystem angemeldet ist, nicht in UVM aufgenommen wurde, wird der UVM-Policy-Editor nicht geöffnet.	Nehmen Sie den Benutzer in UVM auf, und öffnen Sie den UVM-Policy-Editor.
Bei der Verwendung des Administratordienstprogramms wird eine Fehlernachricht angezeigt.	**Maßnahme**
Während Sie das Administratordienstprogramm verwenden, wird möglicherweise die folgende Fehlernachricht angezeigt: Beim Versuch, auf den Client Security Chip zuzugreifen, ist ein Puffer-E/A-Fehler aufgetreten. Der Fehler kann möglicherweise durch einen Warmstart behoben werden.	Schließen Sie die Fehlernachricht, und starten Sie den Computer erneut.
Beim Ändern des Kennworts für den Security Chip wird eine Nachricht über die Inaktivierung des Chips angezeigt.	**Maßnahme**
Wenn Sie versuchen, das Kennwort für den IBM Security Chip zu ändern, und nach der Eingabe des Bestätigungskennworts die Eingabetaste oder die Tabulatortaste zusammen mit der Eingabetaste drücken, wird die Schaltfläche "Chip inaktivieren" aktiviert, und es wird eine Bestätigungsnachricht für das Inaktivieren des Chips angezeigt.	Gehen Sie wie folgt vor: 1. Schließen Sie das Bestätigungsfenster für die Inaktivierung des Chips. 2. Geben Sie zum Ändern des Kennworts für den IBM Security Chip das neue Kennwort ein, geben Sie das Bestätigungskennwort ein, und klicken Sie anschließend auf **Ändern**. Drücken Sie, nachdem Sie das Bestätigungskennwort eingegeben haben, nicht die Eingabetaste oder die Tabulatortaste zusammen mit der Eingabetaste.

Fehlerbehebungsinformationen zum Benutzerkonfigurationsprogramm

Die folgenden Informationen zur Fehlerbehebung können hilfreich sein, wenn bei der Verwendung des Benutzerkonfigurationsprogramms Fehler auftreten.

Fehlersymptom	**Mögliche Lösung**
Benutzer mit eingeschränkter Berechtigung können gewisse Funktionen des Benutzerkonfigurationsprogramms unter Windows XP Professional nicht ausführen	**Maßnahme**
Benutzer von Windows XP Professional mit eingeschränkter Berechtigung können möglicherweise folgende Tasks im Benutzerkonfigurationsprogramm nicht ausführen: • Den UVM-Verschlüsselungstext ändern • Das mit UVM registrierte Windows-Kennwort aktualisieren • Das Schlüsselarchiv aktualisieren	Diese Einschränkungen gelten nicht mehr, nachdem ein Administrator das Administratordienstprogramm gestartet und beendet hat.
Benutzer mit eingeschränkter Berechtigung können das Benutzerkonfigurationsprogramm unter Windows XP Home nicht ausführen	**Maßnahme**
Benutzer von Windows XP Home mit eingeschränkter Berechtigung können in den folgenden Fällen das Benutzerkonfigurationsprogramm nicht verwenden: • Client Security ist auf einer Partition im NTFS-Format installiert. • Der Windows-Ordner befindet sich auf einer Partition im NTFS-Format. • Der Archivordner befindet sich auf einer Partition im NTFS-Format.	Dies ist eine bekannte Einschränkung unter Windows XP Home. Für dieses Problem gibt es keine Lösung.

Fehlerbehebungsinformationen zum ThinkPad

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Verwendung von Client Security auf ThinkPads weiterhelfen können.

Fehlersymptom	**Mögliche Lösung**
Beim Versuch, eine Administratorfunktion von Client Security aufzurufen, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Nach dem Versuch, eine Administratorfunktion von Client Security aufzurufen, wird eine Fehlernachricht mit folgendem Wortlaut angezeigt: ″FEHLER 0197: Ungültige ferne Änderungsanforderung. Drücken Sie <F1>, um Setup aufzurufen.″	Das ThinkPad-Administratorkennwort muss inaktiviert sein, damit Sie bestimmte Administratorfunktionen von Client Security ausführen können. Gehen Sie wie folgt vor, um das Administratorkennwort zu inaktivieren: 1. Rufen Sie mit ″F1″ das Programm ″IBM BIOS Setup Utility″ auf. 2. Geben Sie das aktuelle Administratorkennwort ein. 3. Geben Sie ein leeres neues Administratorkennwort ein, und bestätigen Sie das leere Kennwort. 4. Drücken Sie die Eingabetaste. 5. Drücken Sie die Taste F10, um die Einstellungen zu speichern und das Programm zu beenden.
Ein anderer UVM-Sensor für Fingerabdrücke funktioniert nicht ordnungsgemäß.	**Maßnahme**
Der IBM ThinkPad unterstützt den Wechsel zwischen mehreren UVM-Sensoren für Fingerabdrücke nicht.	Wechseln Sie die Modelle der Sensoren für Fingerabdrücke nicht. Verwenden Sie bei der Arbeit von einem fernen Standort aus stets das gleiche Modell wie bei der Arbeit an einer Andockstation.

