Soluzioni IBM® Client Security

Client Security Software Versione 5.4 - Guida per l'utente e per il responsabile

Soluzioni IBM® Client Security

Client Security Software Versione 5.4 - Guida per l'utente e per il responsabile

Prima edizione (Ottobre 2004)

Prima di utilizzare questo prodotto e le relative informazioni, consultare la sezione Appendice D, "Norme per l'esportazione di Client Security Software", a pagina 101 e l'Appendice E, "**Marchi e informazioni particolari**", a pagina 103.

Indice

Parte 1. Introduzione a Client Security

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

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 sicurezza, 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 TCG (Trusted Computing Group) definite in TCG Main Specification 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. 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. Questa password viene conervata ed 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 sicurezza

- 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
- Mediante 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
- Mediante 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
- Mediante 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 sicurezza del client.** L'autenticazione degli utenti finali a livello di client rappresenta un problema di politica di

sicurezza di rilevante importanza. Client Security Software fornisce l'interfaccia che è richiesta per gestire la politica di sicurezza di un client IBM. Questa interfaccia appartiene al software di autenticazione UVM (User Verification Manager), che rappresenta il componente principale di Client Security Software.

- **Gestione delle chiavi di cifratura per la cifratura delle chiavi pubbliche.** I responsabili creano le chiavi di codifica per l'hardware del computer e per gli utenti dei client con Client Security Software. Quando vengono create le chiavi di cifratura, esse risultano collegate a IBM embedded Security Chip tramite una gerarchia di chiavi, per cui una chiave hardware di livello base viene utilizzata per cifrare le chiavi dei livelli superiori, compreso le chiavi utente che sono associate ad ogni utente client. La cifratura e la memorizzazione delle chiavi su IBM embedded Security Chip aggiunge un ulteriore livello di sicurezza del client, poiché le chiavi vengono collegate in modo sicuro all'hardware del computer.
- **Creazione e memorizzazione del certificato digitale protetto da IBM embedded Security Chip.** Quando si 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.
- **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.

Parte 2. Informazioni per l'utente

Capitolo 2. Istruzioni per gli utenti client

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

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

Utilizzo della protezione UVM per il collegamento al sistema

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

La protezione del collegamento UVM consente di controllare l'accesso al sistema operativo tramite un'interfaccia di collegamento. La protezione del collegamento UVM sostituisce l'applicazione di collegamento Windows, in modo che quando un utente sblocca il computer, viene visualizzata la finestra di collegamento UVM invece di quella Windows. Dopo aver abilitato la protezione UVM per il computer, verrà visualizzata l'interfaccia di collegamento UVM all'avvio del computer.

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

Procedure per sbloccare il client

per sbloccare un client Windows che utilizza la protezione del collegamento UVM, completare la procedura seguante:

1. Immettere il nome utente e il passphrase UVM.
2. Selezionare il dominio a cui si è collegati.
3. Fare clic su **OK**.

   Nota: Anche se UVM riconosce molteplici domini, la password utente deve essere la stessa per tutti i domini.

Nota:

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

User Configuration Utility

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

Funzioni User Configuration Utility

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

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

Limiti di User Configuration Utility con Windows XP

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

Windows XP Professional

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

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

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

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

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

Windows XP Home

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

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

Utilizzo di User Configuration Utility

Per utilizzare User Configuration Utility, procedere nel modo seguente:

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

   Viene visualizzato il pannello principale di IBM Client Security Software User Configuration Utility.
2. Selezionare uno dei separatori di seguito riportati:
   - **Aggiornamento delle password e dell'archivio.** Questo separatore consente di modificare il passphrase UVM, aggiornare la password di Windows in UVM, reimpostare la password Lotus Notes in UVM e aggiornare l'archivio di cifratura.
   - **Configura suoni UVM.** Questo separatore consente di selezionare un file audio da riprodurre quando l'autenticazione è corretta o errata.
   - **Configurazione utente.** Questo separatore consente all'utente di ripristinare la propria configurazione dall'archivio, reimpostarla oppure registrarsi con il server di roaming (se l'elaboratore può essere utilizzato come client di roaming).
3. Fare clic su **OK** per uscire.

E' disponibile un supporto per ogni procedura nel sistema di guida Client Security Software.

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

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

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

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

Utilizzo di Client Security Software con applicazioni Microsoft

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

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

Emissione di un certificato digitale per le applicazioni Microsoft

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

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

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

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

Trasferimento di certificati da Microsoft CSP

La procedura guidata per il trasferimento dei certificati di IBM CSS consente di trasferire certificati creati con il CSP predefinito della Microsoft sul CSP di IBM embedded Security System. Il trasferimento dei certificati aumenta la protezione fornita dalle chiavi private associate ai certificati, in quanto questi ultimi possono essere memorizzati in modo sicuro mediante IBM embedded Security Subsystem, invece di utilizzare il software, che è più vulnerabile.

Esistono due tipi di certificati di protezione che possono essere trasferiti:

- **Certificati utente:** lo scopo di un certificato utente è quello di autorizzare un determinato utente. In genere, il certificato si ottiene dalla CA (Certificate

Authority), come ad esempio cssdesk. Una Certificate Authority è un'entità affidabile che memorizza, rilascia e pubblica i certificati. Un certificato potrebbe essere necessario per firmare e cifrare e-mail o per collegarsi ad un determinato server.

- **Certificati della macchina:** lo scopo di un certificato macchina è quello di identificare un determinato elaboratore. Quando viene utilizzato un certificato macchina, l'autenticazione è basata sull'elaboratore utilizzato, non sul suo utente.

La procedura guidata per il trasferimento dei certificati di CSS trasferisce solo i certificati della Microsoft contrassegnati come esportabili ed è limitata ai certificati di dimensioni della chiave non superiori ai 1024 bit.

Se un utente deve trasferire un certificato macchina, ma non dispone di privilegi del responsabile del sistema, il responsabile può inviare un file di configurazione del responsabile che abilita l'utente al trasferimento del certificato evitando di fornire la password del responsabile. Per creare il file di configurazione del responsabile, utilizzare il programma di utilità Administrator Console, che si trova al seguente percorso `c:\\program files\ibm\security`.

Per utilizzare la procedura guidata al trasferimento dei certificati CSS, completare la procedura di seguito riportata:

1. Fare clic su **Start > Access IBM > IBM Client Security Software > CSS Certificate Transfer Wizard**.

   Viene visualizzato il pannello di benvenuto di IBM CSS Certificate Transfer Wizard.
2. Fare clic su **Avanti** per iniziare.
3. Selezionare i tipi di certificato da trasferire, quindi fare clic su **Avanti**. La procedura guidata al trasferimento dei certificati CSS consente di trasferire solo i certificati memorizzati della Microsoft contrassegnati come esportabili.
4. Selezionare i certificati da trasferire facendo clic sul nome del certificato visualizzato nell'area relativa ai certificati rilasciati dell'interfaccia, quindi fare clic su **Avanti**. Viene visualizzato un messaggio indicante che il certificato è stato trasferito correttamente.

   Nota: Il trasferimento di un certificato macchina richiede la password del responsabile o un file di configurazione del responsabile.
5. Fare clic su **OK** per tornare alla procedura guidata al trasferimento dei certificati CSS.

Una volta trasferiti, i certificati vengono associati al CSP di IBM embedded Security Subsystem, quindi le chiavi private sono protette da IBM embedded Security Subsystem. Qualunque operazione che utilizza le chiavi private, come ad esempio la creazione di firme digitali o la decifrazione di e-mail, viene effettuata nell'ambiente protetto di IBM embedded Security Subsystem.

Aggiornamento dell'archivio di chiavi per le applicazioni Microsoft

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

Utilizzo del certificato digitale per le applicazioni Microsoft

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

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

Configurazione delle preferenze audio UVM

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

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

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

Capitolo 3. IBM Password Manager

Questa sezione fornisce un'introduzione a IBM Password Manager, insieme alle procedure dettagliate sul modo in cui eseguire le funzioni comuni di IBM Password Manager.

Introduzione al programma IBM Password Manager

IBM Password Manager consente di gestire le informazioni di collegamento sensibili e facili da dimenticare, come gli ID utente, le password ed altre informazioni personali utilizzando IBM Client Security. IBM Client Security Password Manager memorizza tutte le informazioni mediante IBM Embedded Security Subsystem, in modo che la politica di autenticazione utente UVM controlli l'accesso alle applicazioni e ai siti web protetti.

Ciò significa che piuttosto che ricordare e fornire una serie di singole password, tutte con regole e date di scadenza diverse, è possibile ricordare un solo passphrase, fornire le impronte digitali, un badge di prossimità o una combinazione degli elementi di identificazione.

IBM Client Security Password Manager consente di effettuare le operazioni di seguito riportate:

- **Cifrare tutte le informazioni memorizzate mediante IBM Embedded Security Subsystem**

  IBM Password Manager cifra automaticamente tutte le informazioni mediante IBM Embedded Security Subsystem. Ciò assicura che tutte le informazioni sulla password sono sicure dai tasti di cifratura del programma IBM Client Security.
- **Trasferire gli ID utente e password in modo rapido e facile mediante una semplice interfaccia trasferimento-tipo**

  Utilizzare l'interfaccia di trasferimento-tipo di IBM Password Manager per posizionare le informazioni direttamente nella finestra di collegamento dell'applicazione o del browser Web. In questo modo, è possibile ridurre gli errori di battitura e salvare le informazioni in modo sicuro mediante IBM embedded Security Subsystem.
- **Password e ID utente di tasto automatico**

  Il programma IBM Password Manager automatizza il processo di collegamento, inserendo le informazioni di collegamento automaticamente quando si accede ai siti Web inseriti nel programma IBM Password Manager.
- **Esportare le informazioni di collegamento sensibili in un browser protetto**

  IBM Password Manager consente di esportare le informazioni di collegamento sensibili in modo sicuro da un elaboratore ad un altro. Quando si esportano le informazioni di collegamento da IBM Password Manager, viene creato un file per l'esportazione protetto da password, che può essere memorizzato su supporti rimovibili. E' possibile utilizzare questo file per accedere alle informazioni e alle password utente.
- **Generare password casuali**

  IBM Password Manager consente di generare password casuali per ciascun sito Web o per ciascuna applicazione. Ciò consente di implementare la protezione dei dati poiché a ciascuna applicazione sarà abilitata un'ulteriore protezione per password. Le password casuali sono molto più sicure delle password

personalizzate poiché la maggior parte degli utenti utilizza le informazioni personali facili da ricordare per password facili da dimenticare.

- **Modificare le voci utilizzando l'interfaccia Password Manager**

  IBM Password Manager consente di modificare tutte le voci di account ed impostare tutte le funzioni della password facoltativa in un'interfaccia facile da utilizzare. Quindi, la gestione delle password e delle informazioni personali è più rapida e più semplice.

- **Accedere a Password Manager dalla barra delle applicazioni sul desktop di Windows o con un semplice tasto di scelta rapida**

  L'icona del programma IBM Password Manager consente all'utente di disporre l'accesso istantaneo ogni qual volta in cui è necessario aggiungere l'applicazione a Password Manager, ad esempio quando si naviga nel Web. Ciascuna funzione di Password Manager può essere acceduta in modo semplice da un semplice tasto di scelta rapida.

- **Archiviare le informazioni di collegamento**

  Utilizzando la funzione di archiviazione di Client Security, il programma IBM Password Manager consente all'utente di ripristinare le informazioni di collegamento da un archivio di Client Security da proteggere da un errore del sistema o dell'unità disco fisso. Per ulteriori informazioni su come archiviare le informazioni, consultare *Guida per l'utente Client Security Software*.

IBM Password Manager - Procedure

IBM Client Security Password Manager consente di immettere informazioni nei siti web e nelle applicazioni mediante l'interfaccia Password Manager. Il programma IBM Password Manager cifra e salva le informazioni immesse nei campi appropriati mediante IBM Embedded Security Subsystem. Una volta salvate le informazioni in Password Manager, questi campi sono riempiti automaticamente con queste informazioni sicure ogni qual volta in cui viene concesso l'accesso al sito Web o all'applicazione a seconda della politica di autenticazione utente UVM.

Creazione delle nuove voci

Per immettere le informazioni relative alla password in IBM Client Security Password Manager, completare la procedura di seguito riportata:

1. Aprire il pannello di collegamento del sito Web o dell'applicazione.
2. Fare clic con il tastino destro del mouse sull'icona di **Password Manager** nella barra delle applicazioni di Windows e selezionare **Crea**.

