IBM Client Security Solutions

Client Security Version 5.3 Installationshandbuch

IBM Client Security Solutions

Client Security Version 5.3 Installationshandbuch

Hinweis:
Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten Sie die Informationen in Anhang B, „**Bemerkungen und Marken**", auf Seite 59 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 (Mai 2004)

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Client Security Solutions Client Security Version 5.3 Installation Guide,
herausgegeben von International Business Machines Corporation, USA

Herausgegeben von:
SW TSC Germany
Kst. 2877
Mai 2004

Inhaltsverzeichnis

Vorwort

Dieser Abschnitt enthält Hinweise zur Verwendung dieses Handbuchs.

Inhalt dieses Handbuchs

Das vorliegende Handbuch enthält Informationen zum Einsatz von IBM Client Security auf IBM Netzwerkcomputern bzw. IBM Clients, auf denen das integrierte IBM Sicherheits-Subsystem (IBM Embedded Security Subsystem) installiert ist. Außerdem finden Sie in diesem Handbuch Anweisungen zum Aktivieren des integrierten IBM Sicherheits-Subsystems sowie zum Festlegen des Administratorkennworts für das Sicherheits-Subsystem.

Das Handbuch umfasst folgende Inhalte:

Kapitel 1, „Einführung", enthält eine kurze Übersicht über grundlegende Sicherheitskonzepte, 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 IBM 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, „Informationen zu Kennwörtern und Verschlüsselungstexten", enthält Kriterien für Verschlüsselungstexte, die auf einen UVM-Verschlüsselungstext angewendet werden können, und Regeln für Kennwörter für Administratorkennwörter.

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/us/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 Sicherheitspolicy 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/us/security/index.html.

Kapitel 1. Einführung

Select ThinkPad™- und ThinkCentre™-Computer sind mit integrierter Verschlüsselungshardware ausgestattet, die mit für den Download verfügbaren Softwaretechnologien arbeitet und einen leistungsfähigen Schutz für Client-PC-Plattformen bietet. In der Gesamtheit wird diese Hardware und Software als das integrierte IBM Sicherheits-Subsystem oder abgekürzt als ESS (Embedded Security Subsystem) bezeichnet. Bei der Hardwarekomponente handelt es sich um den integrierten IBM Security Chip, bei der Softwarekomponente um IBM Client Security (abgekürzt CSS - Client Security Software).

Die Software "IBM Client Security" ist für IBM Computer konzipiert, die den integrierten IBM Security Chip zum Verschlüsseln von Dateien und zum Speichern von Chiffrierschlüsseln verwenden. Diese Software umfasst Anwendungen und Komponenten, die es IBM Clientsystemen ermöglichen, die Client-Sicherheitsfunktionen in einem lokalen Netzwerk, in einem Unternehmen oder im Internet zu nutzen.

IBM ESS

IBM ESS, das integrierte IBM Sicherheits-Subsystem, unterstützt Schlüsselverwaltungslösungen, wie z. B. die PKI-Infrastruktur, und besteht aus den folgenden lokalen Anwendungen:

- Verschlüsselung von Dateien und Ordnern (FFE - File and Folder Encryption)
- Password Manager
- Gesicherte Windows-Anmeldung
- Mehreren konfigurierbaren Authentifizierungsmethoden, wie z. B.:
  - Verschlüsselungstext
  - Fingerabdruck
  - Smartcard
  - Berührungsloser Ausweis (Proximity Card)

Um die Funktionen von IBM ESS effizient nutzen zu können, muss der Sicherheitsadministrator mit einigen grundlegenden Konzepten vertraut sein. In den folgenden Abschnitten werden grundlegende Sicherheitskonzepte beschrieben.

Integrierter IBM Security Chip

Beim integrierten IBM Sicherheits-Subsystem (IBM Embedded Security Subsystem) handelt es sich um die integrierte Verschlüsselungshardware-Technologie, die eine zusätzliche Schutzebene für ausgewählte IBM PC-Plattformen bietet. Durch die Einführung dieses Sicherheits-Subsystems werden Verschlüsselungs- und Authentifizierungsprozesse von der Software, die relativ fehleranfällig ist, auf die sichere Umgebung einer dedizierten Hardware übertragen. So wird die Sicherheit deutlich erhöht.

Das integrierte IBM Sicherheits-Subsystem unterstützt folgende Funktionen:

- RSA3-PKI-Vorgänge, wie z. B. Verschlüsselung aus Datenschutzgründen sowie digitale Unterschriften zur Authentifizierung
- RSA-Schlüsselerstellung

- Erstellung von Zufallszahlen
- Berechnung von RSA-Funktionen in 200 Millisekunden
- EEPROM-Speicher für RSA-Schlüsselpaarspeicherung
- Alle in der Spezifikation Vs. 1.1 definierten TCPA-Funktionen
- Kommunikation mit dem Hauptprozessor über den LPC-Bus (LPC - Low Pin Count)

IBM Client Security

IBM Client Security beinhaltet folgende Softwareanwendungen und Komponenten:

- **Administratordienstprogramm:** Das Administratordienstprogramm ist die Schnittstelle, die vom Administrator zum Aktivieren oder Inaktivieren des integrierten IBM Sicherheits-Subsystems sowie zum Erstellen, Archivieren und Neugenerieren von Chiffrierschlüsseln und Verschlüsselungstexten verwendet wird. Außerdem kann ein Administrator in diesem Dienstprogramm Benutzer in die von Client Security bereitgestellte Sicherheitspolicy aufnehmen.
- **Administratorkonsole:** Die Administratorkonsole von Client Security ermöglicht es einem Administrator, ein Netzwerk mit standortunabhängigem Zugriff mit Berechtigungsnachweis zu konfigurieren, Dateien zu erstellen und zu konfigurieren, die Implementierung ermöglichen, und eine Konfiguration und ein Konfigurations- und Wiederherstellungsprofil ohne Administratorberechtigung zu erstellen.
- **Benutzerkonfigurationsprogramm:** Das Benutzerkonfigurationsprogramm ermöglicht es Clientbenutzern, den UVM-Verschlüsselungstext zu ändern, Windows-Anmeldekennwörter für die Erkennung durch UVM zu aktivieren, Schlüsselarchive zu aktualisieren sowie Fingerabdrücke zu registrieren. Außerdem kann ein Benutzer Sicherungskopien der digitalen Zertifikate erstellen, die vom integrierten IBM Sicherheits-Subsystem erzeugt wurden.
- **User Verification Manager (UVM):** Client Security verwendet UVM, um Verschlüsselungstexte und andere Elemente zur Authentifizierung von Systembenutzern zu verwalten. So kann z. B. ein Lesegerät für Fingerabdrücke von UVM für die Anmeldungsauthentifizierung verwendet werden. Client Security unterstützt die folgenden Funktionen:
  - **UVM-Client-Policy-Schutz:** Client Security ermöglicht es Sicherheitsadministratoren, die Client-Sicherheitspolicy einzurichten, die festlegt, wie ein Clientbenutzer auf dem System authentifiziert wird.

    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-Schutz bei der Anmeldung am System:** Client Security ermöglicht es Administratoren, den Zugriff auf Computer über eine Anmeldeschnittstelle zu steuern. Der UVM-Schutz stellt sicher, dass nur Benutzer, die von der Sicherheitspolicy erkannt werden, auf das Betriebssystem zugreifen können.

Beziehung zwischen Kennwörtern und Schlüsseln

Kennwörter und Schlüssel dienen, zusammen mit weiteren optionalen Authentifizierungsgeräten, zur Prüfung der Identität von Systembenutzern. Zum Verständnis der Funktionsweise von IBM Client Security ist es entscheidend, die Beziehung zwischen Kennwörtern und Schlüsseln zu verstehen.

Administratorkennwort

Das Administratorkennwort wird zur Authentifizierung des Administrators beim integrierten IBM Sicherheits-Subsystem verwendet. Dieses Kennwort, das acht Zeichen lang sein muss, wird innerhalb der sicheren Hardware des integrierten IBM Sicherheits-Subsystems verwaltet und authentifiziert. Wenn es authentifiziert ist, kann der Administrator folgende Aktionen ausführen:

- Benutzer registrieren
- Die Policy-Schnittstelle starten
- Das Administratorkennwort ändern

Das Administratorkennwort kann auf eine der folgenden Arten definiert werden:

- Über den Installationsassistenten von IBM Client Security
- Über das Administratordienstprogramm
- Mit Hilfe von Scripts
- Über die BIOS-Schnittstelle (nur für ThinkCentre-Computer)

Es ist wichtig, zum Erstellen und Verwalten des Administratorkennworts nach einer Strategie vorzugehen. Das Administratorkennwort kann geändert werden, wenn es beschädigt oder vergessen wurde.

Im Vergleich mit TCG-Begriffen und TCG-Terminologie entspricht das Administratorkennwort dem OAV (Owner Authorization Value). Da das Administratorkennwort mit dem integrierten IBM Sicherheits-Subsystem verknüpft ist, wird es manchmal auch als das *Hardwarekennwort* bezeichnet.

Öffentlicher und privater Hardwareschlüssel

Grundsätzlich kann zum integrierten IBM Sicherheits-Subsystem gesagt werden, dass es als *Root of Trust* auf einem Clientsystem fungiert. Diese ″Root″ wird zum Sichern anderer Anwendungen und Funktionen verwendet. Zum Aufbauen einer ″Root of Trust″ ist das Erstellen eines öffentlichen Hardwareschlüssels und eines privaten Hardwareschlüssels erforderlich. Ein öffentlicher und ein privater Schlüssel, die als *Schlüsselpaar* bezeichnet werden, stehen in folgender mathematischer Beziehung zueinander:

- alle mit dem öffentlichen Schlüssel verschlüsselten Daten nur durch den entsprechenden privaten Schlüssel entschlüsselt werden können und
- alle mit dem privaten Schlüssel verschlüsselten Daten nur durch den entsprechenden öffentlichen Schlüssel entschlüsselt werden können.

Der private Hardwareschlüssel wird innerhalb der sicheren Hardware des Sicherheits-Subsystems erstellt, gespeichert und verwendet. Der öffentliche Hardwareschlüssel steht zu verschiedenen Zwecken zur Verfügung (daher die Bezeichnung ″öffentlicher Schlüssel″); er wird jedoch nie außerhalb der gesicherten Hardware des Sicherheits-Subsystems verwendet. Der öffentliche und der private Hardwareschlüssel sind ein kritischer Teil der IBM Schlüsselauslagerungshierarchie, die in einem der folgenden Abschnitte behandelt wird.

Öffentliche und private Hardwareschlüssel können auf eine der folgenden Arten erstellt werden:

- Über den Installationsassistenten von IBM Client Security
- Über das Administratordienstprogramm
- Mit Hilfe von Scripts

In Begriffen und in der Terminologie von TCG (Trusted Computing Group) ausgedrückt würden der öffentliche und der private Hardwareschlüssel als *Storage Root Key* (SRK) bezeichnet.

Öffentlicher und privater Administratorschlüssel

Der öffentliche und der private Administratorschlüssel sind integraler Bestandteil der IBM Schlüsselauslagerungshierarchie. Sie ermöglichen es, dass benutzerspezifische Daten bei einem Ausfall der Systemplatine oder des Festplattenlaufwerks gesichert und wiederhergestellt werden können.

Der öffentliche und der private Administratorschlüssel können entweder auf jedem System eindeutig oder für alle Systeme oder Systemgruppen gleich sein. Es ist wichtig zu beachten, dass diese Administratorschlüssel verwaltet werden müssen und dass das Vorhandensein einer Strategie der Verwendung eindeutiger bzw. bekannter Schlüssel entscheidend ist.

Öffentliche und private Schlüssel können auf eine der folgenden Arten erstellt werden:

- Über den Installationsassistenten von IBM Client Security
- Über das Administratordienstprogramm
- Mit Hilfe von Scripts

ESS-Archiv

Mit Hilfe von öffentlichen und privaten Administratorschlüsseln können benutzerspezifische Daten bei einem Ausfall der Systemplatine oder des Festplattenlaufwerks gesichert und wiederhergestellt werden.

Öffentliche und private Benutzerschlüssel

Das integrierte IBM Sicherheits-Subsystem erstellt öffentliche und private Benutzerschlüssel, um die benutzerspezifischen Daten zu sichern. Diese Schlüsselpaare werden bei der Registrierung eines Benutzers bei IBM Client Security erstellt. Diese Schlüssel werden transparent von der UVM-Komponente (User Verification Manager) von IBM Client Security erstellt und verwaltet. Die Schlüssel werden basierend darauf verwaltet, welcher Windows-Benutzer am Betriebssystem angemeldet ist.

IBM Schlüsselauslagerungshierarchie

Ein wesentlicher Bestandteil der Architektur des integrierten IBM Sicherheits-Subsystems ist die IBM Schlüsselauslagerungshierarchie. Die Basis (oder ″Root″) der IBM Schlüsselauslagerungshierarchie sind der öffentliche und der private Hardwareschlüssel. Der öffentliche und der private Hardwareschlüssel, als *Hardwareschlüsselpaar* bezeichnet, werden von IBM Client Security erstellt und sind auf jedem Client statistisch eindeutig.

Die nächste “Ebene” der Schlüsselhierarchie (über der Basis- oder Rootebene) sind der öffentliche und der private Administratorschlüssel bzw. das *Administratorschlüsselpaar*. Das Administratorschlüsselpaar kann auf jeder Maschine eindeutig sein, oder es kann auf allen Clients oder auf einer Untergruppe von Clients dasselbe sein. Die Verwaltung dieses Schlüsselpaares hängt davon ab, wie Sie Ihr Netzwerk verwalten möchten. Der private Administratorschlüssel ist insofern eindeutig, als er auf dem Clientsystem (durch den öffentlichen Hardwareschlüssel geschützt) an einer vom Administrator definierten Adresse gespeichert ist.

IBM Client Security registriert Windows-Benutzer in der Umgebung des integrierten IBM Sicherheits-Subsystems. Wird ein Benutzer registriert, werden öffentliche und private Benutzerschlüssel (das *Benutzerschlüsselpaar*) erstellt und eine neue "Schlüsselebene" wird erstellt. Der private Benutzerschlüssel wird mit dem öffentlichen Administratorschlüssel verschlüsselt. Der private Administratorschlüssel wird mit dem öffentlichen Hardwareschlüssel verschlüsselt. Daher muss zum Verwenden des privaten Benutzerschlüssels der private Administratorschlüssel (der mit dem öffentlichen Hardwareschlüssel verschlüsselt ist) in das Sicherheits-Subsystem geladen werden. Ist er in den Chip geladen, entschlüsselt der private Hardwareschlüssel den privaten Administratorschlüssel. Der private Administratorschlüssel ist nun für die Verwendung im Sicherheits-Subsystem bereit, so dass Daten, die mit dem entsprechenden öffentlichen Administatorschlüssel verschlüsselt wurden, in das Sicherheits-Subsystem ausgelagert, entschlüsselt und verwendet werden können.