Fehlerbehebungsinformationen zu Microsoft-Anwendungen und -Betriebssystemen

Die folgenden Fehlerbehebungstabellen enthalten Informationen zur Fehlerbehebung bei der Verwendung von Client Security mit Microsoft-Anwendungen oder -Betriebssystemen.

Fehlersymptom	**Mögliche Lösung**
Bildschirmschoner wird nur auf lokaler Anzeige angezeigt	**Maßnahme**
Bei Verwendung des erweiterten Windows-Desktop wird der Client Security-Bildschirmschoner nur auf der lokalen Anzeige angezeigt, obwohl der Zugriff auf das System und die Tastatur geschützt wird.	Wenn sensible Informationen angezeigt werden, verkleinern Sie die Fenster auf Ihrem erweiterten Desktop auf Symbolgröße, bevor Sie den Client Security-Bildschirmschoner aufrufen.
Windows Media Player-Dateien werden verschlüsselt, statt unter Windows XP wiedergegeben zu werden.	**Maßnahme**

Fehlersymptom	Mögliche Lösung
Wenn Sie unter Windows XP einen Ordner öffnen und auf **Alles wiedergeben** klicken, wird der Dateiinhalt verschlüsselt, statt vom Windows Media Player wiedergegeben zu werden.	Gehen Sie wie folgt vor, um die Wiedergabe von Dateien mit dem Windows Media Player zu aktivieren: 1. Starten Sie den Windows Media Player. 2. Wählen Sie alle Dateien im entsprechenden Ordner aus. 3. Ziehen Sie die Dateien in den Bereich ″Wiedergabeliste″ von Windows Media Player.
Client Security funktioniert für einen in UVM registrierten Benutzer nicht ordnungsgemäß.	**Maßnahme**
Der registrierte Clientbenutzer hat möglicherweise seinen Windows-Benutzernamen geändert. Wenn dies zutrifft, geht die gesamte Funktionalität von Client Security verloren.	Registrieren Sie den neuen Benutzernamen in UVM erneut, und fordern Sie alle neuen Berechtigungsnachweise an.
Anmerkung: Unter Windows XP werden in UVM registrierte Benutzer, deren Windows-Benutzername zuvor geändert wurde, von UVM nicht erkannt. Diese Einschränkung gilt selbst dann, wenn der Windows-Benutzername vor der Installation von Client Security geändert wurde.	
Fehler beim Lesen verschlüsselter E-Mails mit Outlook Express	**Maßnahme**
Verschlüsselte E-Mails können nicht entschlüsselt werden, da sich die Verschlüsselungsgrade der Webbrowser, die vom Sender und vom Empfänger verwendet werden, unterscheiden. **Anmerkung:** Wenn Sie Browser mit 128-Bit-Verschlüsselung mit Client Security verwenden möchten, muss der integrierte IBM Security Chip 256-Bit-Verschlüsselung unterstützen. Wenn der integrierte IBM Security Chip 56-Bit-Verschlüsselung unterstützt, müssen Sie einen 40-Bit-Webbrowser verwenden. Der Verschlüsselungsgrad von Client Security ist im Administratordienstprogramm angegeben.	Überprüfen Sie Folgendes: 1. Der Verschlüsselungsgrad des Webbrowsers beim Sender muss mit dem Verschlüsselungsgrad des Webbrowsers des Empfängers kompatibel sein. 2. Der Verschlüsselungsgrad des Webbrowsers muss mit dem Verschlüsselungsgrad der Firmware von Client Security kompatibel sein.
Fehler bei der Verwendung eines Zertifikats von einer Adresse, der mehrere Zertifikate zugeordnet sind	**Maßnahme**
Outlook Express kann mehrere Zertifikate zu einer einzigen E-Mail-Adresse auflisten, und einige dieser Zertifikate können ungültig werden. Ein Zertifikat wird ungültig, wenn der dem Zertifikat zugeordnete private Schlüssel auf dem integrierten IBM Security Chip des Sendercomputers, auf dem das Zertifikat generiert wurde, nicht mehr vorhanden ist.	Bitten Sie den Empfänger, sein digitales Zertifikat erneut zu senden; wählen Sie anschließend dieses Zertifikat im Adressbuch von Outlook Express aus.

