Soluzioni IBM® Client Security

Utilizzo di Client Security Software versione 5.3 con Tivoli® Access Manager

Soluzioni IBM® Client Security

Utilizzo di Client Security Software versione 5.3 con Tivoli® Access Manager

Prima edizione (maggio 2004)

Prima di utilizzare questo prodotto e le relative informazioni, consultare la sezione Appendice A, "Norme per l'esportazione di Client Security Software", a pagina 37 e l'Appendice D, "**Marchi e informazioni particolari**", a pagina 45.

Indice

Prefazione v
A chi si rivolge questa guida v
Modalità di utilizzo di questa guida vi
Riferimenti al manuale *Guida all'installazione di Client Security Software* vi
Riferimenti al manuale *Client Security Software Guida per il responsabile* vi
Ulteriori informazioni vi

Capitolo 1. Introduzione 1
IBM Embedded Security Subsystem 1
IBM Embedded Security Chip 1
IBM Client Security Software 2
Relazione tra password e chiavi 2
Password del responsabile 2
Chiavi hardware pubbliche e private 3
Chiavi pubbliche e private del responsabile . . . 4
Archivio ESS 4
Chiavi utente pubbliche e private 4
Gerarchia basata sullo scambio di chiavi IBM . . 4
Funzioni PKI (Public key Infrastructure) CSS . . . 6

Capitolo 2. Installazione del componente Client Security su un server Tivoli Access Manager 9
Prerequisiti 9
Scaricamento e installazione del componente Client Security 9
Aggiunta del componente Client Security sul server di Tivoli Access Manager 10
Stabilire una connessione protetta tra il client IBM e il server di Tivoli Access Manager 11

Capitolo 3. Configurazione dei client IBM 13
Prerequisiti 13
Configurazione delle informazioni di impostazione di Tivoli Access Manager 13
Impostazione ed uso della funzione di cache locale 14
Abilitazione di Access Manager per controllare gli oggetti del client IBM 14
Modifica di una politica UVM locale 15
Modifica e utilizzo della politica UVM per i client remoti 16

Capitolo 4. Risoluzione dei problemi . . 17
Funzioni del responsabile. 17
Autorizzazione degli utenti 17
Rimozione di utenti 17
Impostazione della password del responsabile di BIOS (ThinkCentre). 17
Impostazione di una password del supervisore (ThinkPad) 18
Protezione della password del responsabile. . . . 19
Annullamento di IBM embedded Security Subsystem (ThinkCentre) 19
Annullamento di IBM embedded Security Subsystem (ThinkPad). 20
Limitazioni note relative a CSS versione 5.2 . . . 20
Limitazioni di roaming 20
Limitazioni del badge di prossimità 22
Ripristino delle chiavi 22
Nomi di dominio e nomi utenti locali 22
Reinstallazione del software per le impronte digitali Targus 22
Passphrase del supervisore di BIOS 23
Utilizzo di 7.x 23
Utilizzo di un minidisco per l'archiviazione . . 23
Limitazioni delle Smart card. 23
Dopo la cifratura viene visualizzato il carattere più (+) sulle cartelle 23
Limitazioni di Windows XP con gli utenti limitati 24
Altre limitazioni 24
Utilizzo di Client Security Software con sistemi operativi Windows 24
Utilizzo di Client Security Software con applicazioni Netscape 24
Certificato IBM embedded Security Subsystem e algoritmi di cifratura 24
Utilizzo della protezione UVM per un ID utente Lotus Notes 25
Limiti di User Configuration Utility 25
Limitazioni relative a Tivoli Access Manager . . 26
Messaggi di errore 26
Prospetti per la risoluzione dei problemi. 26
Informazioni sulla risoluzione dei problemi relativi all'installazione 26
Informazioni sulla risoluzione dei problemi del programma Administrator Utility 27
Informazioni sulla risoluzione dei problemi del programma User Configuration Utility 28
Informazioni sulla risoluzione dei problemi specifici al ThinkPad 29
Informazioni sulla risoluzione dei problemi della Microsoft 30
Informazioni sulla risoluzione dei problemi dell'applicazione Netscape 32
Informazioni sulla risoluzione dei problemi relativi al certificato digitale 34
Informazioni sulla risoluzione dei problemi di Tivoli Access Manager. 34
Informazioni sulla risoluzione dei problemi relativi a Lotus Notes 35
Informazioni sulla risoluzione dei problemi relativi alla cifratura 36
Informazioni sulla risoluzione dei problemi relativi all'unità UVM 36

Appendice A. Norme per l'esportazione di Client Security Software 37

Appendice B. Informazioni sulle password e i passphrase 39
Regole per password e passphrase. 39
Regole per la password del responsabile. . . . 39
Regole per passphrase UVM. 39
Conteggi errati su sistemi TCPA e non TCPA . . . 41
Reimpostazione di un passphrase 41
Reimpostazione remota di un passphrase . . . 41
Reimpostazione manuale di un passphrase . . . 42

Appendice C. Regole sull'uso della protezione UVM per il collegamento del sistema 43

Appendice D. Marchi e informazioni particolari 45
Informazioni particolari 45
Marchi 46

Prefazione

Questa guida contiene le informazioni utili sull'installazione del programma Client Security Software da utilizzare con IBM Tivoli Access Manager.

Questa guida è organizzata nel modo seguente:

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

″Capitolo 2. Installazione del componente Client Security su un server di Tivoli Access Manager″, contiene i prerequisiti e le istruzioni per l'installazione del supporto Client Security sul server Tivoli Access Manager.

″Capitolo 3. Configurazione dei client IBM″, contiene le informazioni sui prerequisiti e le istruzioni sulla configurazione dei client IBM per utilizzare i servizi di autenticazione forniti da Tivoli Access Manager.

″Capitolo 4, "Risoluzione dei problemi"″, contiene le informazioni utili per la risoluzione dei problemi che si possono verificare utilizzando le istruzioni fornite con questa guida.

″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, "Informazioni sulle password e i passphrase",″ contiene i criteri relativi al passphrase applicabili alle regole e ad un passphrase UVM per le password del responsabile.

″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 si rivolge ai responsabili dell'azienda che utilizzano Tivoli Access Manager versione 3.9 per gestire gli oggetti di autenticazione impostati dalla politica di protezione UVM (User Verification Manager) su un client IBM.

I responsabili devono essere a conoscenza dei seguenti concetti e procedure:

- Installazione del protocollo LDAP (lightweight directory access protocol) di SecureWay Directory
- Procedure di installazione e impostazione per l'ambiente di esecuzione di Tivoli Access Manager
- Gestione dello spazio degli oggetti di Tivoli Access Manager

Modalità di utilizzo di questa guida

Utilizzare la guida per configurare il supporto Client Security per Tivoli Access Manager. Questa guida si integra con *Guida all'installazione di Client Security Software*, *Guida per il responsabile di Client Security Software* e *Guida per l'utente di Client Security*.

Questa guida e la relativa documentazione di Client Security possono essere scaricate dal sito web IBM all'indirizzo http://www.pc.ibm.com/us/security/index.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. Dopo aver impostato e configurato il server di Tivoli Access Manager ed installato l'ambiente di esecuzione sul client, utilizzare le istruzioni contenute nella *Guida all'installazione di Client Security Software* per installare Client Security Software sui client IBM. Per ulteriori informazioni, consultare il Capitolo 3, "Configurazione dei client IBM", a pagina 13.

Riferimenti al manuale *Client Security Software Guida per il responsabile*

I riferimenti al manuale *Client Security Software Guida per il responsabile* vengono forniti in questo documento. *La guida per il responsabile di Client Security Software* contiene informazioni su come impostare l'autenticazione utente e la politica UVM per il client IBM. Una volta installato Client Security Software, utilizzare il manuale *Guida per il responsabile di Client Security Software* per impostare l'autenticazione utente e la politica della protezione. Per ulteriori informazioni, consultare il Capitolo 3, "Configurazione dei client IBM", a pagina 13.

Ulteriori informazioni

E' possibile ottenere ulteriori informazioni e aggiornamenti per la protezione dei prodotti, se disponibili, visitando il sito web IBM all'indirizzo http://www.pc.ibm.com/us/security/index.html.

Capitolo 1. Introduzione

Gli elaboratori ThinkPad™ e ThinkCentre™ dispongono di componenti hardware di cifratura, che operando con le tecnologie software scaricabili, forniscono un elevato livello di protezione alle piattaforme client. L'insieme di tali tecnologie hardware e software è denominato IBM Embedded Security Subsystem (ESS). Il componente hardware è IBM Embedded Security Chip, mentre quello software è IBM Client Security Software (CSS).