Der private (mit dem öffentlichen Administratorschlüssel verschlüsselte) Schlüssel des aktuellen Windows-Benutzers wird an das Sicherheits-Subsystem weitergeleitet. Alle von einer Anwendung benötigten Daten, die das integrierte Sicherheits-Subsystem einsetzt, werden ebenso an den Chip weitergeleitet, entschlüsselt und innerhalb der sicheren Umgebung des Sicherheits-Subsystems genutzt. Ein Beispiel hierfür ist ein privater Schlüssel, der zur Authentifizierung bei einem drahtlosen Netzwerk verwendet wird.

Wenn ein Schlüssel erforderlich ist, wird er in das Sicherheits-Subsystem ausgelagert. Die verschlüsselten privaten Schlüssel werden in das Sicherheits-Subsystem ausgelagert und können dann in der geschützten Umgebung des Chips verwendet werden. Die privaten Schlüssel werden niemals ungeschützt außerhalb dieser Hardwareumgebung verwendet. So kann eine beinahe unbegrenzte Datenmenge durch den integrierten IBM Security Chip geschützt werden.

Die privaten Schlüssel werden verschlüsselt, weil sie sehr gut geschützt werden müssen und im integrierten IBM Sicherheits-Subsystem der Speicherplatz begrenzt ist. Es können nur einige Schlüssel gleichzeitig im Sicherheits-Subsystem gespeichert werden. Der öffentliche und der private Hardwareschlüssel sind die einzigen Schlüssel, die bei jedem Booten im Sicherheits-Subsystem gespeichert bleiben. Damit mehrere Schlüssel und mehrere Benutzer zugelassen werden können, implementiert IBM Client Security die IBM Schlüsselauslagerungshierarchie. Wenn ein Schlüssel erforderlich ist, wird er in das integrierte IBM Sicherheits-Subsystem ausgelagert. Die zugehörigen verschlüsselten privaten Schlüssel werden in das Sicherheits-Subsystem ausgelagert und können dann in der geschützten Umgebung des Sicherheits-Subsystems verwendet werden. Die privaten Schlüssel werden niemals ungeschützt außerhalb dieser Hardwareumgebung verwendet.

Der private Administratorschlüssel wird mit dem öffentlichen Hardwareschlüssel verschlüsselt. Der private Hardwareschlüssel, der nur im Sicherheits-Subsystem verfügbar ist, wird zum Entschlüsseln des privaten Administratorschlüssels verwendet. Wenn der private Administratorschlüssel im Sicherheits-Subsystem entschlüsselt wird, kann ein privater Benutzerschlüssel (mit dem öffentlichen Administratorschlüssel verschlüsselt) in das Sicherheits-Subsystem weitergeleitet und mit dem privaten Administratorschlüssel entschlüsselt werden. Mit dem öffentlichen Administratorschlüssel können mehrere private Benutzerschlüssel verschlüsselt werden. Hierdurch kann eine fast unbegrenzte Anzahl an Benutzern auf einem System mit dem IBM ESS arbeiten; für eine optimale Leistung empfiehlt es sich jedoch, die Registrierung auf 25 Benutzer pro Computer zu beschränken.

IBM ESS verwendet eine Schlüsselauslagerungshierarchie, bei der der öffentliche und der private Hardwareschlüssel im Sicherheits-Subsystem zum Sichern weiterer Daten, die außerhalb des Chips gespeichert sind, verwendet werden können. Der private Hardwareschlüssel wird im Sicherheits-Subsystem generiert und verlässt nie diese sichere Umgebung. Der öffentliche Hardwareschlüssel ist außerhalb des Sicherheits-Subsystems verfügbar und wird zum Verschlüsseln oder Sichern weiterer Daten, wie z. B. eines privaten Schlüssels, verwendet. Wenn diese Daten mit dem öffentlichen Hardwareschlüssel verschlüsselt sind, können sie nur durch den privaten Hardwareschlüssel entschlüsselt werden. Da der private Hardwareschlüssel nur in der sicheren Umgebung des Sicherheits-Subsystems verfügbar ist, können die Daten nur in dieser sicheren Umgebung entschlüsselt und verwendet werden. Jeder Computer verfügt über einen eindeutigen öffentlichen und privaten Hardwareschlüssel. Die Zufallszahlfunktion des integrierten IBM Sicherheits-Subsystems stellt sicher, dass jedes Hardwareschlüsselpaar statistisch eindeutig ist.

PKI-Funktionen (Public Key Infrastructure)

Client Security stellt alle erforderlichen Komponenten für die Erstellung einer PKI von öffentlichen Schlüsseln in Ihrem Unternehmen bereit. Zu diesen Komponenten gehören u. a.:

- **Steuerung der Client-Sicherheitspolicy über Administratoren.** Die Authentifizierung auf Clientebene ist ein wichtiger Gesichtspunkt der Sicherheitspolicy. Client Security stellt die Schnittstelle zur Verfügung, die für die Verwaltung der Sicherheitspolicy eines IBM Clients erforderlich ist. Diese Schnittstelle ist Bestandteil der Authentifizierungssoftware von User Verification Manager (UVM), der Hauptkomponente von Client Security.
- **Chiffrierschlüsselverwaltung für die Verschlüsselung öffentlicher Schlüssel:** Die Administratoren erstellen mit Hilfe von Client Security Chiffrierschlüssel für die Computerhardware und die Clientbenutzer. Beim Erstellen von Chiffrierschlüsseln sind sie über eine Schlüsselhierarchie an den integrierten IBM Security Chip gebunden. Hierbei werden über einen Hardwareschlüssel der Basisebene die höherrangigen Schlüssel sowie die Benutzerschlüssel für die einzelnen Clientbenutzer verschlüsselt. Das Verschlüsseln und Speichern der Schlüssel auf dem integrierten IBM Security Chip stellt eine wichtige Zusatzebene der Client-Sicherheit dar, da die Schlüssel fest an die Computerhardware gebunden sind.
- **Erstellung und Speicherung digitaler Zertifikate mit Schutz durch den integrierten IBM Security Chip.** Wenn Sie ein digitales Zertifikat anfordern, das zum digitalen Signieren oder Verschlüsseln einer E-Mail verwendet werden kann, können Sie über Client Security das integrierte IBM Sicherheits-Subsystem als CSP für Anwendungen, die Microsoft CryptoAPI verwenden, auswählen. Zu diesen Anwendungen gehören auch Internet Explorer und Microsoft Outlook Express. Hierdurch wird gewährleistet, dass der private Schlüssel des digitalen Zertifikats mit dem öffentlichen Benutzerschlüssel auf dem integrierten IBM Sicherheits-Subsystem verschlüsselt ist. Benutzer von Netscape können das integrierte IBM Sicherheits-Subsystem als Funktion zur Erstellung privater Schlüssel für digitale Zertifikate auswählen, die für die Sicherheit verwendet werden. Anwendungen, die das PKCS #11-Modul (Public-Key Cryptography Standard) verwenden, wie z. B. Netscape Messenger, können den vom integrierten IBM Sicherheits-Subsystem bereitgestellten Schutz in Anspruch nehmen.
- **Die Möglichkeit, digitale Zertifikate zum integrierten IBM Sicherheits-Subsystem zu übertragen.** Das Tool zur Übertragung von Zertifikaten von IBM Client Security ermöglicht das Übertragen von Zertifikaten, die mit dem Standard-Microsoft-CSP erstellt wurden, zum CSP des integrierten IBM Sicherheits-Subsystems. Dadurch wird der Schutz, den die privaten Schlüssel in Verbindung mit

den Zertifikaten bieten, bedeutend erhöht, da diese nun sicher im integrierten IBM Sicherheits-Subsystem gespeichert werden, anstatt in anfälliger Software.

Anmerkung: Digitale Zertifikate, die durch den CSP des integrierten IBM Sicherheits-Subsystems geschützt wurden, können nicht in einen anderen CSP exportiert werden.

- **Funktion zur Schlüsselarchivierung und -wiederherstellung.** Eine wichtige PKI-Funktion ist das Erstellen eines Schlüsselarchivs, in dem die Schlüssel wiederhergestellt werden können, wenn die Originalschlüssel verloren gegangen sind oder beschädigt wurden. IBM Client Security stellt eine Schnittstelle zur Verfügung, über die Sie ein Archiv für Schlüssel und digitale Zertifikate, die mit dem integrierten IBM Sicherheits-Subsystems erstellt wurden, einrichten können. Außerdem können Sie darüber bei Bedarf die entsprechenden Schlüssel und Zertifikate wiederherstellen.
- **FFE (File and Folder Encryption, Verschlüsselung von Dateien und Ordnern).** Die Verschlüsselung von Dateien und Ordnern ermöglicht es Clientbenutzern, Dateien oder Ordner zu verschlüsseln oder zu entschlüsseln. So steht ein höheres Maß an Datensicherheit an erster Stelle der Maßnahmen zur Systemsicherheit von CSS.
- **Authentifizierung über Fingerabdrücke.** IBM Client Security unterstützt das Lesegerät für Fingerabdrücke von Targus als PC-Karte oder über USB für die Authentifizierung. Client Security 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 bestimmte 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 für das Netzwerk autorisierten Benutzer, jedes System im Netzwerk genau wie die eigene Workstation zu verwenden. Wenn ein Benutzer berechtigt ist, UVM auf irgendeinem bei Client Security registrierten Client zu verwenden, kann er seine persönlichen Daten in alle anderen registrierten Clients im Netzwerk für standortunabhängigen Zugriff mit Berechtigungsnachweis 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 bei jedem Hinzufügen eines Benutzers einen benutzerspezifischen Verschlüsselungstext und eine Policy für das Ablaufen des Verschlüsselungstexts fest.

Kapitel 2. Erste Schritte

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

Hardwarevoraussetzungen

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

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

Integriertes IBM Sicherheits-Subsystem

Das integrierte IBM Sicherheits-Subsystem (IBM Embedded Security Subsystem) ist ein verschlüsselter Mikroprozessor, der in der Systemplatine des IBM Clients integriert ist. Diese grundlegende Komponente von IBM Client Security wandelt die Funktionen der Sicherheitspolicy 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 das integrierte IBM Sicherheits-Subsystem enthalten, unterstützen auch IBM Client Security. Wenn Sie versuchen, die Software herunterzuladen und auf einem Computer zu installieren, der über kein integriertes IBM Sicherheits-Subsystem verfügt, 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/us/security/index.html.

Softwarevoraussetzungen

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

Betriebssysteme

Für die Ausführung von IBM 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 Sicherheitspolicy-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 IBM 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 IBM 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 IBM 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 Sicherheitspolicy für die Authentifizierung über Fingerabdrücke aktiviert werden kann.

- **Ensure-Proximity Badge**

  Bei IBM Client Security ab Version 5.2 müssen die Benutzer des berührungslosen Ausweises (Proximity Badge) ihre Ensure-Software auf Version 7.41 aktualisieren. Bei der Aktualisierung von einer früheren Version von IBM Client Security sollten Sie Ihre Ensure-Software aktualisieren, *bevor* Sie eine Aktualisierung auf Client Security ab Version 5.2 durchführen.

- **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 IBM Client Security bei der Anforderung digitaler Zertifikate unterstützt:

- Internet Explorer 5.0 oder höher
- Netscape 4.51-4.7x und Netscape 7.1

Informationen zum Browser-Verschlüsselungsgrad

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

Verschlüsselungsdienste

IBM 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 IBM Client Security die Verschlüsselungsvorgänge des integrierten IBM Sicherheits-Subsystems 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 das integrierte IBM Sicherheits-Subsystem installiert haben, können Sie mit dem integrierten IBM Sicherheits-Subsystem digitale Zertifikate für Netscape, Entrust, RSA und andere Anwendungen, die das PKCS #11-Modul verwenden, erstellen.

E-Mail-Anwendungen

IBM 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/us/security/index.html heruntergeladen werden.

Registrierungsformular

Wenn Sie die Software herunterladen, müssen Sie ein Registrierungsformular und einen Fragenkatalog ausfüllen und den Lizenzbedingungen zustimmen. Folgen Sie den Anweisungen auf der IBM Website http://www.pc.ibm.com/us/security/index.html, um die Software herunterzuladen.

Die Installationsdateien für IBM Client Security sind in der sich selbst entpackenden Datei mit dem Namen `csec53.exe` enthalten.

Kapitel 3. Vorbereitung der Software-Installation

Dieses Kapitel enthält alle Vorbereitungen zum Ausführen des Installationsprogramms und zum Konfigurieren von IBM Client Security auf IBM Clients.

Alle für die Installation von Client Security erforderlichen Dateien finden Sie auf der IBM Website http://www.pc.ibm.com/us/security/index.html. Auf der Website finden Sie Informationen, mit deren Hilfe Sie sicherstellen können, dass Sie über das integrierte IBM Sicherheits-Subsystem (IBM Embedded Security Subsystem) verfügen und die Ihnen die Auswahl des passenden IBM Client Security-Angebots für Ihr System ermöglichen.

Software-Installation einleiten

Das Installationsprogramm installiert IBM Client Security auf dem IBM Client und aktiviert das integrierte IBM Sicherheits-Subsystem. 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 IBM 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 IBM Client Security zuerst bestimmte Komponenten von Tivoli Access 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 integrierte IBM Sicherheits-Subsystem (IBM Embedded Security Subsystem) aktivieren und Chiffrierschlüssel erstellen, beeinflussen können. Diese Funktionen bestehen aus dem Administratorkennwort und den erweiterten Sicherheitseinrichtungen und können über das Programm "Configuration/Setup Utility" von einem IBM Computer aus verwendet werden. IBM Client Security verfügt über ein eigenes Administratorkennwort. Um Verwechslungen zu vermeiden, wird das Administratorkennwort, das im Programm "Configuration/Setup Utility" festgelegt wird, in den Handbüchern zu Client Security als das *BIOS-Administratorkennwort* bezeichnet.