Fehlersymptom	Mögliche Lösung
Beim Versuch, eine E-Mail digital zu signieren, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn der Verfasser einer E-Mail versucht, eine E-Mail digital zu signieren, jedoch seinem E-Mail-Account noch kein Zertifikat zugeordnet ist, wird eine Fehlernachricht angezeigt.	Verwenden Sie die Sicherheitseinstellungen in Outlook Express, um ein Zertifikat anzugeben, das dem Benutzeraccount zugeordnet werden soll. Weitere Informationen hierzu finden Sie in der Dokumentation zu Outlook Express.
Outlook Express (128 Bit) verschlüsselt E-Mails nur mit dem 3DES-Algorithmus.	**Maßnahme**
Beim Senden verschlüsselter E-Mails zwischen Clients, die Outlook Express mit der 128-Bit-Version von Internet Explorer 4.0 oder 5.0 verwenden, kann nur der 3DES-Algorithmus verwendet werden.	Wenn Sie Browser mit 128-Bit-Verschlüsselung mit Client Security verwenden möchten, muss der integrierte IBM Security Chip 256-Bit-Verschlüsselung unterstützen. Wenn der integrierte IBM Security Chip 56-Bit-Verschlüsselung unterstützt, müssen Sie einen 40-Bit-Webbrowser verwenden. Der Verschlüsselungsgrad von Client Security ist im Administratordienstprogramm angegeben. Aktuelle Informationen zu den Verschlüsselungsalgorithmen, die mit Outlook Express verwendet werden, erhalten Sie bei Microsoft.
Outlook Express-Clients senden E-Mails mit einem anderen Algorithmus zurück.	**Maßnahme**
Eine mit dem RC2(40)-, RC2(64)- oder RC2(128)-Algorithmus verschlüsselte E-Mail wird von einem Client mit Netscape Messenger an einen Client mit Outlook Express (128 Bit) gesendet. Eine vom Outlook Express-Client zurückgesendete E-Mail wird mit dem Algorithmus RC2(40) verschlüsselt.	Es ist keine Maßnahme erforderlich. Eine Verschlüsselungsanforderung gemäß RC2(40), RC2(64) oder RC2(128) von einem Netscape-Client an einen Outlook Express-Client (128 Bit) wird an den Netscape-Client immer mit dem RC2(40)-Algorithmus zurückgesendet. Aktuelle Informationen zu den Verschlüsselungsalgorithmen, die mit den verschiedenen Versionen von Outlook Express verwendet werden, erhalten Sie von Microsoft.
Bei der Verwendung eines Zertifikats in Outlook Express wird nach dem Ausfall eines Festplattenlaufwerks eine Fehlernachricht angezeigt.	**Maßnahme**
Zertifikate können im Administratordienstprogramm mit der Wiederherstellungsfunktion für Schlüssel wiederhergestellt werden. Möglicherweise sind einige Zertifikate, wie z. B. die kostenfreien Zertifikate von VeriSign, nach einer Schlüsselwiederherstellung nicht wiederhergestellt.	Führen Sie nach der Wiederherstellung der Schlüssel einen der folgenden Schritte aus: • Fordern Sie neue Zertifikate an. • Registrieren Sie die Zertifizierungsinstanz erneut in Outlook Express.

Fehlersymptom	Mögliche Lösung
Outlook Express aktualisiert den dem Zertifikat zugeordneten Verschlüsselungsgrad nicht.	**Maßnahme**
Wenn ein Sender den Verschlüsselungsgrad in Netscape auswählt und eine signierte E-Mail an einen Outlook Express-Client mit Internet Explorer 4.0 (128 Bit) sendet, stimmt möglicherweise der Verschlüsselungsgrad der zurückgesendeten E-Mail nicht überein.	Löschen Sie das zugeordnete Zertifikat aus dem Adressbuch von Outlook Express. Öffnen Sie die signierte E-Mail erneut, und fügen Sie dem Adressbuch von Outlook Express das Zertifikat hinzu.
In Outlook Express wird eine Nachricht über Entschlüsselungsfehler angezeigt.	**Maßnahme**
Sie können in Outlook Express eine Nachricht öffnen, indem Sie doppelt darauf klicken. Wenn Sie zu schnell auf eine verschlüsselte Nachricht klicken, wird in einigen Fällen eine Nachricht über Entschlüsselungsfehler angezeigt.	Schließen Sie die Nachricht, und öffnen Sie die verschlüsselte E-Mail erneut.
Darüber hinaus wird möglicherweise in der Voranzeige eine Fehlernachricht angezeigt, wenn Sie eine verschlüsselte Nachricht auswählen.	Wenn in der Voranzeige eine Fehlernachricht angezeigt wird, ist keine Maßnahme erforderlich.
Wenn Sie bei verschlüsselten E-Mails zwei Mal auf die Schaltfläche "Senden" klicken, wird eine Fehlernachricht angezeigt	**Maßnahme**
Wenn Sie in Outlook Express zweimal auf die Schaltfläche zum Senden klicken, um eine verschlüsselte E-Mail zu senden, wird eine Fehlernachricht darüber angezeigt, dass die Nachricht nicht gesendet werden konnte.	Schließen Sie die Fehlernachricht, und klicken Sie einmal auf die Schaltfläche **Senden**.
Beim Anfordern eines Zertifikats wird eine Fehlernachricht angezeigt.	**Maßnahme**
Bei Verwendung von Internet Explorer erhalten Sie möglicherweise eine Fehlernachricht, wenn Sie ein Zertifikat anfordern, das das CSP-Modul des integrierten IBM Security Chips verwendet.	Fordern Sie das digitale Zertifikat erneut an.

