IBM® Client Security
Solutions

Client Security Software versione 5.1 - Guida per il responsabile

IBM® Client Security
Solutions

Client Security Software versione 5.1 - Guida per il responsabile

Prima edizione (aprile 2003)

Prima di utilizzare questo prodotto e le relative informazioni, consultare la sezione Appendice A, “Norme per l’esportazione di Client Security Software”, a pagina 65 e l’Appendice D, “**Marchi e informazioni particolari**”, a pagina 73.

Indice

Prefazione v
A chi si rivolge questa guida. vi
Modalità di utilizzo di questa guida vi
Riferimenti al manuale *Guida all'installazione di Client Security Software* vi
Riferimenti al manuale *Utilizzo di Client Security con Tivoli Access Manager* vi
Riferimenti al manuale *Guida per l'utente di Client Security*. vii
Ulteriori informazioni vii

Capitolo 1. Introduzione a IBM Client Security Software 1
Applicazioni e componenti di Client Security Software. 1
Funzioni PKI (Public Key Infrastructure) 2

Capitolo 2. Cifratura di file e cartelle . . 5
Protezione dei file con il tastino destro del mouse . . 5
Protezione delle cartelle con il tastino destro. . . . 5
Stato di cifratura delle cartelle 5
Suggerimenti per il programma di utilità FFE (File and Folder Encryption) 6
Protezione dell'unità disco fisso 7
Eliminazione di cartelle e file protetti 7
Prima di aggiornare una versione precedente del programma di utilità IBM FFE 7
Prima della disinstallazione del programma di utilità IBM FFE 7
Limitazioni del programma di utilità FFE (File and Folder Encryption) 7
Limitazioni relative allo spostamento di cartelle e file protetti 7
Limitazioni relative all'esecuzione delle applicazioni 7
Limitazioni relative alla lunghezza del nome del percorso 7
Problemi relativi alla protezione delle cartelle . . 8

Capitolo 3. Come utilizzare Client Security Software 9
Esempio 1 - Un client Windows 2000 e un client Windows XP che utilizzano Outlook Express . . . 9
Esempio 2 - Due client IBM con Windows 2000 che utilizzano Lotus Notes e lo screen saver di Client Security 10
Esempio 3 - Numerosi client IBM con Windows 2000 che vengono gestiti da Tivoli Access Manager e che utilizzano Netscape per le e-mail 11

Capitolo 4. Autorizzazione degli utenti 13
Autenticazione per utenti client. 13
Elementi di autenticazione 13
Prima di autorizzare gli utenti 13
Autorizzazione degli utenti 14
Rimozione degli utenti 15
Creazione di nuovi utenti. 16

Capitolo 5. Operazioni da eseguire dopo aver autorizzato gli utenti in UVM. 17
Protezione per il collegamento al sistema operativo di UVM 17
Impostazione della protezione per il collegamento al sistema operativo di UVM . . . 17
Impostazione della protezione per il collegamento al sistema operativo di UVM . . . 18
Registrazione delle impronte digitali degli utenti con UVM 18
Utilizzo della protezione UVM per Lotus Notes . . 19
Abilitazione e configurazione della protezione UVM per un ID utente di Lotus Notes 19
Utilizzo della protezione UVM con Lotus Notes 20
Disabilitazione della protezione UVM per un ID utente di Lotus Notes 20
Impostazione della protezione UVM per un ID utente Lotus Notes diverso 21
Utilizzo di Client Security Software con applicazioni Netscape 21
Installazione del modulo PKCS#11 di IBM embedded Security Chip per applicazioni Netscape 21
Utilizzo della protezione al collegamento PKCS#11 per le applicazioni Netscape 22
Selezione di IBM embedded Security Chip per generare un certificato digitale per le applicazioni Netscape 22
Aggiornamento dell'archivio di chiavi per le applicazioni Netscape 22
Utilizzo del certificato digitale per le applicazioni Netscape 22

Capitolo 6. Funzionalità della politica UVM. 25
Modifica di una politica UVM locale 25
Selezione dell'oggetto 26
Elementi di autenticazione 27
Utilizzo dell'editor della politica UVM 28
Modifica e utilizzo della politica UVM per i client remoti 29

Capitolo 7. Altre funzioni del responsabile per la protezione 31
Utilizzo di Administrator Console 31
Registrazione di un client in una rete di roaming delle credenziali 32
Modifica dell'ubicazione dell'archivio di chiavi . . 33
Modifica della coppia di chiavi dell'archivio . . . 34
Ripristino delle chiavi dall'archivio 35

Reimpostazione del conteggio numeri errori di autenticazione 36
Modifica delle informazioni di impostazione di Tivoli Access Manager 36
Accesso al file di configurazione di Tivoli Access Manager 36
Aggiornamento della cache locale 37
Recupero di un passphrase UVM 37
Modifica della password di IBM Security Chip . . 38
Visualizzazione delle informazioni su Client Security Software 38
Disabilitazione di IBM embedded Security Chip . . 39
Abilitazione di IBM embedded Security Chip e impostazione della password di Security Chip . . . 39
Abilitazione del supporto Entrust 40

Capitolo 8. Istruzioni per gli utenti client 41
Utilizzo della protezione UVM per il collegamento al sistema 41
Procedure per sbloccare il client 41
Screen saver di Client Security 42
Impostazione dello screen saver di Client Security 42
Attività dello screen saver di Client Security . . 42
User Configuration Utility 42
Funzioni User Configuration Utility 43
Limiti di User Configuration Utility con Windows XP 43
Utilizzo di User Configuration Utility 44
Utilizzo di un programma di navigazione sul web e di messaggi e-mail sicuri 44
Utilizzo di Client Security Software con applicazioni Microsoft 45
Emissione di un certificato digitale per le applicazioni Microsoft 45
Trasferimento di certificati da Microsoft CSP . . 45
Aggiornamento dell'archivio di chiavi per le applicazioni Microsoft 46
Utilizzo del certificato digitale per le applicazioni Microsoft 46
Configurazione delle preferenze audio UVM . . . 46

Capitolo 9. Risoluzione dei problemi . . 47
Funzioni del responsabile. 47
Impostazione di una password responsabile (ThinkCentre). 47
Impostazione di una password del supervisore (ThinkPad) 48
Protezione di una password per l'hardware . . 49
Annullamento di IBM embedded Secutity Chip (ThinkCentre). 49
Annullamento di IBM embedded Security Chip (ThinkPad) 49
Administrator Utility 50
Rimozione di utenti 50
Accesso non consentito agli oggetti selezionati con il controllo Tivoli Access Manager 50
Limiti 50
Utilizzo di Client Security Software con sistemi operativi Windows 51
Utilizzo di Client Security Software con applicazioni Netscape 51
Certificato IBM embedded Security Chip e algoritmi di cifratura 51
Utilizzo della protezione UVM per un ID utente Lotus Notes 52
Limiti di User Configuration Utility 52
Messaggi di errore 53
Prospetti per la risoluzione dei problemi. 53
Informazioni sulla risoluzione dei problemi relativi all'installazione 53
Informazioni sulla risoluzione dei problemi del programma Administrator Utility 54
Informazioni sulla risoluzione dei problemi del programma User Configuration Utility 55
Informazioni sulla risoluzione dei problemi specifici al ThinkPad 56
Informazioni sulla risoluzione dei problemi della Microsoft 56
Informazioni sulla risoluzione dei problemi dell'applicazione Netscape 59
Informazioni sulla risoluzione dei problemi relativi al certificato digitale 61
Informazioni sulla risoluzione dei problemi di Tivoli Access Manager. 62
Informazioni sulla risoluzione dei problemi relativi a Lotus Notes 62
Informazioni sulla risoluzione dei problemi relativi alla cifratura 63
Informazioni sulla risoluzione dei problemi relativi all'unità UVM 64

Appendice A. Norme per l'esportazione di Client Security Software 65

Appendice B. Regole per password e passphrase. 67
Regole per la password hardware 67
Regole per passphrase UVM. 67

Appendice C. Regole sull'uso della protezione UVM per il collegamento del sistema 71

Appendice D. Marchi e informazioni particolari 73
Informazioni particolari 73
Marchi 74

Prefazione

Questo manuale contiene informazioni sull'impostazione e sull'utilizzo delle funzioni di sicurezza fornite con Client Security Software.

Questa guida è organizzata nel modo seguente:

″Capitolo 1, "**Introduzione a IBM Client Security Software**",″ contiene una panoramica dei componenti e delle applicazioni inclusi nel software ed una descrizione della funzioni PKI (Public Key Infrastructure).

″Capitolo 2, "Cifratura di file e cartelle",″ contiene informazioni su come utilizzare IBM Client Security Software per proteggere file e cartelle particolari.

″Capitolo 3, "Come utilizzare Client Security Software",″ contiene esempi che utilizzano i componenti forniti da Client Security Software per impostare le funzioni di sicurezza necessarie agli utenti dei client IBM.

″Capitolo 4, "Autorizzazione degli utenti",″ contiene le informazioni sull'autenticazione degli utenti client, inclusa la modalità di autorizzazione e di rimozione degli utenti in UVM (User Verification Manager).

″Capitolo 5, "Operazioni da eseguire dopo aver autorizzato gli utenti in UVM",″ contiene le istruzioni e le informazioni su come impostare la protezione UVM per il collegamento del sistema operativo, utilizzare la protezione UVM per Lotus Notes ed utilizzare Client Security Software con le applicazioni Netscape.

″Capitolo 6, "Funzionalità della politica UVM",″ contiene le istruzioni su come modificare una politica UVM locale, utilizzare una politica UVM per un client remoto e modificare la password per un file della politica UVM.

″Capitolo 7, "Altre funzioni del responsabile per la protezione",″ contiene le istruzioni su come utilizzare il programma Administrator Utility per modificare la posizione dell'archivio della chiave, ripristinare le chiavi dall'archivio, recuperare un passphrase UVM e per abilitare o disabilitare IBM embedded Security Chip.

″Capitolo 8, "Istruzioni per gli utenti client",″ contiene istruzioni sulle diverse attività che l'utente del client può eseguire con Client Security Software. Questo capitolo comprende le istruzioni sull'utilizzo della la protezione del collegamento UVM, dello screen saver di Client Security, del servizio e-mail e del programma User Configuration Utility.

″Capitolo 9, "Risoluzione dei problemi",″ contiene informazioni utili per la risoluzione di limitazioni e problemi noti che si possono verificare quando si utilizzano le istruzioni fornite in questo manuale.

″Appendice A, "Norme per l'esportazione di Client Security Software",″ contiene le informazioni sulle norme relative all'esportazione in U.S. del software.

″Appendice B, "Regole per password e passphrase",″ contiene i criteri della password che possono essere applicati alle regole e ad una passphrase UVM per le password di Security Chip.

″Appendice C, “**Regole sull’uso della protezione UVM per il collegamento del sistema**”,″ contiene informazioni sull’utilizzo della protezione UVM per il collegamento al sistema operativo.

″Appendice D, “**Marchi e informazioni particolari**”,″ contiene le informazioni legali e le informazioni sui marchi.

A chi si rivolge questa guida

Questa guida è destinata ai responsabili della sicurezza per:

- Impostare l’autenticazione dell’utente per il client IBM
- Impostare e modificare la politica di sicurezza UVM per i client IBM
- Utilizzare Administrator Utility per gestire il sottosistema di sicurezza (IBM embedded Security Chip) e le impostazioni associate per i client IBM

Questa guida, inoltre, è destinata ai responsabili di Tivoli Access Manager che utilizzeranno IBM Tivoli Access Manager per gestire gli oggetti di autenticazione forniti nella politica UVM. I responsabili di Tivoli Access Manager devono essere in grado di gestire quanto segue:

- L’object space di Tivoli Access Manager
- I processi di autenticazione, autorizzazione e di acquisizione delle credenziali
- IBM DCE (Distributed Computing Environment)
- Il protocollo LDAP (lightweight directory access protocol) di IBM SecureWay Directory

Modalità di utilizzo di questa guida

Utilizzare questa guida per impostare l’autenticazione utente e la politica di sicurezza UVM per i client IBM. Questa guida si integra con *Guida all’installazione di Client Security Software*, *Utilizzo di Client Security con Tivoli Access Manager*, e *Guida per l’utente di Client Security*. Questa guida e tutta la documentazione per Client Security può essere scaricata dal sito web IBM http://www.pc.ibm.com/ww/security/secdownload.html.

Riferimenti al manuale *Guida all’installazione di Client Security Software*

I riferimenti al manuale *Guida all’installazione di Client Security Software* vengono forniti in questo documento. E’ necessario installare Client Security Software su un client IBM prima di poter utilizzare questo manuale. Le istruzioni per l’installazione del software vengono fornite nel manuale *Guida all’installazione di Client Security Software*.

Riferimenti al manuale *Utilizzo di Client Security con Tivoli Access Manager*

I riferimenti al manuale *Utilizzo di Client Security con Tivoli Access Manager* vengono forniti in questo documento. I responsabili della sicurezza che utilizzeranno Tivoli Access Manager per gestire gli oggetti di autenticazione per la politica UVM dovrebbero consultare il manuale *Utilizzo di Client Security con Tivoli Access Manager*.

Riferimenti al manuale *Guida per l'utente di Client Security*

I riferimenti al manuale *Guida per l'utente di Client Security* vengono forniti in questo documento. I responsabili possono utilizzare questa guida per impostare e gestire la politica UVM sui client IBM che utilizzano Client Security Software. Una volta che il responsabile ha impostato l'autenticazione utente e la politica di sicurezza UVM, un utente client può consultare il manuale *Guida per l'utente di Client Security* per comprendere le modalità di utilizzo di Client Security Software.

La Guida per l'utente contiene informazioni sull'esecuzione delle attività di Client Security Software, quali l'utilizzo di una protezione per il collegamento UVM, l'impostazione dello screen saver Client Security, la creazione di un certificato digitale e l'utilizzo di User Configuration Utility.

Ulteriori informazioni

E' possibile reperire ulteriori informazioni e aggiornamenti sui prodotti di sicurezza, quando sono disponibili, dal sito web IBM http://www.pc.ibm.com/ww/security/index.html.

Capitolo 1. Introduzione a IBM Client Security Software

Client Security Software è stato progettato per i computer IBM che utilizzano IBM embedded Security Chip per codificare i file e memorizzare chiavi di codifica. Questo software comprende applicazioni e componenti che consentono a client IBM di utilizzare client security su una rete locale, in azienda oppure su Internet.

Applicazioni e componenti di Client Security Software

Quando si installa Client Security Software, vengono installati anche i seguenti componenti e applicazioni software:

- **Administrator Utility:** Administrator Utility è l'interfaccia che un responsabile utilizza per attivare o disattivare IBM embedded Security Chip e per creare, archiviare e rigenerare le chiavi di codifica e i passphrase. Inoltre, un responsabile può utilizzare questo programma di utilità per aggiungere utenti alla politica di sicurezza fornita da Client Security Software.
- **UVM (User Verification Manager):** Client Security Software utilizza UVM per gestire passphrase e altri elementi che consentono l'autenticazione degli utenti del sistema. Ad esempio, un lettore di impronte digitali può essere utilizzato da UVM per l'autenticazione del collegamento. Il software UVM fornisce le seguenti funzioni:
  - **Protezione della politica client UVM:** Il software UVM consente ad un responsabile di impostare la politica di sicurezza del client, che indica come un utente client viene autenticato sul sistema.

    Se la politica indica che è necessario fornire le impronte digitali per il collegamento e l'utente non ha registrato tali impronte digitali, verrà visualizzata l'opzione per la registrazione delle impronte digitali come parte del collegamento. Inoltre, se viene richiesta la verifica delle impronte digitali e non è collegato uno scanner, UVM restituirà un errore. Inoltre, se la password di Windows non è stata registrata, oppure è stata registrata in modo errato, con UVM l'utente ha la possibilità di fornire la password corretta di Windows come parte del collegamento.
  - **Protezione del collegamento del sistema UVM:** Il software UVM consente ad un responsabile di controllare l'accesso al computer tramite interfaccia di collegamento. La protezione UVM verifica che solo gli utenti che sono riconosciuti dalla politica di sicurezza siano in grado di accedere al sistema operativo.
  - **Protezione dello screen saver di Client Security di UVM:** Il software UVM consente agli utenti di controllare l'accesso al computer tramite l'interfaccia di uno screen saver di Client Security.
- **Administrator Console:** Client Security Software Administrator Console consente ad un responsabile della protezione di eseguire le attività specifiche in remoto.
- **User Configuration Utility:**User Configuration Utility consente ad un utente client di modificare il passphrase UVM. In Windows 2000 o Windows XP, User Configuration Utility consente agli utenti di modificare le password di collegamento a Windows affinché siano riconosciute da UVM e per aggiornare gli archivi delle chiavi. Un utente può anche creare copie di backup di certificati digitali creati con IBM embedde Security Chip.

Funzioni PKI (Public Key Infrastructure)

Client Security Software fornisce tutti i componenti richiesti per creare una PKI (public key infrastructure) nella propria attività commerciale, quali:

- **Controllo responsabili sulla politica di sicurezza del client.** L'autenticazione degli utenti finali a livello di client rappresenta un problema di politica di sicurezza di rilevante importanza. Client Security Software fornisce l'interfaccia che è richiesta per gestire la politica di sicurezza di un client IBM. Questa interfaccia appartiene al software di autenticazione UVM (User Verification Manager), che rappresenta il componente principale di Client Security Software.
- **Gestione delle chiavi di codifica per la codifica delle chiavi pubbliche.** I responsabili creano le chiavi di codifica per l'hardware del computer e per gli utenti dei client con Client Security Software. Quando vengono create le chiavi di cifratura, esse risultano collegate a IBM embedded Security Chip tramite una gerarchia di chiavi, per cui una chiave hardware di livello base viene utilizzata per cifrare le chiavi dei livelli superiori, compreso le chiavi utente che sono associate ad ogni utente client. La cifratura e la memorizzazione delle chiavi su IBM embedded Security Chip aggiunge un ulteriore livello di sicurezza del client, poiché le chiavi vengono collegate in modo sicuro all'hardware del computer.
- **Creazione e memorizzazione del certificato digitale protetto da IBM embedded Security Chip.** Quando si richiede un certificato digitale che può essere utilizzato per firmare o cifrare digitalmente un messaggio e-mail, Client Security Software consente di selezionare IBM embedded Security Chip come provider dei servizi di cifratura per le applicazioni che utilizzano Microsoft CryptoAPI. Tali applicazioni includono Internet Explorer e Microsoft Outlook Express. In questo modo si è certi che la chiave privata del certificato digitale venga memorizzato su IBM embedded Security Chip. Inoltre, gli utenti di Netscape possono selezionare IBM embedded Security Chip come programmi di creazione delle chiavi private per i certificati digitali utilizzati per la sicurezza. Le applicazioni che utilizzano il PKCS (Public-Key Cryptography Standard) N.11, come Netscape Messenger, possono trarre vantaggi dalla protezione fornita da IBM embedded Security Chip.
- **La capacità di trasferire certificati digitali a IBM embedded Security Chip.** Certificate Transfer Tool di IBM Client Security Software consente di spostare certificati che sono stati creati con il CSP predefinito della Microsoft sul CSP di IBM embedded Security System. Ciò migliora notevolmente la protezione fornita sulle chiavi private associate ai certificati poiché verranno memorizzati in modo sicuro su IBM embedded Security Chip e non su software esposti.
- **Una soluzione per il recupero e l'archiviazione delle chiavi.** Una funzione PKI importante è la creazione di un archivio di chiavi da cui le chiavi possono essere ripristinate se le chiavi di origine risultano perse o danneggiate. Client Security Software fornisce un'interfaccia che consente di definire un archivio per le chiavi e i certificati digitali creati con IBM embedded Security Chip e di ripristinare, se necessario, tali chiavi e certificati.
- **Cifratura di file e cartelle.** La cifratura di file e cartelle consente ad un utente client di cifrare e decifrare file o cartelle in modo semplice e rapido. Quindi, fornisce un elevato livello di protezione dei dati insieme con le misure di protezione del sistema CSS.
- **Autenticazione delle impronte digitali.** IBM Client Security Software supporta per l'autenticazione l'utilità di lettura per le impronte digitali Targus PC Card e Targus USB. Per un corretto funzionamento, è necessario installare Client Security Software prima dei driver di periferica dei programmi di utilità per la lettura delle impronte digitali Targus.

- **Autenticazione Smart card.** IBM Client Security Software supporta alcune smart card come dispositivi di autenticazione. Client Security Software consente l'utilizzo delle smart card come token di autenticazione per un solo utente alla volta. Ciascuna smart card è legata a un sistema se non viene utilizzato il roaming delle credenziali. La richiesta di una smart card rende il sistema più protetto, in quanto è necessario fornire la smart card insieme con la password, che può essere compromessa.
- **Roaming delle credenziali.** Il roaming delle credenziali consente ad un utente della rete autorizzato UVM di utilizzare qualunque sistema della rete come propria stazione di lavoro. Una volta che l'utente è stato autorizzato ad utilizzare UVM su qualunque client registrato CSS, è possibile importare i dati personali su qualsiasi altro client registrato della rete. I dati personali verranno aggiornati automaticamente e memorizzati nell'archivio CSS e in ogni sistema in cui sono stati importati. L'aggiornamento dei dati personali come nuovi certificati o le modifiche dei passphrase saranno immediatamente disponibili su tutti i sistemi.
- **Certificazione FIPS 140-1.** Client Security Software supporta le librerie cifrate certificate FIPS 140-1. Le librerie RSA BSAFE certificate FIPS vengono utilizzate sui sistemi TCPA.
- **Scadenza passphrase.** Client Security Software stabilisce un passphrase specifico per l'utente e una politica di scadenza del passphrase per ciascun utente aggiunto a UVM.
- **Protezione automatica per le cartelle selezionate.** La funzione automatica di protezione delle cartelle consente ad un responsabile di Client Security Software di designare che ciascuna cartella relativa ai Documenti degli utenti sia protetta automaticamente, senza richiedere alcuna attività da parte degli utenti.