Client Security Software è stato progettato per elaboratori IBM che utilizzano IBM Embedded Security Chip per cifrare i file e memorizzarne le chiavi di cifratura. Questo software è costituito da applicazioni e componenti che consentono a sistemi client IBM di utilizzare funzioni di protezione client attraverso un rete locale, un'azienda o attraverso Internet.

IBM Embedded Security Subsystem

IBM ESS supporta soluzioni per la gestione delle chiavi, come ad esempio PKI (Public Key Infrastructure) e comprende le applicazioni logiche di seguito riportate:

- File and Folder Encryption (FFE)
- Password Manager
- Collegamento Windows protetto
- Vari metodi di autenticazione configurabile, compresi:
  - Password
  - Impronte digitali
  - Smart Card
  - Scheda di prossimità

Per utilizzare in modo efficiente le funzioni di IBM ESS, è necessario che un responsabile della protezione acquisisca alcuni concetti di base. Le sezioni di seguito riportate illustrano alcuni concetti di base sulla protezione.

IBM Embedded Security Chip

IBM Embedded Security Subsystem rappresenta la tecnologia hardware di cifratura integrata che fornisce un ulteriore livello di protezione alle piattaforme PC IBM. Con il sottosistema di protezione, le procedure di cifratura e autenticazione vengono trasferite dal software, più vulnerabile in un ambiente più protetto da hardware dedicato. L'incremento di protezione fornito da questa soluzione è tangibile.

IBM Embedded Security Subsystem supporta:

- Operazioni RSA3 PKI, come ad esempio la cifratura per riservatezza e le firme digitali per l'autenticazione
- Generazione chiave RSA
- Generazione numero casuale
- Computo funzione RSA in 200 millisecondi
- Memoria EEPROM per memorizzazione coppia chiavi RSA
- Tutte le funzioni TCPA definite nelle specifiche della versione 1.1

- Comunicazione con il processore principale mediante bus LPC (Low Pin Count)

IBM Client Security Software

IBM Client Security Software è costituito dalle applicazioni software e dai componenti di seguito riportati:

- **Administrator Utility:** Administrator Utility è l'interfaccia che un responsabile utilizza per attivare o disattivare IBM embedded Security Subsystem e per creare, archiviare e rigenerare le chiavi di cifratura e i passphrase. Inoltre, un responsabile può utilizzare questo programma di utilità per aggiungere utenti alla politica di protezione fornita da Client Security Software.
- **Administrator Console:** La console del responsabile di Client Security Software consente al responsabile di configurare una rete di roaming delle credenziali per creare e configurare file che consentono la distribuzione e per creare una configurazione non del responsabile e un profilo di ripristino.
- **User Configuration Utility:** Il programma User Configuration Utility consente ad un utente client di modificare il passphrase UVM, di abilitare le password di collegamento Windows affinché siano riconosciute da UVM, di aggiornare gli archivi delle chiavi e registrare le impronte digitali. Inoltre, un utente può effettuare le copie di backup dei certificati digitali creati con IBM embedded Security Subsystem.
- **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. Client Security Software abilita alle funzioni di seguito riportate:
  - **Protezione della politica del client UVM:** Client Security Software consente al responsabile della protezione di impostare la politica di protezione del client, che stabilisce il modo in cui viene autenticato un utente client nel 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. Se la password di Windows non è registrata oppure è stata registrata in modo non corretto, con UVM, l'utente ha la possibilità di fornire la password corretta di Windows come parte del collegamento.
  - **Protezione del collegamento del sistema UVM:** Client Security Software consente ad un responsabile della protezione di controllare l'accesso all'elaboratore mediante un'interfaccia di collegamento. La protezione UVM verifica che solo gli utenti che sono riconosciuti dalla politica di protezione siano in grado di accedere al sistema operativo.

Relazione tra password e chiavi

Le Password e le chiavi operano in sincronia, insieme alle altre funzioni opzionali di autenticazione per verificare l'identità degli utenti del sistema. La relazione tra le password e le chiavi consente di comprendere il funzionamento di IBM Client Security Software.

Password del responsabile

La password del responsabile viene utilizzata per autenticare un responsabile per IBM Embedded Security Subsystem. La password, che deve essere costituita da

otto caratteri, viene conservata e autenticata nell'ambiente hardware protetto di Embedded Security Subsystem. Una volta autenticato, il responsabile può effettuare quanto di seguito riportato:

- Registrare gli utenti
- Avviare l'interfaccia per la politica di protezione
- Modificare la password del responsabile

La password del responsabile può essere impostata nei seguenti modi:

- Mediante la procedura guidata all'installazione di IBM Client Security
- Mediante il programma Administrator Utility
- Utilizzando gli script
- Mediante l'interfaccia BIOS (solo elaboratori ThinkCentre)

E' importante stabilire dei criteri per la creazione e la conservazione della password del responsabile. E' possibile modificare la password del responsabile se viene dimenticata o corrotta.

Per coloro che conoscono i concetti e la terminologia TCG (Trusted Computing Group), la password del responsabile è uguale al valore di autorizzazione dell'utente cui appartiene. Poiché la password del responsabile è associata a IBM Embedded Security Subsystem, talvolta viene denominata *password dell'hardware*.

Chiavi hardware pubbliche e private

La premessa principale di IBM Embedded Security Subsystem è di fornire una *root* ad elevata affidabilità ad un sistema di client. Questa root viene utilizzata per proteggere altre applicazioni e funzioni. La creazione di un chiave hardware pubblica ed una chiave hardware privata è parte della procedura di istituzione di una root affidabile. Le chiavi pubbliche e private, denominate *coppia di chiavi*, sono matematicamente correlate in modo che:

- I dati cifrati con la chiave pubblica possono essere decifrati solo con la chiave privata corrispondente.
- I dati cifrati con la chiave privata possono essere decifrati solo con la chiave pubblica corrispondente.

La chiave hardware privata viene creata, memorizzata ed utilizzata nell'ambiente hardware protetto del sottosistema di protezione. La chiave hardware pubblica viene resa disponibile per vari scopi (di qui il nome chiave pubblica), ma non è mai esposta fuori dell'ambiente hardware protetto del sottosistema di protezione. Le chiavi hardware pubbliche e private sono parti critiche della gerarchia basata sullo scambio di chiavi IBM descritta nella seguente sezione.

Le chiave hardware pubbliche e private vengono create nei modi di seguito riportati:

- Mediante la procedura guidata all'installazione di IBM Client Security
- Mediante il programma Administrator Utility
- Utilizzando gli script

Per coloro che conoscono i concetti e la terminologia TCGF (Trusted Computing Group), le chiavi hardware pubbliche e private sono denominate *SRK* (Storage Root Key).

Chiavi pubbliche e private del responsabile

Le chiavi pubbliche e private del responsabile sono parte integrante della gerarchia basata sullo scambio di chiavi IBM. Inoltre, consentono di effettuare copie di backup e il ripristino dei dati specifici per l'utente in caso di errore della scheda di sistema o del disco fisso.

Le chiavi pubbliche e private del responsabile possono essere uniche per tutti i sistemi oppure possono essere comuni a tutti i sistemi o gruppi di sistemi. Si noti che le chiavi del responsabile devono essere gestite stabilendo un criterio per l'utilizzo di chiavi uniche contro chiavi note.

Le chiavi pubbliche e private del responsabile possono essere create in uno dei modi di seguito riportati:

- Mediante la procedura guidata all'installazione di IBM Client Security
- Mediante il programma Administrator Utility
- Utilizzando gli script

Archivio ESS

Le chiavi pubbliche e private del responsabile consentono di effettuare copie di backup e ripristino di dati specifici per l'utente in caso di errore della scheda di sistema o del disco fisso.

Chiavi utente pubbliche e private

IBM Embedded Security Subsystem crea chiavi utente pubbliche e private per proteggere dati specifici per l'utente stesso. Queste coppie di chiavi vengono create quando un utente è registrato in IBM Client Security Software. Queste chiavi vengono create e gestite in modo trasparente dal componente UVM (User Verification Manager) di IBM Client Security Software. Sono gestite in base all'utente Windows collegato al sistema operativo.

Gerarchia basata sullo scambio di chiavi IBM

Un elemento essenziale di IBM Embedded Security Subsystem è costituito dalla gerarchia basata sullo scambio di chiavi IBM. La base (o root) della gerarchia basata sullo scambio di chiavi IBM è costituita dalle chiavi hardware pubbliche e private. Le chiavi hardware pubbliche e private, denominate *coppia di chiavi hardware*, vengono create da IBM Client Security Software e sono statisticamente uniche per ciascun client.