Fehlerbehebungsinformationen zu Netscape-Anwendungen

Die folgenden Fehlerbehebungstabellen enthalten Informationen zur Fehlerbehebung bei der Verwendung von Client Security mit Netscape-Anwendungen.

Fehlersymptom	**Mögliche Lösung**
Fehler beim Lesen verschlüsselter E-Mails	**Maßnahme**
Verschlüsselte E-Mails können nicht entschlüsselt werden, da sich die Verschlüsselungsgrade der Webbrowser, die vom Sender und vom Empfänger verwendet werden, unterscheiden. **Anmerkung:** Wenn Sie Browser mit 128-Bit-Verschlüsselung mit Client Security verwenden möchten, muss der integrierte IBM Security Chip 256-Bit-Verschlüsselung unterstützen. Wenn der integrierte IBM Security Chip 256-Bit-Verschlüsselung unterstützt, müssen Sie einen 40-Bit-Webbrowser verwenden. Der Verschlüsselungsgrad von Client Security ist im Administratordienstprogramm angegeben.	Überprüfen Sie Folgendes: 1. Der Verschlüsselungsgrad des vom Sender verwendeten Webbrowsers ist mit dem Verschlüsselungsgrad des vom Empfänger verwendeten Webbrowsers kompatibel. 2. Der Verschlüsselungsgrad des Webbrowsers ist mit dem Verschlüsselungsgrad kompatibel, der von der Firmware von Client Security bereitgestellt wird.
Beim Versuch, eine E-Mail digital zu signieren, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn das Zertifikat des integrierten IBM Security Chips in Netscape Messenger nicht ausgewählt wurde und der Verfasser der E-Mail versucht, diese mit dem Zertifikat zu signieren, wird eine Fehlernachricht angezeigt.	Verwenden Sie zur Auswahl des Zertifikats die Sicherheitseinstellungen in Netscape Messenger. Wenn Netscape Messenger geöffnet ist, klicken Sie in der Symbolleiste auf das Sicherheitssymbol. Das Fenster mit den Sicherheitsinformationen wird geöffnet. Klicken Sie im linken Teilfenster auf **Netscape Messenger**, und wählen Sie anschließend **Zertifikat des integrierten IBM Security Chips** aus. Weitere Informationen hierzu finden Sie in der Dokumentation von Netscape.
Eine E-Mail wird mit einem anderen Algorithmus an den Client zurückgesendet.	**Maßnahme**
Eine mit dem RC2(40)-, RC2(64)- oder RC2(128)-Algorithmus verschlüsselte E-Mail wird von einem Client mit Netscape Messenger an einen Client mit Outlook Express (128 Bit) gesendet. Eine vom Outlook Express-Client zurückgesendete E-Mail wird mit dem Algorithmus RC2(40) verschlüsselt.	Es ist keine Maßnahme erforderlich. Eine Verschlüsselungsanforderung gemäß RC2(40), RC2(64) oder RC2(128) von einem Netscape-Client an einen Outlook Express-Client (128 Bit) wird an den Netscape-Client immer mit dem RC2(40)-Algorithmus zurückgesendet. Aktuelle Informationen zu den Verschlüsselungsalgorithmen, die mit den verschiedenen Versionen von Outlook Express verwendet werden, erhalten Sie von Microsoft.