Capitolo 2. Cifratura di file e cartelle

Il programma di utilità IBM File and Folder Encryption, che può essere scaricato dal sito web di IBM Client Security, consente agli utenti Client Security Software di proteggere file e cartelle sensibili facendo clic con il tastino destro del mouse. Il modo in cui questo programma di utilità protegge i file e le cartelle dipende dalla codifica iniziale del file o della cartella. Leggere le seguenti informazioni per definire quali tecniche di cifratura dovrebbero essere utilizzate per proteggere i propri dati. IBM Client Security Software deve essere installato *prima* di installare il programma di utilità IBM File and Folder Encryption.

il programma di utilità Controllo disco potrebbe essere eseguito durante il riavvio del sistema operativo dopo aver protetto o rimosso la protezione delle cartelle. Verificare il sistema prima di utilizzare l'elaboratore.

Protezione dei file con il tastino destro del mouse

I file possono essere cifrati e decifrati manualmente con il menu contestuale che viene visualizzato facendo clic con il tastino destro del mouse. Quando i file vengono cifrati in questo modo, l'operazione di cifratura aggiunge un'estensione .enc ai file. Tali file cifrati possono quindi essere memorizzati in modo sicuro su server remoti. Rimangono, quindi cifrati e non disponibili per essere utilizzati dalle applicazioni fino a quando l'opzione del tastino destro del mouse non viene usata di nuovo per la decifrazione.

Protezione delle cartelle con il tastino destro

Un utente registrato UVM può selezionare una cartella da proteggere o meno tramite l'interfaccia visualizzata con il tastino destro del mouse. In tal modo, tutti i file contenuti nella cartella o nelle cartelle secondarie saranno cifrati. Quando i file vengono protetti in questo modo, non viene aggiunta alcuna estensione al nome file. Quando un'applicazione tenta di accedere ad un file in una cartella cifrata, il file verrà decifrato in memoria e verrà nuovamente cifrato prima di essere salvato sul disco fisso.

Tutte le operazioni Windows che tentano di accedere ad un file di una cartella protetta avranno accesso ai dati in una forma decifrata. Questa funzione ne migliora l'utilizzo in quanto non è necessario eseguire una decifrazione del file prima di utilizzarlo e, quindi, cifrarlo nuovamente al termine delle operazioni di un programma.

Stato di cifratura delle cartelle

IBM Client Security Software consente agli utenti di proteggere file e cartelle di particolare importanza utilizzando il tastino destro del mouse. Il modo in cui il software protegge un file e le cartelle differisce a seconda di come il file o la cartella viene cifrata inizialmente.

Una cartella può trovarsi in uno dei seguenti stati; ciascuno stato viene gestito in modo diverso dall'opzione di protezione della cartella con il tastino destro del mouse:

- **Cartella non protetta**

Questa cartella e tutte le relative cartelle secondarie sono state designate come protette. L'utente ha la possibilità di proteggere questa cartella.

- **Cartella protetta**

  Una cartella protetta può trovarsi in uno dei seguenti stati:

  – **Protetta dall'utente corrente**

    L'utente corrente ha designato questa cartella come protetta. Tutti i file sono cifrati, compreso i file presenti nelle cartelle secondarie. L'utente ha la possibilità di annullare la protezione della cartella.

  – **Una cartella secondaria di una cartella protetta dall'utente corrente**

    L'utente corrente ha designato una di queste cartelle principali come protetta. Tutti i file sono cifrati. L'utente corrente non ha l'opzione del tastino destro.

  – **Protetta da un utente diverso**

    Un utente diverso ha designato questa cartella come protetta. Tutti i file sono cifrati, compreso i file presenti in tutte le cartelle secondarie e non sono disponibili all'utente corrente. L'utente corrente non ha l'opzione del tastino destro.

- **Cartella principale di una cartella protetta**

  Una cartella principale di una cartella protetta può trovarsi in uno dei tre stati:

  – **Può contenere una o più cartelle secondarie protette dall'utente corrente**

    L'utente corrente ha designato una o più cartelle secondarie come protette. Tutti i file nelle cartelle secondarie protette sono cifrati. L'utente ha la possibilità di proteggere la cartella principale.

  – **Può contenere una o più cartelle secondarie protette da uno o più utenti diversi.**

    Un utente o più utenti diversi hanno designato una o più cartelle secondarie come protette. Tutti i file nelle cartelle secondarie protette sono cifrati e non sono disponibili all'utente corrente. L'utente corrente non ha l'opzione del tastino destro.

  – **Può contenere cartelle secondarie protette dall'utente corrente e uno o più utenti diversi**

    Sia l'utente corrente che uno o più utenti diversi hanno designato le cartelle secondarie come protette. L'utente corrente non ha l'opzione del tastino destro.

- **Cartella critica**

  Una cartella critica è una cartella che si trova in un percorso critico e, quindi, non può essere protetto. Esistono due percorsi critici: il percorso Windows e il percorso di Client Security.

Ciascuno stato viene gestito in modo diverso mediante l'opzione con il tastino destro del mouse.

Suggerimenti per il programma di utilità FFE (File and Folder Encryption)

Le informazioni di seguito riportate potrebbero essere utili durante l'esecuzione di alcune funzioni di cifratura di file e cartelle.

Protezione dell'unità disco fisso

E' possibile utilizzare il programma di utilità IBM FFE per cifrare file e cartelle solo sull'unità C. Il programma di utilità IBM FFE non supporta la cifratura su altre partizioni del disco fisso o unità fisiche.

Eliminazione di cartelle e file protetti

Affinché le cartelle e i file sensibili non siano lasciati non protetti nel cestino, utilizzare la combinazione di tasti Maiusc+Canc per eliminare le cartelle e i file protetti. La sequenza di tasti Maiusc+Canc effettua un'operazione di eliminazione incondizionata evitando di spostare i file nel cestino.

Prima di aggiornare una versione precedente del programma di utilità IBM FFE

Se si desidera aggiornare una versione precedente del programma di utilità IBM FFE (versione 1.04 o precedente) e si dispone di cartelle protette su unità diverse da C, prima di installare la versione 1.05 del programma di utilità IBM FFE, rimuovere la protezione da tali cartelle. Se si desidera proteggere nuovamente tali cartelle dopo l'installazione della versione 1.05, è necessario prima spostare le suddette cartelle sull'unità C, quindi proteggerle nuovamente.

Prima della disinstallazione del programma di utilità IBM FFE

Prima di disinstallare il programma di utilità IBM FFE, utilizzare IBM FFE per rimuovere la protezione dalle cartelle e dai file protetti.

Limitazioni del programma di utilità FFE (File and Folder Encryption)

Il programma di utilità IBM FFE utility presenta le limitazioni di seguito riportate:

Limitazioni relative allo spostamento di cartelle e file protetti

Il programma di utilità IBM FFE non supporta le operazioni di seguito riportate:

- Spostamento di file e cartelle che si trovano in cartelle protette
- Spostamento di file o cartelle tra cartelle protette e non protette

Se si tenta di eseguire tali operazioni di spostamento non supportate, viene visualizzato il messaggio del sistema operativo ″Accesso negato″. Questo messaggio è nella norma. Notifica solo che l'operazione di spostamento non è supportata. In alternativa all'operazione di spostamento, effettuare le operazioni di seguito riportate:

1. Copiare le cartelle e i file protetti nella nuova ubicazione.
2. Eliminare le cartelle e i file di origine utilizzando la combinazione di tasti Maiusc+Canc.

Limitazioni relative all'esecuzione delle applicazioni

Il programma di utilità IBM FFE non supporta l'esecuzione delle applicazioni da una cartella protetta. Ad esempio, se si dispone di un eseguibile denominato PROGRAM.EXE, non è possibile eseguire tale applicazione da una cartella protetta.

Limitazioni relative alla lunghezza del nome del percorso

Se si tenta di proteggere una cartella utilizzando il programma di utilità IBM FFE oppure di copiare o spostare un file o una cartella da una cartella non protetta a una cartella protetta, probabilmente verrà visualizzato il messaggio del sistema

operativo ″Uno o più nomi di percorso sono troppo estesi″. Se si riceve questo messaggio, uno o più file o cartelle dispongono di un nome di percorso che eccede il numero massimo di caratteri consentiti. Per risolvere il problema, riorganizzare la struttura ad albero delle cartelle riducendola oppure ridenominare i file o le cartelle con nomi più brevi.

Problemi relativi alla protezione delle cartelle

Se si tenta di proteggere una cartelle e viene visualizzato il messaggio "Impossibile proteggere la cartella. Uno o più file potrebbero essere in uso," verificare quanto segue:

- Verificare che nessun file contenuto nella cartella sia al momento in uso.
- Se Esplora risorse visualizza una o più cartelle secondarie di una cartella che si sta tentando di proteggere, assicurarsi che la cartella da proteggere sia evidenziata e attiva, ma che non lo siano le cartelle secondarie.

Capitolo 3. Come utilizzare Client Security Software

I responsabili possono utilizzare più componenti forniti da Client Security Software per impostare le funzioni di sicurezza che gli utenti client IBM richiedono. Utilizzare i seguenti esempi per comprendere come pianificare la propria configurazione e politica Client Security. Ad esempio, gli utenti Windows NT possono configurare la protezione UVM per il collegamento al sistema per impedire ad utenti non autorizzati di collegarsi al client IBM.

Esempio 1 - Un client Windows 2000 e un client Windows XP che utilizzano Outlook Express

In questo esempio, su un client IBM (client 1) è installato Windows 2000 e Outlook Express, sull'altro client (client 2) è installato Windows XP e Outlook Express. Tre utenti richiederanno la configurazione di autenticazione con UVM sul client 1; un utente client richiederà la configurazione di autenticazione con UVM sul client 2. Tutti gli utenti client registreranno le proprie impronte digitali in modo che possano essere utilizzate per l'autenticazione. Durante questo esempio, verrà installato un sensore per il rilevamento delle impronte digitali compatibile con UVM. E' stato definito, inoltre, che entrambi i client richiederanno la protezione UVM per il collegamento a Windows. Il responsabile ha deciso che la politica UVM locale sarà modificata e utilizzata su ciascun client.

Per impostare client security, completare la seguente procedura:

1. Installare il software sul client 1 e client 2. Per ulteriori dettagli, fare riferimento a *Guida all'installazione di Client Security Software*.
2. Installare i sensori per il rilevamento delle impronte digitali compatibili con UVM e tutto il software associato su ciascun client.

   Per ulteriori informazioni sui prodotti compatibili con UVM, passare al sito http://www.pc.ibm.com/ww/security/secdownload.html sul web.
3. Impostare l'autenticazione utente con UVM per ciascun client. Effettuare le seguenti operazioni:
   a. Aggiungere gli utenti a UVM assegnando loro un passphrase UVM. Poiché il client 1 ha tre utenti, è necessario ripetere il processo per aggiungere gli utenti a UVM fino a quando sono stati aggiunti tutti gli utenti.
   b. Configurare la protezione UVM per il collegamento a Windows per ciascun client.
   c. Registrare le impronte digitali degli utenti. Poiché una politica verrà impostata indicando che tre utenti utilizzeranno il client 1, tutti e tre gli utenti devono registrare le proprie impronte.

      Nota: Se si configura l'impostazione per cui l'impronta digitale è un requisito per l'autenticazione come parte della politica UVM per un client, ciascun utente deve registrare le proprie impronte digitali.
4. Modificare e salvare una politica UVM locale per ciascun client che richiede l'autenticazione per quanto viene riportato di seguito:
   - Collegamento al sistema operativo
   - Acquisizione di un certificato digitale
   - Utilizzo di una firma digitale per i messaggi e-mail

5. Riavviare ciascun client per abilitare la protezione UVM per il collegamento a Windows.
6. Comunicare agli utenti i passphrase UVM che sono stati impostati per loro e i requisiti di autenticazione che sono stati impostati nella politica UVM per il client IBM.

Gli utenti del client possono eseguire le attività riportate di seguito:

- Utilizzare la protezione UVM per bloccare e sbloccare il sistema operativo.
- Richiedere un certificato digitale e selezionare IBM embedded Security Chip come provider dei servizi cifrati associati al certificato.
- Utilizzare il certificato digitale per cifrare i messaggi e-mail creati con Outlook Express.

Esempio 2 - Due client IBM con Windows 2000 che utilizzano Lotus Notes e lo screen saver di Client Security

In questo esempio, sui due client IBM (client 1 e client 2) sono installati sia Windows 2000 che Lotus Notes. Due utenti richiederanno la configurazione di autenticazione con UVM sul client 1; un utente richiederà la configurazione di autenticazione con UVM sul client 2. Entrambi i client richiederanno la protezione UVM per il collegamento al sistema e utilizzeranno lo screen saver di Client Security e la protezione UVM per Lotus Notes. Il responsabile ha stabilito che una politica UVM per i client remoti sarà modificata sul client 1 e, quindi, copiata sul client 2.

Per impostare client security, completare la seguente procedura:

1. Installare il software sui client 1 e client 2. Poiché verrà utilizzata una politica UVM per i client remoti, è necessario utilizzare la stessa chiave pubblica admin utilizzata in fase di installazione del software su entrambi i client 1 e 2. Per dettagli sull'installazione del software, consultare la *Guida all'installazione di Client Security Software*.
2. Impostare l'autenticazione utente con UVM per ciascun client. Quindi, procedere nel modo seguente:
   a. Aggiungere gli utenti a UVM assegnando loro un passphrase UVM. Poiché il client 1 ha due utenti, è necessario ripetere il processo per aggiungere utenti a UVM fino a quando sono stati aggiunti entrambi gli utenti.
   b. Configurare la protezione UVM per il collegamento a Windows su ciascun client.
3. Abilitare la protezione UVM per Lotus Notes su entrambi i client. Per ulteriori informazioni, consultare la sezione "Utilizzo della protezione UVM per Lotus Notes" a pagina 19.
4. Modificare e salvare una politica UVM per i client remoti sul client 1 e, quindi, copiarla sul client 2. La politica UVM richiederà l'autenticazione utente per rimuovere lo screen saver, per il collegamento a Lotus Notes e il collegamento al sistema operativo. Per ulteriori dettagli, consultare la sezione "Modifica e utilizzo della politica UVM per i client remoti" a pagina 29.
5. Riavviare ciascun client per abilitare la protezione UVM per il collegamento al sistema.
6. Comunicare agli utenti client i passphrase UVM e la politica che è stata impostata per ciascun client.

Gli utenti possono, quindi, consultare la *Guida per l'utente di Client Security Software* per eseguire le attività riportate di seguito:

- Abilitare lo screen saver di Client Security
- Utilizzare la protezione UVM per Windows 2000

Esempio 3 - Numerosi client IBM con Windows 2000 che vengono gestiti da Tivoli Access Manager e che utilizzano Netscape per le e-mail

L'utente per cui è stato progettato il seguente esempio è un responsabile di azienda che desidera utilizzare Tivoli Access Manager per gestire gli oggetti di autenticazione che vengono impostati dalla politica UVM. In questo esempio, sui client IBM sono installati sia Windows 2000 che Netscape. Su tutti i client è installato NetSEAT client, un componente di Tivoli Access Manager. Su tutti i client che utilizzano un server LDAP è installato il client LDAP. La politica UVM per i client remoti verrà installata su tutti i client. La politica UVM consentirà a Tivoli Access Manager di controllare gli oggetti di autenticazione selezionati per i client.

In questo esempio, un utente richiederà la configurazione di autenticazione con UVM su ciascun client. Tutti gli utenti registreranno le proprie impronte digitali in modo che possano essere utilizzate per l'autenticazione. Durante questo esempio, verrà installato un sensore per il rilevamento delle impronte digitali, compatibile con UVM, e tutti client richiederanno la protezione UVM per il collegamento a Windows.

Per impostare client security, completare la seguente procedura:

1. Installare il componente Client Security sul server Tivoli Access Manager. Per ulteriori dettagli, fare riferimento alla guida *Utilizzo di Client Security con Tivoli Access Manager*.
2. Installare Client Security Software su tutti i client. Poiché verrà utilizzata una politica UVM per i client remoti, è necessario utilizzare la stessa chiave pubblica admin utilizzata durante l'installazione del software su tutti i client. Per ulteriori dettagli sull'installazione del software, consultare la *Guida all'installazione di Client Security Software*.
3. Installare i sensori per il rilevamento delle impronte digitali compatibili con UVM e tutto il software associato su ciascun client. Per informazioni sui prodotti disponibili compatibili con UVM, passare al sito http://www.pc.ibm.com/ww/security/secdownload.html sul web.
4. Configurare l'autenticazione utente con UVM su ciascun client. Per le informazioni dettagliate, consultare la sezione "Rimozione degli utenti" a pagina 15. Quindi, procedere nel modo seguente:
   a. Aggiungere gli utenti a UVM assegnando loro un passphrase UVM.
   b. Configurare la protezione UVM per il collegamento a Windows su ciascun client.
   c. Registrare le impronte digitali per ciascun utente client. Se l'autenticazione delle impronte digitali viene richiesto su un client IBM, tutti gli utenti di quel client devono registrare le proprie impronte digitali.
5. Configurare le informazioni sulla configurazione di Tivoli Access Manager su ciascun client. Per ulteriori dettagli, fare riferimento alla guida *Utilizzo di Client Security con Tivoli Access Manager*.

6. Modificare e salvare una politica UVM per i client remoti su uno dei client e, quindi, copiarla sugli altri client. Impostare la politica UVM in modo che Tivoli Access Manager controlli i seguenti oggetti di autenticazione:
   - Collegamento al sistema operativo
   - Acquisizione di un certificato digitale
   - Utilizzo di una firma digitale per i messaggi e-mail

   Per ulteriori dettagli, consultare la sezione “Modifica e utilizzo della politica UVM per i client remoti” a pagina 29.
7. Riavviare ciascun client per abilitare la protezione UVM per il collegamento a Windows.
8. Installare il modulo PKCS#11 di IBM embedded Security Chip su ciascun client. Questo modulo fornisce il supporto per la cifratura sui client che utilizzano Netscape per l’invio e la ricezione di messaggi e-mail e IBM embedded Security Chip per l’acquisizione di certificati digitali. Per ulteriori informazioni, fare riferimento alla guida *Guida all’installazione di Client Security Software*.
9. Abilitare Tivoli Access Manager per controllare gli oggetti IBM Client Security Solutions che vengono visualizzati in Tivoli Access Manager Management Console.
10. Comunicare agli utenti client i passphrase UVM che sono stati impostati e la politica che è stata impostata per ciascun client.
11. Consultare la *Guida per l’utente di Client Security Software* per eseguire le attività riportate di seguito:
    - Utilizzare la protezione UVM per bloccare e sbloccare il sistema operativo
    - Utilizzare User Configuration Utility
    - Richiedere un certificato digitale che utilizza il Security Chip integrato come provider dei servizi di cifratura associati con il certificato
    - Utilizzare il certificato digitale per cifrare i messaggi e-mail creati con Netscape

Capitolo 4. Autorizzazione degli utenti

Le seguenti informazioni sono utili quando si autorizzano gli utenti di Windows ad utilizzare UVM (User Verification Manager).

Autenticazione per utenti client

L'autenticazione degli utenti finali a livello di client è un problema di sicurezza del computer di rilevante importanza. Il programma Client Security Software fornisce l'interfaccia, che viene richiesta per gestire la politica di sicurezza di un client IBM. Questa interfaccia appartiene al software di autenticazione, UVM (User Verification Manager), che rappresenta il principale componente di Client Security Software.

La politica di sicurezza UVM per un client IBM può essere gestita in due modi:

- In modo locale, utilizzando un editor di politiche che risiede sul client IBM
- In tutta l'azienda, utilizzando Tivoli Access Manager

Le chiavi di cifratura dell'hardware vengono generati quando si aggiunge il primo utente.

Elementi di autenticazione

Gli elementi di autenticazione (quali passphrase UVM oppure impronte digitali dell'utente) vengono utilizzati per autorizzare gli utenti con il client IBM. Quando si autorizza un utente di Windows ad utilizzare UVM, viene assegnata una passphrase UVM per l'utente client. Il passphrase UVM, che può contenere fino a 256 caratteri è l'elemento di autenticazione principale utilizzato da UVM. Quando si assegna un passphrase UVM, vengono creare le chiavi cifrate dell'utente per quell'utente client e memorizzate in un singolo file che viene gestito da IBM embedded Security Chip. Se il client IBM utilizza una periferica compatibile con UVM per l'autenticazione, l'elemento di autenticazione, ad esempio impronte digitali, devono essere registrate con UVM.

Durante la configurazione dell'autenticazione utente, è possibile selezionare le seguenti funzioni di sicurezza fornite da Client Security Software:

- **Protezione UVM per il collegamento al sistema operativo.** La protezione UVM verifica che solo gli utenti che vengono riconosciuti da UVM siano in grado di accedere al computer. Prima di abilitare la protezione UVM per il collegamento al sistema, consultare la sezione Impostazione della protezione per il collegamento al sistema operativo di UVM.
- **Screen saver di Client Security.** Dopo aver aggiunto un utente client, l'utente può impostare e utilizzare lo screen saver Client Security. Lo screen saver Client Security è impostato tramite l'opzione Schermo presente all'interno del sistema operativo.

Prima di autorizzare gli utenti

Importante: autorizzare solo gli account utenti che possono essere utilizzati per collegarsi al sistema operativo. Se un account utente, che *non può* essere utilizzato per collegarsi al sistema operativo, è autorizzato, **tutti** gli utenti saranno bloccati dal sistema quando la protezione al collegamento a UVM viene abilitata.

Quando si autorizza un utente client, Administrator Utility fornisce un elenco di nomi utente da cui è possibile effettuare una selezione. I nomi nell'elenco sono gli account degli utenti che sono stati aggiunti utilizzando il sistema operativo. Prima di aggiungere gli utenti al client su UVM, utilizzare il software del sistema operativo per creare gli account utenti e i profili per quegli utenti. Client Security Software viene eseguito insieme alle funzioni di sicurezza fornite dal sistema operativo.

Windows XP e Windows 2000.