   Nota: Inoltre, è possibile accedere alla funzione Crea di Password Manager mediante i tasti di scelta rapida **Ctrl+Maiusc+H**.
3. Inserire le informazioni per un campo nella finestra Password Manager- Crea nuova voce.

   Nota: Le informazioni immesse in questo campo non devono superare i 260 caratteri.
4. Se non si desidera visualizzare il testo inserito, fare clic sulla casella **Nascondi testo inserito per privacy**.

   Nota: Questa casella di controllo consente di selezionare il modo in cui viene visualizzato il testo in Password Manager. Una volta rilasciato il testo in un sito Web o in un'applicazione, le relative proprietà saranno controllate da tale applicazione.

5. Utilizzare l'icona di ″destinazione″ Seleziona campo per trascinare il testo dal programma di utilità Password Manager nel campo appropriato sul sito Web o nell'applicazione.

   Nota: questa icona consente di copiare il testo senza utilizzare gli appunti dell'elaboratore o un'altra ubicazione non sicura.
6. Ripetere i passi da 3 a 5 per ciascun campo nel modo appropriato.
7. Fare clic su **Salva nuova voce**.
8. Immettere un nome descrittivo per la nuova voce.
9. Fare clic sulla casella di controllo **Aggiungi ″Invio″ per inoltrare automaticamente la voce** se si desidera che Password Manager inoltri le informazioni di collegamento in seguito al richiamo.

   Nota: alcuni siti Web non utilizzano il tasto Invio per inoltrare le informazioni di collegamento. Se il collegamento non viene eseguito correttamente, disabilitare questa funzione.
10. Per completare la procedura, fare clic su **Salva nuova voce**.

Richiamo delle voci

Richiamare le password mediante IBM Client Security Password Manager è semplice e veloce.

Per richiamare le informazioni memorizzate in IBM Client Security Password Manager, completare la procedura di seguito riportata:

1. Aprire il pannello di collegamento del sito Web o dell'applicazione per le informazioni che si desidera richiamare.
2. Fare doppio clic sull'icona **Password Manager** nella barra delle applicazioni di Windows. Password Manager inserisce le informazioni memorizzate nei campi del pannello di collegamento.

   Nota: Inoltre, è possibile accedere alla funzione di richiamo di Password Manager mediante i tasti di scelta rapida **Ctrl+Maiusc+G**.
3. Inserire la password UVM o completare i requisiti di accesso specificati dalla politica di autenticazione dell'utente UVM.
4. Se la casella di controllo **Aggiungi ″Invio″ per inoltrare automaticamente la voce** non è selezionata, fare clic sul pulsante di inoltro dell'applicazione o del sito web.

   Se non viene richiamata alcuna voce, viene visualizzata una finestra che richiede all'utente se si desidera creare una nuova voce. Fare clic su **Sì** per avviare la finestra Password Manager- Crea nuova voce.

Gestione delle voci

IBM Client Security Password Manager consente di effettuare operazioni con le informazioni memorizzate in Password Manager. La finestra Password Manager - Gestisci consente di modificare ID utente, password e altre informazioni immesse in Password Manager che si trovano nei campi di un sito web o di un'applicazione.

Per modificare le informazioni memorizzate in IBM Client Security Password Manager, completare la procedura di seguito riportata:

1. Fare clic con il tastino destro del mouse sull'icona **Password Manager** che si trova nella Barra delle applicazioni di Windows, quindi fare clic su **Gestisci**.

Nota: Inoltre, è possibile accedere alla funzion Password Manager - Gestisci mediante i tasti di scelta rapida **Ctrl+Maiusc+B**.

2. Inserire la password UVM o completare i requisiti di accesso, specificati dalla politica di autenticazione utente UVM.
3. Modificare le informazioni. Selezionare le seguenti opzioni:
   - Informazioni sulla voce

     Per modificare le informazioni sulla voce, completare la seguente procedura:
     a. Fare clic con il tastino destro del mouse sulla voce che si desidera modificare.
     b. Selezionare le seguenti azioni:
        – Aggiungi ″Invio″

          Selezionare Aggiungi ″Invio″ per inserire automaticamente le informazioni sulla voce nel sito Web o nell'applicazione. Un'icona di verifica verrà visualizzata accanto ad Aggiungi ″Invio″ quando tale funzione è attivata.
        – Elimina

          Selezionare Elimina per eliminare la voce in modo completo.
     c. Fare clic su **Salva modifiche**.
   - Informazioni sul campo Voce

     Per modificare le informazioni sul campo Voce, completare la seguente procedura:
     a. Fare clic con il tastino destro del mouse sul campo che si desidera modificare.
     b. Selezionare le seguenti azioni:
        – Campo Modifica voce

          Selezionare il campo Modifica voce per modificare le informazioni memorizzate per questo campo. E' possibile modificare un campo della voce in uno dei seguenti modi:
          - Creando una voce casuale

            Per creare una voce casuale, selezionare A caso. Il programma Password Manager crea voci casuali con lunghezza di 7, 14 o 127 caratteri.
          - Modificando manualmente un campo di voce

            Per modificare manualmente un campo di voce, selezionare Modifica ed apportate le modifiche appropriate al campo.
        – Elimina

          Selezionare Elimina per eliminare completamente il campo relativo alla voce.

          Nota: La modifica di un campo in Password Manager aggiorna solo le informazioni di collegamento in Password Manager. Se si desidera implementare la protezione dellle password utilizzando la funzione di generazione casuale di Password Manager, è necessario sincronizzare l'applicazione o il sito web con la nuova password generata da tale funzione. Per trasferire la nuova password casuale nel modulo ″Modifica password″ dell'applicazione o sito web, utilizzare la funzione di trasferimento Password Manager Transfer Field Tool. Verificare che la nuova password sia valida per l'applicazione o per il sito web, quindi utilizzare la funzione Salva modifiche nella finestra Password Manger -

Gestisci. Non è necessario creare di nuovo la voce con la nuova password, poiché le informazioni necessarie sono state conservate.

c. Fare clic su **Salva modifiche**.

4. Fare clic su **Salva modifiche**.

Esportazione delle informazioni di collegamento

IBM Password Manager consente di esportare le informazioni di collegamento sensibili in modo sicuro da un elaboratore ad un altro. Quando si esportano le informazioni di collegamento da IBM Password Manager, viene creato un file di esportazione protetto da password, che può essere memorizzato su supporti rimovibili. E' possibile utilizzare questo file per accedere alle informazioni e alle password utente.

Per esportare le informazioni di collegamento memorizzate in IBM Client Security Password Manager, completare la procedura di seguito riportata:

1. Fare clic con il tastino destro del mouse sull'icona **Password Manager** che si trova nella Barra delle applicazioni di Windows, quindi fare clic su **Gestisci**.

   Nota: Inoltre, è possibile accedere alla funzion Password Manager - Gestisci mediante i tasti di scelta rapida **Ctrl+Maiusc+B**.
2. Inserire la password UVM o completare i requisiti di accesso specificati dalla politica di autenticazione dell'utente UVM.
3. Fare clic su **Esporta**. Viene visualizzata la finestra Salva con nome con il nome file e il percorso predefinito `PwMgrExportReader`.
4. Selezionare la posizione in cui si desidera salvare il file da esportare.
5. Fare clic su **Salva** per salvare il file con il nome e la posizione specificati. Viene visualizzato un pannello che richiede di scegliere un passphrase per il file esportato.
6. Impostare un passphrase per il file esportato, quindi fare clic su **OK**. Il passphrase verrà richiesto per accedere ai dati esportati. Viene visualizzato un messaggio indicante che l'operazione di esportazione è stata completata correttamente.
7. Fare clic su **OK**.
8. Chiudere IBM Password Manager.
9. Richiamare il file di esportazione creato dalla posizione in cui si trova, quindi copiarlo su un supporto rimovibile.

Prima di aprire questo file su un altro elaboratore, viene richiesto il passphrase per l'esportazione scelto durante la procedura di cui sopra. IBM Password Manager visualizza le informazioni sensibili con un'applicazione protetta. Non è possibile salvare le informazioni sul disco fisso dell'elaboratore o stamparle. Fare clic su **OK** per chiudere il file in sola lettura esportato.

Capitolo 4. Roaming delle credenziali CSS

La funzione di roaming delle credenziali di IBM Client Security Software consente di utilizzare le credenziali di un utente' UVM su tutti i computer abilitati ESS in una rete. Questa rete, denominata rete di roaming, potenzia la flessibilità utente la disponibilità delle applicazioni abilitando gli utenti a operare da qualunque elaboratore in rete.

Requisiti per la rete di roaming delle credenziali CSS

Una rete di roaming delle credenziali CSS è costituita dai componenti necessari di seguito riportati:

- Server di roaming
- Client di roaming
- Unità di rete mappata condivisa per memorizzare gli archivi utente UVM

Nota: Il server di roaming ed i client di roaming autorizzati sono semplici computer abilitati ESS con password del responsabile stabilite che dispongono di IBM Client Security Software 5.1 o versione successiva, instalato.

Impostazione di un server di roaming

Per configurare una rete di roaming delle credenziali CSS, è necessario designare un computer come *server* di roaming (denominato sistema A). Gli altri elaboratori, una volta registrati mediante il server di roaming, diventano *client* registrati CSS autorizzati. (Il primo client registrato è denominato sistema B.)

L'elaboratore designato come server di roaming non è diverso dagli altri elaboratori. Quindi, è possibile utilizzare a tale scopo qualunque elaboratore designato come parte della rete di roaming. Il server di roaming è semplicemente l'elaboratore che viene designato per stabilire quali elaboratori sono ″affidabili″ nella rete di roaming. Una volta registrato un elaboratore con il server di roaming, quest'ultimo viene autenticato con tutti gli elaboratori in rete.

La configurazione di una rete di roaming è una processo costituito da sue fasi:

1. Configurare il server di roaming definendo le chiavi, l'archivio e gli utenti di roaming.
2. Registrare un client iniziale (sistema B) e tutti gli altri computer come client di roaming nella rete.

Il server di roaming definisce la rete di roaming ed avvia la registrazione dei client di roaming, ma il punto principale di una rete di roaming delle credenziali CSS è l'unità di rete mappata in cui sono memorizzati gli archivi degli utenti. Questo archivio è il luogo in cui vengono memorizzati tutti gli aggiornamenti alle credenziali utente. E' necessario che l'archivio *non* sia ubicato nel server di roaming o su un qualunque client di roaming. Una volta inizializzati i client CSS, il server di roaming funziona come un qualsiasi client registrato CSS.

Configurazione di un server di roaming

Per configurare un server di roaming, completare la procedura di seguito riportata:

1. Sull'elaboratore designato, avviare Administrator Console, quindi fare clic su **Configura roaming delle credenziali**. O, se il computer è già configurato per il roaming, selezionare **Riconfigura il sistema come server di roaming CSS** e fare clic su **Avanti**.
2. Creare la cartella `c:\roaming` sull'elaboratore designato come server di roaming.
3. Avviare Administrator Console, quindi fare clic su **Configura roaming delle credenziali**.
4. Selezionare **Configura il sistema come server di roaming delle credenziali CSS**, quindi fare clic su **Avanti**.
5. Fare clic su **Configura**.
6. Selezionare **Crea nuove chiavi di archivio**, quindi immettere il percorso della cartella in cui si trovano le nuove chiavi nel campo appropriato, dove la cartella delle chiavi di archivio è memorizzata nella cartella `c:\roaming`.
7. Scegliere di utilizzare una coppia di chiavi esistente o creare una nuova coppia di chiavi, quindi fare clic su **Avanti**.
8. Immettere la posizione della cartella di archivio, quindi fare clic su **Avanti**.

   Nota: La cartella di archivio e la cartella delle chiavi devono essere accessibili agli elaboratori registrati per il roaming (client di roaming). La directory `c:\roaming` deve essere un'unità di rete mappata.

   Se al momento esistono file nell'archivio, viene richiesto il modo in cui gestire tali file.
9. Fare clic su **Fine**.