BIOS-Administratorkennwort

BIOS-Administratorkennwörter verhindern, dass nicht autorisierte Personen die Konfigurationseinstellungen eines IBM Computers ändern. Diese Kennwörter werden über das Programm "Configuration/Setup Utility" auf einem NetVista- oder ThinkCentre-Computer oder das Programm "IBM BIOS Setup Utility" auf einem ThinkPad festgelegt. Sie können das jeweilige Programm aufrufen, indem Sie beim Computerstart die Taste F1 drücken. Dieses Kennwort wird in den Programmen "Configuration/Setup Utility" und "IBM BIOS Setup Utility" als Administratorkennwort (Administrator Password) bezeichnet.

Erweiterte Sicherheitseinrichtungen

Die erweiterten Sicherheitseinrichtungen bieten einen zusätzlichen Schutz für das BIOS-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 Computerstarts 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 das integrierte IBM Sicherheits-Subsystem im Administratordienstprogramm aktivieren und die Chiffrierschlüssel erstellen.

Wenn auf diesen Modellen die erweiterten Sicherheitseinrichtungen aktiviert wurden, müssen Sie nach der Installation von Client Security im Administratordienstprogramm das integrierte IBM Sicherheits-Subsystem aktivieren und die Chiffrierschlüssel erstellen, *nachdem* Sie IBM Client Security installiert haben. 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 das integrierte IBM Sicherheits-Subsystem zu aktivieren und die Chiffrierschlüssel 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 das integrierte IBM Sicherheits-Subsystem über das Programm "Configuration/Setup Utility" aktivieren. *Nachdem* Sie das integrierte IBM Sicherheits-Subsystem aktiviert haben, können Sie im Administratordienstprogramm die Chiffrierschlüssel 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 IBM 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 IBM 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 Modellnummer, und befolgen Sie die auf der Webseite angezeigten Anweisungen.

Administratorschlüsselpaar zur Schlüsselarchivierung verwenden

Das Archivschlüsselpaar ist eine Kopie des Administratorschlüsselpaars, das Sie zur Wiederherstellung auf einem fernen System speichern. Da das Administratordienstprogramm zur Erstellung des Archivschlüsselpaars verwendet wird, müssen Sie IBM Client Security auf einem ersten IBM Client installieren, bevor Sie das Administratorschlüsselpaar erstellen können.

Kapitel 4. Software installieren, aktualisieren und deinstallieren

Dieses Kapitel enthält Anweisungen zum Herunterladen, Installieren und Konfigurieren von IBM 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 IBM Client Security aufrüsten, die älter als Version 5.0 ist, *müssen* Sie alle verschlüsselten Dateien entschlüsseln, *bevor* Sie Client Security ab Version 5.1 installieren. IBM Client Security ab Version 5.1 kann aufgrund von Änderungen bei der Dateiverschlüsselungsimplementierung keine Dateien entschlüsseln, die mit älteren Versionen von IBM Client Security als Version 5.0 verschlüsselt wurden.

Software herunterladen und installieren

Alle für die Installation von Client Security erforderlichen Dateien finden Sie auf der IBM Website http://www.pc.ibm.com/us/security/index.html. Auf der Website finden Sie Informationen, mit deren Hilfe Sie sicherstellen können, dass Sie über das integrierte IBM Sicherheits-Subsystem verfügen und die Ihnen die Auswahl des passenden IBM Client Security-Angebots für Ihr System ermöglichen.

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

1. Rufen Sie in einem Webbrowser folgende IBM Website auf: http://www.pc.ibm.com/us/security/index.html.
2. Klicken Sie auf **Download instructions and links**.
3. Klicken Sie im Bereich mit den Download-Informationen zu IBM Client Security auf die Schaltfläche **Continue**.
4. Klicken Sie auf **Detect my system & continue**, oder geben Sie die siebenstellige Maschinentyp-/Modellnummer in das vorgesehene Feld ein.
5. 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 IBM Client Security geführt.
6. Befolgen Sie die angezeigten Anweisungen, um die erforderlichen Einheitentreiber, Readme-Dateien, Software, Referenzdokumente und zusätzliche Dienstprogramme von IBM Client Security herunterzuladen. Gehen Sie nach der auf der Website angegebenen Download-Reihenfolge vor.
7. Klicken Sie auf dem Windows-Desktop auf **Start > Ausführen**.
8. Geben Sie in das Feld "Ausführen" `d:\directory\csec53.exe` ein. Hierbei gibt d:\directory\ den Laufwerkbuchstaben und das Verzeichnis an, in dem die Datei gespeichert ist.
9. Klicken Sie auf **OK**.

   Das Begrüßungsfenster des InstallShield-Assistenten von IBM Client Security wird angezeigt.
10. 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.

11. 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 Sicherheitspolicy auf einem IBM Client.

Dies umfasst folgende Schritte:

- **Kennwort des Sicherheitsadministrators definieren**

  Das Sicherheitsadministratorkennwort, das in diesen Handbüchern als Administratorkennwort bezeichnet wird, wird zur Steuerung des Zugriffs auf das Administratordienstprogramm von IBM Client Security verwendet, das zur Änderung der Sicherheitseinstellungen für diesen Computer dient. Dieses Kennwort muss genau 8 Zeichen umfassen.

- **Sicherheitsschlüssel für Administratoren erstellen**

  Bei Sicherheitsschlüsseln für Administratoren handelt es sich um eine Gruppe digitaler Schlüssel, die in einer Computerdatei gespeichert sind. Diese Schlüsseldateien werden auch als Administratorschlüssel, Administratorschlüsselpaar oder als Archivschlüsselpaar bezeichnet. Es empfiehlt sich, diese wichtigen Sicherheitsschlüssel auf einem austauschbaren Datenträger oder Laufwerk zu speichern. Wenn im Administratordienstprogramm eine Änderung an der Sicherheitspolicy vorgenommen wird, erfolgt eine Systemanfrage nach einem Administratorschlüssel als Nachweis dafür, dass die Berechtigung zur Änderung der Sicherheitspolicy vorliegt.

  Eine Backup-Version der Sicherheitsdaten wird auch für den Fall gespeichert, dass die Systemplatine oder ein Festplattenlaufwerk des Computers ausgetauscht werden muss. Speichern Sie diese Sicherheitsdaten außerhalb des lokalen Systems.

- **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 Sicherheitspolicy einrichten. Sie können zu einem späteren Zeitpunkt im Administratordienstprogramm von IBM Client Security eine angepasste Sicherheitspolicy 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 auf den Computer 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 oder Smartcards, 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 **Weiter**.

Das Fenster für das Ablaufen des UVM-Verschlüsselungstexts wird angezeigt.

d. Legen Sie die Regel für den Ablauf des Verschlüsselungstextes für den Benutzer fest, und klicken Sie auf **Fertig stellen**.

e. 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**.

Die Nachricht mit dem Inhalt "Sind Sie sicher, dass Sie die Autorisierung aufheben möchten?" wird angezeigt.

c. Klicken Sie auf **Ja**.

d. Klicken Sie auf **Weiter**.

Das Fenster "Sicherheitsstufe des Systems auswählen" wird angezeigt.

9. Wählen Sie eine Systemsicherheitsstufe aus, indem Sie eine der folgenden Aktionen ausführen:
   - Wählen Sie die gewünschten Authentifizierungsbestimmungen aus, indem Sie auf die entsprechenden Markierungsfelder klicken. Sie können mehrere Anforderungen für die Authentifizierung auswählen. Das Markierungsfeld **UVM-Verschlüsselungstext verwenden** ist standardmäßig ausgewählt.
   - Die Einheitentreiber für das Lesegerät für Fingerabdrücke und für die Smartcard müssen installiert werden, bevor der Installationsassistent für IBM Client Security gestartet wird, damit diese Einheiten für den Installationsassistenten verfügbar sind.
   - 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 eine angepasste Sicherheitsrichtlinie definieren, indem Sie den Policy-Editor des Administratordienstprogramms verwenden.
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 Sicherheits-Subsystem aktivieren

Zur Verwendung von IBM Client Security muss das IBM Sicherheits-Subsystem 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 das IBM Sicherheits-Subsystem mit dem Administratordienstprogramm zu aktivieren:

1. Klicken Sie auf **Start > Einstellungen > Systemsteuerung > Integriertes IBM Sicherheits-Subsystem**.

   Es erscheint eine Anzeige mit der Mitteilung, dass das IBM Sicherheits-Subsystem nicht aktiviert ist, und der Frage, ob es jetzt aktiviert werden soll.
2. Klicken Sie auf **Ja**.

   Es wird eine Nachricht angezeigt, die darauf hinweist, dass vor dem Fortfahren das Administratorkennwort oder ein BIOS-Administratorkennwort über das Programm "IBM BIOS Setup Utility" inaktiviert werden muss, falls ein entsprechendes 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 > Integriertes IBM Sicherheits-Subsystem**.

   Es wird eine Nachricht angezeigt, die darauf hinweist, dass das IBM Sicherheits-Subsystem 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 Administratorkennwort 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 13. Bei nicht überwachten Installationen 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.

Massenimplementierung

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

Für die Durchführung einer Massenimplementierung müssen folgende Einheitentreiber installiert sein:

- SM-Buseinheitentreiber
- Atmel-TPM-Einheitentreiber (für TCPA-Systeme)

Eine Massenimplementierung umfasst im Wesentlichen zwei Schritte:

- Masseninstallation
- Massenkonfiguration

Masseninstallation

Zur gleichzeitigen Installation von IBM Client Security auf mehreren 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 `csec.ini`.

   Die Datei `csec.ini` wird erstellt, nachdem der Benutzer den Installationsassistenten von IBM Client Security abgeschlossen hat. Dieser Schritt ist nur erforderlich, wenn Sie beabsichtigen, eine Massenkonfiguration durchzuführen. Im Abschnitt „Massenkonfiguration" auf Seite 25 finden Sie weitere Informationen.
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. Die Verzeichnisposition wird vom Parameter `szIniPath` der Datei `csec.ini` festgelegt. 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.