Utilizzare il programma Utenti e Password per creare nuovi account utenti e gestire account o gruppi di utenti. Per ulteriori informazioni, fare riferimento alla documentazione relativa al sistema operativo.

In Windows XP, il campo Seleziona Utenti di Windows da autorizzare non viene aggiornato quando si seleziona il pulsante **crea nuovo Utente di Windows**. E' necessario uscire e riavviare Administrator Utility per aggiornare questo campo.

Nota:

1. Quando si utilizza il software del sistema operativo per creare nuovi utenti, la password di dominio per ciascun nuovo utente deve essere la stessa.
2. Non autorizzare un utente, il cui nome utente di Windows è stato precedentemente modificato. UVM punterà al primo nome utente mentre con Windows riconoscerà solo il nuovo nome utente.
3. Quando un account utente che è stato autorizzato viene cancellato da Windows, l'interfaccia di protezione di collegamento a UVM continua erroneamente ad elencare l'account come un account che può essere utilizzato per collegarsi a Windows. Questo account *non può* essere utilizzato per collegarsi a Windows.
4. Una volta autorizzato un utente, non modificare il relativo nome utente Windows. In caso contrario, sarà necessario autorizzare nuovamente il nuovo nome utente e richiedere tutte le nuove credenziali.

Autorizzazione degli utenti

Gli utenti devono registrarsi con i privilegi dell'utente responsabile per utilizzare Administrator Utility.

Per autorizzare gli utenti con UVM, completare la seguente procedura:

1. Dal desktop di Windows del client IBM, fare clic su **Start > Impostazioni > Pannello di controllo > IBM Client Security Subsystem**.

   Viene visualizzato il messaggio Inserisci password del responsabile.
2. Immettere la password del responsabile e fare clic su **OK**.

   Viene visualizzata la finestra principale di IBM Security Subsystem Administrator Utility.
3. Nel campo Seleziona utente di Windows da autorizzare, selezionare un nome utente dall'elenco.

   Nota: i nomi utenti nell'elenco vengono definiti dagli account utente creati nel sistema operativo o sulla rete.
4. Fare clic su **Autorizza**.

   Viene visualizzata la finestra Installazione di autenticazione dell'utente.

5. Inserire e confermare un passphrase iniziale UVM (User Verification Manager) per l'utente autorizzato di recente e fare clic su **Avanti**.

   Se il passphrase non soddisfa i requisiti per la politica di sicurezza, viene visualizzata una finestra relativa all'immissione errata del passphrase. Se si verifica tale situazione, fare clic su **OK** e poi su **Visualizza requisiti del passphrase** per visualizzare i parametri, che devono essere soddisfatti da un valido passphrase.

   Quando il passphrase viene accettato, viene visualizzato un messaggio che indica il completamento corretto dell'operazione.

6. Per continuare, fare clic su **OK**.

   Viene visualizzata la finestra Password di collegamento di Windows. Se è abilitato il collegamento protetto UVM, è necessario che la password corrente di Windows dell'utente sia memorizzata in modo tale che l'utente può collegarsi al sistema. Tale finestra consente al responsabile di:

   - **Memorizzare la password corrente di Windows dell'utente.** Per memorizzare la password corrente di Windows dell'utente, immettere e confermare la password dell'utente nei campi forniti e fare clic su **Avanti**.

     Nota: la password immessa deve corrispondere alla password corrente di Windows dell'utente. Tale impostazione non influenza la password memorizzata con il sistema operativo.

   - **L'utente deve memorizzare la relativa password di Windows successivamente mediante User Configuration Utility.** Per permettere all'utente di memorizzare la relativa password di Windows successivamente utilizzando il programma User Configuration Utility, selezionare il pallino appropriato e fare clic su **Avanti**.

   Viene visualizzato un messaggio che indica che l'operazione è stata completata correttamente.

7. Fare clic su **Fine**.

Rimozione degli utenti

Gli utenti devono registrarsi con i privilegi dell'utente responsabile per utilizzare Administrator Utility.

Per annullare l'autorizzazione degli utenti in UVM, completare la seguente procedura:

1. Dal desktop di Windows del client IBM, fare clic su **Start > Impostazioni > Pannello di controllo > IBM Client Security Subsystem**.

   Viene visualizzato il messaggio Inserisci password del responsabile.

2. Immettere la password del responsabile e fare clic su **OK**.

   Viene visualizzata la finestra principale di IBM Security Subsystem Administrator Utility.

3. Nell'area Utenti di Windows autorizzati ad utilizzare UVM, selezionare un nome utente dall'elenco.

4. Fare clic su **Rimuovi utente**.

   Viene visualizzato un messaggio che indica che le informazioni di sicurezza dell'utente selezionato, incluse tutte le password memorizzate e le impronte digitali registrate, i certificati e le chiavi esistenti dell'utente saranno perse.

5. Per continuare, fare clic su **Sì**.

Viene visualizzato un messaggio che richiede se si desidera rimuovere le informazioni archiviate dell'utente. Se si rimuovono tali informazioni, l'utente non sarà in grado di ripristinare qualsiasi impostazione salvata precedentemente su qualsiasi sistema.

6. Per completare l'operazione, fare clic su **Sì**.

Creazione di nuovi utenti

Gli utenti devono registrarsi con i privilegi dell'utente responsabile per utilizzare Administrator Utility.

Per creare nuovi utenti, completare la seguente procedura:

1. Dal desktop di Windows del client IBM, fare clic su **Start > Impostazioni > Pannello di controllo > IBM Client Security Subsystem**.

   Viene visualizzato il messaggio Inserisci password del responsabile.
2. Immettere la password del responsabile e fare clic su **OK**.

   Viene visualizzata la finestra principale di IBM Security Subsystem Administrator Utility.
3. Nel campo Seleziona utenti di Windows da autorizzare, fare clic su **Crea nuovo utente di Windows**.

   Viene visualizzata la finestra Account utenti di Windows.
4. Fare clic su **Crea un nuovo account**.
5. Definire il nuovo account inserendo un nome nel campo fornito; quindi, fare clic su **Avanti**.
6. Scegliere un nome account selezionando il pallino appropriato.
7. Fare clic su **Crea account**.
8. Ritornare alla finestra IBM Client Security Subsystem Administrator Utility.

   Il nuovo account utente viene visualizzato nell'area Seleziona utente di Windows da autorizzare.

Capitolo 5. Operazioni da eseguire dopo aver autorizzato gli utenti in UVM

Una volta che gli utenti sono stati autorizzati, è possibile eseguire un'altra serie di funzioni di Client Security, quali:

- **Impostazione della protezione UVM per il collegamento al sistema operativo.** Per ulteriori informazioni, consultare la sezione "Impostazione della protezione per il collegamento al sistema operativo di UVM".
- **Archiviazione delle chiavi di cifratura utente.** Per ulteriori informazioni, consultare la sezione "Modifica dell'ubicazione dell'archivio di chiavi" a pagina 33.
- **Impostazione dello screen saver di Client Security.** Per ulteriori informazioni, consultare il Capitolo 8, "Istruzioni per gli utenti client", a pagina 41.
- **Registrazione delle impronte digitali degli utenti con UVM.** Per ulteriori informazioni, consultare la sezione "Registrazione delle impronte digitali degli utenti con UVM" a pagina 18.

  Se un sensore per il rilevamento delle impronte digitali compatibile con UVM è stato installato prima di aggiungere gli utenti a UVM, la registrazione delle impronte digitali può essere effettuata in quel momento.

Protezione per il collegamento al sistema operativo di UVM

La protezione del collegamento al sistema UVM migliora la funzione della della password fornita con il proprio sistema operativo. L'interfaccia del collegamento UVM sostituisce il collegamento del sistema operativo, in modo tale che la finestra del collegamento UVM viene visualizzata ogni volta che un utente tenta di collegarsi al sistema.

Impostazione della protezione per il collegamento al sistema operativo di UVM

Seguire le informazioni riportate prima di impostare e utilizzare la protezione UVM per il collegamento al sistema:

- Se la politica UVM indica che l'autenticazione delle impronte digitali viene richiesta per il collegamento ai sistemi e l'utente non ha registrato le proprie impronte digitali, è necessario che l'utente registri le proprie impronte digitali per poter eseguire il collegamento.

  Inoltre, se la password di Windows dell'utente non è registrata (oppure è stata registrata in modo errato) con UVM, l'utente deve fornire la password corretta di Windows per collegarsi.
- Non eliminare IBM embedded Security Chip mentre è abilitata la protezione UVM. In caso contrario, verrà bloccato il sistema. Per ulteriori informazioni, consultare la sezione "Suggerimenti del responsabile" presente nel Capitolo 9, "Risoluzione dei problemi", a pagina 47.
- Se si deseleziona la casella **Sostituisci il collegamento standard di Windows con il collegamento protetto di UVM** in Administrator Utility, il sistema torna al processo di collegamento di Windows senza utilizzare la protezione al collegamento UVM.

- Se si sostituisce il collegamento standard di Windows con il collegamento protetto UVM e si abilita la funzione Cisco LEAP, è necessario reinstallare Cisco ACU (Aironet Client Utility).

Impostazione della protezione per il collegamento al sistema operativo di UVM

Per impostare la protezione UVM per il proprio sistema operativo, completare la seguente procedura:

1. Dal desktop di Windows del client IBM, fare clic su **Start > Impostazioni > Pannello di controllo > IBM Client Security Subsystem**.

   Viene visualizzata la finestra principale di Administrator Utility.
2. Fare clic su **Configura politiche e supporto applicazioni**.

   Viene visualizzato il pannello Configurazione della politica e applicazione UVM.
3. Selezionare la casella **Sostituisci il collegamento standard di Windows con il collegamento protetto di UVM**.
4. Fare clic su **OK**.
5. Riavviare il computer.

Quando il computer viene riavviato, verrà richiesto di collegarsi al computer. Per ulteriori informazioni sulla protezione UVM, consultare la sezione “Protezione per il collegamento al sistema operativo di UVM” a pagina 17.

Registrazione delle impronte digitali degli utenti con UVM

Quando una politica UVM è stata modificata in modo tale da includere l’autenticazione delle impronte digitali, sarà necessario che ciascun utente registri le proprie impronte digitali con UVM.

Nota: Windows XP non supporta i sensori per il rilevamento delle impronte digitali Digital Persona U.are.U Pro.

Per registrare le impronte digitali di un utente con UVM, completare la seguente procedura di Administrator Utility:

1. Nell’area Utenti di Windows autorizzati ad utilizzare UVM, selezionare un nome utente dall’elenco.
2. Fare clic su **Modifica utente**.

   Viene visualizzata la finestra Modifica configurazione chiave di Client Security - Modifica attributi utente UVM.
3. Selezionare la casella **Registrarsi con la periferica compatibile con UVM** e fare clic su **Avanti**.

   Viene visualizzata la finestra Modifica configurazione chiave di Client Security - Unità abilitate UVM.
4. Fare clic su **Registra impronte digitali utente**.
5. Nell’area Seleziona una mano, fare clic su **Sinistra** o **Destra**.
6. Nell’area Seleziona un dito, fare clic sul dito che si desidera eseguire una scansione e fare clic su **Avvia registrazione**.
7. Posizionare il dito sul sensore per il rilevamento delle impronte digitali che utilizza UVM e seguire le istruzioni visualizzate.

A seconda del modello di scanner, potrebbe essere necessario eseguire quattro volte la scansione di ciascuna impronta digitale. Fare clic su **Annulla questo dito** per annullare la scansione delle impronte digitali.

8. Specificare un altro dito da registrare oppure fare clic su **Esci** per terminare.

Utilizzo della protezione UVM per Lotus Notes

UVM fornisce una funzione di protezione della sicurezza migliorato per gli utenti Lotus Notes.

Abilitazione e configurazione della protezione UVM per un ID utente di Lotus Notes

Prima di poter abilitare la protezione UVM per Lotus Notes, è necessario installare Notes sul client IBM, definire un ID utente Notes e una password per l'utente e autorizzare l'utente Notes ad utilizzare UVM.

Per impostare la protezione UVM per Lotus Notes,eseguire la seguente procedura:

1. Dal desktop di Windows del client IBM, fare clic su **Start > Impostazioni > Pannello di controllo > IBM Client Security Subsystem**.

   Viene visualizzata la finestra principale di Administrator Utility.
2. Fare clic su **Configura politiche e supporto applicazioni**.

   Viene visualizzato il pannello Configurazione della politica e applicazione UVM.
3. Selezionare la casella **Abilita supporto Lotus Notes**.

   La protezione UVM per un ID utente di Lotus Notes è abilitata. Se necessario, continuare con i seguenti passi facoltativi per configurare la politica per il collegamento di Lotus Notes.
4. Fare clic su **Politica applicativa**.

   Viene visualizzato il pannello Modifica configurazione politica di Client Security.
5. Fare clic su **Modifica politica**.
6. Immettere la password del responsabile e fare clic su **OK**. Viene visualizzata la finestra Politica IBM UVM: Collegamento di Lotus Notes.
7. Nel separatore Selezione dell'oggetto, selezionare Collegamento a Lotus Notes nel menu a discesa Azione.
8. Nel separatore Elementi di autenticazione, selezionare gli elementi di autenticazione che si desidera richiedere per il Collegamento a Lotus Notes.
9. Fare clic su **Applica** per salvare le selezioni effettuate.

   Viene visualizzata la finestra Chiave privata admin richiesta.
10. Specificare la posizione della Chiave privata immettendo il nome del percorso nel campo fornito oppure facendo clic su **Sfoglia** e selezionando la cartella appropriata.
11. Fare clic su **OK**.

    La finestra IBM UVM (User Verification Manager): Riepilogo della politica visualizza un riepilogo degli oggetti controllati dalla politica del client locale.
12. Avviare Lotus Notes.

    La registrazione della password UVM è completa all'avvio di Lotus Notes.

Utilizzo della protezione UVM con Lotus Notes

Prima di poter utilizzare la protezione UVM per Lotus Notes, è necessario seguire la procedura contenuta nella sezione “Impostazione della protezione UVM con Lotus Notes”.

Impostazione della protezione UVM con Lotus Notes

Per impostare la protezione UVM con Lotus Notes, procedere nel modo seguente:

1. Collegarsi a Lotus Notes.

   Viene visualizzata la finestra IBM User Verification Manager.
2. Inserire e verificare la propria password di Lotus Notes nei campi disponibili.

   La password di Lotus Notes viene quindi registrata con UVM.

Re-impostazione della password di Lotus Notes

Per re-impostare la password di Lotus Notes, procedere nel modo seguente:

1. Collegarsi a Lotus Notes.
2. Dalla barra dei menu di Lotus Notes, fare clic su **File > Strumenti > ID utente**.

   Viene visualizzata la finestra IBM User Verification Manager.
3. Inserire il proprio passphrase UVM e fare clic su **OK**.

   Viene visualizzata la finestra ID utente.
4. Fare clic su **Imposta password**.

   Viene visualizzata la finestra IBM User Verification Manager.
5. Selezionare il pallino **Crea password**.
6. Inserire e verificare la nuova password di Lotus Notes nei campi disponibili e fare clic su **OK**.

Nota: quando si modifica la password all’interno di Lotus Notes con un valore che è stato utilizzato precedentemente, Notes rifiuta la modifica della password, ma non lo comunica a Client Security Software. Di conseguenza, UVM memorizza la password che Notes ha rifiutato.

Se viene visualizzato un messaggio che indica che la password è stata utilizzata prima durante la modifica della password in Lotus Notes, sarà necessario chiudere Lotus Notes, avviare User Configuration Utility e ripristinare la password di Lotus Notes al valore precedente.

Se la password di Lotus Notes è stata generata in modo casuale e viene visualizzato questo errore, non sarà possibile conoscere la password precedente e, quindi, reimpostarla manualmente. E’ necessario richiedere un nuovo file di ID dal proprio responsabile oppure ripristinare una copia del file di ID precedentemente salvato.

Disabilitazione della protezione UVM per un ID utente di Lotus Notes

Se si desidera disabilitare la protezione UVM per un ID utente di Lotus Notes, procedere nel modo seguente:

1. Dal desktop di Windows del client IBM, fare clic su **Start > Impostazioni > Pannello di controllo > IBM Client Security Subsystem**. Dopo aver immesso la password, viene visualizzata l

   a finestra principale di Administrator Utility.
2. Fare clic su **Configura politiche e supporto applicazioni**.

Viene visualizzato il pannello Configurazione della politica e applicazione UVM.

3. Deselezionare la casella **Abilita supporto Lotus Notes**.
4. Fare clic su **OK**.

   Viene visualizzato il pannello Azioni del supporto applicativo con un messaggio che indica che il supporto Lotus Notes è stato disabilitato.

Impostazione della protezione UVM per un ID utente Lotus Notes diverso

Per passare da un ID utente con protezione UVM abilitato ad un altro ID utente, effettuare le seguenti operazioni:

1. Uscire da Lotus Notes.
2. Disabilitare la protezione UVM per l'ID utente corrente. Per informazioni dettagliate, consultare la sezione "Disabilitazione della protezione UVM per un ID utente di Lotus Notes" a pagina 20.
3. Immettere Lotus Notes e cambiare ID utente. Per ulteriori informazioni sul passaggio tra gli ID utenti, fare riferimento alla documentazione relativa a Lotus Notes.
4. Per impostare la protezione UVM per l'ID utente selezionato, avviare lo strumento di configurazione di Lotus Notes (fornita da Client Security Software) e impostare la protezione UVM. Consultare la sezione "Utilizzo della protezione UVM con Lotus Notes" a pagina 20.

Utilizzo di Client Security Software con applicazioni Netscape

Le istruzioni fornite in questa sezione sono specifiche per l'utilizzo di Client Security Software in relazione all'emissione e all'utilizzo dei certificati digitali con le applicazioni che supportano PKCS#11, e in modo specifico con le applicazioni di Netscape.

Per ulteriori dettagli sulle modalità di utilizzo delle impostazioni di sicurezza per le applicazioni Netscape, fare riferimento alla documentazione fornita da Netscape. IBM Client Security Software supporta solo Netscape Versione 4.7x.

Nota: per utilizzare browser a 128-bit con Client Security Software, IBM embedded Security Chip deve supportare la cifratura a 256-bit. La cifratura fornita da Client Security Software può essere rilevata in Administrator Utility facendo clic sul pulsante **Impostazioni del chip**.

Installazione del modulo PKCS#11 di IBM embedded Security Chip per applicazioni Netscape

Prima di poter utilizzare un certificato digitale, è necessario installare il modulo PKCS#11 di IBM embedded Security Chip sul computer. Poiché l'installazione del modulo PKCS#11 di IBM embedded Security Chip richiede un passphrase UVM, è necessario aggiungere almeno un utente alla politica di sicurezza per il computer.

Per installare il modulo PKCS#11 di IBM embedded Security Chip, completare le seguenti procedure:

1. Avviare Netscape e fare clic su **File > Apri pagina**.
2. Rilevare il file di installazione IBMPKCSINSTALL.HTML.

   (Se è stata accettata la directory predefinita quando si installa il software, il file viene situato nella directory C:\Program Files\IBM\Security.)

3. Aprire il file di installazione IBMPKCSINSTALL.HTML in Netscape.

   Quando si apre il file in Netscape, la sequenza di installazione viene avviata e viene visualizzata la finestra del passphrase UVM.
4. Immettere il passphrase UVM e fare clic su **OK**.

   Viene visualizzato un messaggio che richiede se si desidera installare questo modulo di sicurezza.
5. Fare clic su **OK**.

   Viene visualizzato un messaggio che notifica l'installazione del modulo.
6. Fare clic su **OK**.

Utilizzo della protezione al collegamento PKCS#11 per le applicazioni Netscape

Quando la protezione al collegamento PKCS#11 è impostata per il computer, è necessario rispettare i requisiti di autenticazione ogni volta che si esegue un collegamento a Netscape. E' possibile che risulti necessario inserire il passphrase UVM, eseguire una scansione delle impronte digitali oppure entrambi per soddisfare i requisiti di autenticazione. I requisiti di autenticazione vengono definiti nella politica UVM per il computer.

Selezione di IBM embedded Security Chip per generare un certificato digitale per le applicazioni Netscape

Durante la creazione del certificato digitale, verrà richiesto di selezionare la scheda o il database in cui si desidera creare la chiave, selezionare **IBM embedded Security Subsystem**.

Per ulteriori informazioni sulla creazione di un certificato digitale e sul relativo utilizzo con Netscape, consultare la documentazione fornita da Netscape.

Aggiornamento dell'archivio di chiavi per le applicazioni Netscape

Dopo aver creato un certificato digitale, eseguire una copia di backup del certificato aggiornando l'archivio di chiavi. E' possibile aggiornare l'archivio della chiave utilizzando il programma User Configuration Utility.

Utilizzo del certificato digitale per le applicazioni Netscape

Utilizzare le impostazioni di sicurezza nelle proprie applicazioni Netscape per visualizzare, selezionare e utilizzare i certificati digitali. Ad esempio, nelle impostazioni di sicurezza per Netscape Messenger, è necessario selezionare il certificato prima di utilizzarlo per eseguire una firma digitale o per cifrare i messaggi e-mail. Per ulteriori informazioni, fare riferimento alla documentazione fornita da Netscape.

Dopo aver installato il modulo PKCS#11 di IBM embedded Security Chip, UVM richiederà i requisiti di autenticazione ogni qualvolta in cui si utilizza il certificato digitale. E' possibile che risulti necessario inserire il passphrase UVM, eseguire una scansione delle impronte digitali oppure entrambi per soddisfare i requisiti di autenticazione. I requisiti di autenticazione vengono definiti nella politica UVM per il computer.

Se i requisiti di autenticazione impostati dalla politica UVM non vengono soddisfatti, viene visualizzato un messaggio di errore. Facendo clic su **OK**, verrà

aperto Netscape, ma non sarà possibile utilizzare il certificato digitale generato da IBM embedded Security Chip fino al successivo riavvio di Netscape e all'immissione dei corretti passphrase UVM, delle impronte digitali o di entrambi.