IL "livello" superiore della gerarchia (superiore alla root) è costituito dalle chiavi pubbliche e private del responsabile, denominate anche *coppia di chiavi del responsabile*. La coppia di chiavi del responsabile può essere unica per ciascuna macchina o può essere la stessa per tutti i client o sottoinsiemi di client. La gestione di questa coppia di chiavi è correlata alla gestione della rete. La chiave privata del responsabile è unica, in quanto si trova sul sistema client (protetto dalla chiave hardware pubblica) in una posizione definita dal responsabile.

IBM Client Security Software registra gli utenti Windows in ambiente Embedded Security Subsystem. Quando un utente viene registrato, vengono create le chiavi pubbliche e private (*coppia di chiavi utente*) oltre ad un nuovo "livello" di chiavi. La chiave utente privata viene cifrata con la chiave pubblica del responsabile. La chiave privata del responsabile viene cifrata con la chiave hardware pubblica. Quindi, per utilizzare la chiave privata utente, è necessario che venga caricata la chiave privata del responsabile (cifrata con la chiave hardware pubblica) nel

sottosistema di protezione. Una volta nel chip, la chiave hardware privata decifra la chiave privata del responsabile. La chiave privata del responsabile è ora pronta per l'utilizzo nel sottosistema di protezione, in modo che i dati cifrati con la corrispondente chiave pubblica del responsabile possano essere scambiati nel sottosistema di protezione, decifrati e utilizzati. La chiave privata dell'utente corrente di Windows (cifrata con la chiave pubblica del responsabile) viene passata nel sottosistema di protezione. I dati necessari ad un'applicazione che condizionano Embedded security Chip vengono passati nel chip, decifrati e gestiti nell'ambiente protetto del sottosistema di protezione. Un esempio potrebbe essere una chiave privata utilizzata per autenticare una rete senza fili.

Ogni volta che viene richiesta una chiave, lo scambio avviene nel sottosistema di protezione. Le chiavi private cifrate vengono scambiate nel sottosistema di protezione, quindi possono essere utilizzate nell'ambiente protetto del chip stesso. Le chiavi private non sono mai esposte o utilizzate fuori da questo ambiente hardware. Ciò consente di proteggere una quantità di dati illimitata mediante IBM Embedded Security Chip.

Le chiavi private vengono cifrate, sia per motivi di protezione sia per la quantità limitata di spazio disponibile in IBM Embedded Security Subsystem. E' possibile memorizzare solo una coppia di chiavi nel sottosistema di protezione in qualunque momento. Le chiavi hardware pubbliche e private sono le sole chiavi che restano memorizzate nel sottosistema di protezione durante l'avvio. Per consentire la memorizzazione di più chiavi e più utenti, CSS utilizza la gerarchia basata sullo scambio di chiavi IBM. Ogni volta che viene richiesta una chiave, lo scambio avviene in IBM Embedded Security Subsystem. Le chiavi private cifrate correlate vengono scambiate nel sottosistema di protezione, quindi possono essere utilizzate nell'ambiente protetto del chip stesso. Le chiavi private non sono mai esposte o utilizzate fuori da questo ambiente hardware.

La chiave privata del responsabile viene cifrata con la chiave hardware pubblica. La chiave hardware privata, disponibile solo nel sottosistema di protezione, viene utilizzata per decifrare la chiave privata del responsabile. Una volta decifrata la chiave privata del responsabile nel sottosistema di protezione, è possibile passare una chiave utente privata (cifrata con la chiave pubblica del responsabile) nel sottosistema di protezione e decifrarla con la chiave privata del responsabile. Con la chiave pubblica del responsabile, è possibile cifrare più chiavi utente private. Ciò consente di autenticare un numero virtualmente illimitato di utenti su un sistema con IBM ESS, tuttavia, per ottenere prestazioni ottimali, si consiglia di limitare la registrazione a 25 utenti per elaboratore.

IBM ESS utilizza una gerarchia basata sullo scambio di chiavi in cui le chiavi hardware pubbliche e private che si trovano nel sottosistema di protezione vengono utilizzate per proteggere i dati memorizzati fuori del chip stesso. La chiave hardware privata viene generata nel sottosistema di protezione e rimane sempre in questo ambiente protetto. La chiave hardware pubblica è disponibile fuori del sottosistema di protezione ed è utilizzata per cifrare o proteggere altri dati, come ad esempio una chiave privata. Una volta cifrati questi dati con la chiave hardware pubblica, è possibile decifrarli solo con la chiave hardware privata. Poiché la chiave hardware privata è disponibile solo nell'ambiente protetto del sottosistema di protezione, i dati cifrati possono essere solo decifrati ed utilizzati nello stesso ambiente protetto. Si noti che ciascun elaboratore dispone di una chiave hardware pubblica e privata unica. La capacità di numerazione casuale di IBM Embedded Security Subsystem assicura che ciascuna coppia di chiavi hardware sia statisticamente unica.

Funzioni PKI (Public key Infrastructure) CSS

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 protezione del client.** L'autenticazione degli utenti finali a livello di client rappresenta un problema di politica di protezione di rilevante importanza. Client Security Software fornisce l'interfaccia che è richiesta per gestire la politica di protezione 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 cifratura per la cifratura delle chiavi pubbliche.** I responsabili creano le chiavi di cifratura 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 protezione 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 applica un certificato digitale da poter utilizzare per firmare o cifrare digitalmente messaggi e-mail, Client Security Software consente di selezionare IBM embedded Security Subsystem come CSP (cryptographic service provider) per le applicazioni che utilizzano Microsoft CryptoAPI. Tali applicazioni includono Internet Explorer e Microsoft Outlook Express. Ciò assicura che la chiave privata del certificato digitale sia cifrata con la chiave pubblica dell'utente in IBM embedded Security Subsystem. Inoltre, gli utenti di Netscape possono selezionare IBM embedded Security Subsystem come creatore della chiave privata per i certificati digitali utilizzati per la protezione. Le applicazioni che utilizzano (PKCS) #11 (Public-Key Cryptography Standard), ad esempio Netscape Messenger si avvalgono della protezione fornita da IBM embedded Security Subsystem.
- **La capacità di trasferire certificati digitali a IBM embedded Security Subsystem.** IBM Client Security Software Certificate Transfer Tool consente di spostare i certificati creati con Microsoft CSP predefinito in IBM embedded Security Subsystem CSP. Ciò aumenta la protezione fornita alle chiavi private associate con i certificati poiché non sono memorizzate su IBM embedded Security Subsystem, invece del software.

  Nota: I certificati digitali protetti da IBM embedded Security Subsystem CSP non possono essere esportati in un altro CSP.
- **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. IBM Client Security Software dispone di un'interfaccia che consente di stabilire un archivio per le chiavi e i certificati digitali creati con IBM embedded Security Subsystem e di ripristinare tali chiavi e certificati, se occorre.
- **Cifratura di file e cartelle.** Il programma di utilità FFE (File and folder encryption) consente a un utente client di cifrare e decifrare file e cartelle. Questa operazione implementa il livello di protezione dei dati ottimizzando 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 protegge ulteriormente il sistema, in quanto quest'ultima deve essere fornita con una password, che può essere compromessa.
- **Roaming delle credenziali.** Il roaming delle credenziali consente ad un utente della rete autorizzato di utilizzare qualunque elaboratore della rete come propria stazione di lavoro. Una volta che l'utente è autorizzato ad utilizzare UVM su un qualunque client registrato Client Security Software, è possibile importare i dati personali su qualunque altro client registrato nella rete di roaming delle credenziali. I dati personali verranno aggiornati automaticamente e memorizzati nell'archivio di CSS e in ogni elaboratore in cui sono stati importati. L'aggiornamento dei dati personali come nuovi certificati o le modifiche dei passphrase saranno immediatamente disponibili su tutti gli elaboratori connessi alla rete di roaming.
- **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.

Capitolo 2. Installazione del componente Client Security su un server Tivoli Access Manager

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

La politica di protezione 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

Prima di poter utilizzare Client Security con Tivoli Access Manager, è necessario installare il componente Client Security di Tivoli Access Manager. E' possibile scaricare questo componente dal sito web IBM all'indirizzo http://www.pc.ibm.com/us/security/index.html.

Prerequisiti

Prima di poter stabilire una connessione protetta tra il client IBM e il server Tivoli Access Manager, è necessario installare i seguenti componenti sul client IBM:

- IBM Global Security Toolkit
- IBM SecureWay Directory Client
- Ambiente di esecuzione di Tivoli Access Manager

Per informazioni dettagliate sull'installazione e l'uso di Tivoli Access Manager, consultare la documentazione fornita sul sito Web http://www.tivoli.com/products/index/secureway_policy_dir/index.htm.