Registrazione dei client con il server di roaming

Per registrare un client di roaming con il server di roaming, completare la procedura di seguito riportata:

1. Dopo aver completato la configurazione del server di roaming, viene visualizzato il pannello relativo alla configurazione della rete di roaming delle credenziali. Selezionare **Abilita registrazione client**, quindi fare clic su **Avanti**.
2. Immettere il nome dell'utente nel sistema B con privilegi da responsabile che completerà la registrazione del client.
3. Immettere e confermare una password da utilizzare per tale utente. (Attenzione a non confondere questa procedura con quella per autorizzare un utente all'utilizzo di UVM, che deve essere effettuata in seguito.)
4. Se di desidera registrare il client utilizzando il programma User Configuration Utility, è necessario creare un file di configurazione del responsabile per quell'utente. Questa procedura genera un file unico per l'utente. Memorizzare questo file in una posizione accessibile all'utente e al sistema B.

   Nota: Non è necessario generare questo file durante la registrazione di un client che utilizza il programma Administrator Utility.
5. Fare clic su **Avanti**.
6. Se viene creato un file di configurazione del responsabile, salvarlo in una posizione accessibile all'utente e al sistema B.

Una volta completate le procedure illustrate in precedenza, il server di roaming viene configurato. E' necessario completare la registrazione per ciascun client di roaming prima di poter utilizzare la rete di roaming.

Completamento della procedura di registrazione dei client di roaming

Una volta registrato l'elenco dei sistemi affidabili sul server di roaming, è necessario completare una delle procedure di seguito riportate sui sistemi client. E' necessario che il server di roaming sia in esecuzione e collegato all'archivio prima di poter completare la procedura di registrazione dei client di roaming.

Registrazione di un client di roaming utilizzando Administrator Utility

Per registrare un client di roaming utilizzando il programma Administrator Utility, completare la seguente procedura:

1. Fare clic su **Configurazione chiave**.
2. Fare clic su **No** se viene richiesto se si desidera ripristinare le chiavi dall'archivio.
3. Selezionare Registra questo sistema con un server di roaming CSS, quindi fare clic su **Avanti**.
4. Immettere la posizione dell'archivio creata dal sistema A, immettere la password di registrazione del sistema per quest'utente sul sistema A, quindi fare clic su **Avanti**.

   Il completamento della registrazione richiede alcuni minuti.

Registrazione di un client di roaming utilizzando User Configuration Utility

Per registrare un client di roaming utilizzando il programma User Utility, completare la seguente procedura:

1. Dal separatore User Configuration, fare clic su **Registra con un server di roaming CSS**.
2. Selezionare il file di configurazione del responsabile generato sul sistema A, immettere la password di registrazione del sistema designata per il relativo utente sul sistema A, quindi fare clic su **Avanti**.
3. Immettere la posizione dell'archivio creata dal sistema A, quindi fare clic su **Avanti**.

   Il completamento della registrazione richiede alcuni minuti.

Registrazione di un client di roaming utilizzando la distribuzione di massa (non presidiata)

Per registrare un client di roaming in modo non presidiato utilizzando una distribuzione di massa, completare la procedura di seguito riportata:

1. Creare il file `csec.ini`. Per ulteriori informazioni sulla creazione di un file CSS .ini, consultare la *Guida all'installazione di Client Security Software*.
2. Nella sezione `csssetup` del file, aggiungere `"enableroaming=1"`. Questo indica che l'elaboratore dovrebbe essere registrato come client di roaming.
3. Nella stessa sezione, aggiungere la voce `"username=OPTION"`. Sono disponibili tre opzione per questo valore:
   - **Opzione 1: La stringa `"[promptcurrent]"` - parentesi quadre incluse.** La designazione dovrebbe essere utilizzata se viene generato un file .dat per l'utente al momento collegato sul server di roaming e se l'utente corrente conosce la password di registrazione del sistema. Questa opzione apre una finestra a comparsa che richiede all'utente di immettere la password di registrazione del sistema (`sysregpwd`) prima della distribuzione.

- **Opzione 2: La stringa "[current]" - parentesi quadre incluse.** Questa specifica dovrebbe essere utilizzata se è stato generato un file .dat sul server per l'utente al momento collegato. Il parametro `sysregpwd` viene gestito come descritto in seguito.
- **Opzione 3: Un nome utente corrente come "joseph".** Se viene utilizzato tale nome utente, un file `"joseph.dat" deve essere precedentemente generato` dal server di roaming. La relativa stringa `sysregpwd` verrà gestita come descritto nel passo successivo.

4. Se vengono utilizzate le opzioni due e tre, è necessario fornire un altra voce, vale a dire `"sysregpwd=SYSREGPW"`. Questa è la password di registrazione del sistema associata o all'utente corrente (se viene implementata l'opzione due) o all'utente designato (se viene implementata l'opzione tre).
5. Per completare la registrazione dei client, collegare l'elaboratore all'archivio impostato dal server di roaming. Tale archivio è designato nel file `csec.ini`. Anche la cartella delle chiavi è impostata sul server di roaming delle credenziali è designata nel file `csec.ini`.
6. Cifrare il file `csec.ini` utilizzando Administrator Console.

Esempi del file csec.ini

Gli esempi di seguito riportati illustrano un file `csec.ini` e le relative modifiche in base alle opzioni di roaming delle credenziali selezionata. Di seguito sono riportate le opzioni disponibili:

- **Nessun valore di roaming.** Questo file di base non è abilitato per il roaming delle credenziali.
- **Opzione di roaming 1.** Questo file è abilitato per il roaming con l'opzione 1 per la registrazione del client. E' necessario che l'utente corrente immetta la password di registrazione del sistema prima della distribuzione.
- **Opzione di roaming 2.** Questo file è abilitato per il roaming con l'opzione 2 per la registrazione del client. E' necessario che l'utente corrente immetta l'ID utente e la password di registrazione del sistema designati nel file .ini.
- **Opzione di roaming 3.** Questo file è abilitato per il roaming con l'opzione 3 per la registrazione del client. L'utente è designato nel file .ini. La password di registrazione del sistema per l'utente designato deve essere presente nel file .ini.

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

[CSSSetup]	**Opzione 1**	**Opzione 2**	Opzione 3
	[CSSSetup]	[CSSSetup]	[CSSSetup]
suppw=bootup	suppw=bootup	suppw=bootup	suppw=bootup
hwpw=11111111	hwpw=11111111	hwpw=11111111	hwpw=11111111
newkp=1	newkp=1	newkp=1	newkp=1
keysplit=1	keysplit=1	keysplit=1	keysplit=1
kpl=c:\jgk	kpl=c:\\computer name\jgk, dove ″computer″ è memorizzato nella coppia di chiavi sul server di roaming	kpl=c:\\computer name\jgk, dove ″computer″ è memorizzato nella coppia di chiavi sul server di roaming	kpl=c:\\computer name\jgk, dove ″computer″ è memorizzato nella coppia di chiavi sul server di roaming

kal=c:\jgk\archive pub= c:\jk\admin.key pri= c:\jk\private1.key wiz=0	kal=c:\\computer name\archive, dove ″computer″ è memorizzato nell’archivio del server di roaming pub= c:\jk\admin.key pri= c:\jk\private1.key wiz=0	kal=c:\\computer name\archive, dove ″computer″ è memorizzato nell’archivio del server di roaming pub= c:\jk\admin.key pri= c:\jk\private1.key wiz=0	kal=c:\\computer name\archive, dove ″computer″ è memorizzato nell’archivio del server di roaming pub= c:\jk\admin.key pri= c:\jk\private1.key wiz=0
clean=0	**enableroaming=1** **username=** **[promptcurrent]** clean=0	**enableroaming=1** **username=** **[current]** **sysregpwd=12345678** clean=0	**enableroaming=1** **username=** **joseph** **sysregpwd=12345678** clean=0
[UVMEnrollment] enrollall=0 enrollusers=1 user1=joseph user1uvmpw= q1234r user1winpw= user1domain=0 user1ppchange=0 user1ppexppolicy=0 user1ppexpdays= 184	[UVMEnrollment] enrollall=0 enrollusers=1 user1=joseph user1uvmpw=q1234r user1winpw= user1domain=0 user1ppchange=0 user1ppexppolicy=0 user1ppexpdays=184	[UVMEnrollment] enrollall=0 enrollusers=1 user1=joseph user1uvmpw=q1234r user1winpw= user1domain=0 user1ppchange=0 user1ppexppolicy=0 user1ppexpdays=184	[UVMEnrollment] enrollall=0 enrollusers=1 user1=joseph user1uvmpw=q1234r user1winpw= user1domain=0 user1ppchange=0 user1ppexppolicy=0 user1ppexpdays=184
[UVMAppConfig] uvmlogon=0 entrust=0 notes=0 netscape=0 passman=0 folderprotect=0 autoprotect=0	[UVMAppConfig] uvmlogon=0 entrust=0 notes=0 netscape=0 passman=0 folderprotect=0 autoprotect=0	[UVMAppConfig] uvmlogon=0 entrust=0 notes=0 netscape=0 passman=0 folderprotect=0 autoprotect=0	[UVMAppConfig] uvmlogon=0 entrust=0 notes=0 netscape=0 passman=0 folderprotect=0 autoprotect=0

Gestione di una rete di roaming

Il responsabile di una rete di roaming deve autorizzare gli utenti e gestire l’accesso ai client e agli utenti stessi alla rete. Quindi l’importazione di un profilo utente, la sincronizzazione di dati utente o l’aggiunta e la rimozione di utenti e client è rapida e semplice in una rete di roaming CSS. Inoltre, potrebbe essere richiesto di ripristinare la rete di roaming, modificare la coppia di chiavi del responsabile o modificare la posione di archivio.

Autorizzazione degli utenti

Una volta completate le procedure illustrate in precedenza, la rete di roaming delle credenziali CSS viene configurata e i client di roaming sono registrati per il roaming. Quindi, in seguito è possibile autorizzare gli utenti all’utilizzo del programma Administrator Utility.

Sincronizzazione dei dati utente

I dati per ciascun utente vengono memorizzati nella posizione dell'archivio. Una copia dei dati è memorizzata anche localmente su ogni elaboratore con cui è stato effettuato il roaming. Una volta effettuate le modifiche, come ad esempio ottenere un certificato o modificare un passphrase, vengono aggiornati i dati locali. Se l'elaboratore è collegato all'archivio, anche i dati utente vengono aggiornati. Quando l'utente si collega ad un altro elaboratore, gli aggiornamenti vengono automaticamente scaricati su quell'elaboratore, se è collegato all'archivio.

Il collegamento all'archivio non è sempre garantito, quindi talvolta i dati utente possono non corrispondere tra gli elaboratori e l'archivio. Se i dati utente vengono modificati su un elaboratore non collegato all'archivio, le modifiche non vengono aggiornate nell'archivio e di conseguenza neanche sugli altri elaboratori. Quando l'elaboratore è collegato all'archivio, le modifiche vengono aggiornate nell'archivio e l'eventuale non corrispondenza di dati viene risolta successivamente sugli altri elaboratori collegati. Tuttavia, se le modifiche vengono effettuate su un altro elaboratore collegato all'archivio prima che il primo elaboratore contenente le modifiche viene connesso all'archivio, si verifica un problema di inconsistenza dati. I dati contenuti nell'archivio contengono modifiche non presenti sul primo elaboratore, mentre il primo elaboratore contiene modifiche non contenute nell'archivio. Se ciò si verifica, all'utente vengono notificate le due configurazioni diverse e viene richiesto di scegliere quale conservare, la configurazione locale o quella archiviata. Le modifiche della configurazione che non vengono scelte andranno perdute. Quindi, è importante assicurarsi che le modifiche effettuate ad una configurazione utente siano aggiornate nell'archivio prima di effettuare modifiche su altri elaboratori.

Ripristino di un passphrase perduto in un ambiente di roaming

Quando viene perduto o dimenticato un passphrase, il responsabile può reimpostare il passphrase utente sul server di roaming o su un qualunque client registrato. Questa modifica viene aggiornata su tutti i sistemi di rete *escluso* i sistemi che l'utente ha importato per l'abilitazione del collegamento protetto UVM. In questi casi, l'aggiornamento del passphrase *non* viene riflesso sull'elaboratore. Per ottenere l'accesso all'elaboratore, è necessario che l'utente disponga di un file di sovrascrittura della password e che completi la procedura di sovrascrittura password.

Importazione di un profilo utente

E' possibile importare un profilo utente in un nuovo computer su una rete di roaming utilizzando Administrator Utility, User Configuration Utility o l'interfaccia di registrazione di UVM. Se si desidera importare un utente che non dispone di account utente sul nuovo elaboratore, è necessario creare un account utente di Windows mediante il Pannello di controllo.