Capitolo 6. Funzionalità della politica UVM

Prima di tentare di modificare la politica UVM per il client locale, verificare che almeno un utente sia stato autorizzato ad utilizzare UVM. In caso contrario, verrà visualizzato un messaggio di errore quando l'editor della politica effettua un tentativo per aprire il file della politica locale.

Dopo aver autorizzato gli utenti ad utilizzare UVM, è necessario modificare e salvare una politica di sicurezza per ciascun client IBM. La politica di sicurezza fornita da Client Security Software viene definita politica UVM, che combina le impostazioni fornite in "Autorizzazione degli utenti" con i requisiti di autenticazione a livello di client. La politica UVM può essere utilizzata per controllare la politica della sicurezza di un client locale oppure è possibile che sia copiato sui client remoti in rete.

Administrator Utility dispone di un editor della politica UVM integrato che è possibile utilizzare per modificare e salvare la politica UVM per un client locale. Le attività eseguite sul client IBM, quali il collegamento al sistema operativo o l'annullamento dello screen saver, sono definiti oggetti di autenticazione, devono avere i requisiti di autenticazione ad essi assegnati all'interno della politica UVM. Ad esempio, è possibile impostare la politica UVM per richiedere quanto segue:

- Ciascun utente deve inserire un passphrase UVM e utilizzare un'autenticazione con badge per collegarsi al sistema operativo.
- Ciascun utente deve inserire un passphrase UVM ogni qualvolta che venga richiesto un certificato digitale.

Inoltre, è possibile utilizzare Tivoli Access Manager per controllare oggetti specifici di autenticazione come impostati nella politica UVM.

La politica UVM imposta i requisiti per gli oggetti di autenticazione per il client IBM e non per il singolo utente. Quindi, se si imposta la politica UVM per richiedere l'autenticazione delle impronte digitali per un oggetto (ad esempio, il collegamento al sistema operativo), ciascun utente che è autorizzato ad utilizzare UVM deve registrare un'impronta digitale per utilizzare tale oggetto. Per informazioni dettagliate sull'autorizzazione di un utente, consultare la sezione "Rimozione degli utenti" a pagina 15.

La politica UVM viene salvata in un file definito `globalpolicy.gvm`. Per utilizzare UVM sui client remoti, è necessario che la politica UVM sia salvata su un client IBM e quindi copiata sui client remoti. La copia del file della politica UVM sui client remoti consente di risparmiare il tempo per impostare la politica UVM sui client remoti.

Modifica di una politica UVM locale

E' possibile modificare una politica UVM locale e utilizzarla sul client per cui è stato modificato. Se Client Security è installato nell'ubicazione predefinita, la politica locale UVM viene memorizzata come \Program Files\IBM\Security\UVM_Policy\globalpolicy.gvm. Utilizzare l'editor della politica UVM per modificare e salvare una politica UVM locale. Solo un utente che è stato aggiunto a UVM può utilizzare l'editor della politica UVM. L'interfaccia per l'editor della politica UVM viene fornita in Administrator Utility.

Quando si salvano le modifiche sulla politica UVM, viene visualizzato un messaggio che richiede la chiave privata admin. Inserire la chiave privata admin e fare clic su **OK** per salvare le modifiche. Se viene inserita una chiave privata admin non corretta, le modifiche non saranno salvate.

L'autenticazione si verifica in base alle selezioni effettuate nell'editor della politica. Ad esempio, se si seleziona "Nessun passphrase richiesto in seguito al primo utilizzo in questo modo" per il collegamento a Lotus Notes, ogni qualvolta in cui viene eseguito un collegamento a Lotus Notes verrà richiesta l'autenticazione UVM. Per i successivi accessi a Lotus Notes non sarà necessario il passphrase fino a quando non si esegue un riavvio o uno scollegamento.

Quando si imposta la politica UVM per richiedere l'impronta digitale per un oggetto di autenticazione (quali il collegamento al sistema operativo), ciascun utente che viene aggiunto a UVM deve aver registrato le proprie impronte digitali per utilizzare quell'oggetto.

Durante la modifica la politica UVM, è possibile visualizzare le informazioni di riepilogo della politica facendo clic su Riepilogo della politica UVM. Inoltre, è possibile fare clic su **Applica** per salvare le proprie modifiche. Quando si seleziona **Applica**, viene visualizzato un messaggio che richiede la chiave privata admin. Inserire la chiave privata admin e fare clic su **OK** per salvare le modifiche. Se viene inserita una chiave privata admin non corretta, le modifiche non saranno salvate.

Selezione dell'oggetto

Gli oggetti della politica UVM consentono di stabilire politiche di sicurezza diverse per varie azioni utente. Gli oggetti UVM validi sono specificati nel separatore **Selezione dell'oggetto** del pannello Politica UVM IBM nel programma Administrator Utility.

Oggetti di politica UVM validi includono quanto segue:

Collegamento al sistema
Questo oggetto controlla i requisiti di autenticazione necessari per collegarsi al sistema.

Sblocco del sistema
Questo oggetto controlla i requisiti di autenticazione necessari per annullare lo screen saver di Client Security.

Collegamento a Lotus Notes
Questo oggetto controlla i requisiti di autenticazione necessari per collegarsi a Lotus Notes.

Modifica password di Lotus Notes
Questo oggetto controlla i requisiti di autenticazione necessari per utilizzare UVM per generare una password casuale di Lotus Notes.

Firma digitale (e-mail)
Questo oggetto controlla i requisiti di autenticazione necessari quando si seleziona il pulsante per inviare con Microsoft Outlook o Outlook Express.

Decifrazione (e-mail)
Questo oggetto controlla i requisiti di autenticazione necessari quando si seleziona il pulsante per la decifrazione in Microsoft Outlook o Outlook Express.

Protezione file e cartelle
Questo oggetto controlla i requisiti di autenticazione necessari quando si seleziona la cifratura e la decifrazione con il tastino destro del mouse.

Password Manager
Questa applicazione controlla i requisiti di autenticazione necessari durante l 'utilizzo di IBM Password Manager, disponibile sul sito web IBM. Quando attivo,dovrebbe essere selezionata l'opzione ″Nessun passphrase richiesto in seguito al primo utilizzo in questo modo.″

Netscape - Collegamento con PKCS#11
Questo oggetto controlla i requisiti di autenticazione necessari quando viene ricevuta una chiamata C_OpenSession di PKCS#11 dal modulo PKCS#11. La maggior parte degli utenti dovrebbe lasciare questa impostazione su "Nessun passphrase richiesto in seguito al primo utilizzo in questo modo."

Collegamento Entrust
Questo oggetto controlla i requisiti di autenticazione necessari quando Entrust inoltra una chiamata C_OpenSession di PKCS#11 che il modulo PKCS#11 riceverà. La maggior parte degli utenti dovrebbe lasciare questa impostazione su "Nessun passphrase richiesto in seguito al primo utilizzo in questo modo."

Modifica password id collegamento Entrust
Questo oggetto controlla i requisiti di autenticazione necessari per modificare la password di collegamento a Entrust. Entrust esegue questa operazione inoltrando una chiamata C_OpenSession di PKCS#11 che il modulo PKCS#11 riceverà. La maggior parte degli utenti dovrebbe lasciare questa impostazione su "Nessun passphrase richiesto in seguito al primo utilizzo in questo modo."

Elementi di autenticazione

La politica UVM stabilisce gli elementi di autenticazione disponibili che saranno richiesti per ciascun oggetto abilitato. Tale operazione consente di stabilire diverse politiche di sicurezza per varie azioni.

Gli elementi di autenticazione, che possono essere selezionati nel separatore **Elementi di autenticazione** del pannello Politica UVM IBM nel programma Administrator Utility, comprendono quanto segue:

Selezione del passphrase
Tale selezione consente ad un responsabile di stabilire il passphrase UVM per autenticare un utente in uno dei seguenti tre modi:

- Un nuovo passphrase richiesto ogni volta.
- Nessun passphrase richiesto in seguito al primo utilizzo in questo modo.
- Nessun passphrase richiesto se viene fornito al collegamento del sistema.

Selezione delle impronte digitali
Tale selezione consente ad un responsabile di stabilire la scansione di un'impronta digitale per autenticare un utente in uno dei seguenti tre modi:

- Una nuova impronta digitale richiesta ogni volta.
- Nessuna impronta digitale richiesta in seguito al primo utilizzo in questo modo.
- Nessuna impronta digitale richiesta se viene fornita al collegamento del sistema.

Impostazioni delle impronte digitali globali

Tale selezione consente ad un responsabile di stabilire un numero massimo di tentativi di autenticazione prima che il sistema blocca un utente. Tale area consente al responsabile di proteggere l'autenticazione delle impronte digitali da sovrascrivere con il passphrase UVM.

Selezione Smart Card

Questa selezione consente ad un responsabile di richiedere che venga fornita una smart card come ulteriori dispositivo di autenticazione.

Impostazioni globali Smart Card

Questa selezione consente ad un responsabile di impostare la politica relativa alle sovrapposizioni quando viene fornito il passphrase UVM.

Utilizzo dell'editor della politica UVM

Per utilizzare l'editor della politica UVM, completare la seguente procedura del programma Administrator Utility:

1. Fare clic sul pulsante **Configura politica e supporto dell'applicazione**.

   Viene visualizzato il pannello Configurazione della politica e applicazione UVM.

2. Fare clic sul pulsante **Politica applicativa**.

   Viene visualizzato il pannello Modifica configurazione politica di Client Security.

3. Fare clic sul pulsante **Modifica politica**.

   Viene visualizzato il pannello Inserisci password del responsabile.

4. Immettere la password del responsabile e fare clic su **OK**.

   Viene visualizzato il pannello IBM UVM Policy.

5. Nel separatore Selezione dell'oggetto, fare clic su **Azione** o **Tipo oggetto** e selezionare l'oggetto per il quale si desidera assegnare i requisiti di autenticazione.

   Le azioni includono il collegamento al sistema, lo sblocco del sistema e la decifrazione delle e-mail; un esempio di un tipo di oggetto è l'acquisizione di un certificato digitale.

6. Per ciascun oggetto selezionato, completare la seguente operazione:
   - Fare clic sul separatore **Elementi di autenticazione** e modificare le impostazioni per gli elementi di autenticazione che si desidera assegnare agli oggetti.
   - Selezionare **Access Manager controlla l'oggetto selezionato** per abilitare Tivoli Access Manager a controllare l'oggetto scelto. Selezionare questa opzione solo se si desidera che Tivoli Access Manager controlli gli elementi di autenticazione per il client IBM. Per ulteriori informazioni, consultare la sezione *Utilizzo di Client Security con Tivoli Access Manager*.

     Importante: se si abilita Tivoli Access Manager a controllare l'oggetto, viene fornito il controllo dell'object space di Tivoli Access Manager. In tal caso, è necessario installare di nuovo Client Security Software per ristabilire il controllo locale su quell'oggetto.
   - Selezionare **Nega tutti gli accessi all'oggetto selezionato** per impedire l'accesso all'oggetto scelto.
7. Fare clic su **OK** per salvare le modifiche apportate ed uscire.

Modifica e utilizzo della politica UVM per i client remoti

Per utilizzare la politica UVM per più client IBM, modificare e salvare la politica UVM per un client remoto e, quindi, copiare il file della politica UVM su altri client IBM. Se si installa Client Security nella relativa posizione predefinita, il file della politica UVM sarà memorizzato come \Program Files\IBM\Security\UVM_Policy\remote\globalpolicy.gvm.

Copiare i seguenti file su altri client remoti IBM che utilizzano questa politica UVM:

- \IBM\Security\UVM_Policy\remote\globalpolicy.gvm
- \IBM\Security\UVM_Policy\remote\globalpolicy.gvm.sig

Se Client Security Software è installato nell'ubicazione predefinita, la directory radice per i percorsi che precedono è \Program Files. Copiare entrambi i file nel percorso di directory \IBM\Security\UVM_Policy\ sui client remoti.

Capitolo 7. Altre funzioni del responsabile per la protezione

Quando si configura Client Security Software sui client IBM, è possibile utilizzare Administrator Utility per abilitare IBM embedded Security Chip, impostare una password di Security Chip, creare le chiavi hardware e impostare la politica di sicurezza. Questa sezione fornisce istruzioni per l'utilizzo di altre funzioni di Administrator Utility.

Per aprire Administrator Utility, completare la seguente procedura:

1. Dal desktop di Windows del client IBM, fare clic su **Start > Impostazioni > Pannello di controllo > IBM Client Security Subsystem**.

   Poiché l'accesso ad Administrator Utility è protetto dalla password di Security Chip, viene visualizzato un messaggio che richiede di inserire la password di Security Chip.
2. Immettere la password di Security Chip e fare clic su **OK**.

Utilizzo di Administrator Console

Client Security Software Administrator Console consente ad un responsabile di sicurezza di eseguire le attività specifiche in remoto dal relativo sistema.

E' necessario che l'applicazione Administrator Console (console.exe) sia installata ed eseguita dalla directory `\program files\ibm\security`.

L'applicazione Administrator Console consente ad un responsabile della protezione di eseguire le funzioni di seguito riportate:

- **Ignorare o sovrascrivere gli elementi di autenticazione.** Tali funzioni eseguite dal responsabile comprendono quanto di seguito riportato:
  - **Ignora passphrase UVM.** Questa funzione consente al responsabile di ignorare il passphrase UVM. Quando si utilizza questa funzione, viene creato un passphrase temporaneo e casuale, insieme con un file di password. Il responsabile invia il file di password all'utente e comunica la password in altri modi. Questa operazione assicura la protezione del nuovo passphrase.
  - **Visualizza/Modifica impronte digitali/Smart Card sovrascrivi password.** Tale funzione consente al responsabile di sovrascrivere la politica di sicurezza anche se l'impostazione su NO consente la sovrascrittura del passphrase per le impronte digitali o per la smart card. Potrebbe essere necessario se un lettore delle impronte digitali dell'utente risulta danneggiato oppure la smart card non è disponibile. Il responsabile può leggere o inviare tramite e-mail la password di sovrascrittura all'utente.
- **informazioni sulla chiave di archivio di accesso.** Le funzioni cui un responsabile ha accesso comprendono quanto di seguito riportato:
  - **Directory di archivio.** Questo campo consente al responsabile localizzare le informazioni sulla chiave di archivio da un'ubicazione remota.
  - **Ubicazione della chiave privata Admin.** Questo campo consente di localizzare la chiave privata del responsabile.
- **Altre funzioni remote del responsabile.** L'applicazione Administrator Console consente ad un responsabile della protezione di eseguire le funzioni remote di seguito riportate:

- **Crea il file Administrator Configuration.** Tale funzione consente al responsabile di creare il file di configurazione per il responsabile, che viene richiesto quando un utente desidera registrarsi o reimpostarsi mediante Client Utility. Di solito, il responsabile invia tramite e-mail questo file ad un utente.
- **Cifra/Decifra file di configurazione.** Questa funzione consente la cifratura del file di configurazione per una maggiore sicurezza. Inoltre, decifra il file in modo che possa essere editato.
- **Configura roaming delle credenziali.** Questa funzione registra il sistema come server di roaming CSS. Una volta registrato tutti gli utenti della rete autorizzati UVM potranno accedere ai dati personali (passphrase, certificati e altro.) presenti nel sistema.

Registrazione di un client in una rete di roaming delle credenziali

Per registrare automaticamente un client in una rete di roaming delle credenziali, completare la procedura di seguito riportata:

1. Utilizzando la Console, decifrare un file CSEC.INI precedentemente generato. Questo file contiene già la password per l'hardware password e gli utenti da registrare.
2. Nella sezione del file relativa alla configurazione di CSS,aggiungere `"enableroaming=1"`. Questa stringa indica che il sistema dovrebbe essere registrato come un client di roaming.
3. Nella stessa sezione, aggiungere la voce `"username=OPTION"`. Sono disponibili tre opzione per questo valore:
   a. **La stringa `"[promptcurrent]"` - parentesi quadre incluse.** Questa specifica dovrebbe essere utilizzata se è stato generato un file .dat per l'utente al momento collegato sul server di roaming e se l'utente corrente conosce la password di registrazione del sistema. Selezionando questa opzione viene visualizzata una casella a comparsa che richiede all'utente di immettere `sysregpwd`. Ovviamente, in caso di installazione automatica, l'admin evita questa impostazione, in quanto richiede la presenza dell'utente.
   b. **La stringa `"[current]"` - parentesi quadre incluse.** Questa specifica dovrebbe essere utilizzata se è stato generato un file .dat sul server per l'utente al momento collegato. La stringa `sysregpwd` verrà gestita come descritto nel punto elenco.
   c. **Un nome utente corrente come `"joseph"`.** Se viene utilizzato tale nome utente, un file `"joseph.dat" deve essere precedentemente generato` dal server di roaming. La relativa stringa `sysregpwd` verrà gestita come descritto nel punto elenco.
4. Infine, se vengono utilizzate le opzioni numero due e tre, è necessario fornire un'latra voce `"sysregpwd=SYSREGPW"`. La password di otto caratteri associata all'utente corrente (se viene implementata l'opzione numero due) o all'utente designato (se viene implementata l'opzione numero tre).
5. Per completare la registrazione del client, collegare il sistema alla configurazione dell'ubicazione di archivio mediante il server di roaming. L'ubicazione dell'archivio viene designata nel file CSEC.INI.

Esempi del file CSEC.INI

Gli esempi di seguito riportati illustrano un file CSEC.INI di esempio, oltre alle relative modifiche in base all'opzione di roaming delle credenziali selezionata. Di seguito sono riportate le opzioni disponibili:

- **Nessun valore di roaming.** Questo file di base non è abilitato per il roaming delle credenziali.

- **Opzione di roaming 1.** Questo file è abilitato per il roaming con l'opzione 1 per la registrazione del client. E' necessario che l'utente corrente fornisca la password di registrazione del sistema.
- **Opzione di roaming 2.** Questo file è abilitato per il roaming con l'opzione 2 per la registrazione del client.E' necessario che l'utente corrente fornisca l'ID e la password di registrazione del sistema.
- **Opzione di roaming 3.** Questo file è abilitato per il roaming con l'opzione 3 per la registrazione del client. Viene designato l'utente. E' necessario che l'utente designato fornisca la password di registrazione del sistema.

Di seguito sono illustrati gli esempi di quattro diversi file CSEC.INI:

```
[CSSSetup]
suppw=bootup
hwpw=11111111
newkp=1
keysplit=1
kpl=c:\jgk
kal=c:\jgk\archive
clean=0

[UVMEnrollment]
enrollall=0
user1=joseph
user1uvmpw=q1234r
user1winpw=
user1domain=0
user1ppchange=0
user1ppexppolicy=0
user1ppexpdays=184
enrollusers=1
[UVMAppConfig]
uvmlogon=0
entrust=0
notes=0
netscape=0
passman=0
folderprotect=0
autoprotect=0
```

```
[CSSSetup]
suppw=bootup
hwpw=11111111
newkp=1
keysplit=1
kpl=c:\jgk
kal=c:\jgk\archive
enableroaming=1
username=
[promptcurrent]
clean=0

[UVMEnrollment]
enrollall=0
user1=joseph
user1uvmpw=q1234r
user1winpw=
user1domain=0
user1ppchange=0
user1ppexppolicy=0
user1ppexpdays=184
enrollusers=1
[UVMAppConfig]
uvmlogon=0
entrust=0
notes=0
netscape=0
passman=0
folderprotect=0
autoprotect=0
```

```
[CSSSetup]
suppw=bootup
hwpw=11111111
newkp=1
keysplit=1
kpl=c:\jgk
kal=c:\jgk\archive
enableroaming=1
username=[current]

sysregpwd=12345678
clean=0
[UVMEnrollment]
enrollall=0
user1=joseph
user1uvmpw=q1234r
user1winpw=
user1domain=0
user1ppchange=0
user1ppexppolicy=0
user1ppexpdays=184
enrollusers=1
[UVMAppConfig]
uvmlogon=0
entrust=0
notes=0
netscape=0
passman=0
folderprotect=0
autoprotect=0
```

```
[CSSSetup]
suppw=bootup
hwpw=11111111
newkp=1
keysplit=1
kpl=c:\jgk
kal=c:\jgk\archive
enableroaming=1
username=joseph

sysregpwd=12345678
clean=0
[UVMEnrollment]
enrollall=0
user1=joseph
user1uvmpw=q1234r
user1winpw=
user1domain=0
user1ppchange=0
user1ppexppolicy=0
user1ppexpdays=184
enrollusers=1
[UVMAppConfig]
uvmlogon=0
entrust=0
notes=0
netscape=0
passman=0
folderprotect=0
autoprotect=0
```

Modifica dell'ubicazione dell'archivio di chiavi

Quando viene creato l'archivio delle chiavi, vengono anche create copie di tutte le chiavi cifrate e salvate nell'ubicazione specificata durante l'installazione.

Nota: l'utente client può anche modificare l'ubicazione dell'archivio delle chiavi utilizzando User Configuration Utility. Per ulteriori informazioni, consultare il Capitolo 8, "Istruzioni per gli utenti client", a pagina 41.

Per modificare l'ubicazione dell'archivio delle chiavi, completare la seguente procedura di Administrator Utility:

1. Fare clic sul pulsante **Configurazioni chiavi**.

Viene visualizzata la finestra Modifica configurazione chiave client- Configura chiavi.

2. Fare clic sul pallino **Modifica la posizione dell'archivio** e fare clic su **Avanti**.

   Viene visualizzata la finestra Modifica configurazione chiave client - Nuova posizione dell'archivio chiavi.
3. Immettere il nuovo percorso o fare clic su **Sfoglia** per selezionare il percorso.
4. Fare clic su **OK**.

   Viene visualizzato un messaggio che indica il completamento dell'operazione.
5. Fare clic su **Fine**.

Modifica della coppia di chiavi dell'archivio

Quando viene creata inizialmente la coppia di chiavi dell'archivio, di solito, viene memorizzata su un minidisco o su una directory di rete. Se la coppia di chiavi dell'archivio viene danneggiata, è possibile cambiare con una una coppia diversa.

Nota: accertarsi di aggiornare l'archivio prima di modificare la coppia di chiavi dell'archivio.