Scaricamento e installazione del componente Client Security

Il componente Client Security è disponibile gratuitamente sul sito Web IBM.

Per scaricare e installare il componente Client Security sul server Tivoli Access Manager e sul client IBM, completare la seguente procedura:

1. Utilizzando le informazioni sul sito Web, verificare che IBM embedded security chip sia presente sul sistema e che il numero del modello corrisponda a quello fornito nella tabella per i requisiti del sistema; quindi, fare clic su **Continua**.
2. Selezionare il pallino che corrisponde al Tipo di macchina e fare clic su **Continua**.
3. Creare un ID utente, effettuare la registrazione presso la IBM compilando il modulo in linea e consultare l'Accordo di licenza; quindi, fare clic su **Accetto la licenza**.

   Verrà visualizzata la pagina per lo scaricamento del programma Client Security in modo automatico.
4. Seguire la procedura presente nella pagina di scaricamento per installare tutti i driver di periferica necessari, i file README, il software, i documenti di riferimento ed i programmi di utilità aggiuntivi.

5. Installare il programma Client Security Software completando la seguente procedura:
   a. Dal desktop di Windows fare clic su **Start > Esegui**.
   b. Nel campo Esegui, immettere `d:\directory\csec50.exe`, dove d:\directory\ è l'unità e la directory in cui è ubicato il file.
   c. Fare clic su **OK**.

      Viene visualizzata la finestra Benvenuti nella procedura guidata InstallShield per IBM Client Security Software.
   d. Fare clic su **Avanti**.

      La creazione guidata estrae i file ed installa il software. Una volta completata l'installazione, verrà fornita l'opzione per riavviare l'elaboratore in questo momento oppure successivamente.
   e. Selezionare il pallino appropriato e fare clic su **OK**.
6. Una volta riavviato l'elaboratore dal desktop di Windows, fare clic su **Start > Esegui**.
7. Nel campo Esegui, immettere `d:\directory\TAMCSS.exe`, dove d:\directory\ indica la lettera identificativa dell'unità e la directory in cui viene situato il file oppure fare clic su **Sfoglia** per individuare il file.
8. Fare clic su **OK**.
9. Specificare una cartella di destinazione e fare clic su **Decomprimi**.

   La creazione guidata estrae i file nella cartella specificata. Un messaggio indica che i file vengono decompressi in modo corretto.
10. Fare clic su **OK**.

Aggiunta del componente Client Security sul server di Tivoli Access Manager

Il programma pdadmin è uno strumento di riga comandi che un responsabile può utilizzare per eseguire le attività di gestione di Tivoli Access Manager. L'esecuzione di più comandi consente a un responsabile di utilizzare un file che contenga più comandi pdadmin per eseguire un'attività completa o una serie di attività. La comunicazione tra il programma pdadmin e Management Server (pdmgrd) viene protetta su SSL. Il programma di utilità pdadmin viene installato come parte del pacchetto Tivoli Access Manager Runtime Environment (PDRTE).

Il programma di utilità pdadmin accetta un argomento di nome file che identifica l'ubicazione di un tale file, ad esempio:

```
MSDOS>pdadmin [-a <utente-admin >][-p <password >]<nomepercorso-file >
```

Il comando di seguito riportato è un esempio per creare lo spazio oggetti delle Soluzioni IBM, le azioni di Client Security e le singole voci ACL sul server di Tivoli Access Manager:

```
MSDOS>pdadmin -a sec_master -p password C:\TAM_Add_ClientSecurity.txt
```

Fare riferimento al manuale relativo alla guida per il responsabile di *Tivoli Access Manager Base* per ulteriori informazioni sul programma pdadmin e sulla sintassi dei comandi.

Stabilire una connessione protetta tra il client IBM e il server di Tivoli Access Manager

Il client IBM deve stabilire la sua identità autenticata all'interno del dominio protetto di Tivoli Access Manager per richiedere l'autorizzazione dal servizio delle autorizzazioni di Tivoli Access Manager.

E' necessario creare un'identità univoca per l'applicazione nel dominio protetto di Tivoli Access Manager. Affinché l'identità autenticata esegue i controlli di autenticazione, l'applicazione deve essere membro del gruppo remote-acl-users. Quando l'applicazione tenta di collegarsi ad uno dei servizi di dominio protetto, è prima necessario collegarsi al dominio protetto.

Il programma di utilità svrsslcfg consente alle applicazioni IBM Client Security di comunicare con i server di gestione e autorizzazione di Tivoli Access Manager.

Il programma di utilità svrsslcfg consente alle applicazioni IBM Client Security di comunicare con i server di gestione e autorizzazione di Tivoli Access Manager.

Il programma di utilità svrsslcfg consente di effettuare le seguenti attività:

- Crea un'identità utente per l'applicazione. Ad esempio, DemoUser/HOSTNAME
- Crea un file di chiavi SSL per quell'utente. Ad esempio, DemoUser.kdb e DemoUser.sth
- Aggiunge l'utente al gruppo remote-acl-users

E' necessario inserire i seguenti parametri:

- **-f file_cfg** nome e percorso del file di configurazione, utilizzare TAMCSS.conf
- **-d dir_kdb** la directory che deve contenere i file di database key ring per il server.
- **-n nome_server** il nome utente reale Windows nomeutente/UVM dell'utente IBM Client inserito.
- **-P pwd_admin**la password di responsabile di Tivoli Access Manager.
- **-s tipo_server** specificarlo come remoto.
- **-S pwd_server**la password per l'utente appena creato. Questo parametro è obbligatorio.
- **-r num_porta** impostare il numero di porta di ascolto per il client IBM. Si tratta del parametro specificato nella porta server SSL della variabile PDRE (Tivoli Access Manager Runtime) per il server di gestione PD.
- **-e pwd_life** Impostare la scadenza della password in numero di giorni.

Per stabilire una connessione protetta tra il client IBM e il server di Tivoli Access Manager, seguire questa procedura:

1. Creare una directory e spostare il file TAMCSS.conf sulla nuova directory.

   Ad esempio, `MSDOS> mkdir C:\TAMCSS MSDOS> move C:\TAMCSS.conf C:\TAMCSS\`
2. Eseguire svrsslcfg per creare l'utente.

   MSDOS> svrsslcfg -config -f C:\TAMCSS\TAMCSS.conf -d C:\TAMCSS\ -n <server_name> - s remote -S <server_pwd> -P <admin_pwd> -e 365 -r 199

   Nota: sostituire <nome_server> con il nome utente UVM inserito e il nome host del client IBM. Ad esempio: –n DemoUser/MyHostName. Il nome host del client IBM può essere rilevato immettendo "hostname" al

prompt di MSDOS. Il programma svrsslcfg crea una voce valida nel server di Tivoli Access Manager e fornisce il file di chiavi SSL univoco per le comunicazioni cifrate.

3. Eseguire svrsslcfg per aggiungere l'ubicazione di ivacld al file TAMCSS.conf.

   L'impostazione predefinita prevede che il server di autorizzazione PD sia in ascolto sulla porta 7136. Ciò può essere verificato rilevando il parametro tcp_req_port nella stanza ivacld del file ivacld.conf sul server di Tivoli Access Manager. E' importante riportare correttamente il nome host ivacld. Utilizzare il comando di elenco del server pdadmin per ottenere queste informazioni. I server sono definiti come: <nome_server>-<nome_host>. Quello che segue è un esempio di esecuzione dell'elenco del server pdadmin:

```
MSDOS> pdadmin server list ivacld-MyHost.ibm.com
```

Il comando che segue viene poi utilizzato per aggiungere una voce di replica per il server ivacld sopra riportato. Si presume che ivacld sia in ascolto sulla porta predefinita 7136.

```
svrsslcfg -add_replica  -f <config file path> -h <host_name>
MSDOS>svrsslcfg -add_replica  -f C:\TAMCSS\TAMCSS.conf -h MyHost.ibm.com
```

Capitolo 3. Configurazione dei client IBM

Prima di utilizzare Tivoli Access Manager per controllare gli oggetti di autenticazioni per i client IBM, è necessario configurare ciascun client utilizzando Administrator Utility, un componente che viene fornito con Client Security Software. Questa sezione contiene i prerequisiti e le istruzioni per la configurazione dei client IBM.