Nota: Per importare un utente in una rete di roaming, è necessario che tale utente sia autorizzato su un altro elaboratore che fa parte della rete di roaming.

Importazione di un profilo utente utilizzando User Configuration Utility

Per importare un profilo utente in un nuovo elaboratore della rete di roaming utilizzando User Configuration Utility, collegarsi al sistema con l'account utente da importare, quindi fare clic su **Start > Programmi > Access IBM > IBM Client**

Security Software > Modifica le impostazioni di protezione, quindi fare clic su **Importa configurazione esistente dall'archivio** nel separatore User Configuration.

Importazione di un profilo utente utilizzando Administrator Utility

Per importare un profilo utente in un nuovo elaboratore della rete di roaming utilizzando il programma Administrator Utility, selezionare l'utente, quindi fare clic su **Autorizza**. Fare clic su **Sì** quando viene richiesto di importare l'utente dall'archivio.

Importazione di un profilo utente utilizzando l'interfaccia di collegamento di UVM

E' possibile importare un profilo utente in un computer nuovo su una rete di roaming utilizzando l'interfaccia di collegamento UVM. La procedura inizia dal pannello di collegamento di UVM. Se un utente non è autorizzato all'utilizzo di UVM su un determinato sistema nella rete, viene visualizzata un messaggio nel quale si richiede se l'utente desidera essere importato dall'archivio.

Nota:

1. Se si desidera importare un utente che non dispone di un account utente nell'elaboratore, prima di continuare è necessario creare un account utente Windows utilizzando il Pannello di controllo.
2. Per accedere all'archivio sul server di roaming, è necessario che la directory sia un'unità di rete mappata.

Per importate un profilo utente in un nuovo elaboratore della rete di roaming utilizzando UVM GINA su un elaboratore che dispone di Windows 2000, completare la procedura di seguito riportata:

1. Al collegamento, immettere il nome utente ed il passphrase UVM dell'utente da importare. Viene visualizzato un messaggio che richiede se si desidera importare il profilo utente dall'archivio.
2. Fare clic su **Sì** alla richiesta di importazione dell'utente, quindi su **OK**.
3. Se la posizione dell'archivio si trova su un'unità di rete, fare clic su **Sì** indicando che deve essere fornita una condivisione di rete.
4. Immettere la password di Windows nel pannello standard di collegamento. Viene visualizzata una richiesta per il percorso di archivio.
5. Immettere il percorso di rete di archivio.
6. Immettere il nome utente e la password per il percorso di rete.
7. Fare clic su **OK**. Se l'operazione viene completata correttamente, viene visualizzato un messaggio indicante che l'importazione del profilo è riuscita.

Per importare un profilo utente in un nuovo elaboratore in una rete di roaming utilizzando UVM GINA su un elaboratore che dispone del sistema operativo Windows XP, completare la procedura di seguito riportata:

1. Al collegamento, immettere il nome utente ed il passphrase UVM dell'utente da importare. Viene visualizzato un messaggio che richiede se si desidera importare il profilo utente dall'archivio.
2. Fare clic su **Sì** alla richiesta di importazione dell'utente, quindi su **OK**.
3. Se la posizione dell'archivio si trova su un'unità di rete, fare clic su **Sì** indicando che deve essere fornita una condivisione di rete.
4. Alla richiesta dell'unità di rete mappata di Windows, immettere il percorso di rete dell'archivio.
5. Fare clic su **Fine**.

6. Immettere nome utente e password per il percorso di rete, quindi fare clic su **OK**. Se l'operazione viene completata correttamente, viene visualizzato un messaggio indicante che l'importazione del profilo è riuscita.

Nota: Per importare un utente in una rete di roaming, è necessario che tale utente sia autorizzato su un altro elaboratore che fa parte della rete di roaming.

Una volta importato il profilo utente, l'autenticazione con UVM è basata sulla politica di protezione dell'elaboratore. I requisiti per la protezione dell'elaboratore devono essere forniti correttamente prima che l'utente possa collegarsi.

Rimozione e reintegrazione degli utenti in una rete di roaming

Per rimuovere un utente da una rete di roaming, è necessario che il responsabile di rete completi la procedura di Administrator Console di seguito riportata:

1. Avviare il programma di utilità Administrator Console, quindi immettere la password del responsabile.
2. Fare clic su **Configura roaming delle credenziali**.
3. Selezionare **Rimuovi utenti da UVM e dalla rete di roaming delle credenziali**, quindi fare clic su **Avanti**. Ripetere i passi, se occorre.
4. Selezionare l'utente da rimuovere, quindi fare clic su **Rimuovi**.

   Nota: Una volta rimosso un utente dalla rete, tutte le credenziali appartenenti a tale utente vengono perdute definitivamente.

Gli utenti rimossi potrebbero non essere autorizzati ad utilizzare UVM e la rete di roaming fino a quando non vengono reintegrati dal responsabile di rete.

Per reintegrare un utente in una rete di roaming, è necessario che il responsabile di rete completi la procedura di Administrator Console di seguito riportata:

1. Avviare Console Utility, quindi immettere la password del responsabile.
2. Fare clic su **Configura roaming delle credenziali**.
3. Selezionare **Reintegra utenti rimossi**, quindi fare clic su **Avanti**.
4. Selezionare l'utente da reintegrare, quindi fare clic su **Reintegra**. Ripetere i passi, se occorre.

   Una volta reintegrato l'utente, è necessario autorizzarlo di nuovo all'utilizzo di UVM. Il reintegro di un utente, dunque, non lo autorizza automaticamente all'utilizzo di UVM.

Rimozione e reintegro dei client registrati in una rete di roaming

Per rimuovere un client registrato da una rete di roaming, è necessario che il responsabile di rete completi la procedura di Administrator Console di seguito riportata:

1. Avviare Console Utility, quindi immettere la password del responsabile.
2. Fare clic su **Configura roaming delle credenziali**.
3. Selezionare **Rimuovi client registrati dalla rete di di roaming delle credenziali**, quindi fare clic su **Avanti**.
4. Selezionare il sistema da rimuovere, quindi fare clic su **Rimuovi**. Ripetere i passi, se occorre.

Nota: Una volta rimosso un client dalla rete, tutte le credenziali basate sulla macchina appartenenti al sistema andranno perdute in modo definitivo.

I client rimossi non possono essere registrati con il server della rete di roaming fino a quando non vengono reintegrati dal responsabile di rete.

Per reintegrare un client registrato ad una rete di roaming, è necessario che il responsabile di rete completi la procedura di Administrator Console di seguito riportata:

1. Avviare Console Utility, quindi immettere la password del responsabile.
2. Fare clic su **Configura roaming delle credenziali**.
3. Selezionare **Reintegra client rimossi**, quindi fare clic su **Avanti**.
4. Selezionare il client da reintegrare, quindi fare clic su **Reintegra**. Ripetere i passi, se occorre.

   Una volta reintegrato il client, quest'ultimo può essere registrato di nuovo con il server di roaming. La reintegrazione di un client non ne consente la registrazione automatica.

Nota: Tutti gli utenti le cui credenziali erano presenti nel sistema nel momento in cui il client è stato rimosso, potrebbero dover importare di nuovo le credenziali.

Limitazione dell'accesso a client registrati in una rete di roaming

Potrebbe verificarsi che il responsabile di rete desideri autorizzare l'accesso ad alcuni utenti ad un determinato client registrato, limitando l'accesso agli altri utenti.

Per gestire i privilegi di accesso degli utenti, è necessario che il responsabile di rete completi la procedura di Administrator Console di seguito riportata:

1. Avviare Console Utility, quindi immettere la password del responsabile.
2. Fare clic su **Configura roaming delle credenziali**.
3. Selezionare **Gestisci accesso utenti per i client registrati**, quindi fare clic su **Avanti**.
4. Selezionare il client registrato da gestire nella casella **Seleziona un sistema nella rete di roaming CSS**. Gli utenti che dispongono o meno dell'accesso sono elencati nelle due caselle ad elenco.
5. Effettuare una delle seguenti operazioni:
   - Per limitare l'accesso ad un utente, selezionare l'utente dall'elenco **Utenti con accesso**, quindi fare clic su **Limita**. Ripetere i passi, se occorre.
   - Per dare accesso ad un utente limitato, selezionare l'utente dall'elenco **Utenti senza accesso**, quindi fare clic su **Consenti**. Ripetere i passi, se occorre.

Per le funzioni di gestione degli accessi della rete di roaming è necessario creare una nuova cartella nell'archivio. La nuova cartella, denominata Protetta, deve disporre degli attributi di scrittura per il responsabile di rete di sola lettura per gli altri utenti. Se gli utenti dispongono degli attributi di scrittura per quella cartella, potrebbero reintegrare manualmente i loro profili sui sistemi.

Ripristino di una rete di roaming

In caso di errori software o hardware, potrebbe essere necessario ripristinare la rete di roaming. Se il server di roaming o i dati utilizzati da CSS sono corrotti su un client registrato, ripristinare i dati utilizzando Administrator Utility allo stesso

modo di un ambiente non di roaming. Se IBM embedded Security subsystem su un client registrato non funziona o viene annullato, è necessario registrare di nuovo il client con il server di roaming. Non è necessaria alcuna operazione aggiuntiva.

Modifica della coppia di chiavi del responsabile

Non è consigliato modificare la coppia di chiavi del responsabile in una rete di roaming in quanto richiederebbe che ogni client venisse nuovamente registrato con il server di roaming.

Per modificare la coppia di chiavi del responsabile di una rete di roaming, è necessario procedere nel modo seguente affinché le modifiche siano effettuate ed attive su tutti gli elaboratori della rete:

1. Sul server di roaming, modificare la coppia di chiavi del responsabile utilizzando il programma Administrator Utility.
2. Registrare nuovamente tutti i client della rete.
3. Conservare i file esistenti quando viene richiesto.

Modifica della cartella di archivio

La modifica della cartella di archivio in un ambiente di roaming è leggermente diversa rispetto ad un ambiente non di roaming, in quanto ciascun elaboratore in rete accede alla stessa posizione di archivio.

Per modificare la cartella di archivio in una rete di roaming, completare la procedura di seguito riportata:

1. Copiare i file dalla cartella di archivio precedente a quella nuova con la procedura di seguito riportata:
   a. Avviare il programma Administrator Utility, quindi immettere la password del responsabile.
   b. Fare clic su **Configurazione chiave**.
   c. Selezionare Modifica posizione dell'archivio, quindi fare clic su **Avanti**.
   d. Immettere la nuova cartella dell'archivio, quindi fare clic su **Avanti**.
   e. Fare clic su **Sì** quando viene richiesto di copiare tutti i file dalla cartella precedente a quella nuova.
2. Aggiornare tutti gli altri elaboratori in rete, affinché possano utilizzare la nuova cartella di archivio con la procedura di seguito riportata:
   a. Avviare il programma Administrator Utility, quindi immettere la password del responsabile.
   b. Fare clic su **Configurazione chiave**.
   c. Selezionare Modifica posizione dell'archivio, quindi fare clic su **Avanti**.
   d. Immettere la nuova cartella dell'archivio, quindi fare clic su **Avanti**.
   e. Fare clic su **No** quando viene richiesto di copiare tutti i file dalla cartella precedente alla nuova.

File and Folder Encryption (FFE)

Le funzioni di File and Folder Encryption non sono condizionate da un ambiente di roaming. Tuttavia, le cartelle protette sono gestite su base elaboratore-elaboratore. In questo modo, se una cartelle è protetta da un utente A su un sistema A, la stessa cartella sul sistema B non risulta protetta, se l'utente non l'ha protetta anche sul sistema B.

IBM Password Manager

Tutte le password protette utilizzando IBM Password Manager sono disponibili su tutti gli elaboratori nella rete di roaming.

Termini e definizioni per il roaming

Di seguito sono riportati termini che consentono di comprendere i concetti e le procedure relative alla configurazione di una rete di roaming:

Registrazione client di roaming
Il processo di registrazione di un elaboratore con un server di roaming.

Client di roaming
Tutti i computer affidabili nella rete di roaming.

Server di roaming
Il computer ESS utilizzato per inizializzare la rete di roaming.

Password di registrazione client di roaming
La password utilizzata per registrare l'elaboratore con il server di roaming.