Fehlersymptom	Mögliche Lösung
Ein digitales Zertifikat, das vom integrierten IBM Security Chip generiert wurde, kann nicht verwendet werden.	**Maßnahme**
Das vom integrierten IBM Security Chip generierte digitale Zertifikat ist nicht verfügbar.	Überprüfen Sie, ob Sie beim Öffnen von Netscape den richtigen UVM-Verschlüsselungstext eingegeben haben. Wenn Sie den falschen UVM-Verschlüsselungstext eingeben, wird eine Fehlernachricht über einen Authentifizierungsfehler angezeigt. Wenn Sie auf **OK** klicken, wird Netscape geöffnet, Sie können aber das vom integrierten IBM Security Chip generierte Zertifikat nicht verwenden. Sie müssen Netscape verlassen und erneut öffnen und anschließend den richtigen UVM-Verschlüsselungstext eingeben.
Neue digitale Zertifikate vom selben Sender werden innerhalb von Netscape nicht ausgetauscht.	**Maßnahme**
Wenn eine digital signierte E-Mail vom selben Sender mehrmals empfangen wird, wird das erste digitale Zertifikat, das der E-Mail zugeordnet ist, nicht überschrieben.	Wenn Sie mehrere E-Mail-Zertifikate empfangen, ist das einzige Zertifikat das Standardzertifikat. Löschen Sie mit den Sicherheitseinrichtungen in Netscape das erste Zertifikat, und öffnen Sie anschließend das zweite Zertifikat erneut, oder bitten Sie den Sender, eine weitere signierte E-Mail zu senden.
Das Zertifikat des integrierten IBM Security Chips kann nicht exportiert werden.	**Maßnahme**
Das Zertifikat des integrierten IBM Security Chips kann in Netscape nicht exportiert werden. Die Exportfunktion in Netscape können Sie zum Sichern von Zertifikaten verwenden.	Rufen Sie das Administratordienstprogramm oder Benutzerkonfigurationsprogramm auf, um das Schlüsselarchiv zu aktualisieren. Wenn Sie das Schlüsselarchiv aktualisieren, werden von allen Zertifikaten, die dem integrierten IBM Security Chip zugeordnet sind, Kopien erstellt.
Beim Versuch, ein wiederhergestelltes Zertifikat nach dem Ausfall eines Festplattenlaufwerks zu verwenden, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Zertifikate können im Administratordienstprogramm mit der Wiederherstellungsfunktion für Schlüssel wiederhergestellt werden. Möglicherweise sind einige Zertifikate, wie z. B. die kostenfreien Zertifikate von VeriSign, nach einer Schlüsselwiederherstellung nicht wiederhergestellt.	Fordern Sie nach dem Wiederherstellen der Schlüssel ein neues Zertifikat an.

Fehlersymptom	Mögliche Lösung
Der Netscape-Agent wird geöffnet und verursacht einen Fehler in Netscape.	**Maßnahme**
Das Öffnen des Netscape-Agenten führt zum Schließen von Netscape.	Schalten Sie den Netscape-Agenten aus.
Netscape wird mit zeitlicher Verzögerung geöffnet.	**Maßnahme**
Wenn Sie das PKCS #11-Modul des integrierten IBM Security Chips hinzufügen und anschließend Netscape öffnen, verzögert sich das Öffnen von Netscape um kurze Zeit.	Es ist keine Maßnahme erforderlich. Dies dient lediglich zu Ihrer Information.

Fehlerbehebungsinformationen zu digitalen Zertifikaten

Die folgenden Informationen zur Fehlerbehebung können hilfreich sein, wenn bei der Anforderung eines digitalen Zertifikats Fehler auftreten.

Fehlersymptom	Mögliche Lösung
Das Fenster "UVM-Verschlüsselungstext" oder das Fenster für die Authentifizierung über Fingerabdrücke wird bei der Anforderung eines digitalen Zertifikats mehrmals angezeigt.	**Maßnahme**
In der UVM-Sicherheits-Policy ist festgelegt, dass ein Benutzer sich mit einem UVM-Verschlüsselungstext oder über Fingerabdrücke authentifizieren muss, bevor er ein digitales Zertifikat erhalten kann. Wenn der Benutzer versucht, ein Zertifikat zu erhalten, wird das Authentifizierungsfenster, in dem er aufgefordert wird, den UVM-Verschlüsselungstext anzugeben oder die Fingerabdrücke abtasten zu lassen, mehrmals angezeigt.	Geben Sie bei jedem Öffnen des Authentifizierungsfensters den UVM-Verschlüsselungstext ein bzw. lassen Sie ihre Fingerabdrücke abtasten.
Eine Nachricht über einen VBScript- oder JavaScript-Fehler wird angezeigt.	**Maßnahme**
Wenn Sie ein digitales Zertifikat anfordern, wird möglicherweise eine Fehlernachricht angezeigt, die sich auf VBScript oder JavaScript bezieht.	Starten Sie den Computer erneut, und beziehen Sie das Zertifikat erneut.