Prerequisiti

Assicurarsi che il seguente software sia installato sul client IBM nel seguente ordine:

1. **Sistema operativo Microsoft Windows.** E' possibile utilizzare Tivoli Access Manager per controllare i requisiti di autenticazione per i client IBM su cui è in esecuzione Windows XP, Windows 2000 o Windows NT Workstation 4.0.
2. **Client Security Software versione 3.0 o successiva.** Una volta installato il software ed abilitato IBM embedded Security Chip, è possibile utilizzare il programma Client Security Administrator Utility per impostare l'autenticazione utente e per modificare la politica di protezione UVM. Per le istruzioni estese sull'installazione e l'uso di Client Security Software, consultare la *Guida all'installazione di Client Security Software* e la *Guida per il responsabile di Client Security Software*.

Configurazione delle informazioni di impostazione di Tivoli Access Manager

Una volta installato Tivoli Access Manager sul client locale, è possibile configurare le informazioni sull'installazione di Access Manager mediante il programma Administrator Utility, un componente software fornito da Client Security Software. Le informazioni di impostazione di Access Manager comprendono:

- La selezione del percorso completo del file di configurazione
- La selezione dell'intervallo di aggiornamento cache locale

Per configurare le informazioni di impostazione di Tivoli Access Manager sul client IBM, completare la seguente procedura:

1. Fare clic su **Start > Impostazioni > Pannello di controllo > IBM Embedded Security Subsystem**.
2. Inserire la password per il responsabile e fare clic su **OK**.

   Dopo aver immesso la password, viene visualizzata la finestra principale del programma Administrator Utility.
3. Fare clic sul pulsante **Configura politica e supporto dell'applicazione**.

   Viene visualizzato il pannello Configurazione della politica e applicazione UVM.
4. Selezionare la casella **Sostituisci il collegamento Windows standard con il collegamento protetto di UVM**.
5. Fare clic sul pulsante **Politica dell'applicazione**.
6. Nell'area Informazioni di impostazione di Tivoli Access Manager, selezionare il percorso completo del file di configurazione TAMCSS.conf. Ad esempio, `C:\TAMCSS\TAMCSS.conf`

E' necessario che Tivoli Access Manager sia installato sul client per questa area disponibile.

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

   Viene visualizzato il pannello Inserisci password del responsabile.

8. Inserire la password del responsabile nel campo fornito e fare clic su **OK**.

   Viene visualizzata la finestra Politica UVM IBM.

9. Selezionare le azioni che si desidera che Tivoli Access Manager controlli dal menu a discesa Azioni.
10. Selezionare la casella Access Manager controlla l'oggetto selezionato in modo da rendere visibile un segno di spunta nella casella.
11. Fare clic sul pulsante **Applica**.

    Le modifiche vengono applicate al successivo aggiornamento della cache. Se si desidera che le modifiche siano applicate adesso, fare clic sul pulsante **aggiorna cache locale**.

Impostazione ed uso della funzione di cache locale

Una volta selezionato il file di configurazione di Tivoli Access Manager, è possibile impostare l'intervallo di aggiornamento della cache locale. Una replica locale delle informazioni sulla politica di protezione nel modo in cui viene gestito da Tivoli Access Manager viene conservata sul client IBM. E' possibile pianificare un aggiornamento automatico della cache locale con frequenze di mesi (0-12) o giorni (0-30).

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

1. Fare clic su **Start > Impostazioni > Pannello di controllo > IBM Embedded Security Subsystem**.
2. Immettere la password del responsabile, quindi fare clic su **OK**.

   Viene visualizzata la finestra Administrator Utility. Per informazioni complete sull'uso di Administrator Utility, consultare la *guida alla gestione di Client Security Software*.

3. In Administrator Utility, fare clic sul pulsante **Configura politica e supporto dell'applicazione**, quindi fare clic su **Politica dell'applicazione**.

   Viene visualizzata la finestra Modifica configurazione della politica di Client Security.

4. Effettuare una delle seguenti operazioni:
   - Per aggiornare la cache locale, fare clic su **Aggiorna cache locale**.
   - Per impostare la frequenza di aggiornamento, inserire il numero dei mesi (0-12) e dei giorni (0-30) nei campi forniti e fare clic su **Aggiorna cache locale**. La cache locale e data di scadenza del file della cache locale vengono aggiornate in modo da indicare il successivo aggiornamento automatico.

Abilitazione di Access Manager per controllare gli oggetti del client IBM

La politica UVM viene controllata tramite un file globale della politica. Il file della politica globale, chiamato file di politica UVM, contiene i requisiti di autenticazione per le azioni che vengono eseguite sul sistema client IBM, come la registrazione di sistema, l'aggiornamento dello screen saver o la firma dei messaggi di e-mail.

Prima di attivare Tivoli Access Manager in modo da controllare gli oggetti di autenticazione per un client IBM, utilizzare l'editor della politica UVM per modificare il file della politica UVM. L'editor della politica UVM fa parte di Administrator Utility.

Importante: l'attivazione di Tivoli Access Manager per il controllo di un oggetto fornisce 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.

Modifica di una politica UVM locale

Prima di tentare di modificare la politica UVM per il client locale, verificare che almeno un utente sia stato registrato in UVM. Diversamente, un messaggio di errore viene visualizzato quando Policy Editor tenta di aprire il file della politica locale.

Modificare una politica locale UVM ed utilizzarla solo sul client per il quale è stata modificata. Se Client Security è installato nella propria posizione predefinita, la politica locale UVM viene memorizzata come \Program Files\IBM\Security\UVM_Policy\globalpolicy.gvm. Solo un utente che è stato aggiunto a UVM può utilizzare l'editor della politica UVM.

Nota: 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, per utilizzare quell'oggetto deve registrare le proprie impronte digitali.

Per avviare l'editor della politica UVM, completare la seguente procedura di Administrator Utility:

1. Fare clic sul pulsante **Configura politica e supporto dell'applicazione**, quindi fare clic sul pulsante **Politica dell'applicazione**.

   Viene visualizzata la finestra Modifica configurazione della politica di Client Security.
2. Fare clic sul pulsante **Modifica politica**.

   Viene visualizzato il pannello Inserisci password del responsabile.
3. Inserire la password del responsabile nel campo fornito e fare clic su **OK**.

   Viene visualizzata la finestra Politica UVM IBM.
4. Nel separatore Selezione dell'oggetto, fare clic su **Azione** o **Tipo di oggetto** e selezionare l'oggetto per il quale si desidera assegnare in requisiti di autenticazione.

   Gli esempi di azioni valide comprendono il collegamento al sistema, lo sblocco del sistema e la decifra e-mail; un esempio di tipo oggetto è Acquire Digital Certificate.
5. Per ciascun oggetto selezionato, scegliere **Tivoli Access Manager controlla l'oggetto selezionato** per attivare Tivoli Access Manager per quell'oggetto.

   Importante: l'attivazione di Tivoli Access Manager per il controllo di un oggetto fornisce 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.

   Nota: durante la modifica della politica UVM, è possibile visualizzare le informazioni di riepilogo della politica facendo clic su **Riepilogo della politica**.

6. Fare clic su **Applica** per salvare le modifiche apportate.
7. Fare clic su **OK** per 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 è stato installato Client Security Software nella propria posizione predefinita, la directory principale per i percorsi precedenti è \Program Files. Copiare entrambi i file nel percorso di directory \IBM\Security\UVM_Policy\ sui client remoti.

Capitolo 4. 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.

IBM Client Security Software può essere utilizzato solo con elaboratori IBM su cui è installato IBM embedded Security Subsystem. Questo software è costituito da applicazioni e componenti che consentono ai client IBM di proteggere le informazioni sensibili mediante la protezione dell'hardware piuttosto che mediante un software, che è più vulnerabile.

Autorizzazione degli utenti

Prima di proteggere le informazioni dell'utente client, IBM Client Security Software **deve** essere installato sul client e gli utenti **devono** essere autorizzati ad utilizzare il software. Una procedura guidata rende più semplice il processo di installazione.

Importante: almeno un utente client **deve** essere autorizzato ad utilizzare UVM durante l'impostazione. Se non è autorizzato alcun utente all'utilizzo di UVM per l'impostazione iniziale di Client Security Software, le impostazioni di protezione **non** verranno applicate e le informazioni **non** verranno protette.

Se la procedura guidata all'installazione viene completata senza l'autorizzazione di alcun utente, chiudere e riavviare l'elaboratore, quindi eseguire la procedura guidata all'installazione di Client Security dal menu Start di Windows, quindi autorizzare un utente Windows all'utilizzo di UVM. Ciò consente a IBM Client Security Software di applicare le impostazioni di protezione alle informazioni sensibili.