Per modificare la coppia di chiavi dell'archivio, completare la seguente procedura di Administrator Utility:

1. Fare clic sul pulsante **Configurazioni chiavi**.

   Viene visualizzata la finestra Modifica configurazione chiave client- Configura chiavi.
2. Fare clic sul pallino **Modifica coppia di chiavi di IBM Security Subsystem Archive** e fare clic su **Avanti**.

   Viene visualizzata la finestra Modifica configurazione chiavi di Client Security - Nuovo file della chiave pubblica del responsabile UVM.
3. nel campo Nuova chiave di archivio CSS, inserire il nome file per la nuova chiave pubblica dell'archivio nel campo File della chiave pubblica. Inoltre, è possibile fare clic su **Sfoglia** per ricercare il nuovo file o fare clic su **Crea** per creare una nuova chiave pubblica dell'archivio.

   Nota: accertarsi di creare la nuova chiave pubblica in una posizione diversa da quella che contiene i precedenti file dell'archivio.
4. Nel campo Nuova chiave dell'archivio CSS, inserire il nome file per la nuova chiave privata dell'archivio nel campo File della chiave privata. Inoltre, è possibile fare clic su **Sfoglia** per ricercare il nuovo file o fare clic su **Crea** per creare una nuova coppia di chiavi di archivio.

   Nota: accertarsi di creare la nuova coppia di chiavi in una posizione diversa da quella che contiene i precedenti file dell'archivio.
5. Nel campo Vecchia chiave di archivio CSS, inserire il nome file per la vecchia chiave pubblica dell'archivio nel campo File della chiave pubblica o fare clic su **Sfoglia** per ricercare il file.
6. Nell'area Vecchia chiave di archivio CSS, inserire il nome file per la vecchia chiave privata di archivio nel campo File della chiave privata o fare clic su **Sfoglia** per ricercare il file.
7. Nel campo Posizione dell'archivio, inserire il percorso del file in cui l'archivio della chiave viene memorizzato o fare clic su **Sfoglia** per selezionare il percorso.
8. Fare clic su **Avanti**.

Nota: se la coppia delle chiavi di archivio è stata suddivisa in più file, viene visualizzato un messaggio che richiede di inserire l'ubicazione e il nome di ciascun file. Fare clic su **Leggi successivo** dopo aver immesso ciascun nome file nel campo del file di chiavi.

Viene visualizzato un messaggio che indica il completamento corretto dell'operazione.

9. Fare clic su **OK**.

   Viene visualizzato un messaggio che indica il completamento dell'operazione.

10. Fare clic su **Fine**.

Ripristino delle chiavi dall'archivio

E' possibile che risulti necessario ripristinare le chiavi se è stata sostituita una scheda di sistema o se l'unità del disco fisso è stata danneggiata. In fase di ripristino delle chiavi si copiano i file di chiavi utenti più recenti dall'archivio di chiavi e si memorizzano su IBM embedded Security Chip. Tali file di chiavi utente copiati vengono visualizzati nella directory in cui sono stati memorizzati precedentemente sul computer, quali su una directory di rete o su un minidisco.

Se un malfunzionamento dell'unità disco fisso sul computer compromette l'integrità delle chiavi degli utenti, è possibile ripristinare le chiavi dall'archivio di chiavi. Il ripristino delle chiavi sovrascriverà tutte le chiavi che sono state memorizzate.

Se la scheda di sistema viene sostituita sul computer con una scheda di sistema che contiene IBM embedded Security Chip e le chiavi cifrate sono ancora valide sul disco fisso, è possibile ripristinare le chiavi cifrate che sono state precedentemente associate al computer, eseguendo una nuova cifratura con IBM embedded Security Chip sulla nuova scheda di sistema.

L'operazione di un ripristino delle chiavi viene eseguito dopo aver abilitato il nuovo chip e impostato una password di Security Chip. Per ulteriori informazioni, consultare la sezione "Abilitazione di IBM embedded Security Chip e impostazione della password di Security Chip" a pagina 39.

Nota: il collegamento a UVM viene abilitato automaticamente dopo il ripristino di una chiave. Di conseguenza, se è stata richiesta l'autenticazione tramite impronta digitale per il collegamento a UVM, è necessario installare il software delle impronte digitali prima di riavviare dopo un ripristino per ignorare un blocco del sistema.

Le seguenti istruzioni presumono che Administrator Utility non sia stato danneggiato da un malfunzionamento dell'unità del disco fisso. Se l'unità del disco fisso ha danneggiato i file di client security, è possibile che risulti necessario installare di nuovo il software Client Security Software.

Per ripristinare le chiavi cifrate da un archivio di chiavi, completare la seguente procedura di Administrator Utility:

Nota: se si modifica la coppia di chiavi admin dopo aver ripristinato l'archivio, viene visualizzato un messaggio di errore. Se ciò si verifica, è necessario aggiungere gli utenti a UVM e, quindi, richiedere nuovi certificati.

1. Fare clic sul pulsante **Configurazioni chiavi**.

Viene visualizzata la finestra Modifica configurazione chiave client- Configura chiavi.

2. Fare clic sul pallino **Ripristina chiavi di IBM Security Subsystem da archivio** e fare clic su **Avanti**.

   Viene visualizzata la finestra Modifica configurazione chiave client- Ripristina tutte le chiavi di IBM Security Subsystem.

3. Nel campo Directory archivio (percorso), inserire il percorso del file della directory dell'archivio o fare clic su **Sfoglia** per ricercare la directory.
4. Nel campo File della chiave pubblica di archivio CSS, inserire il percorso ed il nome file della chiave pubblica admin o fare clic su **Sfoglia** per ricercare il file.
5. Nel campo File della chiave privata di archivio CSS, immettere il percorso ed il nome file della chiave privata admin o fare clic su **Sfoglia** per ricercare il file.
6. Fare clic su **Avanti**.

   Viene visualizzato un messaggio che indica che l'operazione è stata completata correttamente.

   Nota: se la chiave privata admin è stata suddivisa in più file, viene visualizzato un messaggio che richiede di inserire l'ubicazione e il nome di ciascun file. Fare clic su **Leggi successivo** dopo aver immesso ciascun nome file nel campo del file di chiavi.

7. Fare clic su **OK**.
8. Fare clic su **Fine**.

Reimpostazione del conteggio numeri errori di autenticazione

Per configurare di nuovo il conteggio degli errori di autenticazione per un utente, completare la seguente procedura di Administrator Utility:

1. Nell'area Utenti di Windows autorizzati ad utilizzare UVM, selezionare un utente.
2. Fare clic sul pulsante **Reimposta numero errori**.

   Viene visualizzata la finestra Reimposta conteggio di errori per l'utente.

3. Inserire il passphrase UVM per l'utente selezionare e fare clic su **OK**.

   Viene visualizzato un messaggio che notifica il completamento dell'operazione.

4. Fare clic su **OK**.

Modifica delle informazioni di impostazione di Tivoli Access Manager

Le seguenti informazioni sono destinate ai responsabili della sicurezza che prevedono di utilizzare Tivoli Access Manager per gestire oggetti di autenticazione per la politica di sicurezza UVM. Per ulteriori informazioni, consultare la sezione *Utilizzo di Client Security con Tivoli Access Manager*.

Accesso al file di configurazione di Tivoli Access Manager

Per configurare le informazioni di impostazione di Tivoli Access Manager sul client IBM, Client Security Software utilizza un file di configurazione. Tale file di configurazione consente di collegare Tivoli Access Manager agli oggetti controllati dalla politica UVM. Per accedere alla configurazione di Tivoli Access Manager, completare la seguente procedura di Administrator Utility:

1. Fare clic sul pulsante **Configura politica e supporto di applicazione**.

   Viene visualizzato il pannello Configurazione della politica e applicazione UVM.

2. Nel campo Informazioni di impostazione di Tivoli Access Manager, inserire il percorso ed il nome file del file di configurazione oppure fare clic su **Sfoglia** per ricercare il file.
3. Fare clic sul pulsante **Modifica politica**.
4. Continuare con la procedura di modifica della politica.

Aggiornamento della cache locale

Una replica locale delle informazioni sulla politica di sicurezza nel modo in cui viene gestito da Tivoli Access Manager viene conservata sul client IBM. E' possibile impostare la frequenza di aggiornamento della cache locale con incrementi in mesi e giorni oppure è possibile fare clic su un pulsante per aggiornare immediatamente la cache locale.

Per impostare o aggiornare la cache locale, completare la seguente procedura di Administrator Utility:

1. Fare clic sul pulsante **Configura politica e supporto di applicazione**.

   Viene visualizzato il pannello Configurazione della politica e applicazione UVM.
2. Nel campo Intervallo di aggiornamento della cache locale, procedere nel modo seguente:
   - Per aggiornare la cache locale, fare clic su **Aggiorna cache locale**.
   - Per impostare la frequenza di aggiornamento, inserire il numero dei mesi e dei giorni nei campi forniti. Il valore per i mesi e i giorni rappresenta l'intervallo di tempo tra gli aggiornamenti pianificati.

Recupero di un passphrase UVM

Un passphrase UVM viene creato per ciascun utente che è stato autorizzato dalla politica di sicurezza per il client IBM. Poiché il passphrase può essere perso o dimenticato oppure modificato da un utente client, Administrator Utility consente ad un responsabile di ripristinare un passphrase perduto o dimenticato.

Per ripristinare un passphrase, completare la seguente procedura di Administrator Utility:

1. Selezionare un utente nel campo Utenti di Windows autorizzati ad utilizzare UVM.
2. Fare clic sul pulsante **Modifica passphrase**.

   Viene visualizzato il pannello Modifica passphrase.
3. Nel campo Posizione dell'archivio di IBM Security Subsystem, inserire il percorso ed il nome della directory dell'archivio della chiave oppure fare clic su **Sfoglia** per individuare la directory.
4. Nel campo Chiave dell'archivio di IBM Security Subsystem, inserire il percorso ed il nome file della chiave privata nel campo File della chiave privata oppure fare clic su **Sfoglia** per individuare il file.
5. Nel campo Chiave dell'archivio di IBM Security Subsystem, inserire il percorso ed il nome file della chiave pubblica admin nel campo File della chiave pubblica oppure fare clic su **Sfoglia** per individuare il file.
6. Fare clic su **OK**.

   Viene visualizzato un messaggio che visualizza il passphrase UVM per l'utente.
7. Fare clic su **OK**.

Se la chiave privata admin è stata suddivisa in più file, viene visualizzato un messaggio che richiede di inserire l'ubicazione e il nome di ciascun file. Fare clic su **Leggi successivo** in seguito all'immissione di ciascun file nel campo File della chiave privata.

Questa procedura genera una password temporanea e casuale insieme con un file di password. Entrambi gli elementi sono necessari per ottenere di nuovo l'accesso al sistema bloccato.

8. Il responsabile invia il file all'utente e comunica la password temporanea in altri modi.

Modifica della password di IBM Security Chip

E' necessario impostare una password di Security Chip per abilitare IBM embedded Security Chip per un client. L'accesso a Administrator Utility è protetto anche dalla password di Security Chip. Per una migliore sicurezza, è necessario modificare la password di Security Chip periodicamente. Una password che rimane invariata per un lungo periodo di tempo può anche essere più soggetta a parti esterne. Proteggere la password di Security Chip per impedire ad utenti non autorizzati di modificare le impostazioni del programma Administrator Utility. Per ulteriori informazioni sulle regole della password di Security Chip, consultare l'Appendice B, "Regole per password e passphrase", a pagina 67.

Per modificare la password di Security Chip, completare la seguente procedura di Administrator Utility:

1. Fare clic sul pulsante **Impostazioni chip**.

   Viene visualizzata la finestra Modifica impostazioni IBM Security Chip.
2. Fare clic su **Modifica password del chip**.

   Viene visualizzata la finestra Modifica password di IBM Security Chip.
3. Nel campo Nuova password, immettere la nuova password.
4. Nel campo di conferma, inserire di nuovo la password.
5. Fare clic su **OK**.

   Viene visualizzato un messaggio che notifica il completamento dell'operazione.

   Attenzione: Non premere Invio o il tasto di tabulazione > Invio per salvare le modifiche. In caso contrario, viene visualizzata la finestra Disabilita chip. Se viene visualizzata la finestra Disabilita chip, non disabilitare il chip; uscire dalla finestra.
6. Fare clic su **OK**.

Visualizzazione delle informazioni su Client Security Software

Le seguenti informazioni su IBM embedded Security Chip e su Client Security Software sono disponibili facendo clic sul pulsante **Impostazioni del chip** del programma Administrator Utility:

- Il numero della versione del firmware utilizzato con Client Security Software
- Lo stato della cifratura del Security Chip integrato
- La validità delle chiavi cifrate dell'hardware
- Lo stato di IBM embedded Security Chip

Disabilitazione di IBM embedded Security Chip

Administrator Utility consente di disabilitare IBM embedded Security Chip. Poiché è necessario inserire la password di Security Chip per avviare Administrator Utility e disabilitare il chip, proteggere la password di Security Chip per impedire ad utenti non autorizzati di disabilitare il chip.

Importante: non eliminare IBM embedded Security Chip mentre è abilitata la protezione UVM. In caso contrario, verrà bloccato il sistema. Per disabilitare la protezione UVM, aprire la funzione Administrator Utility e deselezionare la casella **Sostituisci il collegamento Windows standard con il collegamento di sicurezza UVM**. E' necessario riavviare il computer prima di disabilitare la protezione UVM per il collegamento al sistema.

Per disabilitare il Security Chip integrato, completare la seguente procedura di Administrator Utility:

1. Fare clic sul pulsante **Impostazioni chip**.
2. Fare clic sul pulsante **Disabilita chip** e seguire le istruzioni sullo schermo.
3. Se sul computer è stata abilitata la funzione della sicurezza avanzata, potrebbe essere necessario inserire la password del responsabile che è stata impostata in Configuration/Setup Utility per disabilitare il chip.

Per utilizzare IBM embedded Security Chip e le chiavi cifrate dell'hardware una volta disabilitato il chip, è necessario riabilitare il chip.

Abilitazione di IBM embedded Security Chip e impostazione della password di Security Chip

Se risulta necessario abilitare IBM embedded Security Chip dopo aver installato il software, è possibile utilizzare Administrator Utility per reimpostare la password di Security Chip e per configurare le nuove chiavi di cifratura.

E' possibile che risulti necessario abilitare IBM embedded Security Chip per ripristinare l'archivio delle chiavi dopo aver sostituito una scheda di sistema oppure se è stato disabilitato il chip.

Per abilitare il chip e impostare una password di Security Chip, completare la seguente procedura:

1. Dal desktop di Windows del client IBM, fare clic su **Start > Impostazioni > Pannello di controllo > IBM Client Security Subsystem**.

   Viene visualizzato un messaggio che richiede di abilitare IBM embedded Security Chip per il client IBM.
2. Fare clic su **Sì**.

   Viene visualizzato un messaggio che richiede di riavviare il computer. E' necessario riavviare il computer prima che IBM embedded Security Chip venga abilitato. Se sul computer è stata abilitata la funzione di sicurezza avanzata, è possibile che risulti necessario inserire la password del responsabile impostata in Configuration/Setup Utility per abilitare il chip.
3. Fare clic su **OK** per riavviare il computer.
4. Dal desktop di Windows, fare clic su **Start > Impostazioni > Pannello di controllo > IBM Client Security Subsystem**.

Poiché l'accesso ad Administrator Utility è protetto dalla password di Security Chip, viene visualizzato un messaggio che richiede di inserire la password di Security Chip.

5. Immettere una password di Security Chip nel campo Nuova password e, quindi, inserirla di nuovo nel campo di conferma.
6. Fare clic su **OK**.

Abilitazione del supporto Entrust

IBM embedded Security Chip consente a Client Security Software di migliorare le funzioni di sicurezza Entrust. L'abilitazione del supporto Entrust su un computer con Client Security Software trasferisce le funzioni di sicurezza del software Entrust su IBM Security Chip.

Client Security Software rileverà automaticamente il file entrust.ini per abilitare il supporto Entrust; tuttavia, se il file entrust.ini non si trova nel percorso ordinario, viene visualizzata una finestra per l'utente per ricercare il file entrust.ini. Una volta che l'utente ha rilevato e selezionato il file, Client Security può abilitare il supporto Entrust. Una volta selezionato la casella **Abilita supporto Entrust**, è necessario un riavvio prima che Entrust cominci ad utilizzare IBM Embedded Security Chip.

Per abilitare il supporto Entrust, completare la seguente procedura:

1. Dal desktop di Windows del client IBM, fare clic su **Start > Impostazioni > Pannello di controllo > IBM Client Security Subsystem**.

   Viene visualizzata la finestra principale di Administrator Utility.
2. Fare clic su **Configura politiche e supporto applicazioni**.

   Viene visualizzato il pannello Configurazione della politica e applicazione UVM.
3. Selezionare la casella **Abilita supporto Entrust**.
4. Fare clic su **Applica**.

   Viene visualizzata la finestra del supporto Entrust di IBM Client Security con un messaggio che indica che il supporto Entrust è stato abilitato.

Nota: è necessario riavviare il computer per rendere effettive le modifiche.

Capitolo 8. Istruzioni per gli utenti client

Questa sezione fornisce informazioni che consentono ad un utente client di eseguire le attività riportate di seguito:

- Utilizzare la protezione UVM per il collegamento al sistema
- Configurare lo screen saver di Client Security
- Utilizzare User Configuration Utility
- Utilizzare un programma di navigazione sul web e per i messaggi e-mail sicuro
- Configurare le preferenze audio UVM

Utilizzo della protezione UVM per il collegamento al sistema

Questa sezione contiene informazioni sull'utilizzo della protezione del collegamento UVM per il collegamento al sistema. Prima di utilizzare la protezione UVM, è necessario abilitarla per il computer.

La protezione UVM consente di controllare l'accesso al sistema operativo attraverso un'interfaccia di collegamento. La protezione al collegamento UVM sostituisce l'applicazione di collegamento a Windows, in modo che quando un utente sblocca il computer, viene visualizzata la finestra di collegamento a UVM e non la finestra di collegamento a Windows. Una volta abilitata la protezione UVM sul computer, all'avvio del computer verrà visualizzata l'interfaccia di collegamento a UVM.

Quando il computer è in esecuzione, è possibile accedere all'interfaccia di collegamento a UVM premendo **Ctrl + Alt + Canc** per arrestare o bloccare il computer oppure per aprire Task Manager o scollegare l'utente corrente.

Procedure per sbloccare il client

Per sbloccare un client Windows che utilizza la protezione UVM, procedere nel modo seguente:

1. Premere **Ctrl + Alt + Canc** per accedere all'interfaccia di collegamento UVM.
2. Immettere il nome utente e il dominio a cui si è collegati e, quindi, fare clic su **Sblocca**.

   Viene visualizzata la finestra Passphrase UVM.

   Nota: anche se UVM riconosce molteplici domini, la password utente deve essere la stessa per tutti i domini.
3. Immettere il passphrase UVM e fare clic su **OK** per accedere al sistema operativo.

Nota:

1. Se il passphrase UVM non corrisponde al nome utente e al dominio immessi, la finestra di collegamento a UVM viene visualizzata di nuovo.
2. A seconda dei requisiti di autenticazione della politica UVM per il client, è possibile che vengano richiesti ulteriori processi di autenticazione.

Screen saver di Client Security

Lo screen saver di Client Security corrisponde ad una serie di immagini animate che vengono visualizzate quando il proprio computer è in stato di inattività per un certo intervallo di tempo. La configurazione di uno screen saver di Client Security è un modo per controllare l'accesso al computer tramite un'applicazione screen saver. Una volta che lo screen saver di Client Security viene visualizzato sul desktop, è necessario immettere il propria passphrase UVM per accedere al desktop del sistema.

Impostazione dello screen saver di Client Security

Questa sezione contiene informazioni sulla impostazione dello screen saver di Client Security. Prima di poter utilizzare lo screen saver di Client Security, almeno un utente deve essere registrato sulla politica di sicurezza del proprio computer.

Per impostare lo screen saver Client Security, procedere nel modo seguente:

1. Fare clic su **Start > Impostazioni > Pannello di controllo**.
2. Fare doppio clic sull'icona **Schermo**.
3. Fare clic sul separatore **Screen Saver**.
4. Nel menu a discesa Screen Saver, selezionare **Client Security**. Per cambiare la velocità dello screen saver, fare clic su **Impostazioni** e impostare la velocità desiderata.
5. Fare clic su **OK**.

Attività dello screen saver di Client Security

Le attività dello screen saver di Client Security differiscono a seconda delle impostazioni configurate per Administrator Utility di UVM e per lo screen saver di Windows. Il sistema controlla prima le impostazioni di Windows, quindi le impostazioni di UVM Administrator Utility. Di conseguenza, lo screen saver blocca il desktop solo se viene selezionata la casella di controllo **Password protetta** sul separatore delle impostazioni relative allo screen saver di Windows.

Se questa casella viene selezionata, il sistema richiede la password di Windows o il passphrase UVM, se la casella di controllo **Sostituisci il collegamento standard di Windows con il collegamento sicuro di UVM** è stata selezionata in Administrator Utility. Se la casella è stata selezionata. il sistema richiederà il passphrase UVM. Se non è stata selezionata, il sistema richiederà la password per Windows.

Inoltre, è possibile che siano stati impostati altri requisiti di autenticazione nella politica di sicurezza per il computer e, che, quindi, vengano richiesti ulteriori autenticazioni. Ad esempio, potrebbe risultare necessario eseguire una scansione delle impronte digitali per sbloccare il computer.

Nota: se IBM embedded Security Chip è disabilitato oppure se vengono rimossi tutti gli utenti dalla politica di sicurezza, lo screen saver di Client Security non sarà più disponibile.

User Configuration Utility

Il programma User Configuration Utility abilita l'utente client ad eseguire le varie attività di gestione della sicurezza che non richiedono l'accesso con privilegi di responsabile.