Fehlerbehebungsinformationen zu Tivoli Access Manager

Die folgenden Informationen zur Fehlerbehebung können hilfreich sein, wenn bei der Verwendung von Tivoli Access Manager in Verbindung mit Client Security Fehler auftreten.

Fehlersymptom	**Mögliche Lösung**
Die lokalen Policy-Einstellungen entsprechen nicht denen auf dem Server.	**Maßnahme**
Tivoli Access Manager lässt bestimmte Bit-Konfigurationen zu, die von UVM nicht unterstützt werden. Folglich können lokale Policy-Anforderungen Einstellungen überschreiben, die ein Administrator bei der Konfiguration eines PD-Servers vorgenommen hat.	Dies ist eine bekannte Einschränkung.
Kein Zugriff auf die Konfigurationseinstellungen von Tivoli Access Manager	**Maßnahme**
Im Administratordienstprogramm kann auf der Seite zur Policy-Installation weder auf die Konfigurationseinstellungen von Tivoli Access Manager noch auf die entsprechenden Einstellungen zur lokalen Cache-Einrichtung zugegriffen werden.	Installieren Sie Tivoli Access Manager Runtime Environment. Wenn die Laufzeitumgebung (Runtime Environment) auf dem IBM Client nicht installiert ist, sind auf der Seite zur Policy-Installation auch keine Einstellungen für Tivoli Access Manager verfügbar.
Eine Benutzersteuerung gilt sowohl für den Benutzer als auch für die Gruppe.	**Maßnahme**
Wenn Sie beim Konfigurieren des Tivoli Access Manager-Servers einen Benutzer für eine Gruppe definieren, gilt die Benutzersteuerung sowohl für den Benutzer als auch für die Gruppe, wenn die Option **Traverse-bit** aktiviert wurde.	Es ist keine Maßnahme erforderlich.

Fehlerbehebungsinformationen zu Lotus Notes

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Verwendung von Lotus Notes mit Client Security weiterhelfen können.

Fehlersymptom	**Mögliche Lösung**
Nach dem Aktivieren des UVM-Schutzes für Lotus Notes kann Lotus Notes die Konfiguration nicht fertig stellen.	**Maßnahme**
Lotus Notes kann nach dem Aktivieren des UVM-Schutzes mit dem Administratordienstprogramm die Konfiguration nicht fertig stellen.	Dies ist eine bekannte Einschränkung. Lotus Notes muss konfiguriert werden und aktiv sein, bevor die Lotus Notes-Unterstützung im Administratordienstprogramm aktiviert wird.
Beim Versuch, das Notes-Kennwort zu ändern, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie das Notes-Kennwort bei Verwendung von Client Security ändern, wird dies in einer Fehlernachricht angezeigt.	Wiederholen Sie die Kennwortänderung. Wurde der Fehler dadurch nicht behoben, starten Sie den Client neu.
Nach dem Festlegen eines Kennworts per Zufallsgenerator wird eine Fehlernachricht angezeigt.	**Maßnahme**
Wenn Sie folgende Vorgänge ausführen, wird möglicherweise eine Fehlernachricht angezeigt: • Verwenden des Tools zur Lotus Notes-Konfiguration zur Einstellung des UVM-Schutzes für eine Notes-ID • Öffnen von Notes und Verwenden der Notes-Funktion zur Kennwortänderung für die Datei mit der Notes-ID • Schließen von Notes sofort nach der Kennwortänderung	Klicken Sie auf **OK**, um die Fehlernachricht zu schließen. Es ist keine weitere Maßnahme erforderlich. Entgegen der Fehlernachricht wurde das Kennwort geändert. Das neue Kennwort wurde von Client Security per Zufallsgenerator festgelegt. Die Datei mit der Notes-ID wird nun mit dem per Zufallsgenerator festgelegten Kennwort verschlüsselt, und der Benutzer benötigt keine neue Benutzer-ID-Datei. Wenn der Endbenutzer das Kennwort erneut ändert, generiert UVM ein neues, per Zufallsgenerator festgelegtes Kennwort für die Notes-ID.

Fehlerbehebungsinformationen zur Verschlüsselung

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Verschlüsselung von Dateien unter Verwendung von Client Security ab Version 3.0 weiterhelfen können.