Rimozione di utenti

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

Impostazione della password del responsabile di BIOS (ThinkCentre)

Le impostazioni di protezione disponibili in Configuration/Setup Utility consentono ai responsabili di:

- Abilitare o disabilitare IBM embedded Security Subsystem
- Eliminare IBM embedded Security Subsystem

Attenzione:

- Quando IBM embedded Security Subsystem viene eliminato, tutte le chiavi di cifratura e i certificati memorizzati nel sottosistema andranno perduti.

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

Per impostare la password del responsabile di BIOS:

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

   Viene visualizzato il menu principale di Configuration/Setup Utility.
3. Selezionare **Protezione 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 di BIOS, viene visualizzata una richiesta ogni volta che si accede a Configuration/Setup Utility.

Importante: conservare un record della password del responsabile di BIOS in un luogo sicuro. Se si perde o si dimentica la password del responsabile di BIOS, non è possibile accedere a Configuration/Setup Utility, quindi non sarà possibile modificare o eliminare la password del responsabile di BIOS senza rimuovere il coperchio dell'elaboratore e spostare un cavallotto che si trova 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 protezione disponibili nel programma di utilità di impostazione IBM BIOS consentono ai responsabili di:

- Abilitare o disabilitare IBM embedded Security Subsystem
- Eliminare IBM embedded Security Subsystem

Attenzione:

- 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:

Esempio 1

1. Chiudere e riavviare il computer.
2. Quando viene visualizzata la finestra Setup Utility, premere il tasto F1.

   Viene aperto il menu principale di 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.

Esempio 2

1. Chiudere e riavviare il computer.
2. Quando viene visualizzato il messaggio ″To interrupt normal startup, press the blue Access IBM button″, premere il pulsante blu Access IBM.

   Viene aperta Access IBM Predesktop Area.
3. Fare doppio clic su **Start setup utility**.
4. Selezionare **Protezione** utilizzando i tasti di spostamento cursore per spostarsi nel menu.
5. Selezionare **Password**.
6. Selezionare **Password supervisore**.
7. Immettere la password e premere Invio.
8. Immettere di nuovo la password e premere Invio.
9. Fare clic su **Continua**.
10. Premere F10 per salvare e uscire.

Dopo aver impostato la password del supervisore, viene visualizzata una richiesta ogni volta che si accede a BIOS Setup Utility.

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 della password del responsabile

La password del responsabile limita l'accesso al programma Administrator Utility. Tenere in un luogo sicuro la password del responsabile per impedire agli utenti non autorizzati di modificare le impostazioni del programma Administrator Utility.

Annullamento di IBM embedded Security Subsystem (ThinkCentre)

Se si desidera cancellare tutte le chiavi di cifratura dell'utente da IBM embedded Security Subsystem ed eliminare la password del responsabile del sistema, è necessario azzerare le impostazioni del chip. Prima di riazzerare IBM embedded Security Subsystem, leggere le informazioni di seguito riportate.

Attenzione:

- Quando IBM embedded Security Subsystem viene eliminato, tutte le chiavi di cifratura e i certificati memorizzati nel sottosistema andranno perduti.

Per eliminare IBM embedded Security Subsystem, completare la procedura di seguito riportata:

1. Chiudere e riavviare il computer.
2. Quando viene visualizzata la finestra Setup Utility, premere il tasto F1.

   Viene aperto il menu principale di Setup Utility.

3. Selezionare **Security**.
4. Selezionare **IBM TCPA Setup**.
5. Selezionare **Clear IBM TCPA Security Feature**, quindi premere Invio.
6. Selezionare **Yes**.
7. Premere F10, quindi selezionare **Yes**.
8. Premere Invio. L'elaboratore viene riavviato.

Annullamento di IBM embedded Security Subsystem (ThinkPad)

Se si desidera cancellare tutte le chiavi di cifratura dell'utente da IBM embedded Security Subsystem ed eliminare la password del responsabile, è necessario azzerare le impostazioni del sottosistema. Prima di riazzerare IBM embedded Security Subsystem, leggere le informazioni di seguito riportate.

Attenzione:

- Quando IBM embedded Security Subsystem viene eliminato, tutte le chiavi di cifratura e i certificati memorizzati nel sottosistema andranno perduti.

Per eliminare IBM embedded Security Subsystem, completare la procedura di seguito riportata:

1. Chiudere l'elaboratore
2. Tenere premuto il tasto Fn durante il riavvio dell'elaboratore.
3. Quando viene visualizzata la finestra Setup Utility, premere il tasto F1.
   Viene aperto il menu principale di Setup Utility.
4. Selezionare **Config**.
5. Selezionare **IBM Security Chip**.
6. Selezionare **Clear IBM Security Chip**.
7. Selezionare **Yes**.
8. Premere Invio per continuare.
9. Premere F10 per salvare e uscire.

Limitazioni note relative a CSS versione 5.2

Le informazioni di seguito riportate potrebbero essere utili per le funzioni di Client Security Software versione 5.2.

Limitazioni di roaming

Utilizzo di un server di roaming CSS

La richiesta della password del responsabile di CSS viene visualizzata ogni volta che un utente tenta di collegarsi al server di roaming CSS. Tuttavia, l'elaboratore può essere utilizzato normalmente evitando di immettere la password.

Utilizzo di IBM Security Password Manager in un ambiente di roaming

Le password memorizzate in un sistema con IBM Client Security Password Manager possono essere utilizzate in altri sistemi che fanno parte dell'ambiente di roaming. Le nuove voci vengono automaticamente richiamate dall'archivio quando l'utente si collega ad un altro sistema (se l'archivio è disponibile) della rete di

roaming. Pertanto, se un utente è già collegato ad un sistema, è necessario che si scolleghi e si ricolleghi prima che le nuove voci siano disponibili nella rete di roaming.

Certificati di Internet Explorer e intervallo di aggiornamento di roaming

I certificati di Internet Explorer vengono aggiornati nell'archivio ogni 20 secondi. Quando viene generato un nuovo certificato di Internet Explorer da un utente di roaming, tale utente deve attendere almeno 20 secondi prima di importare , ripristinare o modificare la configurazione CSS su un altro sistema. Se si tenta di effettuare una di queste operazioni prima dei 20 secondi di intervallo di aggiornamento, il certificato verrà perduto. Inoltre, se l'utente non era collegato all'archivio quando è stato generato il certificato, è necessario attendere 20 secondi dopo la connessione all'archivio per essere certi che il certificato sia stato aggiornato nell'archivio stesso.

Password di Lotus Notes e roaming delle credenziali

Se il supporto Lotus Notes è abilitato, la password utente di Lotus Notes viene memorizzata da UVM. Per accedere a Lotus Notes, non è necessario immettere la password Notes per collegarsi a Lotus Notes. Per accedere a Lotus Notes, sono richiesti il passphrase UVM, le impronte digitali, le smart card e altri metodi di autenticazione (in base alle impostazioni di politica di protezione).

Se un utente modifica la password Notes dall'ambiente Lotus Notes, il file contenente l'ID Notes ID viene aggiornato con la nuova password e viene aggiornata anche la copia UVM' della nuova password Notes. In un ambiente di roaming, le credenziali utente UVM sono disponibili su altri sistemi sulla rete di roaming cui l'utente può accedere. E' possibile che la copia UVM della password di Notes possa non corrispondere alla password di Notes presente nel file contenente l'ID su altri sistemi nella rete di roaming se il file ID di Notes ID contenente la password aggiornata non è disponibile sugli altri sistemi. In questo caso, non sarà possibile accedere a Lotus Notes.

Se un file contenente l'ID Notes con una password aggiornata non è ancora disponibile su un altro sistema, tale file aggiornato dovrebbe essere copiato su altri sistemi della rete di roaming in modo che la password contenuta nel file corrisponda alla copia memorizzata da UVM. Altrimenti, è possibile eseguire Modify Your Security Settings dal menu Start, quindi modificare la password in modo che corrisponda a quella precedente. Quindi, la password Notes può essere aggiornata di nuovo con Lotus Notes.

Disponibilità delle credenziali al collegamento in un ambiente di roaming

Quando l'archivio è in condivisione, le serie più recenti di credenziali utente vengono scaricate dall'archivio quando l'utente vi accede. Al collegamento, gli utenti non dispongono ancora dell'accesso alle condivisioni di rete, quindi non è possibile scaricare le credenziali più recenti fino a quando non viene completato il collegamento. Ad esempio, se il passphrase UVM è stato modificato su un altro sistema nella rete di roaming o se sono state registrate le impronte digitali su un altro sistema, tali aggiornamenti non sono disponibili se non viene completata la procedura di collegamento. Se non sono disponibili le credenziali utente, è necessario immettere il passphrase precedente o altre impronte registrate per collegarsi al sistema. Dopo aver completato il collegamento, le credenziali utente aggiornate sono disponibili e i nuovi passphrase e impronte digitali verranno registrate con UVM.