Der vollständige Inhalt der Datei `Setup.iss`, die in dem durch die obigen Schritte extrahierten CSS-Installationspaket enthalten ist, ist unten mit einigen Beschreibungen aufgeführt:

```
[InstallShield Silent]
Version=v6.00.000
File=Response File
szIniPath=d:\csssetup.ini
(Beim obigen Parameter handelt es sich um den Namen und die Position der .ini-Datei, die für die Massenkonfiguration erforderlich ist. 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
(Beim obigen Parameter handelt es sich um das Verzeichnis zum Installieren von Client Security.) 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
(Beim obigen Parameter handelt es sich um die Programmgruppe für Client Security.)
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	(BIOS-)Administratorkennwort. Keine Angabe, falls nicht erforderlich.
hwpw=11111111	Administratorkennwort für das integrierte IBM Sicherheits-Subsystem. Muss 8 Zeichen lang sein. Angabe immer erforderlich. Richtige Angabe erforderlich, falls Administratorkennwort bereits definiert wurde.
newkp=1	1: Generieren eines neuen Administratorschlüsselpaars, 0: Verwenden eines vorhandenen Administratorschlüsselpaars.
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	Position des Benutzerschlüsselarchivs. Handelt es sich hierbei um ein Netzlaufwerk, muss das Laufwerk verbunden sein.
pub=c:\jk\admin.key	Position des öffentlichen Administratorschlüssels, wenn ein vorhandenes Administratorschlüsselpaar verwendet wird. Handelt es sich hierbei um ein Netzlaufwerk, muss das Laufwerk verbunden sein.
pri=c:\jk\private1.key	Position des privaten Administratorschlüssels, wenn ein vorhandenes Administratorschlüsselpaar verwendet wird. Handelt es sich hierbei um ein Netzlaufwerk, muss das Laufwerk verbunden sein.
wiz=0	Gibt an, ob diese Datei vom Installationsassistent von CSS generiert wurde. Dieser Eintrag ist nicht erforderlich. Wenn Sie ihn in die Datei aufnehmen, sollte der Wert 0 sein.
clean=0	1: .ini-Datei nach Initialisierung löschen, 0: .ini-Datei nach Initialisierung nicht löschen.
enableroaming=1	1 zur Aktivierung von standortunabhängigem Zugriff für den Client, 0 zur Inaktivierung von standortunabhängigem Zugriff für den Client.

username= [promptcurrent]	[promptcurrent]: der derzeitige Benutzer wird zur Eingabe des Registrierungskennworts für den Client mit standortunabhängigem Zugriff aufgefordert. [current]: wenn das Registrierungskennworts für den Client mit standortunabhängigem Zugriff für den derzeitigen Benutzer durch den Eintrag `sysregpwd` geliefert wird und der derzeitige Benutzer zum Registrieren des Systems über den Server für den standortunabhängigen Zugriff berechtigt ist. [<Entsprechender Benutzeraccount>]: wenn der designierte Benutzer zum Registrieren des Systems über den Server für den standortunabhängigen Zugriff berechtigt ist und wenn das Systemregistrierungskennwort für diesen Benutzer durch den Eintrag `sysregpwd` geliefert wird. Verwenden Sie diesen Eintrag nicht, wenn der Wert für `enableroaming` 0 ist oder wenn der Eintrag nicht vorhanden ist.
sysregpwd=12345678	Systemregistrierungskennwort. Definieren Sie für diesen Wert das richtige Kennwort, um das System für die Registrierung über den Server für den standortunabhängigen Zugriff zu aktivieren. Nehmen Sie diesen Eintrag nicht auf, wenn der Wert für `username` als [promptcurrent] definiert ist oder wenn der Eintrag für den Benutzernamen nicht vorhanden ist.
[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.
defaultppchange=0	Wenn `enrollall` = 1, gilt die Policy für das Ändern des UVM-Verschlüsselungstexts für alle Benutzer. 1: anfordern, dass der Benutzer den UVM-Verschlüsselungstext bei der nächsten Anmeldung ändert, 0: nicht anfordern, dass der Benutzer den UVM-Verschlüsselungstext bei der nächsten Anmeldung ändert.
defaultppexppolicy=1	Wenn `enrollall` = 1, gilt die Policy für das Ablaufen des UVM-Verschlüsselungstexts für alle Benutzer. 0: Der UVM-Verschlüsselungstext läuft ab. 1: Der UVM-Verschlüsselungstext läuft nicht ab.
defaultppexpdays=0	Wenn `enrollall` = 1, wird die Anzahl von Tagen bis zum Ablaufen des UVM-Verschlüsselungstextes für alle Benutzer festgelegt. Wenn `ppexppolicy` = 0, definieren Sie diesen Wert, um die Anzahl von Tagen bis zum Ablaufen des UVM-Verschlüsselungstextes festzulegen.
enrollusers=2	Wenn `enrollall` = 0, wird hiermit die Anzahl der Benutzer angegeben, die in UVM registriert werden.

user1=jknox	Anzahl der zu registrierenden Benutzer mit 1 beginnend aufzählen. Die Benutzernamen müssen die Accountnamen sein. Gehen Sie wie folgt vor, um den Accountnamen unter Windows 2000 abzurufen: 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. Um den Accountnamen unter Windows XP von der Windows-Systemsteuerung aus aufzurufen, klicken Sie auf das Symbol für die Benutzeraccounts. Die Benutzeraccounts werden angezeigt.
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-Kennwort 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.
user1ppchange=0	1: anfordern, dass der Benutzer den UVM-Verschlüsselungstext bei der nächsten Anmeldung ändert, 0: nicht anfordern, dass der Benutzer den UVM-Verschlüsselungstext bei der nächsten Anmeldung ändert.
user1ppexppolicy=1	0: anzeigen, dass der UVM-Verschlüsselungstext abläuft, 1: anzeigen, dass der UVM-Verschlüsselungstext nicht abläuft.
user1ppexpdays=0	Wenn ppexppolicy = 0, definieren Sie diesen Wert, um die Anzahl von Tagen bis zum Ablaufen des UVM-Verschlüsselungstextes anzugeben.
user2=russell user2uvmpw=left user2winpw=right user2domain=0 user2ppchange=1 user2ppexppolicy=0 user2ppexpdays=90	
[UVMAppConfig]	Abschnittsüberschrift für Installation von UVM-sensitiven Anwendungen und Modulen.
uvmlogon=0	1: Verwendung von UVM-Anmeldeschutz, 0: Verwendung der Windows-Anmeldung.
entrust=0	1: Verwendung von UVM für Entrust-Authentifizierung, 0: Verwendung der Entrust-Authentifizierung.
notes=1	1: Aktivierung von Lotus Notes-Unterstützung. 0: Inaktivierung von Lotus Notes-Unterstützung.
netscape=0	1: Signieren und Verschlüsseln von E-Mails mit dem IBM PKCS#11-Modul, 0: kein Signieren und Verschlüsseln von E-Mails mit dem IBM PKCS#11-Modul.
passman=0	1: Verwendung von Password Manager, 0: keine Verwendung von Password Manager
folderprotect=0	1: Verwendung der Verschlüsselung von Dateien und Ordnern, 0: keine Verwendung der Verschlüsselung von Dateien und Ordnern.

Softwareversion von Client Security aktualisieren

Bei Clients, auf denen frühere Versionen von Client Security installiert sind, sollten Sie die Software auf diese Version aktualisieren, um die neuen Client Security-Funktionen nutzen zu können.

Wichtig: Bei TCPA-Systemen, auf denen IBM Client Security Version 4.0x installiert war, muss Version 4.0x der Software deinstalliert und der Chip gelöscht werden, um diese Version von IBM Client Security zu installieren. 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 Programm "IBM BIOS Setup Utility".
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 von Version 5.1 auf aktuellere Versionen mit vorhandenen Sicherheitsdaten durchführen

Gehen Sie wie folgt vor, um ein Upgrade von Client Security Version 5.1 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 **Schlüsselarchiv 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. Klicken Sie auf dem Windows-Desktop auf **Start > Ausführen**.
   b. Geben Sie in das Feld "Ausführen" `d:\directory\csec5xxus_00yy.exe` ein. Hierbei gibt d:\directory\ den Laufwerkbuchstaben und das Verzeichnis an, in dem die ausführbare Datei gespeichert ist. `xx` und `yy` bestehen aus alphanumerischen Zeichen.
   c. Wählen Sie die Option **Sicherheit** aus.
   d. Führen Sie einen Neustart des Systems durch.

Client Security deinstallieren

Stellen Sie sicher, dass die verschiedenen Dienstprogramme (IBM Client Security Password Manager, Dienstprogramm zur Verschlüsselung von Dateien und Ordnern von IBM Client Security, FFE), die die Funktionalität von Client Security verbessern, deinstalliert wurden, bevor Sie IBM Client Security deinstallieren. 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. Das Administratorkennwort ist zum Deinstallieren von Client Security erforderlich.

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 auf **Weiter**, um die Software zu deinstallieren.
8. Klicken Sie auf **OK**, um diese Aktion zu bestätigen.
9. Geben Sie das Administratorkennwort in die vorgesehene Schnittstelle ein, und klicken Sie auf **OK**.
10. 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.

    Die Nachricht mit dem Inhalt "Sollen die Daten zu diesem System aus dem Archiv gelöscht werden?" wird angezeigt. Wenn Sie **Nein** auswählen, können Sie diese Daten wiederherstellen, wenn Sie die aktuellere Version von IBM Client Security installieren.

11. Klicken Sie nach dem Entfernen der Software auf **Fertig stellen**.
    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.

Kapitel 5. Fehlerbehebung

Dieses Kapitel enthält nützliche Informationen zum Verhindern oder Erkennen und Beheben möglicher Fehler bei der Verwendung von Client Security.

Administratorfunktionen

Dieser Abschnitt enthält Informationen, die sich für den Administrator beim Einrichten und Verwenden von Client Security als hilfreich erweisen können.

IBM Client Security kann nur für IBM Computer verwendet werden, auf denen das integrierte IBM Sicherheits-Subsystem (IBM Embedded Security Subsystem) installiert ist. Diese Software besteht aus Anwendungen und Komponenten, die IBM Clients die Sicherung ihrer schutzwürdigen Daten über gesicherte Hardware anstelle von ungesicherter Software ermöglichen.

Benutzer autorisieren

Bevor Sie die Clientbenutzerinformationen schützen können, **muss** IBM Client Security auf dem Client installiert werden und die Benutzer **müssen** für diese Software berechtigt werden. Ein benutzerfreundlicher Installationsassistent führt Sie durch den gesamten Installationsprozess.

Wichtig: Mindestens ein Clientbenutzer **muss** während der Installation für die Verwendung von UVM berechtigt sein. Ist bei der Erstinstallation von Client Security kein Benutzer für die Verwendung von UVM berechtigt, werden die Sicherheitseinstellungen **nicht** übernommen, und Ihre Daten werden **nicht** geschützt.

Wenn Sie den Installationsassistenten abgeschlossen haben, ohne Benutzer zu berechtigen, führen Sie einen Neustart Ihres Computers durch; führen Sie dann den Installationsassistenten von Client Security vom Windows-Startmenü aus, und berechtigen Sie einen Windows-Benutzer für die Verwendung von UVM. Hierdurch übernimmt IBM Client Security Ihre Sicherheitseinstellungen und schützt Ihre schutzwürdigen Daten.

Benutzer löschen

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

BIOS-Administratorkennwort festlegen (ThinkCentre)

Mit den im Programm "Configuration/Setup Utility" verfügbaren Sicherheitseinstellungen können die Administratoren folgende Vorgänge durchführen:

- Integriertes IBM Sicherheits-Subsystem aktivieren oder inaktivieren
- Inhalt des integrierten IBM Sicherheits-Subsystems löschen

Achtung:

- Wenn der Inhalt des integrierten IBMcherheits-Subsystems gelöscht wird, gehen alle auf dem Sicherheits-Subsystem gespeicherten Chiffrierschlüssel und Zertifikate verloren.

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 BIOS-Administratorkennwort festzulegen:

1. Schalten Sie den Computer aus, und starten Sie ihn erneut.
2. Wenn die Eingabeaufforderung für das Programm "Configuration/Setup Utility" am Bildschirm angezeigt wird, drücken Sie **F1**.

   Das Hauptmenü des Programms "Configuration/Setup Utility" wird geöffnet.
3. Wählen Sie **System Security** aus.
4. Wählen Sie **Administrator Password** aus.
5. Geben Sie Ihr Kennwort ein, und drücken Sie den Abwärtspfeil auf der Tastatur.
6. Geben Sie Ihr Kennwort erneut ein, und drücken Sie den Abwärtspfeil.
7. Wählen Sie **Change Administrator password** aus, und drücken Sie die Eingabetaste. Drücken Sie anschließend erneut die Eingabetaste.
8. Drücken Sie **Esc**, um die Einstellungen zu speichern und das Menü zu verlassen.

Wenn Sie ein BIOS-Administratorkennwort festgelegt haben, wird bei jedem Zugriff auf das Programm "Configuration/Setup Utility" eine Eingabeaufforderung angezeigt.

Wichtig: Notieren Sie sich das BIOS-Administratorkennwort, und bewahren Sie es an einem sicheren Platz auf. Wenn Sie das BIOS-Administratorkennwort verlieren oder vergessen, können Sie auf das Programm "Configuration/Setup Utility" nicht mehr zugreifen und das Kennwort nicht mehr ändern oder löschen, ohne die Abdeckung des Computers zu entfernen und eine Brücke auf die Systemplatine zu versetzen. Weitere Informationen hierzu finden Sie in der Hardwaredokumentation zu Ihrem Computer.

Administratorkennwort festlegen (ThinkPad)

Mit den im Programm "IBM BIOS Setup Utility" verfügbaren Sicherheitseinstellungen können die Administratoren folgende Tasks durchführen:

- Integriertes IBM Sicherheits-Subsystem aktivieren oder inaktivieren
- Inhalt des integrierten IBM Sicherheits-Subsystems löschen

Achtung:

- Auf einigen ThinkPad-Modellen müssen Sie das Administratorkennwort vorübergehend inaktivieren, bevor Sie Client Security installieren oder aktualisieren können.

Wenn Sie Client Security konfiguriert haben, legen Sie ein Administratorkennwort fest, um zu verhindern, dass diese Einstellungen durch nicht autorisierte Benutzer geändert werden.

Gehen Sie nach einer der beiden folgenden Prozeduren vor, um ein Administratorkennwort festzulegen:

Beispiel 1

1. Schalten Sie den Computer aus, und starten Sie ihn erneut.

2. Wenn die Eingabeaufforderung für das Konfigurationsdienstprogramm am Bildschirm angezeigt wird, drücken Sie die Taste F1.

   Das Hauptmenü des Konfigurationsdienstprogramms wird geöffnet.
3. Wählen Sie **Password** aus.
4. Wählen Sie **Supervisor Password** aus.