Funzioni User Configuration Utility

Il programma User Configuration Utility consente ad un utente client di procedere nel modo seguente:

- **Aggiornamento delle password e dell'archivio.** Questo separatore consente di eseguire le funzioni di seguito riportate:
  - **Cambiare il passphrase UVM.** Per migliorare la sicurezza, è possibile modificare periodicamente il passphrase UVM.
  - **Aggiornare la password di Windows.** Quando viene modificata la password di Windows per un client autorizzato UVM con il programma Windows User Manager, occorre modificare anche la password utilizzando IBM Client Security Software - User Configuration Utility. Se un responsabile utilizza Administrator Utility per modificare la password di collegamento a Windows per un utente, tutte le chiavi cifrate dell'utente create per quell'utente saranno eliminate e i certificati digitali associati non saranno più validi.
  - **Reimpostare la password Lotus Notes.** Per migliorare la sicurezza, è possibile modificare la password Lotus Notes.
  - **Aggiornare l'archivio delle chiavi.** Se si creano certificati digitali e si desidera creare copie della chiave privata memorizzata su IBM embedded Security Chip oppure se si desidera spostare l'archivio delle chiavi su un'altra ubicazione, aggiornare l'archivio delle chiavi.
- **Configurare le preferenze audio UVM.** User Configuration Utility consente di selezionare un file audio da riprodurre in caso di autenticazione riuscita o non riuscita.
- **Configurazione utente.** Questo separatore consente di eseguire le funzioni di seguito riportate:
-
  - **Reimposta utente.** Questa funzione consente di reimpostare la configurazione di sicurezza. Quando si reimposta la configurazione di sicurezza, tutte le chiavi, i certificati, le impronte digitali precedenti vengono cancellati.
  - **Ripristinare la configurazione di sicurezza utente dall'archivio.** Questa funzione consente di ripristinare le impostazioni dall'archivio. Tale funzione è utile se i file sono stati corrotti o se si desidera ripristinare una configurazione precedente.
  - **Registra con un server di roaming CSS.** Questa funzione consente di registrare il sistema con un server di roaming CSS. Una volta registrato il sistema, è possibile importare la configurazione corrente in questo sistema.

Limiti di User Configuration Utility con Windows XP

Windows XP impone alcune restrizioni per l'accesso che limitano le funzioni disponibili ad un utente del client in determinate circostanze.

Windows XP Professional

In Windows XP Professional, le restrizioni dell'utente client potrebbero essere applicate nelle seguenti situazioni:

- Client Security Software è installato su una partizione che viene convertita successivamente in un formato NTFS
- La cartella Windows si trova su una partizione che viene convertita successivamente in un formato NTFS
- La cartella di archivio si trova su una partizione che viene convertita successivamente in un formato NTFS

Nelle situazioni precedenti, Windows XP Professional Limited Users potrebbe non essere in grado di eseguire le attività di User Configuration Utility di seguito riportate:

- Cambiare il passphrase UVM
- Aggiornare la password di Windows registrata con UVM
- Aggiornare l'archivio delle chiavi

Tali limitazioni vengono eliminate quando un responsabile avvia ed esce da Administrator Utility.

Windows XP Home

Windows XP Home Limited Users non sarà in grado di utilizzare User Configuration Utility in una delle seguenti situazioni:

- Client Security Software è installato su una partizione formattata NTFS
- La cartella Windows si trova su una partizione formattata NTFS
- La cartella di archivio si trova su una partizione formattata NTFS

Utilizzo di User Configuration Utility

Per utilizzare User Configuration Utility, procedere nel modo seguente:

1. Fare clic su **Avvio > Programmi > Access IBM > IBM Client Security Software > Modifica le impostazioni di sicurezza**.

   Viene visualizzato il pannello principale di IBM Client Security Software User Configuration Utility.
2. Immettere il passphrase UVM per l'utente client che richiede un passphrase UVM oppure la modifica della password di Windows e, fare clic su **OK**.
3. Selezionare uno dei separatori di seguito riportati:
   - **Aggiornamento delle password e dell'archivio.** Questo separatore consente di modificare il passphrase UVM, aggiornare la password di Windows in UVM, reimpostare la password Lotus Notes in UVM e aggiornare l'archivio di cifratura.
   - **Configura suoni UVM.** Questo separatore consente di selezionare un file audio da riprodurre in caso di autenticazione riuscita o non riuscita.
   - **Configurazione utente.** Questo separatore consente all'utente di ripristinare la configurazione utente dall'archivio o reimpostare la configurazione di sicurezza.
4. Fare clic su **OK** per uscire.

Utilizzo di un programma di navigazione sul web e di messaggi e-mail sicuri

Se si inviano transazioni non protette su Internet, tali transazioni possono essere intercettate e lette. E' possibile impedire gli accessi non autorizzati alle transazioni su Internet richiamando un certificato digitale e utilizzandolo per eseguire una firma digitale e per cifrare i propri messaggi e-mail o per rendere più sicuro il proprio browser web.

Un certificato digitale (definito anche ID digitale o certificato di sicurezza) è una credenziale elettronica immessa e inserita con una firma digitale da un'autorità certificata. Quando viene emesso un certificato digitale, l'autorità di certificazione convalida l'identità dell'utente in quanto possessore del certificato. Un'autorità di

certificazione è un fornitore sicuro di certificati digitali e può essere un'azienda non IBM, come ad esempio VeriSign oppure tale autorità di certificazione può essere configurata come server all'interno della propria azienda. Il certificato digitale contiene l'identità dell'utente, come ad esempio il nome e l'indirizzo e-mail, le date di scadenza del certificato, una copia della chiave pubblica, l'identità dell'autorità di certificazione e la firma digitale.

Utilizzo di Client Security Software con applicazioni Microsoft

Le istruzioni fornite in questa sezione sono specifiche per l'utilizzo di Client Security Software in relazione all'emissione e all'utilizzo di certificati digitali con le applicazioni che supportano Microsoft CryptoAPI, come ad esempio Outlook Express.

Per ulteriori dettagli su come creare le impostazioni di sicurezza e utilizzare applicazioni e-mail quali Outlook Express e Outlook, fare riferimento alla documentazione fornita con tali applicazioni.

Nota: per utilizzare browser a 128-bit con Client Security Software, IBM embedded Security Chip deve supportare la cifratura a 256-bit. La lunghezza della cifratura fornita da Client Security Software può essere ricercata in Administrator Utility.

Emissione di un certificato digitale per le applicazioni Microsoft

Quando si utilizza un'autorità di certificazione per creare un certificato digitale da utilizzare per le applicazioni Microsoft, verrà richiesto di selezionare un CSP (Cryptographic Service Provider) per il certificato.

Per utilizzare le funzioni di cifratura di IBM embedded Security Chip per le applicazioni Microsoft, assicurarsi di selezionare **IBM embedded Security Subsystem CSP** come provider di servizi di cifratura una volta ottenuto il certificato digitale. Questa operazione assicura che la chiave privata del certificato digitale venga memorizzata in IBM Security Chip.

Inoltre, selezionare la cifratura forte (o alta), se disponibile, per una ulteriore sicurezza. Poiché IBM embedded Security Chip consente una cifratura fino a 1024 bit della chiave privata del certificato digitale, selezionare questa opzione, se disponibile, nell'interfaccia relativa all'autorità di certificazione; la cifratura a 1024 bit è inoltre denominata cifratura forte.

Dopo aver selezionato **IBM embedded Security Subsystem CSP** come CSP, è possibile che venga richiesto di immettere il passphrase UVM, di eseguire una scansione delle impronte digitali o entrambi per soddisfare i requisiti di autenticazione per ottenere un certificato digitale. I requisiti di autenticazione vengono definiti nella politica UVM per il computer.

Trasferimento di certificati da Microsoft CSP

Certificate Transfer Tool di IBM Client Security Software consente di spostare certificati che sono stati creati con il CSP predefinito della Microsoft sul CSP di IBM embedded Security System. Ciò migliora notevolmente la protezione fornita sulle chiavi private associate ai certificati poiché verranno memorizzati in modo sicuro su IBM embedded Security Chip e non su software esposti.

Per eseguire il Certificate Transfer Tool, completare la seguente procedura:

1. Eseguire il programma `xfercert.exe` dalla directory radice di security software (di norma è C:\Program Files\IBM\Security). La finestra principale visualizza certificati associati al CSP predefinito della Microsoft.

   Nota: solo i certificati le cui chiavi private sono contrassegnate come *esportabili* dopo la creazione verranno visualizzati in questo elenco.
2. Selezionare i certificati che si desidera trasferire al CSP di IBM embedded Security System.
3. Premere il pulsante **Trasferisci certificati**.

I certificati vengono, quindi, associati al CSP di IBM embedded Security System e le chiavi private sono protette da IBM embedded Security Chip. Tutte le operazioni che utilizzano tali chiavi private, quali la creazione di firme digitali o la decifrazione di e-mail, verrà eseguita in un ambiente protetto del chip.

Aggiornamento dell'archivio di chiavi per le applicazioni Microsoft

Dopo aver creato un certificato digitale, eseguire una copia di backup del certificato aggiornando l'archivio di chiavi. E' possibile aggiornare l'archivio di chiavi utilizzando Administrator Utility.

Utilizzo del certificato digitale per le applicazioni Microsoft

Utilizzare le impostazioni di sicurezza nelle proprie applicazioni Microsoft per visualizzare e utilizzare certificati digitali. Per ulteriori informazioni, fare riferimento alla documentazione fornita dalla Microsoft.

Dopo aver creato il certificato digitale e averlo utilizzato per firmare un messaggio e-mail, UVM richiederà i requisiti di autenticazione la prima volta in cui si utilizza una firma digitale su un messaggio e-mail. E' possibile che risulti necessario inserire il passphrase UVM, eseguire una scansione delle proprie impronte digitali oppure entrambi per soddisfare i requisiti di autenticazione necessari per poter utilizzare il certificato digitale. I requisiti di autenticazione vengono definiti nella politica UVM per il computer.

Configurazione delle preferenze audio UVM

User Configuration Utility consente di configurare le preferenze audio utilizzando l'interfaccia fornita. Per modificare le preferenze audio predefinite, procedere nel modo seguente:

1. Fare clic su **Avvio > Programmi > Access IBM > IBM Client Security Software > Modifica le impostazioni di sicurezza**.

   Viene visualizzato il pannello di IBM Client Security Software user Configuration Utility.
2. Selezionare il separatore **Configura suoni UVM**.
3. Nell'area relativa ai suoni di autenticazione UVM, immettere il percorso del file audio da associare ad un'autenticazione riuscita nel campo relativo all'autenticazione riuscita oppure fare clic su **Sfoglia** per selezionare il file.
4. Nell'area relativa ai suoni di autenticazione UVM, immettere il percorso del file audio da associare ad un'autenticazione non riuscita oppure fare clic su **Sfoglia** per selezionare il file.
5. Fare clic su **OK** per completare l'operazione.

Capitolo 9. Risoluzione dei problemi

La seguente sezione riporta informazioni utili a prevenire o identificare e correggere i problemi che potrebbero sorgere quando si utilizza Client Security Software.

Funzioni del responsabile

Questa sezione contiene informazioni che un responsabile potrebbe trovare utili quando si imposta e si utilizza Client Security Software.

Impostazione di una password responsabile (ThinkCentre)

Le impostazioni di sicurezza disponibili in Configuration/Setup Utility consentono agli amministratori di:

- Modificare la password hardware per IBM embedded Security Chip
- Abilitare o disabilitare IBM embedded Security Chip .
- Disabilitare IBM embedded Security Chip

Attenzione:

- Non annullare o disabilitare IBM embedded Security Chip quando è attivata la protezione UVM. Se si disabilita il chip, il contenuto del disco fisso diventa inutilizzabile e sarà necessario riformattare l'unità disco fisso e installare di nuovo tutto il software.

  Per disabilitare la protezione UVM, aprire Administrator Utility, quindi fare clic su **Configura politiche e supporto applicazione** e deselezionare la casella di controllo **Sostituisci il collegamento Windows standard con il collegamento di sicurezza UVM**. E' necessario riavviare il computer prima di disabilitare la protezione UVM.
- Non annullare o disabilitare IBM embedded Security Chip quando è attivata la protezione UVM. In caso contrario, verrà bloccato il sistema.
- Quando IBM embedded Security Chip viene disabilitato, tutte le chiavi di cifratura e i certificati memorizzati sul chip vanno perduti.

Poichè alle impostazioni di sicurezza è possibile accedere tramite Configuration/Setup Utility, impostare una password di responsabile per evitare che utenti non autorizzati possano modificare le impostazioni.

Per impostare una password di responsabile:

1. Chiudere e riavviare il computer.
2. Quando viene visualizzato sul pannello di Configuration/Setup Utility, premere **F1**.

   Viene visualizzato il menu principale di Configuration/Setup Utility.
3. Selezionare **Sicurezza del sistema**.
4. Selezionare **Password responsabile**.
5. Immettere la password e premere freccia giù sulla tastiera.
6. Immettere di nuovo la password e premere freccia giù.
7. Selezionare **Modifica password responsabile** e premere Invio; premere di nuovo Invio.

8. Premere **Esc** per uscire e salvare le impostazioni.

Dopo aver impostato la password del responsabile, ogni volta che si desidera accedere a Configuration/Setup Utility viene visualizzata una richiesta.

Importante: conservare la password del responsabile in un luogo sicuro. Se si perde o si dimentica la password del responsabile, non è possibile accedere a Configuration/Setup Utility e non è possibile modificare o cancellare la password senza rimuovere il coperchio del computer e spostare un cavallotto sulla scheda di sistema. Per ulteriori informazioni, consultare la documentazione sull'hardware fornita con il computer.

Impostazione di una password del supervisore (ThinkPad)

Le impostazioni di sicurezza disponibili nel programma di utilità di impostazione IBM BIOS consentono agli amministratori di:

- Abilitare o disabilitare IBM embedded Security Chip
- Disabilitare IBM embedded Security Chip

Attenzione:

- Non annullare o disabilitare IBM embedded Security Chip quando è attivata la protezione UVM. In caso contrario, verrà bloccato il sistema.

  Per disabilitare la protezione UVM, aprire Administrator Utility, quindi fare clic su **Configura politiche e supporto applicazione** e deselezionare la casella di controllo **Sostituisci il collegamento Windows standard con il collegamento di sicurezza UVM**. E' necessario riavviare il computer prima di disabilitare la protezione UVM.

  Quando IBM embedded Security Chip viene disabilitato, tutte le chiavi di cifratura e i certificati memorizzati sul chip vanno perduti.
- E' necessario disabilitare temporaneamente la password del supervisore su alcuni modelli ThinkPad prima di installare o aggiornare Client Security Software.

Una volta impostato Client Security Software, impostare una password del supervisore per evitare che utenti non autorizzati possano modificare queste impostazioni.

Per impostare una password del supervisore, procedere nel modo seguente:

1. Chiudere e riavviare il computer.
2. Quando viene visualizzato sul pannello IBM BIOS Setup Utility, premere **F1**.

   Viene visualizzato il menu principale di IBM BIOS Setup Utility.
3. Selezionare **Password**.
4. Selezionare **Password supervisore**.
5. Immettere la password e premere Invio.
6. Immettere di nuovo la password e premere Invio.
7. Fare clic su **Continua**.
8. Premere F10 per salvare e uscire.

Dopo aver impostato la password del supervisore, ogni volta che si desidera accedere al programma di impostazione IBM BIOS viene visualizzata una richiesta.

Importante: conservare la password del supervisore in un luogo sicuro. Se si perde o si dimentica la password del supervisore, non è possibile accedere al programma

di utilità di impostazione IBM BIOS e non è possibile modificare o cancellare la password. Per ulteriori informazioni, consultare la documentazione sull'hardware fornita con il computer.

Protezione di una password per l'hardware

Impostare la password di Security Chip per abilitare IBM embedded Security Chip per un client. L'accesso a Administrator Utility è protetto anche dalla password di Security Chip. Proteggere la password di Security Chip per impedire ad utenti non autorizzati di modificare le impostazioni del programma Administrator Utility.

Annullamento di IBM embedded Secutity Chip (ThinkCentre)

Per cancellare tutte le chiavi di cifratura dell'utente da IBM embedded Security Chip e annullare la password hardware per il chip, azzerare le impostazioni del chip. Consultare le informazioni contenute nella casella di attenzione prima di azzerare IBM embedded Security Chip .

Attenzione:

- Non annullare o disabilitare IBM embedded Security Chip quando è attivata la protezione UVM. In caso contrario, verrà bloccato il sistema.

  Per disabilitare la protezione UVM, aprire Administrator Utility, quindi fare clic su **Configura politiche e supporto applicazione** e deselezionare la casella di controllo **Sostituisci il collegamento Windows standard con il collegamento di sicurezza UVM**. E' necessario riavviare il computer prima di disabilitare la protezione UVM.
- Quando IBM embedded Security Chip viene disabilitato, tutte le chiavi di cifratura e i certificati memorizzati sul chip vanno perduti.

Per disabilitare IBM embedded Security Chip, procedere nel modo seguente:

1. Chiudere e riavviare il computer.
2. Quando viene visualizzato sul pannello di Configuration/Setup Utility, premere F1.

   Viene visualizzato il menu principale di Configuration/Setup Utility.
3. Selezionare **Sicurezza**.
4. Selezionare **IBM TCPA Setup**.
5. Selezionare **Annulla funzione IBM TCPA Security**.
6. Selezionare **Sì**.
7. Per continuare, premere il tasto Esc.
8. Premere Esc per uscire e salvare le impostazioni.

Annullamento di IBM embedded Security Chip (ThinkPad)

Per cancellare tutte le chiavi di cifratura dell'utente da IBM embedded Security Chip e annullare la password hardware per il chip, azzerare le impostazioni del chip. Consultare le informazioni contenute nella casella di attenzione prima di azzerare IBM embedded Security Chip .

Attenzione:

- Non annullare o disabilitare IBM embedded Security Chip quando è attivata la protezione UVM. Se si disabilita il chip, il contenuto del disco fisso diventa inutilizzabile e sarà necessario riformattare l'unità disco fisso e installare di nuovo tutto il software.

Per disabilitare la protezione UVM, aprire Administrator Utility, quindi fare clic su **Configura politiche e supporto applicazione** e deselezionare la casella di controllo **Sostituisci il collegamento Windows standard con il collegamento di sicurezza UVM**. E' necessario riavviare il computer prima di disabilitare la protezione UVM.

- Quando IBM embedded Security Chip viene disabilitato, tutte le chiavi di cifratura e i certificati memorizzati sul chip vanno perduti.

Per disabilitare IBM embedded Security Chip, procedere nel modo seguente:

1. Chiudere e riavviare il computer.
2. Quando viene visualizzato sul pannello di IBM BIOS Setup Utility, premere Fn.

   Nota: su alcuni modelli ThinkPad, potrebbe essere necessario premere il tasto F1 all'accensione per accedere a IBM BIOS Setup Utility. Per ulteriori informazioni, consultare il messaggio di aiuto nel programma IBM BIOS Setup Utility.

   Viene visualizzato il menu principale di IBM BIOS Setup Utility.
3. Selezionare **Config**.
4. Selezionare **IBM Security Chip**.
5. Selezionare **Annulla IBM embedded Security Chip** .
6. Selezionare **Sì**.
7. Premere Invio per continuare.
8. Premere F10 per salvare e uscire.

Administrator Utility

La seguente sezione contiene informazioni importanti sull'uso del programma Administrator Utility.

Rimozione di utenti

Quando viene eliminato un utente, il nome utente viene eliminato dall'elenco degli utenti Administrator Utility.

Accesso non consentito agli oggetti selezionati con il controllo Tivoli Access Manager

La casella di controllo **Nega tutti gli accessi all'oggetto selezionato** non risulta disabilitata quando viene selezionato il controllo Tivoli Access Manager. Nell'editor della politica UVM, se viene selezionato **Access Manager controlla l'oggetto selezionato** per consentire a Tivoli Access Manager di controllare un oggetto di autenticazione, la casella di controllo **Nega tutti gli accessi all'oggetto selezionato** non è disabilitata. Sebbene la casella di controllo **Nega tutti gli accessi all'oggetto selezionato** risulti disabilitata, non può essere selezionata per sovrascrivere il controllo di Tivoli Access Manager.

Limiti

Questa sezione contiene le informazioni sui limiti di Client Security Software.

Utilizzo di Client Security Software con sistemi operativi Windows

Tutti i sistemi Windows presentano i seguenti limiti: se un utente client registrato con UVM modifica il nome utente di Windows, si perde la funzionalità Client Security. In caso contrario, sarà necessario registrare nuovamente il nuovo nome utente in UVM e richiedere tutte le nuove credenziali.

I sistemi operativi Windows XP presentano i seguenti limiti: gli utenti registrati in UVM che hanno modificato in precedenza il nome utente Windows non vengono riconosciuti da UVM. UVM punterà al primo nome utente mentre con Windows riconoscerà solo il nuovo nome utente. Questo problema si verifica anche se il nome utente di Windows è stato modificato prima di installare Client Security Software.

Utilizzo di Client Security Software con applicazioni Netscape

Dopo un problema di autorizzazione viene aperto Netscape: se viene aperta la finestra passphrase di UVM, è necessario immettere il passphrase UVM e fare clic su **OK** prima di continuare. Se viene immesso un passphrase UVM non corretto (o viene fornita un'impronta non corretta su un dispositivo di scansione impronte), viene visualizzato un messaggio di errore. Se si preme **OK**, Netscape verrà aperto, ma non sarà possibile utilizzare il certificato digitale generato da IBM embedded Security Chip . E' necessario uscire, riaprire Netscape ed immettere il passphrase UVM prima di poter utilizzare il certificato IBM embedded Security Chip .

Gli algoritmi non vengono visualizzati: tutti gli algoritmi hash supportati da IBM embedded Security Chip , modulo PKCS#11, non vengono selezionati se il modulo viene visualizzato in Netscape. I seguenti algoritmi sono supportati dal modulo IBM Security Chip PKCS#11 integrato, ma non sono considerati come supportati quando vengono visualizzati in Netscape:

- SHA-1
- MD5

Certificato IBM embedded Security Chip e algoritmi di cifratura

Vengono fornite le seguenti informazioni come guida all'identificazione di questioni inerenti agli algoritmi di cifratura che è possibile utilizzare con il certificato IBM embedded Security Chip . Consultare Microsoft o Netscape per informazioni sugli algoritmi di cifratura utilizzati con le proprie applicazioni e-mail.