Fehlersymptom	**Mögliche Lösung**
Bereits verschlüsselte Dateien werden nicht entschlüsselt.	**Maßnahme**
Dateien, die mit früheren Versionen von Client Security verschlüsselt wurden, werden nach dem Upgrade auf Client Security ab Version 3.0 nicht entschlüsselt.	Dies ist eine bekannte Einschränkung. Sie müssen alle mit früheren Versionen von Client Security verschlüsselten Dateien entschlüsseln, *bevor* Sie Client Security ab Version 3.0 installieren. Client Security 3.0 kann Dateien, die von früheren Versionen von Client Security verschlüsselt wurden, nicht entschlüsseln, da in dieser Version die Implementierung der Dateiverschlüsselung geändert wurde.

Fehlerbehebungsinformationen zu UVM-sensitiven Einheiten

Im folgenden Abschnitt finden Sie Informationen, die Ihnen bei der Behebung von Fehlern bei der Verwendung UVM-sensitiver Einheiten weiterhelfen können.

Fehlersymptom	**Mögliche Lösung**
Eine UVM-sensitive Einheit funktioniert nicht mehr ordnungsgemäß.	**Maßnahme**
Wenn Sie eine UVM-sensitive Einheit vom USB-Anschluss (Universal Serial Bus) trennen und die Einheit danach erneut am USB-Anschluss anschließen, funktioniert die Einheit möglicherweise nicht ordnungsgemäß.	Starten Sie nach dem erneuten Anschluss der Einheit an den USB-Anschluss den Computer erneut.

Anhang A. Regeln für Kennwörter und Verschlüsselungstexte

In diesem Anhang finden Sie Informationen zu den Regeln für verschiedene Systemkennwörter.

Regeln für Hardwarekennwörter

Für Hardwarekennwörter gelten die folgenden Regeln:

Länge Das Kennwort muss genau acht Zeichen lang sein.

Zeichen
Das Kennwort darf nur alphanumerische Zeichen enthalten. Die Kombination von Buchstaben und Ziffern ist zulässig. Es sind keine speziellen Zeichen wie das Leerzeichen und die Zeichen !, ?, % zulässig.

Merkmale
Sie können das Kennwort für den IBM Security Chip festlegen, um den integrierten IBM Security Chip im Computer zu aktivieren. Dieses Kennwort müssen Sie bei jedem Zugriff auf das Administratordienstprogramm eingeben.

Fehlversuche
Wenn Sie das Kennwort zehnmal falsch eingegebenen haben, wird der Computer 1 Stunde und 17 Minuten lang gesperrt. Wenn Sie nach diesem Zeitraum das Kennwort zehn weitere Male falsch eingeben, wird der Computer 2 Stunden und 34 Minuten lang gesperrt. Die Dauer der Computersperrung verdoppelt sich jedes Mal, wenn Sie das Kennwort zehnmal falsch eingeben.

Regeln für UVM-Verschlüsselungstexte

Die Sicherheit wird dadurch erhöht, dass der UVM-Verschlüsselungstext länger und eindeutiger ist als ein herkömmliches Kennwort. Die Policy für den UVM-Verschlüsselungstext wird über das Administratordienstprogramm von IBM Client Security gesteuert.

Das Fenster ″Policy für UVM-Verschlüsselungstext″ des Administratordienstprogramms stellt Sicherheitsadministratoren eine einfache Schnittstelle zur Steuerung von Kriterien für Verschlüsselungstexte bereit. Über das Fenster ″Policy für UVM-Verschlüsselungstext″ kann der Administrator folgende Regeln für Verschlüsselungstexte festlegen:

Anmerkung: Die Standardeinstellung für jedes Kriterium ist unten in Klammern angegeben.

- ob eine Mindestanzahl an alphanumerischen Zeichen festgelegt werden soll (ja, 6)

  Wenn z. B. der Wert ″6″ festgelegt ist, ist der Verschlüsselungstext `1234567xxx` ungültig.
- ob eine Mindestanzahl an Ziffern festgelegt werden soll (ja, 1)

  Wenn z. B. der Wert ″1″ festgelegt ist, ist der Verschlüsselungstext `thisismypassword` ungültig.