Parte 3. Informazioni per il responsabile

Capitolo 5. Come utilizzare Client Security Software

I responsabili possono utilizzare più componenti forniti da Client Security Software per impostare le funzioni di protezione che richiedono gli utenti client CSS. Utilizzare i seguenti esempi per comprendere come pianificare la propria configurazione e politica Client Security. Ad esempio, é possibile che gli utenti Windows 2000 e Windows XP impostino la protezione UVM per il collegamento del sistema che impedisce agli utenti non autorizzati di collegarsi al client CSS.

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

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

Per impostare client security, completare la seguente procedura:

1. Installare Client Security Software sul client 1 e sul client 2. Fare riferimento al manuale *Client Guida per l'installazione di Security Software* per i dettagli.
2. Installare i sensori di rilevamento delle impronte digitali compatibili con UVM e tutto il software associato su ciascun client.

   Per ulteriori informazioni sui prodotti compatibili con UVM, passare al sito http://www.pc.ibm.com/us/security/secdownload.html sul web.
3. Impostare l'autenticazione utente con UVM per ciascun client. Procedere nel modo seguente:
   a. Autorizzare gli utenti a UVM assegnando loro un passphrase UVM. Poiché il client 1 ha tre utenti, è necessario ripetere il processo per autorizzare gli utenti in UVM fino all'autorizzazione di tutti gli utenti.
   b. Configurare la protezione UVM per il collegamento a Windows per ciascun client.
   c. Registrare le impronte digitali dell'utente. Poiché sarà impostata una politica che indicherà che tra utenti utilizzeranno il il client 1, è necessario che tutti e tre gli utenti registrino le rispettive impronte digitali sul client 1. Almeno uno deve registrare le impronte digitali sul client 2.

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

5. Riavviare ciascun client per abilitare la protezione del collegamento UVM per il collegamento a Windows.
6. Informare gli utenti dei passphrase UVM impostati e dei requisiti di autenticazione, impostati nella politica UVM per il client CSS.

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

- Utilizzare la protezione UVM per bloccare e sbloccare Windows.
- Richiedere un certificato digitale e selezionare IBM Embedded Security Subsystem come provider dei servizi crittografici associati al certificato.
- Utilizzare il certificato digitale per cifrare i messaggi e-mail creati con Outlook Express.

Esempio 2 - Due client CSS Windows 2000 che utilizzano Lotus Notes

In questo esempio, i due client CSS (client 1 e client 2) dispongono di Windows 2000 e Lotus Notes. Gli utenti richiedono l'installazione di autenticazione UVM sul client 1; un utente richiede l'installazione di autenticazione con UVM sul client 2; entrambi i client richiedono la protezione del collegamento UVM per il collegamento Windows. Il responsabile decide di modificare la politica UVM sul client 1 e copiarlo nel client 2.

Per impostare client security, completare la seguente procedura:

1. Installare Client Security Software sul client 1 e sul client 2. Poichè verrà utilizzato lo stesso file della politica UVM, sarà necessario utilizzare la stessa chiave pubblica del responsabile quando verrà installato il software su entrambi i client. Leggere il manuale *Guida per l'installazione di Client Security Software* per i dettagli relativi all'installazione del software.
2. Impostare l'autenticazione utente con UVM per ciascun client. Quindi, procedere nel modo seguente:
   a. Autorizzare gli utenti a UVM assegnando loro un passphrase UVM. Poiché il client 1 ha due utenti, è necessario ripetere il processo per autorizzare gli utenti a UVM fino a quando sono stati autorizzati entrambi gli utenti.
   b. Impostare la protezione del collegamento UVM per il collegamento di Windows su ciascun client.
3. Abilitare il supporto Lotus Notes della protezione UVM su entrambi i client.
4. Modificare e salvare una politica UVM sul client 1, quindi copiarla sul client 2. La politica UVM richiede l'autenticazione dell'utente per eliminare lo screen saver, collegarsi a Lotus Notes e collegarsi a Windows. Per ulteriori dettagli, consultare la sezione "Modifica e utilizzo di una politica UVM" a pagina 58.
5. Riavviare ciascun client per abilitare la protezione del collegamento UVM per il collegamento a Windows.
6. Comunicare agli utenti client i passphrase UVM e la politica che è stata impostata per ciascun client.

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

L'utente per cui è stato progettato il seguente esempio è un responsabile di azienda che desidera utilizzare Tivoli Access Manager per gestire gli oggetti di autenticazione che vengono impostati dalla politica UVM. In questo esempio, più client CSS dispongono di Windows 2000 e Netscape. Su tutti i client è installato NetSEAT client, un componente di Tivoli Access Manager. Su tutti i client che

utilizzano un server LDAP è installato il client LDAP. La politica UVM abilita Tivoli Access Manager per controllare gli oggetti di autenticazione selezionati per i client.

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

Per impostare client security, completare la seguente procedura:

1. Installare il componente Client Security sul server Tivoli Access Manager. Per ulteriori dettagli, fare riferimento alla guida *Utilizzo di Client Security con Tivoli Access Manager*.
2. Installare Client Security Software su tutti i client. Poiché verrà utilizzata una politica UVM, è necessario utilizzare la stessa chiave pubblica del responsabile utilizzata durante l'installazione del software su tutti i client. Per ulteriori dettagli sull'installazione del software, consultare la *Guida all'installazione di Client Security Software*.
3. Installare i sensori di rilevamento delle impronte digitali compatibili con UVM e tutto il software associato su ciascun client. Per informazioni sui prodotti disponibili compatibili con UVM, passare al sito http://www.pc.ibm.com/us/security/index.html sul web.
4. Impostare l'autenticazione con UVM su ciascun client. Per le informazioni dettagliate, consultare la sezione "Rimozione degli utenti" a pagina 45. Quindi, procedere nel modo seguente:
   a. Autorizzare gli utenti a UVM assegnando loro un passphrase UVM.
   b. Configurare la protezione del collegamento UVM per il collegamento a Windows su ciascun client.
   c. Registrare le impronte digitali per ciascun utente del client. Se viene richiesta l'autenticazione delle impronte digitali su un client CSS, è necessario che tutti gli utenti di tale client registrino le proprie impronte digitali.
5. Configurare le informazioni sulla configurazione di Tivoli Access Manager su ciascun client. Per ulteriori dettagli, fare riferimento alla guida *Utilizzo di Client Security con Tivoli Access Manager*.
6. Modificare e salvare una politica UVM su uno dei client, copiarla sugli altri client. Impostare la politica UVM in modo che Tivoli Access Manager controlli i seguenti oggetti di autenticazione:
   - Collegamento a Windows
   - Acquisto di un certificato digitale
   - Utilizzo di una firma digitale per Outlook Express

   Per ulteriori dettagli, consultare la sezione "Modifica e utilizzo di una politica UVM" a pagina 58.
7. Riavviare ciascun client per abilitare la protezione del collegamento UVM per il collegamento a Windows.
8. Installare il modulo PKCS#11 di IBM Embedded Security Chip su ciascun client. Questo modulo fornisce il supporto per la cifratura sui client che utilizzano Netscape per l'invio e la ricezione di messaggi e-mail e IBM Embedded Security Subsystem per l'acquisizione di certificati digitali. Per ulteriori informazioni, fare riferimento alla guida *Guida all'installazione di Client Security Software*.

9. Abilitare Tivoli Access Manager per controllare gli oggetti IBM Client Security Solutions che vengono visualizzati in Tivoli Access Manager Management Console.
10. Informare gli utenti del client dei passphrase UVM impostati e della politica impostata per ciascun client.
11. Consultare la *Guida per l'utente di Client Security Software* per eseguire le attività riportate di seguito:
    - Utilizzare la protezione UVM per bloccare e sbloccare Windows
    - Utilizzare User Configuration Utility
    - Richiedere un certificato digitale che utilizza Embedded Security Subsystem come provider dei servizi di cifratura associati con il certificato
    - Utilizzare il certificato digitale per cifrare i messaggi e-mail creati con Netscape

Capitolo 6. Autorizzazione degli utenti

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

Autenticazione per utenti client

L'autenticazione degli utenti a livello client è un passo fondamentale per la protezione del computer. Client Security Software fornisce l'interfaccia richiesta per gestire la politica di sicurezza di un client CSS. Questa interfaccia appartiene al software di autenticazione UVM (User Verification Manager), che è il componente principale del programma Client Security Software.

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

- Localmente, utilizzando un editor di politica che risiede sul client CSS
- In tutta l'azienda, utilizzando Tivoli Access Manager

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

Elementi di autenticazione

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

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

- **Protezione UVM per il collegamento al sistema operativo.** La protezione UVM verifica che solo questi utenti, rilevati da UVM, sono in grado di accedere all'elaboratore. Prima di abilitare la protezione UVM per il collegamento al sistema, consultare la sezione "Impostazione della protezione del collegamento UVM" a pagina 47 per ulteriori informazioni.
- **Screen saver di Client Security.** Una volta aggiunto un utente del client, è possibile che l'utente installati ed utilizzi lo screen saver di Client Security. Lo screen saver di Client Security è impostato tramite l'opzione Schermo all'interno del pannello di controllo di Windows. E' necessario abilitare la protezione UVM per il collegamento al sistema per utilizzare lo screen saver di Client Security.

Prima di autorizzare gli utenti

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

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.

Quando si autorizza un utente client, Administrator Utility fornisce un elenco di nomi utente da cui è possibile effettuare una selezione. I nomi presenti in questo elenco sono gli account utente che sono stati aggiunti mediante Windows. Prima di aggiungere gli utenti client in UVM, utilizzare Windows per creare gli account utente ed i profili per tali utenti. Client Security Software funziona insieme alle funzioni di sicurezza di Windows.

Utilizzare il programma Users and Passwords per creare i nuovi account utente e per gestire i gruppi e gli account dell'utente. Per ulteriori informazioni, consultare la documentazione di Microsoft.

Nota:

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

Autorizzazione degli utenti

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

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

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

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

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

   Nota: I nomi utente, presenti nell'elenco, sono definiti dagli account utente creati in Windows.
4. Fare clic su **Autorizza**.

   Viene visualizzato il pannello di configurazione per l'autenticazione dell'utente.
5. Riesaminare e selezionare le impostazioni di scadenza passphrase per il nuovo utente. Per impostazione predefinita, viene selezionata la casella di controllo

L'utente deve cambiare password all'utilizzo successivo ed la scadenza del passphrase viene impostata dopo 184 giorni.

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

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

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

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

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

   - **L'utente deve memorizzare la relativa password di Windows successivamente mediante User Configuration Utility.** Per memorizzare la password di Windows mediante User Configuration Utility, selezionare il pulsante di opzione appropriato, quindi fare clic su **Avanti**.
   - **Memorizzare la password corrente di Windows dell'utente.** Per memorizzare la password corrente di Windows dell'utente, immettere e confermare la password dell'utente nei campi forniti, quindi fare clic su **Avanti**.

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

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

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

Rimozione degli utenti

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

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

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

   Viene visualizzato il messaggio Inserisci password del responsabile.

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

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

3. Nell'area Utenti di Windows autorizzati ad utilizzare UVM, selezionare un nome utente dall'elenco.
4. Fare clic su **Rimuovi utente**.

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

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

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

Creazione di nuovi utenti

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

Per creare nuovi utenti, completare la seguente procedura:

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

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

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

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

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

Capitolo 7. Capacità UVM aggiuntive

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

- **Autenticazione Enhanced Windows.** Per ulteriori informazioni, consultare la sezione "Pianificazione protezione collegamento UVM".
- **Protezione di autenticazione migliorata per gli utenti Lotus Notes.**
- **Abilitazione applicazioni compatibili con PKCS#11.**
- **Reimpostazione passphrase.**
- **Registrazione impronte digitali degli utenti.** Per ulteriori informazioni, consultare la sezione "Registrazione delle impronte digitali degli utenti" a pagina 53.

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

Autenticazione Enhanced Windows

La protezione del collegamento UVM per Windows potenzia la funzione della password, fornita con Windows. L'interfaccia di collegamento UVM sostituisce il collegamento Windows in modo che si apra la finestra di collegamento UVM ogni volta che un utente tenta di collegarsi al sistema.

Pianificazione protezione collegamento UVM

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

- Se la politica UVM indica che l'autenticazione delle impronte digitali viene richiesta per il collegamento di Windows e l'utente non ha registrato le impronte digitali, è necessario che l'utente registri le impronte digitali per collegarsi.