Invio di posta elettronica da un client Outlook Express (128-bit) ad un altro client Outlook Express (128-bit): se risulta possibile utilizzare Outlook Express con la versione a 128-bit di Internet Explorer 4.0 o 5.0 per inviare posta elettronica ad altri client utilizzando Outlook Express (128-bit), i messaggi di posta elettronica cifrati con certificato IBM embedded Security Chip possono utilizzare solo l'algoritmo 3DES.

Invio di posta elettronica tra un client Outlook Express (128-bit) e un client Netscape: al client Netscape con algoritmo RC2(40) viene sempre restituita una richiesta di cifratura RC2(40), RC2(64) o RC2(128) da un client Netscape a un client Outlook Express (128-bit).

Alcuni algoritmi potrebbero non essere disponibili per la selezione in un client Outlook Express (128-bit): a seconda di come è stata configurata o aggiornata la versione di Outlook Express (128-bit), alcuni algoritmi RC2 o altri potrebbero non essere disponibili per essere utilizzati con il certificato di IBM embedded Security Chip . Consultare Microsoft per le informazioni correnti sugli algoritmi cifrati utilizzati con la versione di Outlook Express.

Utilizzo della protezione UVM per un ID utente Lotus Notes

La protezione UVM non opera se vengono attivati gli ID utente all'interno di una sessione Notes: è possibile impostare la protezione UVM solo per l'ID utente corrente di una sessione Notes. Per passare da un ID utente con protezione UVM abilitato ad un altro ID utente, procedere nel modo seguente:

1. Uscire da Notes.
2. Disabilitare la protezione UVM per l'ID utente corrente.
3. Aprire Notes e attivare gli ID utente. Consultare la documentazione Lotus Notes per informazioni su come attivare gli ID utente.

   Per impostare la protezione UVM per l'ID utente attivato, procedere al passo 4.
4. Aprire il programma di configurazione Lotus Notes fornito da Client Security Software ed impostare la protezione UVM.

Limiti di User Configuration Utility

Windows XP impone restrizioni di accesso che limitano le funzioni disponibili ad un utente client in determinate circostanze.

Windows XP Professional

In Windows XP Professional, le restrizioni dell'utente client potrebbero essere applicate nelle seguenti situazioni:

- Client Security Software è installato su una partizione che viene convertita successivamente in un formato NTFS
- La cartella Windows si trova su una partizione che viene convertita successivamente in un formato NTFS
- La cartella di archivio si trova su una partizione che viene convertita successivamente in un formato NTFS

Nelle situazioni precedenti, Windows XP Professional Limited Users potrebbe non essere in grado di eseguire le attività di User Configuration Utility tasks di seguito riportate:

- Modificare il passphrase UVM
- Aggiornare la password di Windows registrata con UVM
- Aggiornare l'archivio delle chiavi

Tali restrizioni vengono eliminate quando un responsabile avvia ed esce da Administrator Utility.

Windows XP Home

Gli utenti limitati di Windows XP Home non potranno utilizzare il programma User Configuration Utility in una delle seguenti situazioni:

- Client Security Software è installato su una partizione formattata NTFS
- La cartella Windows si trova su una partizione formattata NTFS
- La cartella di archivio si trova su una partizione formattata NTFS

Messaggi di errore

I messaggi di errore relativi a Client Security Software sono registrati nel log di eventi: Client Security Software utilizza un driver di periferica che crea i messaggi di errore nel log di eventi. Gli errori associati con questi messaggi non influenzano il normale funzionamento del computer.

UVM richiama i messaggi di errore creati dal programma associato se l'accesso è negato per un oggetto di autenticazione: se la politica UVM è impostata per negare l'accesso per un oggetto di autenticazione, ad esempio la cifratura dell'e-mail, il messaggio che indica l'accesso negato varia in base al tipo di software utilizzato. Ad esempio, un messaggio di errore di Outlook Express che indica l'accesso negato ad un oggetto di autenticazione sarà diverso da un messaggio di errore Netscape, che indica che l'accesso è negato.

Prospetti per la risoluzione dei problemi

Le seguenti informazioni sulla risoluzione dei problemi possono essere utili se si rilevano problemi quando si installa il programma Client Security Software.

Informazioni sulla risoluzione dei problemi relativi all'installazione

Le seguenti informazioni sulla risoluzione dei problemi possono essere utili se si rilevano problemi quando si installa il programma Client Security Software.

Problema	**Possibile soluzione**
Un messaggio di errore viene visualizzato durante l'installazione	**Azione**
Un messaggio viene visualizzato quando si installa il software che richiede di rimuovere l'applicazione selezionata e tutti i relativi componenti.	Per uscire dalla finestra, fare clic su **OK**. Iniziare di nuovo il processo di installazione per installare la nuova versione del programma Client Security Software.
Un messaggio viene visualizzato durante l'installazione che indica che una versione precedente del programma Client Security Software è già installata.	Fare clic su **OK** per uscire dalla finestra. Procedere nel modo seguente: 1. Disinstallare il software. 2. Reinstallare il software. **Nota:** se si desidera utilizzare la stessa password hardware per proteggere IBM embedded Security Chip , non è necessario eliminare il chip e reimpostare la password.
L'accesso di installazione viene negato a causa di una password hardware sconosciuta	**Azione**
Durante l'installazione del software su un client IBM con IBM Security Chip abilitato, la password hardware per IBM Security Chip è sconosciuta.	Eliminare il chip per continuare con l'installazione.
Il file setup.exe non risponde correttamente (CSS versione 4.0x)	**Azione**
Se vengono estratti tutti i file dal file csec4_0.exe in una directory comune, il file setup.exe non funzionerà correttamente.	Eseguire il file smbus.exe per installare il driver di periferica SMBus e poi eseguire il file csec4_0.exe per installare il codice del programma Client Security Software.

Informazioni sulla risoluzione dei problemi del programma Administrator Utility

Le seguenti informazioni sulla risoluzione dei problemi possono essere utili se si conoscono i problemi quando si utilizza il programma Administrator Utility.

Problema	**Possibile soluzione**
Politica passphrase UVM non applicata	**Azione**
La casella di controllo **non contiene più di 2 caratteri ripetuti** non opera in IBM Client Security Software versione 5.0	Questa è una limitazione nota per IBM Client Security Software versione 5.0.
Il pulsante Avanti non è disponibile in seguito all'immissione e alla conferma del passphrase UVM nel programma Administrator Utility	**Azione**
Quando si aggiungono utenti a UVM, il pulsante **Avanti** potrebbe non essere disponibile dopo aver immesso e confermato il passphrase UVM in Administrator Utility.	Fare clic sulla voce **Informazioni** nella barra delle applicazioni di Windows e continuare la procedura.
Un messaggio di errore viene visualizzato quando si tenta di modificare la politica UVM locale	**Azione**
Quando si modifica la politica UVM locale, è possibile che un messaggio di errore sia visualizzato se nessun utente viene registrato in UVM.	Aggiungere un utente a UVM prima di modificare il file di politica.
Un messaggio di errore viene visualizzato quando si modifica la chiave pubblica admin	**Azione**
Quando si elimina l'IBM Security Chip e poi si ripristina l'archivio della chiave, è possibile che un messaggio di errore sia visualizzato se si modifica la chiave pubblica Admin.	Aggiungere gli utenti a UVM e richiedere i nuovi certificati, se validi.
Un messaggio di errore viene visualizzato quando si ripristina un passphrase UVM.	**Azione**
Quando si modifica la chiave pubblica Admin e poi si ripristina una passphrase UVM per un utente, è possibile che sia visualizzato un messaggio di errore.	Eseguire una delle seguenti operazioni: • Se il passphrase UVM per l'utente non è necessario, non viene richiesta alcuna azione. • Se il passphrase UVM per l'utente è necessario, è necessario aggiungere l'utente a UVM e richiedere i nuovi certificati, se validi.
Un messaggio di errore viene visualizzato quando si salva il file di politica UVM	**Azione**
Quando si tenta di salvare un file di politica UVM (globalpolicy.gvm) facendo clic su **Applica** o **Salva**, viene visualizzato un messaggio di errore.	Chiudere il messaggio di errore, modificare di nuovo il file di politica UVM per apportare le modifiche e salvare poi il file.
Un messaggio di errore viene visualizzato quando si tenta di aprire l'editor di politica UVM	**Azione**

Problema	Possibile soluzione
Se l'utente corrente (collegato al sistema operativo) non è stato aggiunto a UVM, l'editor della politica UVM non sarà visualizzato.	Aggiungere l'utente a UVM ed visualizzare UVM Policy Editor.
Un messaggio di errore viene visualizzato quando si utilizza il programma Administrator Utility	**Azione**
Quando si utilizza il programma Administrator Utility, è possibile che sia visualizzato il seguente messaggio di errore: Si è verificato un errore I/E buffer durante il tentativo di accesso al chip del Client Security. E' possibile che questo problema sia risolto da un riavvio.	Uscire dal messaggio di errore e riavviare il computer.
Un messaggio di disabilitazione chip viene visualizzato se si tenta di modificare la password di Security Chip	**Azione**
Quando si tenta di modificare la password di Security Chip e si premere Invio o il separatore > Invio in seguito all'immissione della password di conferma, il pulsante Disabilita il chip sarà abilitato e viene visualizzato un messaggio di conferma della disabilitazione del chip.	Procedere nel modo seguente: 1. Uscire dalla finestra di conferma di disabilitazione del chip. 2. Per modificare la password di Security Chip, inserire la nuova password, inserire la password di conferma e fare clic su **Modifica**. Non premere Invio o il tasto di tabulazione > Invio dopo aver immesso la password di conferma.

Informazioni sulla risoluzione dei problemi del programma User Configuration Utility

Le seguenti informazioni sulla risoluzione dei problemi possono essere utili se si verificano problemi durante l'utilizzo del programma User Configuration Utility.

Problema	Possibile soluzione
Limited Users non è abilitato a eseguire alcune funzioni User Configuration Utility in Windows XP Professional	**Azione**
Windows XP Professional Limited Users potrebbe non essere in grado di eseguire le attività User Configuration Utility di seguito riportate: • Modificare il passphrase UVM • Aggiornare la password di Windows registrata con UVM • Aggiornare l'archivio delle chiavi	Tali restrizioni vengono eliminate quando un responsabile avvia ed esce da Administrator Utility.
Limited Users non è abilitato a utilizzare User Configuration Utility in Windows XP Home	**Azione**

Problema	Possibile soluzione
Gli utenti limitati di Windows XP Home non potranno utilizzare il programma User Configuration Utility in una delle seguenti situazioni: • Client Security Software è installato su una partizione formattata NTFS • La cartella Windows si trova su una partizione formattata NTFS • La cartella di archivio si trova su una partizione formattata NTFS	Si tratta di un limite conosciuto con Windows XP Home. Non esiste alcuna soluzione per questo problema.

Informazioni sulla risoluzione dei problemi specifici al ThinkPad

Le seguenti informazioni sulla risoluzione dei problemi possono risultare utili se si conoscono i problemi quando si utilizza il programma Client Security Software su computer ThinkPad.

Problema	Possibile soluzione
Viene visualizzato un messaggio di errore quando si tenta l'esecuzione di una funzione del responsabile di Client Security	**Azione**
Il seguente messaggio di errore viene visualizzato al tentativo di esecuzione di una funzione del responsabile di Client Security. ERRORE 0197: Richiesta modifica remota non valida. Premere <F1> per l'installazione	E' necessario che la password del responsabile del ThinkPad sia disabilitata per effettuare determinate funzioni del responsabile di Client Security. Per disabilitare la password del supervisore, procedere nel modo seguente: 1. Premere il tasto F1 per accedere al programma IBM BIOS Setup Utility. 2. Inserire la password corrente del responsabile. 3. Inserire una nuova password vuota del responsabile e confermare una password vuota. 4. Premere Invio. 5. Premere F10 per salvare e uscire.
Un diverso sensore per le impronte digitali UVM non funziona correttamente	**Azione**
Il computer IBM ThinkPad non supporta l'interscambio di più sensori per le impronte digitali UVM.	Non commutare i modelli del sensore per le impronte digitali. Utilizzare lo stesso modello durante il funzionamento remoto come durante il funzionamento da una stazione per espansione.

Informazioni sulla risoluzione dei problemi della Microsoft

I seguenti grafici sulla risoluzione dei problemi contengono informazioni che possono essere utili se si conoscono i problemi quando si utilizza il programma Client Security Software con le applicazioni o i sistemi operativi della Microsoft.

Problema	Possibile soluzione
Lo screen saver viene visualizzato solo sullo schermo locale	**Azione**
Durante l'utilizzo della funzione Windows Extended Desktop, lo screen saver di Client Security Software sarà visualizzato solo sullo schermo locale anche se l'accesso al sistema e la tastiera sono protetti.	Se vengono visualizzate le informazioni sensibili, ridurre le finestre del desktop esteso prima di richiamare lo screen saver Client Security.
I file di Windows Media Player sono cifrati piuttosto che riprodotti in Windows XP	**Azione**
In Windows XP, quando si apre una cartella e si seleziona **Riproduci tutto**, il contenuto del file sarà cifrato piuttosto che riprodotto da Windows Media Player.	Per abilitare Windows Media Player al fine di riprodurre i file, completare la seguente procedura: 1. Avviare Windows Media Player. 2. Selezionare tutti i file nella cartella appropriata. 3. Trascinare i file nell'area della lista di esecuzione di Windows Media Player.
Client Security non funziona correttamente per un utente registrato in UVM	**Azione**
E' possibile che l'utente client registrato non abbia modificato il proprio nome utente di Windows. Se si verifica tale situazione, la funzionalità del programma Client Security è persa.	Registrare di nuovo il nuovo nome utente in UVM e richiedere tutte le nuove credenziali.
Nota: In Windows XP, gli utenti registrati in UVM che precedentemente hanno modificato i relativi nomi utente di Windows, non saranno rilevati da UVM. Questo problema si verifica anche se il nome utente di Windows è stato modificato prima di installare Client Security Software.	
Problemi durante la lettura dell'e-mail cifrata mediante Outlook Express	**Azione**
Le e-mail cifrate non possono essere decifrate a causa delle differenze di cifratura dei browser Web utilizzati dal mittente e dal destinatario. **Nota**: per utilizzare i browser Web a 128 bit con il programma Client Security Software, è necessario che IBM embedded Security Chip supporti una cifratura a 256 bit. Se l'IBM embedded Security Chip supporta la cifratura a 56 bit, è necessario utilizzare un browser Web a 40 bit. E' possibile rilevare la cifratura fornita da Client Security Software nel programma Administrator Utility.	Verificare quanto segue: 1. La cifratura per il browser Web utilizzata dal mittente è compatibile con la cifratura del browser Web utilizzata dal destinatario. 2. La cifratura per il browser Web è compatibile con la cifratura fornita dal firmware del programma Client Security Software.
Problemi durante l'utilizzo di un certificato da un indirizzo dotato di più certificati associati	**Azione**

Problema	Possibile soluzione
Outlook Express può elencare più certificati associati con un singolo indirizzo e-mail ed alcuni di questi certificati possono diventare non validi. Un certificato può diventare non valido se la chiave privata associata con il certificato non esiste più in IBM embedded Security Chip del computer del mittente in cui è stato creato il certificato.	Richiedere al destinatario di rinviare il proprio certificato digitale; quindi, selezionare tale certificato nella rubrica per Outlook Express.
Messaggio di errore quando si firma un messaggio e-mail in modo digitale	**Azione**
Se il mittente di un messaggio e-mail prova a firmare un messaggio e-mail in modo digitale quando il mittente non ha già un certificato associato con il relativo account e-mail, viene visualizzato un messaggio di errore.	Utilizzare le impostazioni di sicurezza in Outlook Express per specificare un certificato da associare con l'account utente. Per ulteriori informazioni, consultare la documentazione fornita per Outlook Express.
Outlook Express (128 bit) cifratura i messaggi e-mail con l'algoritmo 3DES	**Azione**
Durante l'invio dell'e-mail cifrata tra i client che utilizzano Outlook Express con la versione a 128 bit di Internet Explorer 4.0 o 5.0, è possibile utilizzare solo l'algoritmo 3DES.	Per utilizzare browser a 128-bit con Client Security Software, IBM embedded Security Chip deve supportare la cifratura a 256-bit. Se l'IBM embedded Security Chip supporta la cifratura a 56 bit, è necessario utilizzare un browser Web a 40 bit. E' possibile rilevare la cifratura fornita da Client Security Software nel programma Administrator Utility. Consultare la Microsoft per le informazioni correnti sugli algoritmi di cifratura, utilizzati con Outlook Express.
I client Outlook Express restituiscono i messaggi e-mail con un diverso algoritmo	**Azione**
Un messaggio e-mail cifrato con l'algoritmo RC2(40), RC2(64) o RC2(128) viene inviato da un client su cui è in uso Netscape Messenger ad un client, su cui è in uso Outlook Express (a 128 bit). Un messaggio e-mail restituito dal client Outlook Express viene cifrato con l'algoritmo RC2(40).	Non è richiesta alcuna azione. Una richiesta di cifratura RC2(40), RC2(64) o RC2(128) da un client di Netscape ad un client di Outlook Express (a 128 bit) viene restituita sempre sul client di Netscape con l'algoritmo RC2(40). Consultare Microsoft per le informazioni correnti sugli algoritmi cifrati utilizzati con la versione di Outlook Express.
Messaggio di errore durante l'utilizzo di un certificato in Outlook Express in seguito ad un errore dell'unità disco fisso	**Azione**
I certificati possono essere ripristinati utilizzando la funzione per il ripristino della chiave nel programma Administrator Utility. E' possibile che alcuni certificati, ad esempio i certificati disponibili, forniti da VeriSign, non siano ripristinati in seguito ad un ripristino della chiave.	Una volta ripristinate le chiavi, procedere nel modo seguente: • reperire i nuovi certificati • registrare di nuovo l'autorizzazione del certificato in Outlook Express
Outlook Express non aggiorna la cifratura associata con un certificato	**Azione**

Problema	Possibile soluzione
Quando un mittente seleziona la cifratura in Netscape ed invia un messaggio e-mail firmato ad un client su cui è in uso Outlook Express con Internet Explorer 4.0 (a 128 bit), è possibile che la cifratura dell'e-mail restituita non corrisponda.	Eliminare il certificato associato dalla rubrica di Outlook Express. Visualizzare di nuovo l'e-mail firmata ed aggiungere il certificato alla rubrica di Outlook Express.
Un messaggio di errore viene visualizzato in Outlook Express	**Azione**
E' possibile visualizzare un messaggio in Outlook Express quando si fa doppio clic. In alcuni casi, quando si fa doppio clic su un messaggio cifrato in modo rapido, viene visualizzato un messaggio di errore relativo alla decifrazione.	Chiudere il messaggio ed aprire nuovamente il messaggio email cifrato.
Inoltre, è possibile che un messaggio di errore relativo alla decifrazione sia visualizzato nel pannello precedente quando si seleziona un messaggio cifrato.	Se il messaggio di errore viene visualizzato nel pannello precedente, non è richiesta alcuna azione.
Un messaggio di errore viene visualizzato se si fa clic sul pulsante Invia due volte su e-mail cifrate	**Azione**
Quando si utilizza Outlook Express, se si fa doppio clic sul pulsante di invio per inviare un messaggio e-mail cifrato, viene visualizzato un messaggio di errore indicante che il messaggio non può essere inviato.	Chiudere questo messaggio di errore e fare clic sul pulsante **Invia** una volta.
Un messaggio di errore viene visualizzato quando viene richiesto un certificato	**Azione**
Quando si utilizza Internet Explorer, è possibile ricevere un messaggio di errore se si richiede un certificato che utilizza IBM embedded Security Chip CSP.	Richiedere di nuovo il certificato digitale.

Informazioni sulla risoluzione dei problemi dell'applicazione Netscape

I seguenti grafici sulla risoluzione dei problemi contengono informazioni che possono essere utili se si conoscono i problemi quando si utilizza il programma Client Security Software con le applicazioni di Netscape.