Limitazioni del badge di prossimità

Abilitazione del collegamento protetto UVM con i badge di prossimità Xyloc

Per abilitare correttamente il collegamento protetto UVM per l'utilizzo con il badge di prossimità CSS, è necessario installare i componenti nell'ordine di seguito riportato:

1. Installare Client Security Software.
2. Abilitare il collegamento protetto UVM utilizzando CSS Administrator Utility.
3. Riavviare il computer.
4. Installare il software Xyloc per il supporto del badge di prossimità.

Nota: Se è installato prima il software del badge di prossimità Xyloc, l'interfaccia di collegamento di Client Security Software non viene visualizzata. In questo caso, è necessario disinstallare Client Security Software, quindi il software Xyloc e poi reinstallarli nell'ordine indicato in precedenza per ripristinare il collegamento protetto UVM.

Supporto Cisco LEAP e badge di prossimità

L'abilitazione della protezione del badge di prossimità e del supporto Cisco LEAP potrebbe causare un comportamento inaspettato. Si consiglia di non installare o utilizzare questi componenti sullo stesso sistema.

Supporto software Ensure

Client Security Software 5.2 richiede agli utenti dei badge di prossimità di aggiornare il software Ensure alla versione 7.41. Se si aggiorna una versione precedente di Client Security Software, aggiornare il software Ensure prima di installare Client Security Software 5.2.

Ripristino delle chiavi

Dopo aver eseguito un'operazione di ripristino delle chiavi, è necessario riavviare l'elaboratore prima di continuare ad utilizzare Client Security Software.

Nomi di dominio e nomi utenti locali

Se i nomi di dominio e nomi utente locali sono uguali, è necessario utilizzare la stessa password di Windows per entrambi gli account. IBM User Verification Manager memorizza solo una password di Windows per ID, in modo che gli utenti utilizzino la stessa password per il collegamento locale e di dominio. Altrimenti, viene richiesto di aggiornare la password Windows di IBM UVM quando si commuta tra il collegamento di dominio e quello locale quando è abilitata la sostituzione del collegamento Windows protetto IBM UVM.

CSS non dispone della possibilità di registrate utenti separati locali e di dominio a parte con lo stesso nome account. Se si tenta di registrare utenti locali e di dominio con lo stesso ID, viene visualizzato il seguente messaggio: L'ID utente selezionato è già stato configurato. CSS non consente una registrazione separata di ID utente locale e di dominio comuni su un sistema, in modo che l'ID utente comune disponga dell'accesso alla stessa serie di credenziali, come ad esempio i certificati, le impronte digitali memorizzate e altro.

Reinstallazione del software per le impronte digitali Targus

Se il software per le impronte digitali Targus viene rimosso e reinstallato, le voci di registro necessarie per l'abilitazione del supporto alle impronte digitali in Client

Security Software devono essere aggiunte manualmente affinché sia abilitato il relativo supporto. Scaricare il file di registro contenente le voci necessarie (atplugin.reg), quindi fare doppio clic per unire le voci al registro. Fare clic su Sì, quando viene richiesto, per confermare l'operazione. E' necessario riavviare il sistema affinché Client Security Software riconosca le modifiche e abiliti il supporto per le impronte digitali.

Nota: Per aggiungere queste voci di registro, è necessario disporre dei privilegi del responsabile del sistema.

Passphrase del supervisore di BIOS

IBM Client Security Software 5.2 e la versione precedente non supportano la funzione passphrase supervisore BIOS disponibile su alcuni sistemi ThinkPad. Se si abilita l'utilizzo del passphrase del supervisore di BIOS, è necessario effettuare qualunque abilitazione o disabilitazione del sottosistema di protezione dal Setup del BIOS.

Utilizzo di 7.x

Netscape 7.x funziona in modo differente da Netscape 4.x. La richiesta del passphrase non viene visualizzata all'avvio di Netscape. Il modulo PKCS#11 viene caricato solo quando necessario, in modo che la richiesta passphrase viene visualizzata solo quando si esegue un'operazione che richiede tale modulo.

Utilizzo di un minidisco per l'archiviazione

Se si specifica un minidisco come posizione di archivio durante la configurazione del software di protezione, potrebbe verificarsi un lungo intervallo di tempo di attesa corrispondente al processo di scrittura dei dati su minidisco. E' possibile considerare altri supporti di memorizzazione, come ad esempio la rete o una chiave USB.

Limitazioni delle Smart card

Registrazione delle smart card

E' necessario registrare le Smart card con UVM prima di autenticare correttamente un utente all'utilizzo della smart card. Se viene assegnata una sola smart card a più utenti, solo l'ultimo utente che l'ha registrata può utilizzarla. Di conseguenza, è necessario registrare le smart card per un solo account utente.

Autenticazione delle smart card

Se viene richiesta una smart card per l'autenticazione, viene visualizzato un dialogo in UVM che richiede la smart card. Quando la smart card viene inserita nel lettore, viene visualizzato un dialogo che richiede il PIN della smart card. Se viene immesso un PIN non corretto, UVM richiede di nuovo la smart card. E' necessario rimuovere la smart card e inserirla nuovamente prima di immettere di nuovo il PIN. E' necessario effettuare tale operazione fino a quando non viene immesso il PIN corretto per la smart card.

Dopo la cifratura viene visualizzato il carattere più (+) sulle cartelle

Dopo la cifratura di file e cartelle, Esplora risorse visualizza un segno più (+) prima dell'icona della cartella. Questo carattere aggiuntivo non viene più visualizzato quando il pannello di Esplora risorse viene aggiornato.

Limitazioni di Windows XP con gli utenti limitati

In Windows XP, con gli utenti limitati, non è possibile aggiornare i passphrase UVM, le password di Windows o aggiornare le chiavi di archivio con User Configuration Utility.

Altre limitazioni

Questa sezione contiene informazioni sulle limitazioni note relative a 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

Netscape si apre dopo un errore di autorizzazione: se viene visualizzata la finestra Passphrase UVM, è necessario immettere il passphrase UVM, quindi 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. Facendo clic su **OK**, viene aperto Netscape, ma non sarà possibile utilizzare il certificato digitale generato da IBM embedded Security Subsystem. Prima di poter utilizzare il certificato di IBM embedded Security Subsystem, è necessario uscire e riavviare Netscape, quindi immettere il passphrase UVM corretto.

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

- SHA-1
- MD5

Certificato IBM embedded Security Subsystem e algoritmi di cifratura

Le seguenti informazioni vengono fornite per identificare le emissioni sugli algoritmi di cifratura che possono essere utilizzati con il certificato di IBM embedded Security Subsystem. 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 Subsystem 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): in base alla configurazione o all'aggiornamento della 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 Subsystem . 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 di seguito riportate:

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

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

Limitazioni relative a 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.

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.

Problema	Possibile soluzione
Viene visualizzato un messaggio durante l'installazione indicante che è necessario aggiornare o rimuovere il programma.	Eseguire una delle seguenti operazioni: • Se è installata una versione precedente a Client Security Software 5.0, selezionare **Rimuovi**, quindi azzerare il sottosistema di protezione utilizzando IBM BIOS Setup Utility. • In caso contrario, selezionare **Aggiorna**, quindi continuare con l'installazione.
L'accesso all'installazione viene negato a causa della password del responsabile sconosciuta	**Azione**
Durante l'installazione su un client IBM con IBM embedded Security Subsystem abilitato, la password del responsabile di IBM embedded Security Subsystem è sconosciuta.	Azzerare Security Subsystem per continuare con l'installazione.