  Inoltre, se la password di Windows dell'utente non è registrata (oppure è stata registrata in modo errato) con UVM, l'utente deve fornire la password corretta di Windows per collegarsi.
- Non eliminare IBM embedded Security Chip mentre è abilitata la protezione UVM. In caso contrario, verrà bloccato il sistema. Per ulteriori informazioni, consultare la sezione "Suggerimenti del responsabile" presente nel Appendice A, "Risoluzione dei problemi", a pagina 73.
- Se si deseleziona la casella di controllo **Abilita sostituzione collegamento Windows** in Administrator Utility, il sistema ritorna al processo di collegamento Windows senza utilizzare la protezione del collegamento UVM.
- Se si abilita la sostituzione del collegamento Windows con il collegamento protetto UVM e viene abilitata la funzione Cisco LEAP, è necessario reinstallare l'ACU (Cisco Aironet Client) Utility.

Impostazione della protezione del collegamento UVM

Per impostare la protezione del collegamento UVM per Windows, completare la seguente procedura:

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

Viene visualizzata la finestra principale Administrator Utility.

2. Fare clic su **Configura politiche e supporto applicazioni**.

   Viene visualizzato il pannello Configurazione della politica e applicazione UVM.
3. Selezionare la casella di controllo **Abilita sostituzione collegamento Windows**.
4. Fare clic su **OK**.
5. Fare clic su **Esci**.
6. Chiudere tutte le applicazioni.
7. Riavviare il computer.

Una volta riavviato l'elaboratore, sarà richiesto di collegarsi. Per ulteriori informazioni sulla protezione UVM, consultare la sezione "Autenticazione Enhanced Windows" a pagina 47.

Recupero di un passphrase UVM

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

Per avviare una procedura di ripristino di un passphrase, completare la seguente procedura:

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

   Viene visualizzata la finestra principale Administrator Utility.
2. Selezionare un utente nel campo Utenti di Windows autorizzati ad utilizzare UVM.
3. Fare clic su **Modifica passphrase**.

   Viene visualizzato il pannello Modifica passphrase.
4. Inserire il percorso ed il nome della directory dell'archivio della chiave oppure fare clic su **Sfoglia** per individuare la directory.
5. Inserire il percorso ed il nome file della chiave privata administrator nel campo File della chiave privata di archivio oppure fare clic su **Sfoglia** per individuare il file.
6. Fare clic su **OK**.

   Se la chiave privata del responsabile è stata suddivisa in più file, viene visualizzato un messaggio che richiede di inserire l'ubicazione e il nome di ciascun file. Fare clic su **Leggi successivo** dopo aver immesso ciascun nome file nel campo del file di chiavi.
7. Inserire il nuovo passphrase UVM per l'utente nel campo del passphrase UVM e confermare il passphrase nel campo. Fare clic su **Visualizza requisiti passphrase** per visualizzare un elenco delle regole imposte dalla politica di protezione UVM.
8. Selezionare e impostare le regole di scadenza del passphrase disponibile nell'area di scadenza del passphrase.
9. Fare clic su **Avanti**. Viene visualizzato un messaggio che indica il completamento corretto dell'operazione.
10. Fare clic su **Fine**.

Protezione di autenticazione migliorata per gli utenti Lotus Notes

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

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

Prima di poter abilitare la protezione del collegamento UVM per Lotus Notes, è necessario che Lotus Notes sia installato sul client IBM, siano stabiliti una password ed un ID utente Notes per l'utente e sia autorizzato un utente Lotus Notes per utilizzare UVM.

Per impostare la protezione del collegamento UVM per Lotus Notes, completare la seguente procedura:

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

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

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

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

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

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

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

    La registrazione della password UVM è completa quando viene avviato Lotus Notes.

Utilizzo della protezione di collegamento UVM per Lotus Notes

Prima di poter utilizzare la protezione UVM per Lotus Notes, è necessario seguire la procedura contenuta nella sezione "Impostazione della protezione di collegamento UVM per Lotus Notes" a pagina 50.

Impostazione della protezione di collegamento UVM per Lotus Notes

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

1. Collegarsi a Lotus Notes.

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

   La password di Lotus Notes è registrata con UVM.

Re-impostazione della password di Lotus Notes

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

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

   Viene visualizzata la finestra IBM UVM (User Verification Manager).
3. Immettere il passphrase UVM, quindi fare clic su **OK**.

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

   Viene visualizzata la finestra IBM UVM (User Verification Manager).
5. Selezionare il pallino **Crea password**.
6. Immettere e verificare la nuova password per Lotus Notes nei campi disponibili, quindi fare clic su **OK**.

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

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

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

Disabilitazione della protezione del collegamento UVM per un ID utente di Lotus Notes

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

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

   In seguito all'immissione della password del responsabile, viene visualizzata la finestra principale del programma Administrator Utility.
2. Fare clic su **Configura politiche e supporto applicazioni**.

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

4. Fare clic su **OK**.

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

Impostazione della protezione di collegamento UVM per un ID Utente passato a Lotus Notes

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

1. Uscire da Lotus Notes.
2. Disabilitare la protezione UVM per l'ID utente corrente. Per informazioni dettagliate, consultare la sezione "Disabilitazione della protezione del collegamento UVM per un ID utente di Lotus Notes" a pagina 50.
3. Immettere Lotus Notes e cambiare ID utente. Per ulteriori informazioni sul passaggio tra gli ID utenti, fare riferimento alla documentazione relativa a Lotus Notes.
4. Per impostare la protezione UVM per l'ID utente commutato, attivare lo strumento Configurazione di Lotus Notes (fornito da Client Security Software) ed impostare la protezione UVM. Consultare la sezione "Utilizzo della protezione di collegamento UVM per Lotus Notes" a pagina 49.

Abilitazione applicazioni compatibili con PKCS#11

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

Per ulteriori dettagli sulle modalità di utilizzo delle impostazioni di sicurezza per le applicazioni Netscape, fare riferimento alla documentazione fornita da Netscape. IBM Client Security Software supporta solo Netscape Versioni 4.8 e 7.1.

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

Installazione del modulo PKCS#11 di IBM embedded Security Chip

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

Per utilizzare Netscape per installare il modulo PKCS#11 di IBM embedded Security Chip, completare la seguenti procedura:

1. Aprire Netscape, quindi fare clic su **File > Apri**.
2. Collocare il file di installazione `ibmpkcsinstallt.html` o `ibmpkcsinstalls.html` .

   (Se è stata accettata la directory predefinita quando si installa il software, il file viene situato nella directory C:\Program Files\IBM\Security.)
3. Aprire il file di installazione `ibmpkcsinstallt.html` o `ibmpkcsinstalls.html` con Netscape.

Viene visualizzato un messaggio che richiede se si desidera installare questo modulo di sicurezza.

4. Fare clic su **OK**.

   Viene visualizzata la finestra Passphrase UVM.

5. Immettere il passphrase UVM e fare clic su **OK**.

   Viene visualizzato un messaggio che notifica l'installazione del modulo.

Selezionare IBM embedded Security Subsystem per creare un certificato digitale

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

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

Aggiornare l'archivio delle chiavi

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

Utilizzo del certificato digitale del modulo PKCS#11

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

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

Se i requisiti di autenticazione impostati dalla politica UVM non vengono soddisfatti, viene visualizzato un messaggio di errore. Facendo clic su **OK**, verrà aperta l'applicazione ma non sarà possibile utilizzare il certificato digitale generato da IBM embedded Security Chip fino al successivo riavvio di e all'immissione dei corretti passphrase UVM, delle impronte digitali o di entrambi.

Reimpostazione del passphrase

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

Reimpostazione del passphrase in remoto

Per reimpostare una password in remoto, 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 del passphrase

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

Registrazione delle impronte digitali degli utenti

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

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

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

   Viene visualizzata la finestra Modifica configurazione utente di Client Security - Modifica attributi dell'utente UVM.
3. Selezionare la casella **Registra impronte digitali e/o smart card**, quindi fare clic su **Avanti**.

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

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

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

Capitolo 8. Funzionalità della politica UVM

Nota: Prima di tentare di modificare la politica UVM per il client locale, verificare che le chiavi siano impostate. In caso contrario, verrà visualizzato un messaggio di errore quando l'editor della politica effettua un tentativo per aprire il file della politica locale.

Dopo aver autorizzato gli utenti ad accedere a UVM, è necessario modificare e salvare una politica di sicurezza per ogni client IBM. La politica di sicurezza fornita da Client Security Software viene definita politica UVM, che combina le impostazioni fornite in "Autorizzazione degli utenti" con i requisiti di autenticazione a livello di client. Un file della politica UVM può essere copiato nei client della rete.

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

- E' necessario che ogni utente immetta un passphrase UVM ed utilizzi l'autenticazione per impronta digitale per collegarsi a Windows.
- Ciascun utente deve inserire un passphrase UVM ogni qualvolta che venga richiesto un certificato digitale.

Inoltre, è possibile utilizzare Tivoli Access Manager per controllare oggetti specifici di autenticazione come impostati nella politica UVM. Consultare *Utilizzo Client Security Software con Tivoli Access Manager* per ulteriori informazioni.

La politica UVM imposta i requisiti per gli oggetti di autenticazione per il client IBM e non per il singolo utente. Quindi, se si imposta la politica UVM per richiedere l'autenticazione delle impronte digitali per un oggetto (quali il collegamento di Windows), ciascun utente autorizzato ad utilizzare UVM deve registrare un'impronta digitale per utilizzare tale oggetto. Per informazioni dettagliate sull'autorizzazione di un utente, consultare la sezione "Rimozione degli utenti" a pagina 45.

La politica UVM viene salvata in un file definito `globalpolicy.gvm`. Per utilizzare UVM in una rete, la politica UVM deve essere salvata su un client IBM e, quindi, copiato su client remoti. La copia del file di politica UVM su altri client consente di risparmiare tempo per configurare la politica UVM su tali remoti.

Modifica di una politica UVM

E' possibile modificare una politica UVM e utilizzarla sul client per cui è stato modificato. Se Client Security è installato nell'ubicazione predefinita, il file della politica UVM viene memorizzato come \Program Files\IBM\Security\UVM_Policy\globalpolicy.gvm. Utilizzare UVM Policy Editor per modificare e salvare un file della politica locale UVM. L'interfaccia per l'editor della politica UVM viene fornita in Administrator Utility.

L'autenticazione si verifica in base alle selezioni effettuate nell'editor della politica. Ad esempio, se si seleziona "Nessun passphrase richiesto in seguito al primo

utilizzo in questo modo" per il collegamento a Lotus Notes, ogni qualvolta in cui viene eseguito un collegamento a Lotus Notes verrà richiesta l'autenticazione UVM. Per i successivi accessi a Lotus Notes non sarà necessario il passphrase fino a quando non si esegue un riavvio o uno scollegamento.

Quando si imposta la politica UVM per richiedere le impronte digitali per un oggetto di autenticazione (ad esempio il collegamento di Windows), è necessario che ogni utente autorizzato UVM abbia registrato le impronte digitali per utilizzare tale oggetto.

durante la modifica della politica UVM, è possibile visualizzare le informazioni di riepilogo della politica facendo clic su **Riepilogo della politica UVM**. Inoltre, è possibile fare clic su **Applica** per salvare le proprie modifiche. Quando si seleziona **Applica**, viene visualizzato un messaggio che richiede la chiave privata del responsabile. Immettere tale chiave, quindi fare clic su **OK** per salvare le modifiche. Se viene fornita una chiave privata del responsabile errata, le modifiche non saranno salvate.

Selezione dell'oggetto

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

Oggetti di politica UVM validi includono quanto segue:

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

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

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

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

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

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

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

Password Manager
Questa applicazione controlla i requisiti di autenticazione necessari durante l 'utilizzo di IBM Password Manager, disponibile sul sito web IBM.

Quando attivo,dovrebbe essere selezionata l'opzione ″Nessun passphrase richiesto in seguito al primo utilizzo in questo modo.″

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

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

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

Elementi di autenticazione

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

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

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

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

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

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

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

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

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

Utilizzo dell'editor della politica UVM

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

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

   Viene visualizzato il pannello Configurazione della politica e applicazione UVM.
2. Fare clic sul pulsante **Politica applicativa**.

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

   Viene visualizzato il pannello Inserisci password del responsabile.
4. Immettere la password del responsabile, quindi fare clic su **OK**.