Problema	Possibile soluzione
Problemi durante la lettura dell'e-mail cifrata	**Azione**

Problema	Possibile soluzione
Le e-mail cifrate non possono essere decifrate a causa delle differenze di cifratura dei browser Web utilizzati dal mittente e dal destinatario. **Nota:** per utilizzare i browser a 128 bit con il programma Client Security Software, è necessario che IBM embedded Security Chip supporti una cifratura a 256 bit. Se IBM embedded Security Chip supporta la cifratura a 256-bit, è necessario utilizzare un browser Web a 40 bit. E' possibile rilevare la cifratura fornita da Client Security Software nel programma Administrator Utility.	Verificare quanto segue: 1. Che la cifratura per il browser Web utilizzata dal mittente sia compatibile con la cifratura del browser Web utilizzata dal destinatario. 2. Che la cifratura per il browser Web sia compatibile con la cifratura fornita dal firmware del programma Client Security Software.
Messaggio di errore quando si firma un messaggio e-mail in modo digitale	**Azione**
Se il certificato di IBM embedded Security Chip non è stato selezionato in Netscape Messenger ed un writer di un messaggio e-mail tenta di firmare il messaggio con il certificato, viene visualizzato un messaggio di errore.	Utilizzare le impostazioni di sicurezza in Netscape Messenger per selezionare il certificato. Quando viene aperto Netscape Messenger, fare clic sull'icona Sicurezza, situata sulla barra degli strumenti. Viene visualizzata la finestra Info sicurezza. Fare clic su **Messenger** situato nel pannello sinistro e poi selezionare il **certificato di IBM embedded Security Chip** . Per ulteriori informazioni, fare riferimento alla documentazione fornita da Netscape.
Un messaggio e-mail viene restituito al client con un diverso algoritmo	**Azione**
Un messaggio e-mail cifrato con l'algoritmo RC2(40), RC2(64) o RC2(128) viene inviato da un client su cui è in uso Netscape Messenger ad un client, su cui è in uso Outlook Express (a 128 bit). Un messaggio e-mail restituito dal client Outlook Express viene cifrato con l'algoritmo RC2(40).	Non è richiesta alcuna azione. Una richiesta di cifratura RC2(40), RC2(64) o RC2(128) da un client di Netscape ad un client di Outlook Express (a 128 bit) viene restituita sempre sul client di Netscape con l'algoritmo RC2(40). Consultare Microsoft per le informazioni correnti sugli algoritmi cifrati utilizzati con la versione di Outlook Express.
Impossibile utilizzare il certificato digitale, creato di IBM embedded Security Chip	**Azione**
Il certificato digitale creato dall'IBM Security Chip non è disponibile per essere utilizzato.	Verificare che il passphrase UVM corretto sia stato inserito quando viene visualizzato Netscape. Se si inserisce il passphrase UVM errato, viene visualizzato un messaggio di errore di autenticazione. Se si fa clic su **OK**, Netscape viene visualizzato, ma l'utente non sarà in grado di utilizzare il certificato creato da IBM embedded Security Chip . E' necessario uscire e riaprire Netscape, quindi inserire il passphrase corretto UVM.
I nuovi certificati digitali dallo stesso mittente non sono sostituiti all'interno di Netscape	**Azione**

Problema	Possibile soluzione
Quando viene ricevuta un'e-mail firmata in modo digitale più di una volta dallo stesso mittente, il primo certificato digitale associato con l'e-mail non viene sovrascritto.	Se si ricevono più certificati e-mail, solo un certificato è quello predefinito. Utilizzare le funzioni di sicurezza di Netscape per eliminare il primo certificato, quindi riaprire il secondo certificato o richiedere al mittente di inviare un'altra e-mail firmata.
Impossibile esportare il certificato di IBM embedded Security Chip	**Azione**
Il certificato di IBM embedded Security Chip non può essere esportato in Netscape. La funzione di esportazione di Netscape può essere utilizzata per eseguire il backup dei certificati.	Passare al programma Administrator Utility o User Configuration Utility per aggiornare l'archivio chiave. Quando si aggiorna l'archivio della chiave, sono create le copie di tutti i certificati associati con IBM embedded Security Chip .
Un messaggio di errore viene visualizzato durante il tentativo di utilizzare un certificato ripristinato in seguito ad un errore del disco fisso	**Azione**
I certificati possono essere ripristinati utilizzando la funzione per il ripristino della chiave nel programma Administrator Utility. E' possibile che alcuni certificati, ad esempio i certificati disponibili, forniti da VeriSign, non siano ripristinati in seguito ad un ripristino della chiave.	Una volta ripristinate le chiavi, reperire un nuovo certificato.
L'agente di Netscape viene visualizzato e causa un errore relativo a Netscape	**Azione**
L'agente di Netscape visualizza e chiude Netscape.	Disattivare l'agente di Netscape.
Netscape ritarda quando si tenta di aprirlo	**Azione**
Se si aggiunge il modulo PKCS#11 di IBM embedded Security Chip e poi si apre Netscape, si verifica un breve ritardo prima della visualizzazione di Netscape.	Non è richiesta alcuna azione. Queste informazioni sono valide solo a scopo informativo.

Informazioni sulla risoluzione dei problemi relativi al certificato digitale

Le seguenti informazioni sulla risoluzione dei problemi possono essere utili se si conoscono i problemi relativi al reperimento di un certificato digitale.

Problema	Possibile soluzione
La finestra del passphrase UVM o la finestra di autenticazione delle impronte digitali viene visualizzata più volte durante una richiesta del certificato digitale.	**Azione**

Problema	Possibile soluzione
La politica di sicurezza UVM indica che un utente fornisce il passphrase UVM o le impronte digitali prima di poter acquistato un certificato digitale. Se l'utente tenta di acquistare un certificato, la finestra di autenticazione richiede che la scansione delle impronte digitali o il passphrase UVM viene visualizzato più di una volta.	Inserire il passphrase UVM oppure eseguire la scansione delle impronte digitali ogni volta che viene visualizzata la finestra di autenticazione.
Viene visualizzato un messaggio di errore VBScript o JavaScript	**Azione**
Se si richiede un certificato digitale, è possibile che sia un messaggio di errore relativo a VBScript o JavaScript.	Riavviare il computer e reperire di nuovo il certificato.

Informazioni sulla risoluzione dei problemi di Tivoli Access Manager

Le seguenti informazioni sulla risoluzione dei problemi potrebbero essere utili se si verificano problemi durante l'utilizzo di Tivoli Access Manager con Client Security Software.

Problema	Possibile soluzione
Le impostazioni sulla politica locali non corrispondono a quelle sul server	**Azione**
Tivoli Access Manager consente alcune configurazioni non supportate da UVM. Di conseguenza, i requisiti sulla politica locali possono ignorare le impostazioni del responsabile durante la configurazione del server PD.	Si tratta di un limite conosciuto.
Le impostazioni di Tivoli Access Manager non sono accessibili.	**Azione**
Le impostazioni di Tivoli Access e della cache locale non sono accessibili dalla pagina relativa in Administrator Utility.	Installare Tivoli Access runtime Environment. Se Runtime Environment non è installato sul client IBM, le impostazioni di Tivoli Access sulla pagina relativa non saranno disponibili.
Il controllo utente è valido sia per l'utente che per il gruppo	**Azione**
Quando viene configurato il server di Tivoli Access, se si definisce l'utente di un gruppo, il controllo utente è valido sia per l'utente che per il gruppo.	Non è richiesta alcuna azione.

Informazioni sulla risoluzione dei problemi relativi a Lotus Notes

Le seguenti informazioni sulla risoluzione dei problemi possono essere utili se si conoscono i problemi quando si utilizza Lotus Notes con il programma Client Security Software.

Problema	Possibile soluzione
Dopo l'abilitazione della protezione UVM per Lotus Notes, Notes non è in grado di terminare l'installazione	**Azione**
Lotus Notes non è in grado di terminare l'installazione dopo che viene abilitata la protezione UVM utilizzando il programma Administrator Utility.	Si tratta di un limite conosciuto. E' necessario che Lotus Notes sia configurato e sia in esecuzione prima che sia abilitato il supporto Lotus Notes nel programma Administrator Utility.
Un messaggio di errore viene visualizzato quando si tenta di modificare la password di Notes	**Azione**
E' possibile che la modifica della password di Notes durante l'utilizzo del programma Client Security Software visualizzi un messaggio di errore.	Riprovare la modifica della password. Se non funziona, riavviare il client.
Un messaggio di errore viene visualizzato in seguito ad una creazione casuale di una password	**Azione**
E' possibile che un messaggio di errore sia visualizzato quando si procede nel modo seguente: • Utilizzare lo strumento Configurazione di Lotus Notes per impostare la protezione UVM per un ID Notes • Visualizzare Notes ed utilizzare la funzione fornita da Notes per modificare la password per il file ID Notes • Chiudere Notes immediatamente dopo la modifica della password	Fare clic su **OK** per chiudere il messaggio di errore. Non è richiesta ulteriore azione. Diversamente dal messaggio di errore, la password è stata modificata. La nuova password è una password creata in modo casuale dal programma Client Security Software. Il file ID Notes viene cifrato con la password creata in modo casuale e l'utente non necessita di un nuovo file ID utente. Se l'utente modifica di nuovo la password, UVM crea una nuova password casuale per ID Notes.

Informazioni sulla risoluzione dei problemi relativi alla cifratura

le seguenti informazioni sulla risoluzione dei problemi possono risultare utili se si conoscono i problemi quando si cifrano i file utilizzando il programma Client Security Software 3.0 o successive.

Problema	Possibile soluzione
I file cifrati precedentemente non saranno decifrati	**Azione**
I file cifrati con le versioni precedenti del programma Client Security Software non sono cifrati in seguito all'aggiornamento del programma Client Security Software 3.0 o successive.	Si tratta di un limite conosciuto. E' necessario decifrare tutti i file che sono stati cifrati, utilizzando versioni precedenti del programma Client Security Software, *prima* di installare il programma Client Security Software 3.0. Il programma Client Security Software 3.0 non può decifrare i file che sono stati cifrati utilizzando le versioni precedenti del programma Client Security Software a causa delle modifiche contenute nell'implementazione di cifra del file.

Informazioni sulla risoluzione dei problemi relativi all'unità UVM

Le seguenti informazioni sulla risoluzione dei problemi possono essere utili se si conoscono i problemi quando si utilizzano le unità UVM.

Problema	**Possibile soluzione**
Un'unità UVM interrompe il funzionamento correttamente	**Azione**
Quando un'unità UVM viene scollegata dalla porta USB (Universal Serial Bus) e poi l'unità viene collegata di nuovo alla porta USB, è possibile che l'unità non funzioni correttamente.	Riavviare il computer una volta collegata nuovamente l'unità alla porta USB.

Appendice A. Norme per l'esportazione di Client Security Software

Il pacchetto IBM Client Security Software è stato revisionato dalla IBM Export Regulation Office (ERO) e come richiesto dalle norme di esportazione del governo americano, IBM ha inoltrato la documentazione appropriata e ottenuto l'approvazione per la classificazione di commercio al dettaglio per un supporto di cifratura fino a 256 bit dal Department of Commerce americano per la distribuzione internazionale ad eccezione dei paesi in cui il governo americano ha imposto l'embargo. Le norme negli Stati Uniti D'America e negli altri paesi sono soggette a modifiche da parte del governo del rispettivo paese.

Se non è possibile scaricare il pacchetto Client Security Software, contattare gli uffici vendita IBM per verificare con IBM Country Export Regulation Coordinator (ERC).

Appendice B. Regole per password e passphrase

Questa appendice contiene informazioni relative alle regole delle varie password di sistema.

Regole per la password hardware

Le seguenti regole si applicano alla password hardware:

Lunghezza
Le password devono essere costituite esattamente da otto caratteri.

Caratteri
La password deve contenere solo caratteri alfanumerici. E' consentita una combinazione di lettere e di numeri. Non è consentito alcun carattere aggiuntivo, come lo spazio, !, ?, %.

Proprietà
Impostare la password Security Chip per abilitare IBM embedded Security Chip nel computer. E' necessario che questa password sia inserita ogni volta che si accede al programma Administrator Utility.

Tentativi non corretti
Se si inserisce la password in modo non corretto per dieci volte, il computer viene bloccato per 1 ora e 17 minuti. Se trascorre tale periodo di tempo, inserire la password in modo non corretto per più di dieci volte, il computer viene bloccato per 2 ore e 34 minuti. L'intervallo di tempo della disabilitazione del computer raddoppia ogni volta che si inserisce in modo errato la password per dieci volte.

Regole per passphrase UVM

Per migliorare la sicurezza, il passprhase UVM è più lunga e può essere più univoca rispetto alla password tradizionale. La politica passphrase UVM è controllata da IBM Client Security Administrator Utility.

L'interfaccia relativa alla politica passphrase UVM in Administrator Utility consente ai responsabili della sicurezza di controllare i criteri passphrase tramite una semplice interfaccia. L'interfaccia relativa alla politica passphrase UVM consente al responsabile di stabilire le regole passphrase di seguito riportate:

Nota: l'impostazione predefinita per ciascun criterio di passphrase viene fornita di seguito tra parentesi.

- Stabilire se impostare un numero minimo di caratteri alfanumerici consentiti (si, 6)

  Ad esempio, quando è impostato a ″6″ caratteri consentiti,1234567xxx è una password non valida.
- Stabilire se impostare un numero minimo di caratteri numerici consentiti (si, 1)

  Ad esempio, quando è impostato a ″1″, questaèlapassword è una password non valida.
- Stabilire se impostare un numero minimo di spazi consentiti (nessun minimo)

  Ad esempio, quando è impostato a ″2″, non sono qui è una password non valida.

- Stabilire se consentire più di due caratteri ripetuti (no)

  Ad esempio, quando è stabilito,`aaabcdefghijk` è una password non valida.
- Stabilire se consentire che il passphrase inizi con un carattere numerico (no)

  Ad esempio, per impostazione predefinita, `1password` è una password non valida.
- Stabilire se consentire che il passphrase termini con un carattere numerico (no)

  Ad esempio, per impostazione predefinita, `password8` è una password non valida.
- Stabilire se consentire che il passphrase contenga un ID utente (no)

  Ad esempio, per impostazione predefinita, `Nome Utente` è una password non valida, dove `Nome Utente` è un ID utente.
- Stabilire se consentire che il nuovo passphrase sia diverso dagli ultimi x passphrase, dove x è un campo editabile (si, 3)

  Ad esempio, per impostazione predefinita, `password` è una password non valida se qualcuna delle ultime tre password era `password`.
- Stabilire se il passphrase può contenere più di tre caratteri consecutivi identici in qualunque posizione rispetto alla password precedente (no)

  Ad esempio, per impostazione predefinita, `paswor` è una password non valida se la password precedente era `pass` o `word`.

Inoltre, l'interfaccia relativa alla politica passphrase UVM in Administrator Utility consente ai responsabili della sicurezza di controllare i criteri di scadenza dei passphrase. L'interfaccia relativa alla politica passphrase UVM consente al responsabile di scegliere tra le regole di scadenza passphrase di seguito riportate:

- stabilire se il passphrase scade dopo un numero di giorni precedentemente impostato (si, 184)

  Ad esempio, per impostazione predefinita il passphrase scade ogni 184 giorni. E' necessario che il nuovo passphrase sia conforme alla politica dei passphrase stabilita.
- stabilire se il passphrase non scade

  Quando viene selezionata questa opzione, il passphrase non scade.

La politica della passphrase viene controllata nel programma Administrator Utility quando l'utente viene registrato e verificato anche quando l'utente modifica la passphrase nel programma Client Utility. Le due impostazioni dell'utente relative alla password precedente saranno reimpostate e qualsiasi cronologia per il passphrase sarà rimossa.

Le seguenti regole generali sono relative alla passhrase UVM:

Lunghezza
: Il passphrase può contenere fino a 256 caratteri.

Caratteri
: Il passphrase può contenere qualsiasi combinazione di caratteri prodotti dalla tastiera, includendo spazi e caratteri non alfanumerici.

Proprietà
: Il passphrase UVM è diverso da una password da utilizzare per collegarsi ad un sistema operativo. Il passphrase UVM può essere utilizzato insieme ad altre unità di autenticazione, ad esempio un sensore per le impronte digitali UVM.

Tentativi non corretti

Se si inserisce il passphrase UVM in modo non corretto per più volte durante una sessione, il computer non viene bloccato. Non è presente alcun limite sul numero dei tentativi errati.

Appendice C. Regole sull'uso della protezione UVM per il collegamento del sistema

La protezione UVM verifica che solo gli utenti aggiunti a UVM per un client IBM specifico, sono in grado di accedere al sistema operativo. I sistemi operativi Windows comprendono le applicazioni che forniscono la protezione del collegamento. Sebbene la protezione UVM sia designata per lavorare in parallelo con queste applicazioni del collegamento di Windows, la protezione UVM varia in base al sistema operativo.

L'interfaccia del collegamento UVM sostituisce il collegamento del sistema operativo, in modo tale che la finestra del collegamento UVM viene visualizzata ogni volta che un utente tenta di collegarsi al sistema.

Leggere i seguenti suggerimenti prima di impostare ed utilizzare la protezione UVM per il collegamento di sistema:

- Non eliminare IBM embedded Security Chip mentre è abilitata la protezione UVM. In tal caso, il contenuto del disco fisso diventa inutilizzabile ed è necessario riformattare l'unità disco fisso e reinstallare tutto il software.
- Se si deseleziona la casella di controllo **Sostituisci il collegamento standard di Windows con il collegamento sicuro di UVM** in Administrator Utility, il sistema torna al processo di collegamento di Windows senza la protezione del collegamento UVM.
- E' possibile specificare il numero massimo dei tentativi consentiti per immettere la corretta password per l'applicazione del collegamento di Windows. Questa opzione non *viene applicata* alla protezione del collegamento UVM. Non esiste alcun limite da impostare per il numero di tentativi consentiti per immettere il passphrase UVM.

Appendice D. Marchi e informazioni particolari

La presente appendice contiene informazioni particolari relative ai prodotti IBM e le informazioni sui marchi.

Informazioni particolari

Queste informazioni sono state sviluppate per prodotti e servizi offerti negli Stati Uniti

I riferimenti contenuti in questa pubblicazione relativi a prodotti o servizi IBM non implicano che l'IBM intenda renderli disponibili in tutti i paesi in cui opera. Consultare il rappresentante IBM locale per informazioni relative a prodotti e servizi disponibili nel proprio paese. Qualsiasi riferimento a prodotti, programmi o servizi IBM non implica che possano essere utilizzati soltanto tali prodotti, programmi o servizi. In sostituzione a quelli forniti dall'IBM, possono essere utilizzati prodotti, programmi o servizi funzionalmente equivalenti che non comportino violazione dei diritti di proprietà intellettuale dell'IBM. Tuttavia, è responsabilità dell'utente valutare e verificare la possibilità di utilizzare altri programmi e/o prodotti non forniti dall'IBM.

IBM può avere brevetti o domande di brevetto in corso relativi a quanto trattato nel presente documento. La fornitura di questa pubblicazione non implica la concessione di alcuna licenza su di essi. Coloro che desiderassero ricevere informazioni relative alle licenze, potranno rivolgersi per iscritto a:

IBM Director of Commercial Relations IBM Europe 1070 - Boeblingen Schoenaicher Str.220 Deutschland.

Il seguente paragrafo non è valido per il regno Unito o per tutti i paesi le cui leggi nazionali siano in contrasto con le disposizioni locali: L'INTERNATIONAL BUSINESS MACHINES CORPORATION FORNISCE QUESTA PUBBLICAZIONE ″NELLO STATO IN CUI SI TROVA″ SENZA ALCUNA GARANZIA, ESPLICITA O IMPLICITA, IVI INCLUSE EVENTUALI GARANZIE DI COMMERCIABILITA' ED IDONEITA' AD UNO SCOPO PARTICOLARE. Alcuni stati non consentono la rinuncia a garanzie esplicite o implicite in determinate transazioni; quindi la presente dichiarazione potrebbe non essere a voi applicabile.

Questa pubblicazione potrebbe contenere imprecisioni tecniche o errori tipografici. Le informazioni incluse in questo documento vengono modificate periodicamente; tali modifiche verranno integrate nelle nuove edizioni della pubblicazione. L'IBM si riserva il diritto di apportare miglioramenti e/o modifiche al prodotto e/o al programma descritto nel manuale in qualsiasi momento e senza preavviso.

Coloro che detengono la licenza su questo programma e desiderano avere informazioni su di esso allo scopo di consentire (1) uno scambio di informazioni tra programmi indipendenti ed altri (compreso questo) e (ii) l'uso reciproco di tali informazioni, dovrebbero rivolgersi a IBM Corporation, Department 80D,P.O. Box 12195, 3039 Cornwallis, Research Triangle Park, NC 27709 U.S.A. Queste informazioni possono essere rese disponibili secondo condizioni contrattuali appropriate, compreso, in alcuni casi, il pagamento di un addebito.

Il programma su licenza descritto in questo manuale e tutto il materiale su licenza ad esso relativo sono forniti dall'IBM nel rispetto dei termini dell'IBM Customer Agreement, dell'IBM International Program License Agreement o ad ogni altro accordo equivalente.

Marchi

IBM e SecureWay sono marchi IBM Corporation.

Tivoli è un marchio Tivoli Systems Inc.

Microsoft, Windows e Windows NT sono marchi della Microsoft Corporation negli Stati Uniti, negli altri paesi o entrambi.

I nomi di altre società, prodotti e servizi potrebbero essere marchi di altre società.

Riservato ai commenti del lettore

IBM® Client Security
Solutions
Client Security Software versione 5.1 - Guida per il responsabile

Numero parte 59P7640

Commenti relativi alla pubblicazione in oggetto potranno contribuire a migliorarla. Sono graditi commenti pertinenti alle informazioni contenute in questo manuale ed al modo in cui esse sono presentate. Si invita il lettore ad usare lo spazio sottostante citando, ove possibile, i riferimenti alla pagina ed al paragrafo.

Si prega di non utilizzare questo foglio per richiedere informazioni tecniche su sistemi, programmi o pubblicazioni e/o per richiedere informazioni di carattere generale.

Per tali esigenze si consiglia di rivolgersi al punto di vendita autorizzato o alla filiale IBM della propria zona oppure di chiamare il ″Supporto Clienti″ IBM al numero verde 800-017001.

I suggerimenti ed i commenti inviati potranno essere usati liberamente dall'IBM e dalla Selfin e diventeranno proprietà esclusiva delle stesse.

Commenti:

Si ringrazia per la collaborazione.

Per inviare i commenti è possibile utilizzare uno dei seguenti modi.

- Spedire questo modulo all'indirizzo indicato sul retro.
- Inviare un fax al numero: +39-081-660236
- Spedire una nota via email a: translationassurance@selfin.it

Se è gradita una risposta dalla Selfin, si prega di fornire le informazioni che seguono:

Nome

Indirizzo

Società

Numero di telefono

Indirizzo e-mail

Indicandoci i Suoi dati, Lei avrà l'opportunità di ottenere dal responsabile del Servizio di Translation Assurance della Selfin S.p.A. le risposte ai quesiti o alle richieste di informazioni che vorrà sottoporci. I Suoi dati saranno trattati nel rispetto di quanto stabilito dalla legge 31 dicembre 1996, n.675 sulla "Tutela delle persone e di altri soggetti rispetto al trattamento di dati personali". I Suoi dati non saranno oggetto di comunicazione o di diffusione a terzi; essi saranno utilizzati "una tantum" e saranno conservati per il tempo strettamente necessario al loro utilizzo.

Selfin S.p.A.
Translation Assurance

Via F. Giordani, 7

80122 NAPOLI

Numero parte: 59P7640

Printed in Denamrk by IBM Danmark A/S

(1P) P/N: 59P7640