5. Geben Sie Ihr Kennwort ein, und drücken Sie die Eingabetaste.
6. Geben Sie Ihr Kennwort erneut ein, und drücken Sie die Eingabetaste.
7. Klicken Sie auf **Continue**.
8. Drücken Sie die Taste F10, um die Eingaben zu speichern und das Menü zu verlassen.

Beispiel 2

1. Schalten Sie den Computer aus, und starten Sie ihn erneut.
2. Wenn die Nachricht ″To interrupt normal startup, press the blue Access IBM button″ angezeigt wird, drücken Sie die blaue Taste ″Access IBM″.

   Access IBM Predesktop Area wird geöffnet.
3. Klicken Sie doppelt auf **Start setup utility**.
4. Navigieren Sie mit Hilfe der Cursortasten im Menü, und wählen Sie die Option **Security** aus.
5. Wählen Sie **Password** aus.
6. Wählen Sie **Supervisor Password** aus.
7. Geben Sie Ihr Kennwort ein, und drücken Sie die Eingabetaste.
8. Geben Sie Ihr Kennwort erneut ein, und drücken Sie die Eingabetaste.
9. Klicken Sie auf **Continue**.
10. Drücken Sie die Taste F10, um die Eingaben zu speichern und das Menü zu verlassen.

Wenn Sie ein Administratorkennwort festgelegt haben, wird bei jedem Zugriff auf das Programm ″IBM BIOS Setup Utility″ eine Eingabeaufforderung angezeigt.

Wichtig: Notieren Sie sich das Administratorkennwort, und bewahren Sie es an einem sicheren Platz auf. Wenn Sie das Administratorkennwort verlieren oder vergessen, können Sie auf das Programm ″IBM BIOS Setup Utility″ nicht mehr zugreifen und das Kennwort nicht mehr ändern oder löschen. Weitere Informationen hierzu finden Sie in der Hardwaredokumentation zu Ihrem Computer.

Administratorkennwort schützen

Das Administratorkennwort schützt den Zugriff auf das Administratordienstprogramm. Bewahren Sie das Administratorkennwort an einem sicheren Ort auf, um zu verhindern, dass die Einstellungen im Administratordienstprogramm durch nicht autorisierte Benutzer geändert werden.

Inhalt des integrierten IBM Sicherheits-Subsystems löschen (ThinkCentre)

Wenn Sie alle Chiffrierschlüssel für Benutzer aus dem integrierten IBM Sicherheits-Subsystem entfernen und das Administratorkennwort für das Sicherheits-Subsystem löschen möchten, müssen Sie den Inhalt des Chips löschen. Lesen Sie die folgenden Hinweise, bevor Sie den Inhalt des integrierten IBM Sicherheits-Subsystems löschen.

Achtung:

- Wenn der Inhalt des integrierten IBMcherheits-Subsystems gelöscht wird, gehen alle auf dem Sicherheits-Subsystem gespeicherten Chiffrierschlüssel und Zertifikate verloren.

Gehen Sie wie folgt vor, um den Inhalt des integrierten IBM Sicherheits-Subsystems zu löschen:

1. Schalten Sie den Computer aus, und starten Sie ihn erneut.
2. Wenn die Eingabeaufforderung für das Konfigurationsdienstprogramm am Bildschirm angezeigt wird, drücken Sie die Taste F1.

   Das Hauptmenü des Konfigurationsdienstprogramms wird geöffnet.
3. Wählen Sie **Security** aus.
4. Wählen Sie **IBM TCPA Feature Setup** aus.
5. Wählen Sie **Clear IBM TCPA Security Feature** aus, und drücken Sie die Eingabetaste.
6. Klicken Sie auf **Yes**.
7. Drücken Sie die Taste F10, und wählen Sie **Yes** aus.
8. Drücken Sie die Eingabetaste. Der Computer wird erneut gestartet.

Inhalt des integrierten IBM Sicherheits-Subsystems löschen (ThinkPad)

Wenn Sie alle Chiffrierschlüssel für Benutzer aus dem integrierten IBM Sicherheits-Subsystem entfernen und das Administratorkennwort löschen möchten, müssen Sie den Inhalt des Sicherheits-Subsystems löschen. Lesen Sie die folgenden Hinweise, bevor Sie den Inhalt des integrierten IBM Sicherheits-Subsystems löschen.

Achtung:

- Wenn der Inhalt des integrierten IBMcherheits-Subsystems gelöscht wird, gehen alle auf dem Sicherheits-Subsystem gespeicherten Chiffrierschlüssel und Zertifikate verloren.

Gehen Sie wie folgt vor, um den Inhalt des integrierten IBM Sicherheits-Subsystems zu löschen:

1. Fahren Sie den Computer herunter.
2. Halten Sie die Taste Fn beim Starten des Computers gedrückt.
3. Wenn die Eingabeaufforderung für das Konfigurationsdienstprogramm am Bildschirm angezeigt wird, drücken Sie die Taste F1.

   Das Hauptmenü des Konfigurationsdienstprogramms wird geöffnet.
4. Wählen Sie **Config** aus.
5. Wählen Sie **IBM Security Chip** aus.
6. Wählen Sie **Clear IBM Security Chip** aus.
7. Klicken Sie auf **Yes**.
8. Drücken Sie die Eingabetaste, um fortzufahren.
9. Drücken Sie die Taste F10, um die Eingaben zu speichern und das Menü zu verlassen.

Bekannte Probleme und Einschränkungen bei CSS Version 5.2

Die folgenden Informationen sind möglicherweise bei der Verwendung der Funktionen von Client Security Software Version 5.2 hilfreich.

Einschränkungen bei standortunabhängigem Zugriff

CSS-Roaming-Server verwenden

Die Aufforderung zur Eingabe des CSS-Administratorkennworts wird angezeigt, wenn ein Benutzer sich beim CSS-Roaming-Server anmelden möchte. Der Computer kann jedoch wie gewohnt ohne Eingabe dieses Kennworts verwendet werden.

IBM Security Password Manager in einer Umgebung mit standortunabhängigem Zugriff verwenden

Kennwörter, die mit IBM Client Security Password Manager auf einem System gespeichert wurden, können auch auf anderen Systemen innerhalb der Umgebung mit standortunabhängigem Zugriff verwendet werden. Neue Einträge werden automatisch aus dem Archiv abgerufen, wenn sich der Benutzer an einem anderen System innerhalb des Netzwerks mit standortunabhängigem Zugriff anmeldet (wenn das Archiv verfügbar ist). Wenn also ein Benutzer bereits bei einem System angemeldet ist, muss er sich abmelden und erneut anmelden, damit die neuen Einträge im Netzwerk mit standortunabhängigem Zugriff verfügbar sind.

Internet Explorer-Zertifikat und Verzögerung der Aktualisierung bei standortunabhängigem Zugriff

Internet Explorer-Zertifikate werden im Archiv alle 20 Sekunden aktualisiert. Wird ein neues Internet Explorer-Zertifikat von einem Benutzer mit standortunabhängigem Zugriff generiert, dauert es mindestens 20 Sekunden, bis der Benutzer seine CSS-Konfiguration auf einem anderen System importieren, wiederherstellen oder ändern kann. Bei dem Versuch, eine dieser Aktionen vor dem Ende des Aktualisierungsintervalls von 20 Sekunden durchzuführen, geht das Zertifikat verloren. Auch wenn der Benutzer keine Verbindung zum Archiv hatte, während das Zertifikat erstellt wurde, sollte er 20 Sekunden warten, nachdem die Verbindung zum Archiv hergestellt wurde, um sicherzustellen, dass das Zertifikat im Archiv aktualisiert wurde.

Lotus Notes-Kennwort und standortunabhängiger Zugriff mit Berechtigungsnachweis

Wenn die Lotus Notes-Unterstützung aktiviert ist, wird das Lotus Notes-Kennwort des Benutzers durch UVM gespeichert. Die Benutzer brauchen ihr Notes-Kennwort künftig nicht mehr einzugeben, um sich bei Lotus Notes anzumelden. Sie werden nach ihrem UVM-Verschlüsselungstext, dem Fingerabdruck, der Smartcard usw. (je nach Einstellungen der Sicherheitsstrategie) gefragt, um auf Lotus Notes zugreifen zu können.

Wenn ein Benutzer sein Notes-Kennwort von Lotus Notes aus ändert, wird die Lotus Notes-ID-Datei mit dem neuen Kennwort aktualisiert und die UVM-Kopie des neuen Notes-Kennworts wird ebenfalls aktualisiert. In einer Umgebung mit standortunabhängigem Zugriff sind die UVM-Berechtigungsnachweise des Benutzers auch in anderen Systemen des Netzwerks mit standortunabhängigem Zugriff verfügbar, auf die der Benutzer zugreifen kann. Es ist möglich, dass die Kopie des Notes-Kennworts von UVM nicht mit dem Notes-Kennwort in der ID-Datei auf anderen Systemen im Netzwerk mit standortunabhängigem Zugriff übereinstimmt, wenn die Notes-ID-Datei mit dem aktualisierten Kennwort nicht ebenfalls auf einem anderen System verfügbar ist. Wenn dies der Fall ist, kann der Benutzer nicht auf Lotus Notes zugreifen.

Wenn die Notes-ID-Datei mit dem aktualisierten Kennwort eines Benutzers nicht auch in einem anderen System verfügbar ist, sollte die aktualisierte Notes-ID-Datei in die anderen Systeme innerhalb des Netzwerks mit standortunabhängigem Zugriff kopiert werden, so dass das Kennwort in der ID-Datei mit der durch UVM gespeicherten Kopie übereinstimmt. Alternativ können die Benutzer im Startmenü auch die Anwendung 'Sicherheitseinstellungen ändern' ausführen und das Notes-Kennwort in den alten Wert ändern. Das Notes-Kennwort kann dann über Lotus Notes wieder aktualisiert werden.

Verfügbarkeit von Berechtigungsnachweisen bei der Anmeldung in einer Umgebung mit standortunabhängigem Zugriff

Befindet sich ein Archiv in einem gemeinsam benutzten Netzwerk, wird die aktuellste Gruppe von Benutzerberechtigungen aus dem Archiv heruntergeladen, sobald der Benutzer auf das Archiv zugreifen kann. Bei der Anmeldung haben die Benutzer nicht sofort Zugriff auf das gemeinsam benutzte Netzwerk, so dass die aktuellsten Berechtigungsnachweise erst heruntergeladen werden können, nachdem die Anmeldung am System abgeschlossen ist. Wenn z. B. der UVM-Verschlüsselungstext auf einem anderen System im Netzwerk mit standortunabhängigem Zugriff geändert wurde oder wenn neue Fingerabdrücke in einem anderen System registriert wurden, sind diese Aktualisierungen erst verfügbar, wenn der Anmeldeprozess beendet ist. Sind die aktualisierten Benutzerberechtigungen nicht verfügbar, sollten die Benutzer versuchen, sich mit dem früheren Verschlüsselungstext oder mit anderen registrierten Fingerabdrücken am System anzumelden. Sobald die Anmeldung beendet ist, sind die aktualisierten Benutzerberechtigungen verfügbar, und das neue Kennwort sowie der Fingerabdruck sind bei UVM registriert.

Einschränkungen bei berührungslosem Ausweis (Proximity Badge)

Sicheren UVM-Anmeldeschutz mit berührungslosem Ausweis (Proximity Badge) von XyLoc aktivieren

Um die Unterstützung des sicheren UVM-Anmeldeschutzes für die Verwendung eines berührungslosen Ausweises (Proximity Badge) bei CSS erfolgreich zu aktivieren, müssen Sie die Komponenten in folgender Reihenfolge installieren:

1. Installieren Sie Client Security.
2. Aktivieren Sie den sicheren UVM-Anmeldeschutz mit Hilfe des CSS-Administratordienstprogramms.
3. Starten Sie den Computer erneut.
4. Installieren Sie die Software von XyLoc für die Unterstützung von berührungslosen Ausweisen (Proximity Badges).

Anmerkung: Wenn die Software von XyLoc für den berührungslosen Ausweis zuerst installiert wird, wird die Anmeldeschnittstelle für Client Security nicht angezeigt. Wenn dies eintritt, müssen Sie Client Security und XyLoc deinstallieren und anschließend in der oben genannten Reihenfolge erneut installieren, um den sicheren UVM-Anmeldeschutz wiederherzustellen.

Unterstützung von berührungslosem Ausweis (Proximity Badge) und Cisco LEAP

Durch das Aktivieren des Zugriffsschutzes mit berührungslosem Ausweis (Proximity Badge) und die Unterstützung von Cisco LEAP können unerwartete Ergebnisse auftreten. Es wird empfohlen, diese Komponenten nicht zusammen auf demselben System zu installieren oder zu verwenden.

Ensure Technologies-Softwareunterstützung

Bei Client Security 5.2 müssen die Benutzer des berührungslosen Ausweises (Proximity Badge) ihre Ensure-Software auf Version 7.41 aktualisieren. Bei der Aktualisierung von einer früheren Version von IBM Client Security sollten Sie Ihre Ensure-Software aktualisieren, bevor Sie eine Aktualisierung auf Client Security 5.2 durchführen.

Schlüssel wiederherstellen

Nach der Durchführung einer Wiederherstellungsoperation für die Schlüssel müssen Sie den Computer erneut starten, bevor Sie Client Security weiterhin verwenden können.

Namen des lokalen Benutzers und des Domänenbenutzers

Wenn die Namen des Domänenbenutzers und des lokalen Benutzers gleich sind, sollten Sie für beide Accounts dasselbe Windows-Kennwort verwenden. IBM User Verification Manager speichert nur ein Windows-Kennwort pro ID. Die Benutzer sollten daher dasselbe Kennwort für die lokale Anmeldung und für die Domänenanmeldung verwenden. Wenn dies nicht der Fall ist, werden die Benutzer dazu aufgefordert, das IBM UVM Windows-Kennwort zu aktualisieren, wenn sie zwischen lokaler und Domänenanmeldung umschalten, wenn die Ersetzung der gesicherten IBM UVM Windows-Anmeldung aktiviert ist. CSS ist nicht in der Lage, getrennte Domänenbenutzer und lokale Benutzer mit demselben Accountnamen zu registrieren. Wenn Sie versuchen, lokale Benutzer und Domänenbenutzer mit derselben ID zu registrieren, wird folgende Nachricht angezeigt: Die ausgewählte Benutzer-ID wurde bereits konfiguriert. Bei CSS ist es nicht möglich, allgemeine IDs von Domänen- und von lokalen Benutzern einzeln in einem System zu registrieren, so dass mit der allgemeinen Benutzer-ID auf dieselbe Gruppe von Berechtigungsnachweisen, wie z. B. Zertifikate, gespeicherte Fingerabdrücke usw., zugegriffen werden kann.

Targus-Software zum Lesen von Fingerabdrücken erneut installieren

Wurde die Targus-Software zum Lesen von Fingerabdrücken entfernt und anschließend erneut installiert, müssen die erforderlichen Registrierungseinträge zum Aktivieren der Unterstützung für das Lesen von Fingerabdrücken bei Client Security manuell aktiviert werden. Laden Sie die Registrierungsdatei mit den erforderlichen Einträgen (atplugin.reg) herunter, und klicken Sie doppelt darauf, um die Registrierungseinträge dem Register hinzuzufügen. Klicken Sie bei entsprechender Aufforderung auf ″Ja″, um diese Operation zu bestätigen. Das System muss erneut gestartet werden, damit die Änderungen von Client Security erkannt werden und die Unterstützung für das Lesen von Fingerabdrücken aktiviert wird.

Anmerkung: Für das Hinzufügen dieser Registrierungseinträge ist die Administratorberechtigung auf dem System erforderlich.

Administratorverschlüsselungstext für das BIOS

IBM Client Security 5.2 und frühere Versionen unterstützen nicht die auf einigen ThinkPad-Systemen verfügbare Funktion für den Administratorverschlüsselungstext für das BIOS. Wenn Sie die Verwendung des Administratorverschlüsselungstextes für das BIOS aktivieren, muss jede Aktivierung und Inaktivierung des Sicherheits-Subsystems über das Programm "IBM BIOS Setup Utility" vorgenommen werden.