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

   Le azioni comprendono Collegamento del sistema, Sblocco del sistema e Decifrazione dell'e-mail; un esempio di un tipo di oggetto è Acquista certificato digitale.
6. Per ciascun oggetto selezionato, completare la seguente operazione:
   - Fare clic sul separatore **Elementi di autenticazione** e modificare le impostazioni per gli elementi di autenticazione che si desidera assegnare agli oggetti.
   - Selezionare **Access Manager controlla l'oggetto selezionato** per abilitare Tivoli Access Manager a controllare l'oggetto scelto. Selezionare questa opzione solo se si desidera che Tivoli Access Manager controlli gli elementi di autenticazione per il client IBM. Per ulteriori informazioni, consultare la sezione *Utilizzo di Client Security con Tivoli Access Manager*.

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

Modifica e utilizzo di una politica UVM

Per utilizzare la politica UVM tra più client IBM, modificare e salvare la politica UVM e 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.

Capitolo 9. Altre funzioni del responsabile per la protezione

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

Per aprire Administrator Utility, completare la seguente procedura:

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

   Poiché l'accesso al programma Administrator Utility è protetto dalla password del responsabile, viene visualizzato un messaggio che richiede l'immissione della password di administrator Chip.
2. Immettere la password del responsabile, quindi fare clic su **OK**.

Utilizzo di Administrator Console

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

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

La console del responsabile consente ad un responsabile della protezione di effettuare le seguenti attività:

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

- **Altre funzioni remote del responsabile.** L'applicazione Administrator Console consente ad un responsabile della protezione di eseguire le funzioni remote di seguito riportate:
  - **Crea il file Administrator Configuration.** Questa funzione consente al responsabile di creare il file di configurazione per il responsabile, che viene richiesto quando si registra o reimposta un utente con Client Utility. Di solito, il responsabile invia tramite e-mail questo file ad un utente.
  - **Cifra/Decifra file di configurazione.** Questa funzione consente la cifratura del file di configurazione per una maggiore sicurezza. Inoltre, decifra il file in modo che possa essere editato.
  - **Configura roaming delle credenziali.** Questa funzione registra il sistema come server di roaming CSS. Una volta registrato tutti gli utenti della rete autorizzati UVM potranno accedere ai dati personali (passphrase, certificati e altro.) presenti nel sistema.

Modifica dell'ubicazione dell'archivio di chiavi

Quando viene creato prima l'archivio della chiave, le copie di tutte le chiavi di cifratura sono create e salvate sulla posizione specificata all'installazione.

Nota: l'utente client può anche modificare l'ubicazione dell'archivio delle chiavi utilizzando User Configuration Utility. Per ulteriori informazioni, consultare il Capitolo 2, "Istruzioni per gli utenti client", a pagina 13.

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

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

   Viene visualizzata la finestra Modifica configurazione chiave client- Configura chiavi.
2. Fare clic sul pallino **Modifica posizione dell'archivio**, quindi fare clic su **Avanti**.

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

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

Modifica della coppia di chiavi dell'archivio

Quando vengono salvate le chiavi del responsabile in una posizione di archivio, le chiavi copiate cono chiamate coppia di chiavi di archivio. Tali chiavi vengono di solito memorizzate su un minidisco o una directory di rete.

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

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

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

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

2. Fare clic sul pallino **Modifica chiavi di archivio** e, quindi, su **Avanti**.

   viene visualizzato il pannello Modifica configurazione chiave - Chiave pubblica .
3. Nel campo Nuove chiavi di archivio, inserire il nome file per la nuova chiave pubblica dell'archivio nel campo chiave pubblica dell'archivio. Inoltre, è possibile fare clic su **Sfoglia** per ricercare il nuovo file o fare clic su **Crea** per creare una nuova chiave pubblica dell'archivio.

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

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

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

   Viene visualizzato un messaggio che indica il completamento corretto dell'operazione.
9. Fare clic su **OK**.

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

Ripristino delle chiavi dall'archivio

E' necessario ripristinare le chiavi in seguito ad una sostituzione della scheda di sistema o se un errore del disco fisso compromette l'integrità delle chiavi utente. Quando si ripristinano le chiavi, copiare i file aggiornati della chiave dell'utente dall'archivio della chiave e memorizzarli su IBM embedded Security Subsystem. Il ripristino delle chiavi sovrascriverà tutte le chiavi memorizzate in security chip.

Se la scheda di sistema originale viene sostituita sul computer con una nuova scheda di sistema che contiene IBM embedded Security Subsystem e le chiavi crittografiche sono ancora valide sul disco fisso, è possibile ripristinare le chiavi crittografiche che sono state precedentemente associate al computer, crittografandole nuovamente con IBM embedded Security Subsystem sulla nuova scheda di sistema. L'operazione di ripristino delle chiavi viene eseguita*dopo* aver abilitato il nuovo chip e impostato una password di responsabile.

Per dettagli sull'abilitazione del sottosistema di sicurezza e l'impostazione di una password di responsabile, fare riferimento a "Abilitazione di IBM embedded Security Subsystem e impostazione della password del responsabile" a pagina 68.

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

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

Requisiti per il ripristino della chiave

Le operazioni di ripristino della chiave possono verificarsi correttamente solo se vengono rispettate le seguenti condizioni:

- Il nome del computer del sistema ripristinato deve corrispondere al nome del computer del sistema originale.
- Il sistema ripristinato deve poter accedere alla coppia di chiavi del responsabile CSS e alla ubicazione di archivio del sistema originale.
- Il sistema ripristinato deve disporre di IBM Security Subsystem ripristinato. (Utilizzare BIOS per abilitare e ed eliminare il chip.)
- E' necessario che il sistema ripristinato disponga dello stesso livello di IBM Security Subsystem del sistema originale (per esempio, TCG o diverso da TCG).

Scenari di ripristino

Sono possibile i tre scenari di ripristino di IBM Client Security riportati di seguito:

- **Sostituzione della scheda di sistema.** Se la scheda di sistema originale deve essere sostituita e se il disco fisso deve essere trasferito in un nuovo sistema, è necessario ripristinare IBM Security Subsystem con le chiavi che coincidono al sistema originale dall'archivio di chiavi.
- **Sostituzione del sistema completo.** Se il sistema originale va perso o viene sottratto, è necessario ripristinare IBM Security Subsystem e IBM Client Security Software dalle informazioni memorizzate nell'ubicazione di archivio.
- **Sostituzione del disco fisso.** Se il disco fisso non funziona sul sistema originale e viene posto un nuovo disco fisso, IBM Client Security Software deve essere ripristinato dall'ubicazione di archivio.

Sostituzione della scheda di sistema

Per sostituire la scheda di sistema da un computer che contiene IBM embedded Security Subsystem abilitato, completare la seguente procedura:

1. Fare clic sull'icona di **IBM Client Security Subsystem** nel pannello di controllo di Windows.
2. Immettere e confermare la password del responsabile; quindi fare clic su **OK**.
3. Immettere l'ubicazione di archivio e della chiave del responsabile del sistema originale nei campi appropriati; quindi fare clic su **OK**.
4. Fare clic su **OK**.
5. Fare clic su **Esci** per chiudere Administrator Utility.

   Il computer è ora completamente ripristinato. Riavviare il computer prima di continuare.

Sostituzione del sistema completo

Dopo aver installato IBM Client Security Software su un nuovo sistema, la creazione guidata di installazione di CSS viene eseguita automaticamente quando viene riavviato il sistema. Per iniziare la sostituzione del sistema completo e ripristinare le informazioni memorizzate nell'ubicazione di archivio, completare la seguente procedura:

1. Fare clic su **Avanti** nella pagina iniziale della creazione guidata di installazione di CSS.
2. Immettere e confermare la password del responsabile per il nuovo sistema e, quindi, fare clic su **Avanti**.
3. Selezionare il pallino **Utilizzare una chiave di sicurezza esistente** ed immettere l'ubicazione della chiave pubblica del responsabile archiviata e la chiave privata del responsabile del sistema originale nei campi appropriati.
4. Nella sezione sulle informazioni di sicurezza di backup, immettere un'ubicazione di archivio temporanea.

   Nota:

   a. Eliminare questa ubicazione dopo aver ripristinato completamente il sistema dall'archivio di sistema originale.
   b. Il promemoria delle informazioni viene sovrascritto durante il ripristino dell'archivio di sistema originale; quindi, utilizza i valori predefiniti.
5. Fare clic su **Avanti**.
6. Fare clic su **Avanti** nel pannello Proteggere le applicazioni con IBM Client Security.
7. Fare clic su **Avanti** nel pannello di autorizzazione degli utenti.
8. Fare clic su **Avanti** nel pannello Selezionare il livello di protezione del sistema.
9. Fare clic su **Fine** nel pannello Revisione delle impostazioni di protezione.
10. Fare clic su **OK**.
11. Continuare completando la procedura "Sostituzione del disco fisso".

Sostituzione del disco fisso

Per ripristinare IBM Client Security Software dall'ubicazione di archivio dopo la sostituzione del disco fisso , completare la seguente procedura:

1. Fare clic sull'icona di **IBM Client Security Subsystem** nel pannello di controllo di Windows.
2. Immettere la password del responsabile fornita nella creazione guidata di installazione di CSS e fare clic su **OK**.
3. Fare clic su **Configurazione chiave**.
4. Selezionare il pallino **Ripristina chiavi di IBM Security Subsystem da archivio** e fare clic su **Avanti**.
5. Immettere le ubicazioni di archivio e della chiave del responsabile del sistema originale nei campi appropriati e fare clic su **Avanti**.
6. Fare clic su **OK**.
7. Fare clic su **Fine** per tornare al pannello di configurazione principale.
8. Fare clic su **Esci** per chiudere Administrator Utility.

   Il computer è ora completamente ripristinato. Riavviare il computer prima di continuare.

Reimpostazione del conteggio numeri errori di autenticazione

Per reimpostare il contatore di errore di autenticazione per un utente, completare la seguente procedura del programma Administrator Utility:

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

   Viene visualizzata la finestra Reimposta conteggio di errori per l'utente.
3. Immettere l'ubicazione dell'archivio IBM Security Subsystem nel campo appropriato o fare clic su **Sfoglia** per selezionare l'ubicazione di archivio IBM Security Subsystem per l'utente selezionato.
4. Immettere il nome del file della chiave privata dell'archivio nel campo appropriato o fare clic su **Sfoglia** per selezionare il file della chiave privata dell'archivio per l'utente selezionato.
5. Fare clic su **OK**.

   Viene visualizzato un messaggio che notifica il completamento dell'operazione.
6. Fare clic su **OK**.

Modifica delle informazioni di impostazione di Tivoli Access Manager

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

Configurazione informazioni di impostazione di Tivoli Access Manager in un client

Una volta installato Tivoli Access Manager sul client locale, è possibile configurare le informazioni sull'installazione di Access Manager mediante il programma Administrator Utility. Per configurare le informazioni di impostazione di Tivoli Access Manager sul client IBM, Client Security Software utilizza un file di configurazione. Tale file di configurazione consente di collegare Tivoli Access Manager agli oggetti controllati dalla politica UVM.

Per configurare le informazioni sull'installazione di Tivoli Access Manager sul client, completare la seguente procedura di Administrator Utility:

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

   Viene visualizzato il pannello Configurazione della politica e applicazione UVM.
2. Selezionare la casella di controllo **Abilita sostituzione collegamento Windows**.
3. Fare clic sul pulsante **Politica applicativa**. Viene visualizzata la finestra Modifica configurazione della politica di Client Security.
4. 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. Inoltre, è possibile fare clic su **Sfoglia** per ricercare il file di configurazione.
5. Fare clic sul pulsante **Modifica politica** ed immettere la password del responsabile.
6. Selezionare le azioni che si desidera che Tivoli Access Manager controlli dal menu a discesa Azioni.

7. Selezionare la casella **Access Manager controlla l'oggetto selezionato** in modo da rendere visibile un segno di spunta nella casella.
8. Fare clic sul pulsante **Applica**. Le modifiche saranno rese effettive al successivo aggiornamento della cache. Se si desidera che le modifiche siano applicate adesso, fare clic sul pulsante **aggiorna cache locale** nel pannello Modifica configurazione della politica di Client Security.

Aggiornamento della cache locale

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

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

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

   Viene visualizzato il pannello Configurazione della politica e applicazione UVM.
2. Fare clic sul pulsante **Politica applicativa**. Viene visualizzata la finestra Modifica configurazione della politica di Client Security.
3. Nel campo Intervallo di aggiornamento della cache locale, procedere nel modo seguente:
   - Per aggiornare la cache locale, fare clic su **Aggiorna cache locale**.
   - Per impostare la velocità di aggiornamento, inserire il numero relativo al mese e al giorno nei campi forniti. Il valore per i mesi e i giorni rappresenta l'intervallo di tempo tra gli aggiornamenti pianificati.