- ob eine Mindestanzahl an Leerzeichen festgelegt werden soll (keine Mindestanzahl)

  Wenn z. B. der Wert ″2″ festgelegt ist, ist der Verschlüsselungstext `i am not here` ungültig.
- ob mehr als zwei wiederkehrende Zeichen zulässig sein sollen (nein)

  Wenn dies z. B. festgelegt ist, ist der Verschlüsselungstext `aaabcdefghijk` ungültig.
- ob der Verschlüsselungstext mit einer Ziffer beginnen darf (nein)

  Standardmäßig ist z. B. der Verschlüsselungstext `1password` ungültig.
- ob der Verschlüsselungstext mit einer Ziffer enden darf (nein)

  Standardmäßig ist z. B. der Verschlüsselungstext `password8` ungültig.
- ob der Verschlüsselungstext eine Benutzer-ID enthalten darf (nein)

  Standardmäßig ist z. B. der Verschlüsselungstext `Benutzername` ungültig, wobei es sich bei `Benutzername` um eine Benutzer-ID handelt.
- ob der neue Verschlüsselungstext sich von den letzten x Verschlüsselungstexten unterscheiden muss (ja, 3)

  Standardmäßig ist z. B. der Verschlüsselungstext `mypassword` ungültig, wenn einer der drei vorherigen Verschlüsselungstexte `mypassword` war.
- ob der Verschlüsselungstext mehr als drei identische aufeinander folgende Zeichen des letzten Kennworts enthalten darf (nein)

  Standardmäßig ist z. B. der Verschlüsselungstext `password` ungültig, wenn einer der drei vorherigen Verschlüsselungstexte `pass` oder `word` war.

Das Fenster ″Policy für UVM-Verschlüsselungstext″ des Administratordienstprogramms ermöglicht Sicherheitsadministratoren zudem eine Steuerung des Ablaufs der Verschlüsselungstexte. Über das Fenster ″Policy für UVM-Verschlüsselungstext″ kann der Administrator aus den folgenden Regeln für Verschlüsselungstexte auswählen:

- Verschlüsselungstext ist nicht mehr gültig nach (ja, 184).

  In diesem Beispiel läuft der Verschlüsselungstext standardmäßig nach 184 Tagen ab. Der neue Verschlüsselungstext muss der vorhandenen Policy für den Verschlüsselungstext entsprechen.
- Verschlüsselungstext läuft nie ab.

  Wenn diese Option ausgewählt ist, läuft der Verschlüsselungstext nie ab.

Die Policy für den Verschlüsselungstext wird vom Administratordienstprogramm bei der Registrierung des Benutzers und bei der Änderung des Verschlüsselungstextes durch den Benutzer über das Clientdienstprogramm überprüft. Die beiden Benutzereinstellungen zum vorherigen Kennwort werden zurückgesetzt, und Protokolle zum Verschlüsselungstext werden entfernt.

Folgende allgemeine Regeln gelten für UVM-Verschlüsselungstexte:

Länge Der Verschlüsselungstext kann bis zu 256 Zeichen lang sein.

Zeichen
Der Verschlüsselungstext kann jede beliebige Kombination von Zeichen enthalten, die die Tastatur erzeugt, einschließlich Leerzeichen und nicht alphanumerische Zeichen.

Merkmale

Der UVM-Verschlüsselungstext unterscheidet sich von einem Kennwort, das Sie zur Anmeldung am Betriebssystem verwenden können. Der UVM-Verschlüsselungstext kann in Verbindung mit anderen Authentifizierungseinheiten verwendet werden, z. B. mit einem UVM-Sensor für Fingerabdrücke.

Fehlversuche

Wenn Sie während einer Sitzung den UVM-Verschlüsselungstext mehrmals falsch eingeben, wird der Computer nicht gesperrt. Für die Anzahl der Fehlversuche besteht keine Begrenzung.

Anhang B. Bemerkungen und Marken

Dieser Anhang enthält rechtliche Hinweise zu IBM Produkten und Informationen zu Marken.

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in diesem Dokument beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Dienstleistungen von IBM verwendet werden können. Anstelle der Produkte, Programme oder Dienstleistungen können auch andere, ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen oder andere Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremddienstleistungen liegt beim Kunden.

Für in diesen Dokument beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder IBM Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanfragen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Europe
Director of Licensing
92066 Paris
La Defense, Cedex
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekannt gegeben. IBM kann jederzeit ohne Vorankündigung Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse: IBM Corporation, Department 80D, P.O. Box 12195, 3039 Cornwallis, Research Triangle Park, NC 27709, U.S.A. Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesem Dokument aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der Allgemeinen Geschäftsbedingungen der IBM, der Internationalen Nutzungsbedingungen der IBM für Programmpakete oder einer äquivalenten Vereinbarung.

Marken

IBM und SecureWay sind in gewissen Ländern Marken der IBM Corporation.

Tivoli ist in gewissen Ländern eine Marke von Tivoli Systems Inc.

Microsoft, Windows und Windows NT sind in gewissen Ländern Marken der Microsoft Corporation.

Andere Namen von Unternehmen, Produkten und Dienstleistungen können Marken oder Dienstleistungsmarken anderer Unternehmen sein.