Netscape 7.x verwenden

Netscape 7.x unterscheidet sich von Netscape 4.x. Die Eingabeaufforderung für den Verschlüsselungstext erscheint nicht, sobald Netscape gestartet wurde. Stattdessen wird das PKCS#11-Modul nur bei Bedarf geladen, so dass die Eingabeaufforderung für den Verschlüsselungstext nur dann angezeigt wird, wenn eine Operation ausgeführt wird, bei der das PKCS#11-Modul erforderlich ist.

Diskette zum Archivieren verwenden

Wenn Sie bei der Konfiguration der Sicherheitssoftware eine Diskette als Archivposition angegeben haben, müssen Sie mit langen Verzögerungen rechnen, wenn die Daten während des Konfigurationsprozesses auf die Diskette geschrieben werden. Ein anderer Datenträger, wie z. B. ein gemeinsam benutztes Netzwerk oder ein USB Memory Key, eignet sich möglicherweise besser als Archivposition.

Einschränkungen bei Smartcards

Smartcards registrieren

Smartcards müssen erst bei UVM registriert werden, bevor ein Benutzer eine Authentifizierung mit Hilfe der Karte erfolgreich durchführen kann. Wenn eine Karte mehreren Benutzern zugeordnet ist, kann nur der letzte Benutzer, der die Karte registrieren ließ, diese auch verwenden. Aus diesem Grund sollten Smartcards nur für ein Benutzeraccount registriert werden.

Smartcards authentifizieren

Ist für die Authentifizierung eine Smartcard erforderlich, zeigt UVM ein Dialogfeld an, in dem die Smartcard angefordert wird. Wenn die Smartcard in die Leseeinheit eingelegt wird, erscheint ein Dialogfenster, in dem die PIN-Nummer der Smartcard angefordert wird. Gibt der Benutzer eine falsche PIN-Nummer ein, fordert UVM die Smartcard noch einmal an. Die Smartcard muss entnommen und erneut eingelegt werden, bevor die PIN-Nummer erneut eingegeben werden kann. Die Benutzer müssen die Smartcard so oft entnehmen und erneut einlegen, bis die richtige PIN-Nummer für die Karte eingegeben wurde.

Pluszeichen (+) wird auf Ordnern nach der Verschlüsselung angezeigt

Nach der Verschlüsselung von Dateien oder Ordnern zeigt der Windows Explorer möglicherweise ein Pluszeichen (+) vor dem Ordnersymbol an. Dieses zusätzliche Zeichen wird nicht mehr angezeigt, wenn das Explorer-Fenster aktualisiert wird.

Einschränkungen für Benutzer mit eingeschränkter Berechtigung unter Windows XP

Benutzer mit eingeschränkter Berechtigung unter Windows XP können ihren UVM-Verschlüsselungstext, das Windows-Kennwort oder ihr Schlüsselarchiv nicht mit Hilfe des Benutzerkonfigurationsprogramms aktualisieren.

Weitere Einschränkungen

Dieser Abschnitt enthält Informationen zu weiteren bekannten Problemen und Einschränkungen von Client Security.

Client Security unter Windows-Betriebssystemen verwenden

Alle Windows-Betriebssystem weisen die folgende bekannte Einschränkung auf: Wenn ein Clientbenutzer, der bei UVM registriert ist, seinen Windows-Benutzernamen ändert, geht die gesamte Funktionalität von Client Security verloren. Der Benutzer muss sich mit dem neuen Benutzernamen erneut bei UVM registrieren und kann erst anschließend alle neuen Berechtigungsnachweise anfordern.

Windows XP-Betriebssysteme weisen die folgende bekannte Einschränkung auf: Die Benutzer, die bei UVM registriert sind und ihren zuvor verwendeten Windows-Benutzernamen geändert haben, werden von UVM nicht erkannt. UVM verweist auf den alten 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 verwenden

Netscape wird nach der Anzeige eines Berechtigungsfehlers geöffnet: Wenn das Fenster für 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 der gescannte Fingerabdruck fehlerhaft ist), wird eine Fehlernachricht angezeigt. Wenn Sie auf **OK** klicken, wird Netscape zwar geöffnet, Sie können jedoch das durch das integrierte IBM Sicherheits-Subsystem erstellte, digitale Zertifikat nicht verwenden. Sie müssen erst Netscape schließen und erneut öffnen und den korrekten UVM-Verschlüsselungstext eingeben, bevor Sie das Zertifikat des integrierten IBM Sicherheits-Subsystems verwenden können.

Algorithmen werden nicht angezeigt: Beim Anzeigen des Moduls in Netscape ist keiner der vom PKCS #11-Modul des integrierten IBM Sicherheits-Subsystems unterstützten Hashverfahren-Algorithmen ausgewählt. Folgende Algorithmen werden zwar vom PKCS #11-Modul des integrierten IBM Sicherheits-Subsystems unterstützt, in der Netscape-Anzeige jedoch nicht als unterstützt angegeben.

- SHA-1
- MD5

Verschlüsselungsalgorithmen und Zertifikat des integrierten IBM Sicherheits-Subsystems

Folgende Informationen helfen Ihnen, Fehler zu erkennen, die bei Verschlüsselungsalgorithmen, die im Zertifikat des integrierten IBM Sicherheits-Subsystems verwendet werden können, möglicherweise auftreten. Aktuelle Informationen zu Verschlüsselungsalgorithmen für die jeweilige E-Mail-Anwendung erhalten Sie von Microsoft oder Netscape.

Beim Versand von E-Mails von einem Outlook Express-Client (128-Bit-Version) an einen anderen Outlook Express-Client (128-Bit-Version): Wenn Sie Outlook Express mit der 128-Bit-Version von Internet Explorer 4.0 oder 5.0 zum Senden verschlüsselter E-Mails über Outlook Express (128-Bit-Version) an andere Clients verwenden, können die E-Mails, die mit dem Zertifikat des integrierten IBM Sicherheits-Subsystems verschlüsselt wurden, nur den 3DES-Algorithmus verwenden.

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

Einige Algorithmen stehen im Outlook Express-Client (128-Bit-Version) möglicherweise nicht zur Verfügung: Je nachdem, auf welche Weise Ihre Version von Outlook Express (128-Bit-Version) konfiguriert oder aktualisiert wurde, können möglicherweise einige RC2-Algorithmen und andere Algorithmen nicht im Zertifikat des integrierten IBM Sicherheits-Subsystems verwendet werden. Unter Microsoft finden Sie aktuelle Informationen zu den Verschlüsselungsalgorithmen, die in Ihrer Version von Outlook Express verwendet werden.

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

UVM-Schutz ist nicht aktiviert, wenn Sie in einer Notes-Sitzung zwischen verschiedenen Benutzer-IDs wechseln: Sie können einen UVM-Schutz nur für die aktuelle Benutzer-ID in einer Notes-Sitzung einrichten. Gehen Sie wie folgt vor, um von einer Benutzer-ID, für die UVM-Schutz aktiviert wurde, zu einer anderen Benutzer-ID zu wechseln:

1. Beenden Sie Notes.
2. Inaktivieren Sie den UVM-Schutz für die aktuelle Benutzer-ID.
3. Öffnen Sie Notes, und wechseln Sie zu einer anderen Benutzer-ID. Weitere Informationen zum Wechseln zwischen verschiedenen Benutzer-IDs finden Sie in der Dokumentation zu Lotus Notes.

   Wenn Sie einen UVM-Schutz für die Benutzer-ID einrichten möchten, zu der Sie gewechselt haben, fahren Sie mit Schritt 4 fort.
4. Starten Sie das Tool zur Lotus Notes-Konfiguration, das von Client Security bereitgestellt wird, und richten Sie einen UVM-Schutz ein.

Einschränkungen für das Benutzerkonfigurationsprogramm

Unter Windows XP gibt es bestimmte Zugriffsbeschränkungen, die die einem Clientbenutzer bereitgestellten Funktionen unter gewissen Umständen einschränken.

Windows XP Professional

Unter Windows XP Professional kann es in folgenden Fällen Einschränkungen für Clientbenutzer geben:

- Client Security ist auf einer Partition installiert, die zu einem späteren Zeitpunkt in ein NTFS-Format konvertiert wird
- Der Windows-Ordner befindet sich auf einer Partition, die zu einem späteren Zeitpunkt in ein NTFS-Format konvertiert wird
- Der Archivordner befindet sich auf einer Partition, die zu einem späteren Zeitpunkt in ein NTFS-Format konvertiert wird

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

- Ihre UVM-Verschlüsselungstexte ändern
- Das bei UVM registrierte Windows-Kennwort aktualisieren
- Das Schlüsselarchiv aktualisieren

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 ist auf einer Partition im NTFS-Format installiert
- Der Archivordner ist auf einer Partition im NTFS-Format installiert

Einschränkungen bei Tivoli Access Manager

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 es nicht als Ersatz für die Tivoli Access Manager-Steuerung ausgewählt werden.

Fehlernachrichten

Fehlernachrichten in Zusammenhang mit Client Security werden im Ereignisprotokoll erzeugt: Client Security verwendet einen Einheitentreiber, der Fehlernachrichten im Ereignisprotokoll erzeugen kann. Die Fehler, die mit diesen Nachrichten zusammenhängen, beeinträchtigen die normale Arbeitsweise des Computers nicht.

UVM ruft Fehlernachrichten auf, die vom zugehörigen Programm erzeugt werden, wenn der Zugriff auf ein Authentifizierungsobjekt nicht zugelassen wird: Wenn eine UVM-Policy so festgelegt wurde, dass ein Zugriff auf ein Authentifizierungsobjekt, z. B. durch E-Mail-Entschlüsselung, nicht zugelassen wird, kann die Nachricht über den nicht zugelassenen Zugriff in Abhängigkeit von der jeweils verwendeten Software unterschiedlich ausfallen. So weicht z. B. die Fehlernachricht in Outlook Express, die besagt, dass ein Zugriff auf ein Authentifizierungsobjekt nicht möglich ist, von der Fehlernachricht ab, die für den gleichen Sachverhalt in Netscape angezeigt wird.

Fehlerbehebungstabellen

Der folgende Abschnitt enthält Fehlerbehebungstabellen, die sich beim Auftreten von Fehlern in Client Security Fehler als hilfreich erweisen können.

Fehlerbehebungsinformationen zur Installation

Die folgenden Informationen zur Fehlerbehebung können hilfreich sein, wenn bei der Installation von Client Security Fehler auftreten.

Fehlersymptom	Mögliche Lösung
Während der Softwareinstallation wird eine Fehlernachricht angezeigt	**Maßnahme**
Während der Softwareinstallation wird eine Nachricht angezeigt, in der Sie gefragt werden, ob Sie die ausgewählte Anwendung und alle zugehörigen Komponenten entfernen möchten.	Klicken Sie auf **OK**, um das Fenster zu schließen. Starten Sie den Installationsprozess noch ein Mal, um die neue Softwareversion von Client Security zu installieren.
Bei der Installation wird eine Nachricht angezeigt, dass Sie einen Programm-Upgrade durchführen oder dieses Programm entfernen müssen.	Führen Sie einen der folgenden Schritte aus: • Wenn eine ältere Client Security-Version als 5.0 installiert ist, wählen Sie **Entfernen** aus, und löschen Sie den Inhalt des Sicherheits-Subsystems mit Hilfe des Programms "IBM BIOS Setup Utility". • Wählen Sie andernfalls **Upgrade** aus, und fahren Sie mit der Installation fort.
Unbekanntes Administratorkennwort. Installationszugriff wird nicht zugelassen	**Maßnahme**
Wenn Sie die Software auf einem IBM-Client mit einem aktivierten integrierten IBM Sicherheits-Subsystem installieren, ist das Administratorkennwort für das integrierte IBM Sicherheits-Subsystem unbekannt.	Löschen Sie den Inhalt des Sicherheits-Subsystems, um mit der Installation fortzufahren.

Fehlerbehebungsinformationen zum Administratordienstprogramm

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

Fehlersymptom	Mögliche Lösung
Wenn Sie den UVM-Verschlüsselungstext in das Administratordienstprogramm eingegeben und ihn bestätigt haben, ist die Schaltfläche "Weiter" nicht mehr verfügbar	**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 den Eintrag **Informationen**, und fahren Sie mit der Prozedur fort.
Beim Ändern des öffentlichen Schlüssels für Administratoren wird eine Fehlernachricht angezeigt	**Maßnahme**
Wenn Sie den Inhalt des integrierten IBM Sicherheits-Subsystems löschen und anschließend das Schlüsselarchiv wiederherstellen, wird beim Ändern des öffentlichen Schlüssels für Administratoren möglicherweise eine Fehlernachricht angezeigt.	Nehmen Sie die Benutzer in UVM auf, und fordern Sie ggf. neue Zertifikate an.
Beim Versuch, einen UVM-Verschlüsselungstext wiederherzustellen, wird eine Fehlernachricht angezeigt	**Maßnahme**
Wenn Sie den 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: • Wenn kein UVM-Verschlüsselungstext für den Benutzer benötigt wird, muss keine Maßnahme durchgeführt werden. • Wenn ein UVM-Verschlüsselungstext für den Benutzer benötigt wird, müssen Sie den Benutzer in UVM aufnehmen und ggf. auch neue Zertifikate anfordern.
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, um Ihre Änderungen vorzunehmen, und speichern Sie anschließend die Datei.
Beim Versuch, den UVM-Policy-Editor zu öffnen, wird eine Fehlernachricht angezeigt	**Maßnahme**
Wenn der aktuelle (am Betriebssystem angemeldete) Benutzer 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.

Fehlersymptom	Mögliche Lösung
Bei der Ausführung des Administratordienstprogramms wird eine Fehlernachricht angezeigt	**Maßnahme**
Wenn Sie das Administratordienstprogramm ausführen, wird möglicherweise folgende Fehlernachricht angezeigt: Beim Versuch, auf das integrierte IBM Sicherheits-Subsystem zuzugreifen, ist ein Puffer-E/A-Fehler aufgetreten. Dieser Fehler kann möglicherweise durch einen Warmstart behoben werden.	Schließen Sie die Fehlernachricht, und starten Sie den Computer erneut.
Beim Ändern des Administratorkennworts wird eine Nachricht über die Inaktivierung des Chips angezeigt	**Maßnahme**
Wenn Sie versuchen, das Administratorkennwort 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 eine Bestätigungsnachricht über die Inaktivierung des Chips angezeigt.	Gehen Sie wie folgt vor: 1. Schließen Sie das Bestätigungsfenster mit der Nachricht über die Inaktivierung des Chips. 2. Um das Administratorkennwort zu ändern, geben Sie das neue Kennwort ein, geben Sie anschließend das Bestätigungskennwort ein, und klicken Sie 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: • Ihre UVM-Verschlüsselungstexte ändern • Das bei UVM registrierte Windows-Kennwort aktualisieren • Das Schlüsselarchiv aktualisieren	Dies ist eine bekannte Einschränkung von Windows XP Professional. Zu diesem Fehler gibt es zurzeit keine Lösung.