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
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.
Viene visualizzato un messaggio di errore quando si modifica la chiave pubblica del responsabile	**Azione**
Quando si elimina embedded Security Subsystem e poi si ripristina l'archivio della chiave, è possibile che venga visualizzato un messaggio di errore se si modifica la chiave pubblica del responsabile.	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 del responsabile e si tenta di recuperare una passphrase UVM per un utente, potrebbe essere visualizzato un messaggio di errore.	Effettuare 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 necessaria, 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**

Problema	Possibile soluzione
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**
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/O buffer durante l'accesso a IBM embedded Security Subsystem. E' possibile che questo problema sia risolto da un riavvio.	Uscire dal messaggio di errore e riavviare il computer.
Quando si modifica la password del responsabile, viene visualizzato un messaggio di errore	**Azione**
Quando si tenta di modificare la password del responsabile e si preme Invio o il tasto Tab > Invio in seguito all'immissione della password di conferma, viene abilitato il pulsante **Disabilita chip**, quindi viene visualizzato un messaggio di conferma della disabilitazione di tale chip.	Procedere nel modo seguente: 1. Uscire dalla finestra di conferma di disabilitazione del chip. 2. Per modificare la password del responsabile, immettere la nuova password, immetterla di nuovo per conferma, quindi 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**

Problema	Possibile soluzione
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	Questa è una limitazione nota con Windows XP Professional. Non esiste alcuna soluzione per questo problema.
Limited Users non è abilitato a utilizzare User Configuration Utility in Windows XP Home	**Azione**
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	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**
Viene visualizzato un messaggio di errore durante l'esecuzione di una funzione da responsabile di Client Security.	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**

Problema	Possibile soluzione
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.
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.	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**
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 al certificato non esiste più in IBM embedded Security Subsystem dell'elaboratore del mittente su cui è stato creato il certificato.	Richiedere al destinatario di rinviare il proprio certificato digitale; quindi, selezionare tale certificato nella rubrica per Outlook Express.

Problema	Possibile soluzione
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 protezione 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.	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**
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 e-mail cifrato.

Problema	Possibile soluzione
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, quindi fare clic sul pulsante **Invia**.
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 Subsystem 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**
Le e-mail cifrate non possono essere decifrate a causa delle differenze di cifratura dei browser Web utilizzati dal mittente e dal destinatario.	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 Subsystem non è stato selezionato in Netscape Messenger e il mittente del messaggio e-mail tenta di firmare tale messaggio con il certificato, viene visualizzato un messaggio di errore.	Utilizzare le impostazioni di protezione in Netscape Messenger per selezionare il certificato. Quando viene aperto Netscape Messenger, fare clic sull'icona Protezione, situata sulla barra degli strumenti. Viene visualizzata la finestra Info protezione. 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.

Problema	Possibile soluzione
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 un certificato digitale generato da IBM embedded Security Subsystem	**Azione**
Il certificato digitale generato da IBM embedded Security Subsystem non è disponibile per l'utilizzo.	Verificare che il passphrase UVM corretto sia stato inserito quando viene visualizzato Netscape. Se si inserisce il passphrase UVM errata, viene visualizzato un messaggio di errore di autenticazione. Facendo clic su **OK**, viene aperto Netscape, ma non sarà possibile utilizzare il certificato generato da IBM embedded Security Subsystem. 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**
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 protezione 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 Subsystem	**Azione**
Il certificato di IBM embedded Security Subsystem 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 la chiave di archivio, vengono create le copie di tutti i certificati associati a IBM embedded Security Subsystem.
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**

Problema	Possibile soluzione
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 Subsystem e si apre Netscape, quest'ultimo viene aperto dopo un intervallo di tempo maggiore rispetto alla norma.	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**
La politica di protezione 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 visualizzata 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**

Problema	Possibile soluzione
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**
Una periferica protetta da UVM, come ad esempio una smart card, un lettore per smart card o per le impronte digitali non sta funzionando correttamente.	Confermare se la periferica è stata configurata correttamente. Una volta configurata la periferica, è necessario riavviare il sistema per avviarla correttamente. Per informazioni sulla risoluzione dei problemi per la periferica, consultare la documentazione fornita con la periferica stesso o rivolgersi al relativo fornitore.
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. Informazioni sulle password e i passphrase

L'appendice contiene informazioni sulle password e i passphrase.

Regole per password e passphrase

In un sistema protetto, sono presenti varie password e passphrase. Le varie password dispongono di regole diverse. Questa sezione contiene informazioni sulla password del responsabile e sui passphrase UVM.

Regole per la password del responsabile

Le regole per la password del responsabile non possono essere modificate dal responsabile della protezione.

Di seguito sono riportate le regole applicate alla password del responsabile:

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 del responsabile per abilitare IBM Embedded Security Chip nell'elaboratore. E' necessario che questa password sia immessa ogni volta che si accede ai programmi Administrator Utility e Administrator Console.

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

IBM Client Security Software consente ai responsabili della protezione di impostare le regole dei passphrase UVM per gli utenti. Per migliorare la protezione, il passphrase UVM è più lunga e può essere più univoca rispetto alla password tradizionale. La politica passphrase UVM è controllata da Administrator Utility.

L'interfaccia relativa alla politica passphrase UVM in Administrator Utility consente ai responsabili della protezione 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 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 protezione 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 dopo 184 giorni. E' necessario che il nuovo passphrase sia conforme alla politica dei passphrase stabilita.
- stabilire se il passphrase scade (sì)

  Quando viene selezionata questa opzione, il passphrase non scade.

La politica passphrase è controllata in Administrator Utility quando l'utente si iscrive, quindi viene anche controllato quando l'utente modifica il passphrase da Client Utility. Le due impostazioni utente collegate alla password precedente verranno reimpostate e verrà rimossa la cronologia dei passphrase.

Le seguenti regole si applicano al passphrase UVM:

Lunghezza
: Il passphrase può contenere fino a 256 caratteri.

Caratteri
: Il passphrase può contenere qualunque combinazione di caratteri prodotti dalla tastiera, compresi gli spazi e i 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 immette il passphrase UVM in modo non corretto per più volte durante una sessione, l'elaboratore sperimenta una serie di ritardi. Questi ritardi sono specificati nella sezione di seguito riportata.

Conteggi errati su sistemi TCPA e non TCPA

La tabella di seguito riportata illustra le impostazioni relative al ritardo per un sistema TCPA:

Tentativi	Ritardo al malfunzionamento successivo
15	1,1 minuti
31	2,2 minuti
47	4,4 minuti
63	8,8 minuti
79	17,6 minuti
95	35,2 minuti
111	1,2 ore
127	2,3 ore
143	4,7 ore

I sistemi TCPA non distinguono tra passphrase utente e password del responsabile. Qualunque autenticazione con IBM Embedded Security Chip è sottoposta alla stessa politica. Il timeout massimo è di 4,7. I sistemi TCPA non ritardano per un intervallo di tempo superiore alle 4,7.

I sistemi non TCPA distinguono tra password del responsabile e passphrase utente. Su sistemi non TCPA, la password del responsabile dispone di un ritardo di 77 dopo dieci tentativi non riusciti, quindi il tempo di blocco raddoppia dopo ogni 32 tentativi non riusciti.

Reimpostazione di un passphrase

Se un utente dimentica il passphrase, il responsabile può abilitare l'utente per riazzerare tale passphrase.

Reimpostazione remota di un passphrase

Per impostare in remoto una password, completare la procedura di seguito riportata:

- **Responsabili**

  E' necessario che un responsabile remoto effettui le operazioni di seguito riportate:

  1. Creare e comunicare la nuova password temporanea all'utente.
  2. Inviare un file di dati all'utente.

I file di dati possono essere inviati all'utente mediante e-mail, copiati su un supporto rimovibile, come ad esempio un minidisco o scritti direttamente nel file di archivio dell'utente (se l'utente dispone dell'accesso al sistema). Il file cifrato viene utilizzato come corrispondenza alla nuova password temporanea.

- **Utenti**

  Gli utenti possono procedere nel modo seguente:

  1. Collegarsi all'elaboratore.
  2. Quando viene richiesto il passphrase, contrassegnare la casella di controllo "Passphrase dimenticato".
  3. Immettere la password temporanea comunicata dal responsabile remoto, quindi fornire la posizione del file inviato da quest'ultimo.

     Una volta che UVM ha verificato che le informazioni del file corrispondono alla password fornita, è concesso l'accesso all'utente. Viene richiesto di modificare immediatamente il passphrase dell'utente.

Questo è il modo consigliato per riazzerare un passphrase dimenticato.

Reimpostazione manuale di un passphrase

Se il responsabile può collegarsi al sistema di un utente che ha dimenticato il passphrase, può anche collegarsi al sistema dell'utente come responsabile, fornire la chiave privata del responsabile in Administrator Utility, quindi modificare manualmente il passphrase dell'utente. Per modificare il passphrase, non è necessario che il responsabile conosca il passphrase precedente.

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 **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 la protezione al 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:

Director of Commercial Relations
IBM Europe
Shoenaicher Str. 220
D-7030 Boeblingen
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

Soluzioni IBM® Client Security
Utilizzo di Client Security Software versione 5.3 con Tivoli® Access Manager

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: +39-0823-353137
- 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 Pozzillo

Località Ponteselice
81100 CASERTA