Modifica della password del responsabile

E' necessario impostare la password del responsabile per abilitare IBM embedded Security Subsystem per un client. In seguito all'impostazione di una password del responsabile, l'accesso al programma Administrator Utility è protetto da questa password. Per una migliore sicurezza, è necessario cambiare la password del responsabile periodicamente. Una password che rimane invariata per un lungo periodo di tempo può anche essere più soggetta a parti esterne. Proteggere la password del responsabile per impedire agli utenti non autorizzati di modificare le impostazioni del programma Administrator Utility. Per ulteriori informazioni sulle regole della password del responsabile, fare riferimento a Appendice B, "Informazioni sulle password e i passphrase", a pagina 93.

Per modificare la password del responsabile, completare la seguente procedura del programma Administrator Utility:

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

   Viene visualizzato il pannello Modifica delle impostazioni di IBM Security Chip.
2. Fare clic su **Modifica password del chip**.

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

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

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

6. Fare clic su **OK**.

Visualizzazione delle informazioni su Client Security Software

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

- Il numero della versione del firmware utilizzato con Client Security Software
- Lo stato della crittografia di Embedded Security Chip
- La validità delle chiavi di cifratura hardware
- Lo stato di IBM Embedded Security Chip

Disabilitazione di IBM embedded Security Subsystem

Il programma Administrator Utility fornisce una modalità per disabilitare IBM embedded Security Subsystem. Poiché è necessario inserire la password del responsabile per avviare Administrator Utility e disabilitare il sottosistema di protezione, proteggere la password del responsabile per impedire ad utenti non autorizzati di disabilitare il sottosistema.

Importante: non eliminare IBM embedded Security Subsystem mentre è abilitata la protezione UVM. In caso contrario, verrà bloccato il sistema. Per disabilitare la protezione UVM, aprire la funzione Administrator Utility e deselezionare la casella **Abilita sostituzione collegamento Windows**. E' necessario riavviare l'elaboratore prima che la protezione UVM viene disabilitata per il collegamento del sistema.

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

1. Fare clic sul pulsante **Impostazioni chip**.
2. Fare clic sul pulsante **Disabilita chip** e seguire le istruzioni sullo schermo.
3. Se l'elaboratore ha abilitato Enhanced Security, è necessario inserire la password del responsabile BIOS, impostata nel programma Configuration/Setup Utility per disabilitare il chip.

Per utilizzare IBM embedded Security Subsystem e le chiavi cifrate dopo aver disabilitato il sottosistema, è necessario riabilitare il sottosistema di protezione.

Abilitazione di IBM embedded Security Subsystem e impostazione della password del responsabile

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

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

Per abilitare il sottosistema di protezione e impostare la password del responsabile, completare la seguente procedura:

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

   Viene visualizzato un messaggio che richiede l'abilitazione di IBM embedded Security Subsystem per il client IBM.
2. Fare clic su **Sì**.

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

   Poiché l'accesso al programma Administrator Utility è protetto dalla password del responsabile, viene visualizzato un messaggio che richiede l'immissione della password di administrator Chip.
5. Immettere una password del responsabile nel campo Nuova password e, quindi, inserirla di nuovo nel campo di conferma.
6. Fare clic su **OK**.

Abilitazione del supporto Entrust

IBM Embedded Security Chip opera con Client Security Software per potenziare le funzioni di protezione Entrust. L'abilitazione del supporto Entrust su un computer con Client Security Software trasferisce le funzioni di sicurezza del software Entrust su IBM Security Chip.

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

Per abilitare il supporto Entrust, completare la seguente procedura:

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

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

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

   Viene visualizzato il pannello IBM Client Security - Supporto Entrust con un messaggio che indica l'abilitazione del supporto Entrust.

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

Parte 4. Appendici

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

Per impostare 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 **Sicurezza del sistema**.
4. Selezionare **Password responsabile**.
5. Immettere la password e premere freccia giù sulla tastiera.
6. Immettere di nuovo la password e premere freccia giù.
7. Selezionare **Modifica password responsabile** e premere Invio; premere di nuovo Invio.
8. Premere **Esc** per uscire e salvare le impostazioni.

Dopo aver impostato la password del responsabile 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 sicurezza 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 l'elaboratore.
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 l'elaboratore.
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 l'elaboratore.
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 Security Feature** quindi premere Invio.
5. Selezionare **Yes**.
6. Premere Invio per confermare la scelta.
7. Premere F10 per salvare le modifiche ed uscire dal programma di utilità di inizializzazione.
8. Selezionare **Sì** e 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 e riavviare l'elaboratore.
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 Security Chip** e premere Invio.
5. Premere Invio e selezionare **Disabilitato**.
6. Premere Invio per confermare la scelta.
7. Premere Invio per continuare.
8. Premere F10 per salvare le modifiche ed uscire dal programma di utilità di inizializzazione.
9. Selezionare **Sì** e premere Invio. L'elaboratore viene riavviato.

Limitazioni note relative a CSS Versione 5.4

Le seguenti informazioni potrebbero essere utili per le funzioni di Client Security Software Versione 5.4.

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. Viene richiesto il passphrase, le impronte digitali, la smart card o altro (in base alle impostazioni 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.

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 5.4 e la versione precedente non supportano la funzione di 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.
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** per rimuoverla. Quindi, riavviare il computer ed 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**

Problema	Possibile soluzione
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**
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**
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
Un diverso sensore per le impronte digitali UVM non funziona correttamente	**Azione**
Il computer IBM ThinkPad non supporta l'interscambio di più sensori per le impronte digitali UVM.	Non commutare i modelli del sensore per le impronte digitali. Utilizzare lo stesso modello durante il funzionamento remoto come durante il funzionamento da una stazione per espansione.

Informazioni sulla risoluzione dei problemi della Microsoft

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

Problema	Possibile soluzione
Lo screen saver viene visualizzato solo sullo schermo locale	**Azione**
Durante l'utilizzo della funzione Windows Extended Desktop, lo screen saver di Client Security Software sarà visualizzato solo sullo schermo locale anche se l'accesso al sistema e la tastiera sono protetti.	Se vengono visualizzate le informazioni sensibili, ridurre le finestre del desktop esteso prima di richiamare lo screen saver Client Security.
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.
Messaggio di errore quando si firma un messaggio e-mail in modo digitale	**Azione**
Se il mittente di un messaggio e-mail prova a firmare un messaggio e-mail in modo digitale quando il mittente non ha già un certificato associato con il relativo account e-mail, viene visualizzato un messaggio di errore.	Utilizzare le impostazioni di sicurezza in Outlook Express per specificare un certificato da associare con l'account utente. Per ulteriori informazioni, consultare la documentazione fornita per Outlook Express.
Outlook Express (128 bit) cifratura i messaggi e-mail con l'algoritmo 3DES	**Azione**

Problema	Possibile soluzione
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.
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**

Problema	Possibile soluzione
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 Sicurezza, situata sulla barra degli strumenti. Viene visualizzata la finestra Info sicurezza. Fare clic su **Messenger** situato nel pannello sinistro e poi selezionare il **certificato di IBM embedded Security Chip** . Per ulteriori informazioni, fare riferimento alla documentazione fornita da Netscape.
Un messaggio e-mail viene restituito al client con un diverso algoritmo	**Azione**

Problema	Possibile soluzione
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 sicurezza di Netscape per eliminare il primo certificato, quindi riaprire il secondo certificato o richiedere al mittente di inviare un'altra e-mail firmata.
Impossibile esportare il certificato di IBM embedded Security 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**
L'agente di Netscape visualizza e chiude Netscape.	Disattivare l'agente di Netscape.

Problema	Possibile soluzione
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 sicurezza UVM indica che un utente fornisce il passphrase UVM o le impronte digitali prima di poter acquistato un certificato digitale. Se l'utente tenta di acquistare un certificato, la finestra di autenticazione richiede che la scansione delle impronte digitali o il passphrase UVM viene 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 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

L'interfaccia in Administrator Utility consente ai responsabili della sicurezza di controllare i criteri della password del responsabile tramite una semplice interfaccia. Tale interfaccia consente ad un responsabile di definire le seguenti regole per la password del responsabile:

Nota: L'impostazione predefinita per ciascun criterio di passphrase viene fornita di seguito tra parentesi. La password del responsabile non scade mai.

- 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.

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

Lunghezza
La password più essere costituita da un massimo di 256 caratteri.

Caratteri
La password può contenere qualunque combinazione di caratteri prodotti dalla tastiera, inclusi gli spazi ed i caratteri non alfanumerici.

Proprietà
La password del responsabile è diversa da una password da utilizzare per collegarsi ad un sistema operativo. La password del responsabile può essere utilizzata insieme ad altri dispositivi di autenticazione, come un sensore per le impronte digitali compatibile UVM.

Tentativi non corretti

Se si immette la password del responsabile in modo non corretto più volte durante una sessione, il computer sperimenta una serie di ritardi.

Regole per passphrase UVM

IBM Client Security Software consente ai responsabili della sicurezza di impostare le regole dei passphrase UVM per gli utenti. Per migliorare la sicurezza, 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 sicurezza di controllare i criteri passphrase tramite una semplice interfaccia. L'interfaccia relativa alla politica passphrase UVM consente al responsabile di stabilire le regole passphrase di seguito riportate:

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

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

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

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

  Ad esempio, quando è impostato a ″2″, non sono qui è una password non valida.
- stabilire se consentire che il passphrase inizi con un carattere numerico (no)

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

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

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

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

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

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

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

Ad esempio, per impostazione predefinita il passphrase scade dopo 184 giorni. E' necessario che il nuovo passphrase sia conforme alla politica dei passphrase stabilita.

- stabilire se il passphrase ha una scadenza (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 qualsiasi combinazione di caratteri prodotti dalla tastiera, includendo spazi e caratteri non alfanumerici.

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

Tentativi non corretti
Se si 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 che utilizzano National TPM

La seguente tabella mostra le impostazioni relative al ritardo per un sistema National TPM:

Tentativi	Ritardo al malfunzionamento successivo
7-13	ogni 4 secondi
14-20	ogni 8 secondi
21-27	ogni 16 secondi
28-34	ogni 32 secondi
35-41	ogni 64 secondi (ogni 1.07 minuti)
42-48	ogni 128 secondi (ogni 2.13 minuti)
49-55	ogni 256 secondi (ogni 4.27 minuti)
56-62	ogni 512 secondi (ogni 8.53 minuti)
63-69	ogni 1,024 secondi (ogni 17.07 minuti)
70-76	ogni 2,048 secondi (ogni 34.13 minuti)
77-83	ogni 68.26 minuti (ogni 1.14 ora)
84-90	ogni 136.52 minuti (ogni 2.28 ore)
91-97	ogni 273.04 minuti (ogni 4.55 ore)
98-104	ogni 546.08 minuti (ogni 9.1 ore)
105-111	ogni 1,092.16 minuti (ogni 18.2 ore)

Tentativi	Ritardo al malfunzionamento successivo
112-118	ogni 2,184.32 minuti (ogni 36.4 ore)

I sistemi National TPM non distinguono tra passphrase utente e password del responsabile. Qualunque autenticazione con IBM Embedded Security Chip è sottoposta alla stessa politica. Non esiste un timeout massimo. Ogni tentativo non riuscito fa scattare il ritardo sopra indicato. I ritardi non terminato al 118.mo tentativo; piuttosto continuano nel modo sopra illustrato all'infinito.

Conteggi errati su sistemi che utilizzano Atmel TPM

La tabella seguente mostra le impostazioni relative al ritardo per un sistema Atmel TPM:

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 TPM 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 TPM non ritardano per un intervallo di tempo superiore alle 4.7 ore.

Reimpostazione del passphrase

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

Reimpostazione del passphrase in remoto

Per reimpostare una password in remoto, 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 del passphrase

Il responsabile può collegarsi al sistema dell'utente che ha dimenticato il passphrase come responsabile, fornire la chiave privata del responsabile ad Administrator Utility, quindi modificare manualmente il passphrase 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 di controllo **Abilita sostituzione collegamento Windows** in Administrator Utility, il sistema torna al processo di collegamento 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. 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 E. 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.

Stampato in Italia