Fehlersymptom	Mögliche Lösung
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 ist auf einer Partition im NTFS-Format installiert • Der Archivordner ist auf einer Partition im NTFS-Format installiert	Dies ist eine bekannte Einschränkung von Windows XP Home. Zu diesem Fehler gibt es zurzeit keine Lösung.

Fehlerbehebungsinformationen zum ThinkPad

Die folgenden Informationen zur Fehlerbehebung können hilfreich sein, wenn bei der Verwendung von Client Security auf ThinkPad-Computern Fehler auftreten.

Fehlersymptom	Mögliche Lösung
Beim Versuch, eine Administratorfunktion von Client Security aufzurufen, wird eine Fehlernachricht angezeigt.	**Maßnahme**
Nach dem Versuch, eine Client Security-Administratorfunktion auszuführen, wird eine Fehlermeldung angezeigt.	Das ThinkPad-Administratorkennwort muss inaktiviert sein, damit bestimmte Administratorfunktionen von Client Security durchgeführt werden können. Gehen Sie wie folgt vor, um das Administratorkennwort zu inaktivieren: 1. Drücken Sie die Taste F1, um das Programm "IBM BIOS Setup Utility" aufzurufen. 2. Geben Sie das aktuelle Administratorkennwort ein. 3. Geben Sie als neues Administratorkennwort ein leeres Kennwort ein, und bestätigen Sie dieses wiederum mit einem leeren Kennwort. 4. Drücken Sie die Eingabetaste. 5. Drücken Sie die Taste F10, um die Eingaben zu speichern und das Menü zu verlassen.
Ein anderer UVM-Sensor für Fingerabdrücke arbeitet nicht ordnungsgemäß	**Maßnahme**
Vom IBM ThinkPad-Computer wird der Wechsel zwischen mehreren UVM-Sensoren für Fingerabdrücke nicht unterstützt.	Wechseln Sie nicht zwischen verschiedenen Sensormodellen für Fingerabdrücke. 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, die sich für Sie möglicherweise als hilfreich erweisen können, wenn bei der Verwendung von Client Security in Verbindung mit Microsoft-Anwendungen oder -Betriebssystemen Fehler auftreten.

Fehlersymptom	**Mögliche Lösung**
Bildschirmschoner wird nur auf lokaler Anzeige angezeigt	**Maßnahme**
Bei Verwendung des erweiterten Windows-Desktops wird der Client Security-Bildschirmschoner nur auf der lokalen Anzeige angezeigt, obwohl der Zugriff auf das System und die Tastatur geschützt werden.	Wenn sensible Informationen angezeigt werden, verkleinern Sie die Fenster auf Ihrem erweiterten Desktop auf Symbolgröße, bevor Sie den Client Security-Bildschirmschoner aufrufen.
Client Security wird für einen bei UVM registrierten Benutzer nicht ordnungsgemäß ausgeführt	**Maßnahme**
Der registrierte Clientbenutzer hat möglicherweise seinen Windows-Benutzernamen geändert. In diesem Fall geht die gesamte Funktionalität von Client Security verloren.	Sie müssen den neuen Benutzernamen erneut bei UVM registrieren und alle neuen Berechtigungsnachweise anfordern.
Anmerkung: Unter Windows XP werden bei UVM registrierte Benutzer, die zuvor ihren Windows-Benutzernamen geändert haben, 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**
Eine verschlüsselte E-Mail kann nicht entschlüsselt werden, da die Verschlüsselungsgrade der von Sender und Empfänger verwendeten Webbrowser voneinander abweichen.	Prüfen Sie folgende Sachverhalte auf ihre Richtigkeit: 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.
Fehler bei der Verwendung eines Zertifikats von einer Adresse, die über mehrere, ihr zugeordnete Zertifikate verfügt	**Maßnahme**
Outlook Express kann mehrere Zertifikate für eine einzelne E-Mail-Adresse enthalten, wobei einige dieser Zertifikate möglicherweise ungültig sind. Ein Zertifikat kann ungültig sein, wenn der private Schlüssel für das Zertifikat im integrierten IBM Sicherheits-Subsystem des Sender-Computers, in dem das Zertifikat erstellt wurde, nicht mehr existiert.	Bitten Sie den Empfänger, das digitale Zertifikat erneut zu senden. Wählen Sie dieses Zertifikat anschließend 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, seine Nachricht zu signieren, obwohl seinem E-Mail-Account kein Zertifikat zugeordnet ist, wird eine entsprechende Fehlernachricht angezeigt.	In den Sicherheitseinstellungen von Outlook Express können Sie ein Zertifikat angeben, das dem Benutzeraccount zugeordnet werden soll. Weitere Informationen hierzu finden Sie in der Dokumentation zu Outlook Express.
Outlook Express (128-Bit-Version) verschlüsselt E-Mails nur mit dem 3DES-Algorithmus	**Maßnahme**
Für den Versand von verschlüsselten E-Mails zwischen Clients, die Outlook Express mit der 128-Bit-Version von Internet Explorer 4.0 bzw. 5.0 verwenden, kann nur der 3DES-Algorithmus eingesetzt werden.	Unter Microsoft finden Sie aktuelle Informationen zu den Verschlüsselungsalgorithmen, die in Outlook Express verwendet werden.
Outlook Express-Clients geben E-Mails mit einem anderen Algorithmus zurück	**Maßnahme**
Eine E-Mail, die mit den Algorithmen RC2(40), RC2(64) oder RC2(128) verschlüsselt wurde, wird von einem Netscape Messenger-Client an einen Outlook Express-Client (128-Bit-Version) versendet. Die vom Outlook Express-Client zurückgesendete E-Mail wird mit Hilfe des RC2(40)-Algorithmus verschlüsselt.	Es muss keine Maßnahme durchgeführt werden. Eine Verschlüsselungsanforderung vom Typ RC2(40), RC2(64) oder RC2(128) von einem Netscape-Client an einen Outlook Express-Client (128-Bit-Version) wird stets mit dem RC2(40)-Algorithmus an den Netscape-Client zurückgesendet. Unter Microsoft finden Sie aktuelle Informationen zu den Verschlüsselungsalgorithmen, die in Ihrer Version von Outlook Express verwendet werden.
Nach dem Ausfall eines Festplattenlaufwerks wird bei der Verwendung eines Zertifikats in Outlook Express eine Fehlernachricht angezeigt	**Maßnahme**
Die Zertifikate können über die Funktion zur Schlüsselwiederherstellung im Administratordienstprogramm wiederhergestellt werden. Einige Zertifikate, wie z. B. die von VeriSign bereitgestellten kostenfreien Zertifikate, können möglicherweise nach einer Schlüsselwiederherstellung nicht mehr wiederhergestellt werden.	Wenn Sie die Schlüssel wiederhergestellt haben, wählen Sie eine der folgenden Möglichkeiten: • Neue digitale Zertifikate anfordern • Zertifizierungsinstanz erneut bei Outlook Express registrieren
In Outlook Express wird der Verschlüsselungsgrad eines Zertifikats nicht aktualisiert	**Maßnahme**
Wenn ein Sender den Verschlüsselungsgrad in Netscape auswählt und eine signierte E-Mail an einen Client sendet, der Outlook Express mit Internet Explorer 4.0 (128-Bit-Version) verwendet, wird bei der Antwort-E-Mail möglicherweise ein abweichender Verschlüsselungsgrad verwendet.	Löschen Sie das entsprechende Zertifikat aus dem Adressbuch von Outlook Express. Öffnen Sie die signierte E-Mail erneut, und nehmen Sie das Zertifikat in das Adressbuch von Outlook Express auf.

Fehlersymptom	Mögliche Lösung
In Outlook Express wird eine Nachricht über Entschlüsselungsfehler angezeigt.	**Maßnahme**
Sie können eine Nachricht in Outlook Express durch Doppelklicken öffnen. In einigen Fällen wird Ihnen, wenn Sie zu schnell auf eine verschlüsselte Nachricht doppelklicken, möglicherweise eine Nachricht über einen Entschlüsselungsfehler angezeigt.	Schließen Sie die Nachricht, und öffnen Sie die verschlüsselte E-Mail erneut.
Eine Nachricht über einen Entschlüsselungsfehler kann auch bei der Auswahl einer verschlüsselten Nachricht in der Voranzeige erscheinen.	Wenn in der Voranzeige eine Fehlernachricht erscheint, muss keine weitere Maßnahme durchgeführt werden.
Wenn Sie bei verschlüsselten E-Mails zwei Mal auf die Schaltfläche ″Senden″ klicken, wird eine Fehlernachricht angezeigt	**Maßnahme**
Wenn Sie in Outlook Express zwei Mal auf ″Senden″ klicken, um eine verschlüsselte E-Mail zu senden, wird eine Fehlernachricht angezeigt, die besagt, dass die Nachricht nicht versendet werden konnte.	Schließen Sie die Fehlernachricht, und klicken Sie ein Mal auf die Schaltfläche **Senden**.
Beim Anfordern eines Zertifikats wird eine Fehlernachricht angezeigt	**Maßnahme**
Wenn Sie Internet Explorer verwenden, wird Ihnen bei der Anforderung eines Zertifikats, das das CSP-Modul des integrierten IBM Sicherheits-Subsystems verwendet, möglicherweise eine Fehlernachricht angezeigt.	Fordern Sie das digitale Zertifikat erneut an.

Fehlerbehebungsinformationen zu Netscape-Anwendungen

Die folgenden Fehlerbehebungstabellen enthalten Informationen, die sich für Sie möglicherweise als hilfreich erweisen können, wenn bei der Verwendung von Client Security in Verbindung mit Netscape-Anwendungen Fehler auftreten.

Fehlersymptom	Mögliche Lösung
Fehler beim Lesen verschlüsselter E-Mails	**Maßnahme**
Eine verschlüsselte E-Mail kann nicht entschlüsselt werden, da die Verschlüsselungsgrade der von Sender und Empfänger verwendeten Webbrowser voneinander abweichen.	Prüfen Sie folgende Sachverhalte auf ihre Richtigkeit: 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.

Fehlersymptom	Mögliche Lösung
Beim Versuch, eine E-Mail digital zu signieren, wird eine Fehlernachricht angezeigt	**Maßnahme**
Wenn das Zertifikat des integrierten IBM Sicherheits-Subsystems in Netscape Messenger nicht ausgewählt wurde und der Verfasser einer E-Mail versucht, die Nachricht mit dem Zertifikat zu signieren, wird eine Fehlernachricht angezeigt.	Im Programm "Netscape Messenger" können Sie über die Sicherheitseinstellungen das Zertifikat auswählen. 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 Netscape-Dokumentation.
Eine E-Mail wird mit einem anderen (abweichenden) Algorithmus an den Client zurückgesendet	**Maßnahme**
Eine E-Mail, die mit den Algorithmen RC2(40), RC2(64) oder RC2(128) verschlüsselt wurde, wird von einem Netscape Messenger-Client an einen Outlook Express-Client (128-Bit-Version) versendet. Die vom Outlook Express-Client zurückgesendete E-Mail wird mit Hilfe des RC2(40)-Algorithmus verschlüsselt.	Es muss keine Maßnahme durchgeführt werden. Eine Verschlüsselungsanforderung vom Typ RC2(40), RC2(64) oder RC2(128) von einem Netscape-Client an einen Outlook Express-Client (128-Bit-Version) wird stets mit dem RC2(40)-Algorithmus an den Netscape-Client zurückgesendet. Unter Microsoft finden Sie aktuelle Informationen zu den Verschlüsselungsalgorithmen, die in Ihrer Version von Outlook Express verwendet werden.
Die Verwendung eines digitalen Zertifikats, das durch das integrierte IBM Sicherheits-Subsystem erstellt wurde, ist nicht möglich	**Maßnahme**
Das digitale Zertifikat, das durch das integrierte IBM Sicherheits-Subsystem erstellt wurde, kann nicht verwendet werden.	Prüfen Sie, ob der korrekte UVM-Verschlüsselungstext beim Öffnen von Netscape eingegeben worden ist. Wenn Sie einen fehlerhaften UVM-Verschlüsselungstext eingeben, wird eine Fehlernachricht angezeigt, die besagt, dass ein Authentifizierungsfehler aufgetreten ist. Wenn Sie auf **OK** klicken, wird Netscape geöffnet. Sie können jedoch das durch das integrierte IBM Sicherheits-Subsystem erstellte Zertifikat nicht verwenden. Sie müssen erst Netscape beenden und erneut öffnen und dann den korrekten UVM-Verschlüsselungstext eingeben.

Fehlersymptom	Mögliche Lösung
Neue digitale Zertifikate vom selben Sender werden in Netscape nicht ersetzt.	**Maßnahme**
Wenn eine digital signierte E-Mail vom selben Sender mehrmals eingeht, wird das erste digitale Zertifikat für die E-Mail nicht überschrieben.	Wenn Sie mehrere E-Mail-Zertifikate erhalten, ist nur eines davon das Standardzertifikat. Verwenden Sie die Sicherheitseinrichtungen von Netscape, um das das erste Zertifikat zu löschen. Öffnen Sie anschließend das zweite Zertifikat erneut oder bitten Sie den Sender, eine weitere signierte E-Mail zu senden.
Zertifikat des integrierten IBM Sicherheits-Subsystems kann nicht exportiert werden	**Maßnahme**
Das Zertifikat des integrierten IBM Sicherheits-Subsystems kann nicht in Netscape exportiert werden. Die Exportfunktion von Netscape kann zum Sichern von Zertifikaten verwendet werden.	Rufen Sie das Administratordienstprogramm oder Benutzerkonfigurationsprogramm auf, um das Schlüsselarchiv zu aktualisieren. Wenn Sie das Schlüsselarchiv aktualisieren, werden Kopien von allen Zertifikaten des integrierten IBM Sicherheits-Subsystems erstellt.
Beim Versuch, ein wiederhergestelltes Zertifikat nach einem Ausfall des Festplattenlaufwerks zu verwenden, wird eine Fehlernachricht angezeigt	**Maßnahme**
Die Zertifikate können über die Funktion zur Schlüsselwiederherstellung im Administratordienstprogramm wiederhergestellt werden. Einige Zertifikate, wie z. B. die von VeriSign bereitgestellten kostenfreien Zertifikate, können möglicherweise nach einer Schlüsselwiederherstellung nicht mehr wiederhergestellt werden.	Wenn Sie die Schlüssel wiederhergestellt haben, können Sie ein neues Zertifikat anfordern.
Der Netscape-Agent öffnet Netscape und erzeugt einen Netscape-Fehler	**Maßnahme**
Der Netscape-Agent öffnet und schließt Netscape.	Schalten die den Netscape-Agent aus.
Netscape wird mit zeitlicher Verzögerung geöffnet.	**Maßnahme**
Wenn Sie das PKCS #11-Modul des integrierten IBM Sicherheits-Subsystems hinzufügen und anschließend Netscape öffnen, kommt es zu einer kurzen zeitlichen Verzögerung, bevor Netscape geöffnet wird.	Es muss keine Maßnahme durchgeführt werden. Diese Angaben dienen nur zur allgemeinen 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**
Während der Anforderung eines digitalen Zertifikats wird das Fenster für den UVM-Verschlüsselungstext bzw. das Fenster zur Authentifizierung über Fingerabdrücke mehrmals angezeigt	**Maßnahme**
Die UVM-Sicherheitspolicy schreibt vor, dass ein Benutzer zuerst den UVM-Verschlüsselungstext eingeben oder die Authentifizierung über Fingerabdrücke erbringen muss, bevor er ein digitales Zertifikat anfordern kann. Versucht der Benutzer, ein Zertifikat anzufordern, wird das Authentifizierungsfenster, in dem der Benutzer den UVM-Verschlüsselungstext eingeben oder eine Scannerabtastung des Fingerabdrucks hinterlassen muss, mehrmals angezeigt.	Geben Sie in jedes geöffnete Authentifizierungsfenster den entsprechenden UVM-Verschlüsselungstext ein bzw. hinterlassen Sie die Scannerabtastung Ihres Fingerabdrucks.
VBScript- oder JavaScript-Fehlernachricht wird angezeigt	**Maßnahme**
Wenn Sie ein digitales Zertifikat anfordern, wird möglicherweise eine Fehlernachricht für VBScript oder JavaScript angezeigt.	Starten Sie den Computer erneut, und fordern Sie das Zertifikat erneut an.

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 stimmen nicht mit denjenigen auf dem Server überein	**Maßnahme**
Tivoli Access Manager lässt bestimmte Bit-Konfigurationen zu, die von UVM nicht unterstützt werden. Daher können bei der Konfiguration des PD-Servers die von einem Administrator eingegebenen Einstellungen mit den Einstellungen für die lokalen Policy-Bestimmungen überschrieben werden.	Dies ist eine bekannte Einschränkung.

Fehlersymptom	Mögliche Lösung
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.
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 **Traversebit** aktiviert wurde.	Es muss keine Maßnahme durchgeführt werden.

Fehlerbehebungsinformationen zu Lotus Notes

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

Fehlersymptom	Mögliche Lösung
Nach dem Aktivieren des UVM-Schutzes für Lotus Notes kann die Konfiguration von Lotus Notes nicht abgeschlossen werden.	**Maßnahme**
Lotus Notes kann die Installation nicht abschließen, wenn der UVM-Schutz mit Hilfe des Administratordienstprogramms aktiviert wurde.	Dies ist eine bekannte Einschränkung. Lotus Notes muss konfiguriert und ausgeführt werden, bevor die Lotus Notes-Unterstützung im Administratordienstprogramm aktiviert wird.
Beim Versuch, das Notes-Kennwort zu ändern, wird eine Fehlernachricht angezeigt	**Maßnahme**
Wenn Sie während der Verwendung von Client Security das Notes-Kennwort ändern, kann dies zur Anzeige einer Fehlernachricht führen.	Versuchen Sie noch ein Mal, das Kennwort zu ändern. Wenn dieser Versuch fehlschlägt, starten Sie den Client erneut.

Fehlersymptom	Mögliche Lösung
Nachdem Sie ein Kennwort per Zufallsgenerator festgelegt haben, wird eine Fehlernachricht angezeigt	**Maßnahme**
Möglicherweise wird eine Fehlernachricht angezeigt, wenn Sie folgende Schritte ausführen: • Über das Tool zur Lotus Notes-Konfiguration UVM-Schutz für eine Notes-ID festlegen • Notes aufrufen und über die entsprechende Notes-Funktion das Kennwort für die Notes-ID-Datei ändern • Notes sofort nach dem Ändern des Kennworts schließen	Klicken Sie auf **OK**, um die Fehlernachricht zu schließen. Es müssen keine weiteren Maßnahmen durchgeführt werden. Entgegen der Fehlernachricht wurde das Kennwort geändert. Bei dem neuen Kennwort handelt es sich um ein per Zufallsgenerator festgelegtes Kennwort, das von Client Security erstellt wurde. Die Datei mit der Notes-ID wird nun mit dem per Zufallsgenerator festgelegten Kennwort verschlüsselt. Der Benutzer benötigt keine Datei mit einer neuen Benutzer-ID. Wenn der Endbenutzer das Kennwort erneut ändert, wird in UVM ein neues, per Zufallsgenerator festgelegtes, Kennwort für die Notes-ID erstellt.

Fehlerbehebungsinformationen zur Verschlüsselung

Die folgenden Informationen zur Fehlerbehebung können hilfreich sein, wenn beim Verschlüsseln von Dateien mit Hilfe von Client Security ab Version 3.0 Fehler auftreten.

Fehlersymptom	Mögliche Lösung
Zuvor 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 Dateien entschlüsseln, die mit Hilfe älterer Versionen von Client Security verschlüsselt wurden, *bevor* Sie Client Security ab Version 3.0 installieren. Client Security 3.0 kann aufgrund von Änderungen bei der Dateiverschlüsselungsimplementierung keine Dateien entschlüsseln, die mit früheren Versionen von Client Security verschlüsselt wurden.

Fehlerbehebungsinformationen zu UVM-sensitiven Einheiten

Die folgenden Informationen zur Fehlerbehebung können hilfreich sein, wenn bei der Verwendung von UVM-sensitiven Einheiten Fehler auftreten.

Fehlersymptom	**Mögliche Lösung**
Eine UVM-sensitive Einheit funktioniert nicht mehr ordnungsgemäß.	**Maßnahme**
Eine UVM-sensitive Sicherheitskomponente, wie z. B. eine Smartcard, ein Smartcard-Lesegerät oder ein Lesegerät für Fingerabdrücke, funktioniert nicht ordnungsgemäß.	Stellen Sie fest, ob die Komponente vom System ordnungsgemäß konfiguriert wurde. Nach dem Konfigurieren einer Komponente müssen Sie möglicherweise das System erneut booten, damit der Service ordnungsgemäß gestartet wird. Schlagen Sie in den Informationen zur Fehlerbehebung an der Komponente in der Dokumentation zur Komponente nach, oder wenden Sie sich an den Hersteller der Komponente.
Eine UVM-sensitive Einheit funktioniert nicht mehr ordnungsgemäß.	**Maßnahme**
Wenn Sie eine UVM-sensitive Einheit vom USB-Port trennen und anschließend die Verbindung der Einheit zum USB-Port wiederherstellen, kann es sein, dass die Einheit nicht mehr einwandfrei funktioniert.	Starten Sie den Computer erneut, nachdem Sie die Einheit erneut an den USB-Anschluss angeschlossen haben.

Anhang A. Informationen zu Kennwörtern und Verschlüsselungstexten

Dieser Anhang enthält Informationen zu Kennwörtern und Verschlüsselungstexten.

Regeln für Kennwörter und Verschlüsselungstexte

In einem sicheren System gibt es viele verschiedene Kennwörter und Verschlüsselungstexte. Für die verschiedenen Kennwörter gelten unterschiedliche Regeln. Dieser Abschnitt enthält Informationen zum Administratorkennwort sowie zum UVM-Verschlüsselungstext.

Regeln für Administratorkennwörter

Die Regeln für ein Administratorkennwort können von einem Sicherheitsadministrator nicht geändert werden.

Folgende Regeln gelten für Administratorkennwörter:

Länge Das Kennwort muss genau 8 Zeichen umfassen.

Zeichen
Das Kennwort darf nur alphanumerische Zeichen enthalten. Eine Kombination aus Buchstaben und Zahlen ist zulässig. Sonderzeichen, wie z. B. Leerzeichen, !, ?, % sind unzulässig.

Merkmale
Legen Sie das Administratorkennwort fest, um den integrierten IBM Security Chip im Computer zu aktivieren. Dieses Kennwort muss bei jedem Zugriff auf das Administratordienstprogramm und die Administratorkonsole eingegeben werden.

Fehlversuche
Wenn Sie 10 Mal hintereinander ein fehlerhaftes Kennwort eingeben, wird der Computer für 1 Stunde und 17 Minuten gesperrt. Wenn Sie nach Ablauf dieser Zeit das Kennwort wiederum 10 Mal falsch eingeben, wird der Computer für 2 Stunden und 34 Minuten gesperrt. Die Zeitdauer der Inaktivierung des Computers wird jedes Mal verdoppelt, wenn Sie 10 Mal hintereinander ein fehlerhaftes Kennwort eingeben.

Regeln für UVM-Verschlüsselungstexte

In IBM Client Security können Administratoren Regeln für UVM-Verschlüsselungstexte der Benutzer festlegen. Zur Erhöhung der Sicherheit kann der UVM-Verschlüsselungstext länger und eindeutiger abgefasst sein als ein herkömmliches Kennwort. Die Policy für den UVM-Verschlüsselungstext wird über das Administratordienstprogramm 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 in Klammern angegeben.

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

  Wenn z. B. ″6″ erlaubte Zeichen definiert sind, ist `1234567xxx` ein ungültiges Kennwort.
- ob eine Mindestanzahl an Ziffern festgelegt werden soll (ja, 1)

  Wenn hierfür ″1″ festgelegt ist, ist `thisismypassword` ein ungültiges Kennwort.
- ob eine Mindestanzahl an Leerzeichen festgelegt werden soll (keine Mindestanzahl)

  Wenn hierfür ″2″ festgelegt ist, ist `i am not here` ein ungültiges Kennwort.
- ob der Verschlüsselungstext mit einer Ziffer beginnen darf (nein)

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

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

  Standardmäßig ist z. B. `Benutzername` ein ungültiges Kennwort, 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. `mypassword` ein ungültiges Kennwort, wenn eines der drei vorherigen Kennwörter `mypassword` war.
- ob der Verschlüsselungstext mehr als drei identische aufeinanderfolgende Zeichen des letzten Kennworts enthalten darf (nein)

  Standardmäßig ist z. B. `paswor` ein ungültiges Kennwort, wenn das vorherige Kennwort `pass` oder `word` lautete.

Das Fenster ″Policy für UVM-Verschlüsselungstext″ des Administratordienstprogramms stellt Sicherheitsadministratoren eine einfache Schnittstelle zur Steuerung des Ablaufs von Verschlüsselungstexten bereit. Über das Fenster ″Policy für UVM-Verschlüsselungstext″ kann der Administrator zwischen den folgenden Regeln für Verschlüsselungstexte auswählen:

- Verschlüsselungstext läuft nach einer bestimmten Anzahl von Tagen ab (ja, 184).

  Standardmäßig läuft der Verschlüsselungstext z. B. nach 184 Tagen ab. Der neue Verschlüsselungstext muss mit der festgelegten Richtlinie für Verschlüsselungstexte übereinstimmen.
- Entscheiden, ob der Verschlüsselungstext ablaufen soll (ja)

  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 umfassen.

Zeichen

Der Verschlüsselungstext kann sich aus jeder beliebigen Kombination von Zeichen zusammensetzen, die auf der Tastatur enthalten sind. Dazu gehören auch Leerzeichen und nicht alphanumerische Zeichen.

Merkmale

Der UVM-Verschlüsselungstext weicht von einem Kennwort, das Sie für die Anmeldung an einem Betriebssystem verwenden können, ab. Der UVM-Verschlüsselungstext kann zusammen mit anderen Authentifizierungseinheiten, wie z. B. einem UVM-Sensor für Fingerabdrücke, verwendet werden.

Fehlversuche

Wenn Sie den UVM-Verschlüsselungstext während einer Sitzung mehrmals falsch eingeben, führt der Computer eine Reihe von Anti-Hammering-Verzögerungen aus. Diese Verzögerungen werden im folgenden Abschnitt näher beschrieben.

Zählung fehlgeschlagener Versuche auf TCPA-Systemen und anderen Systemen

In der folgenden Tabelle werden die Einstellungen für Anti-Hammering-Verzögerung für ein TCPA-System angezeigt:

Versuche	Verzögerung beim nächsten Fehlschlagen
15	1,1 Minuten
31	2,2 Minuten
47	4,4 Minuten
63	8,8 Minuten
79	17,6 Minuten
95	35,2 Minuten
111	1,2 Stunden
127	2,3 Stunden
143	4,7 Stunden

TCPA-Systeme unterscheiden nicht zwischen Benutzerverschlüsselungstexten und dem Administratorkennwort. Jede Authentifizierung über den integrierten IBM Security Chip unterliegt der gleichen Policy. Das maximale Zeitlimit liegt bei 4,7 Stunden. Die Verzögerung überschreitet bei TCPA-System nicht 4,7 Stunden.

Andere Systeme unterscheiden zwischen dem Administratorkennwort und Benutzerverschlüsselungstexten. Bei diesen anderen Systemen gibt es für das Administratorkennwort eine Verzögerung von 77 Minuten nach 10 fehlgeschlagenen Versuchen; für Benutzer gibt es nur eine Verzögerung von 1 Minute nach 32 fehlgeschlagenen Versuchen, bei allen weiteren 32 fehlgeschlagenen Versuchen verdoppelt sich die Sperrzeit.

Verschlüsselungstext zurücksetzen

Wenn ein Benutzer seinen Verschlüsselungstext vergisst, kann der Administrator den Benutzer diesen Verschlüsselungstext wiederherstellen lassen.

Verschlüsselungstext über Remotezugriff zurücksetzen

Gehen Sie wie folgt vor, um ein Kennwort über Remotezugriff zurückzusetzen:

- **Administratoren**

  Ein ferner Administrator muss wie folgt vorgehen:

  1. Erstellen Sie ein neues Kennwort für den einmaligen Gebrauch, und teilen Sie es dem Benutzer mit.
  2. Senden Sie dem Benutzer eine Datendatei.

     Die Datendatei kann dem Benutzer per E-Mail gesendet werden, auf einen austauschbaren Datenträger wie z. B. eine Diskette kopiert werden oder direkt in die Archivdatei des Benutzers geschrieben werden (vorausgesetzt, dass der Benutzer auf dieses System zugreifen kann). Diese verschlüsselte Datei wird zum Abgleich mit dem neuen Kennwort für den einmaligen Gebrauch verwendet.

- **Benutzer**

  Der Benutzer muss wie folgt vorgehen:

  1. Melden Sie sich am Computer an.
  2. Wenn Sie zum Eingeben des Verschlüsselungstextes aufgefordert werden, wählen Sie das Markierungsfeld "Verschlüsselungstext vergessen" aus.
  3. Geben Sie das Kennwort für den einmaligen Gebrauch, das der ferne Administrator Ihnen mitgeteilt hat, ein, und geben Sie die Position der vom Administrator gesendeten Datei an.

     Nachdem UVM überprüft hat, ob die Informationen in der Datei mit dem angegebenen Verschlüsselungstext übereinstimmen, wird dem Benutzer Zugriff gewährt. Der Benutzer wird dann unverzüglich aufgefordert, den Verschlüsselungstext zu ändern.

Dies ist die empfohlene Vorgehensweise, um einen vergessenen Verschlüsselungstext wiederherzustellen.

Verschlüsselungstext manuell zurücksetzen

Wenn der Administrator direkt auf das System des Benutzers, der seinen Verschlüsselungstext vergessen hat, zugreifen kann, kann er sich am System des Benutzers als Administrator anmelden, im Administratordienstprogramm den privaten Administratorschlüssel angeben und manuell den Verschlüsselungstext des Benutzers ändern. Der Administrator muss zum Ändern des Verschlüsselungstextes den alten Verschlüsselungstext des Benutzers nicht kennen.

Anhang B. Bemerkungen und Marken

Dieser Anhang enthält rechtliche Hinweise auf IBM Produkte sowie Informationen zu den 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 IBM Produkte, Programme oder Dienstleistungen können auch andere ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremddienstleistungen liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder 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 Handbuch aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der Allgemeinen Geschäftsbedingungen der IBM, der ICA-Lizenzbedingungen (IBM Customer Agreement), der IPLA-Lizenzbedingungen (International Program License Agreement) oder einer äquivalenten Vereinbarung.

Marken

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

Tivoli ist in gewissen Ländern eine Marke der 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.