Soluzioni IBM® Client Security

Client Security Software Versione 5.4 - Guida per l'installazione

Soluzioni IBM® Client Security

Client Security Software Versione 5.4 - Guida per l'installazione

Prima edizione (Ottobre 2004)

Prima di utilizzare questo prodotto e le relative informazioni, consultare la sezione Appendice A, "Norme per l'esportazione di Client Security Software", a pagina 35 e l'Appendice C, "**Marchi e informazioni particolari**", a pagina 43.

Indice

Prefazione

Questa sezione fornisce informazioni relative all'uso di questa guida.

Informazioni sulla guida

Questa guida contiene informazioni relative all'installazione di IBM Client Security Software su un elaboratore di rete IBM, denominato anche client IBM che dispone di IBM embedded Security Subsystem. Inoltre, questa guida contiene istruzioni relative all'abilitazione di IBM embedded Security subsystem e all'impostazione della password del responsabile per il sottosistema di protezione.

La guida è organizzata nel modo seguente:

"Capitolo 1, "Introduzione"," contiene uno schema dei concetti di protezione di base, una panoramica dei componenti e delle applicazioni inclusi nel software ed una descrizione della funzioni PKI (Public Key Infrastructure).

"Capitolo 2, "Introduzione"," contiene prerequisiti sull'installazione hardware e software come pure istruzioni per il download del software.

"Capitolo 3, "Operazioni precedenti all'installazione del software"," contiene istruzioni sui prerequisiti per l'installazione di IBM Client Security Software.

"Capitolo 4, "Scaricamento, installazione e configurazione software"," contiene istruzioni per l'installazione, l'aggiornamento e la disinstallazione del software.

"Capitolo 5, "Risoluzione dei problemi"", contiene le informazioni utili per la risoluzione dei problemi che si possono verificare utilizzando le istruzioni fornite con questa guida.

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

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

"Appendice C, "**Marchi e informazioni particolari**"," contiene le informazioni legali e le informazioni sui marchi.

A chi si rivolge questa guida

Questa guida è rivolta ai responsabili di sistema o di rete che si occupano della sicurezza relativa ai computer client IBM. E' richiesta la conoscenza dei concetti relativi alla sicurezza, quali PKI (public key infrastructure) e la gestione dei certificati digitali in un ambiente di rete.

Modalità di utilizzo di questa guida

Utilizzare questa guida per installare ed impostare la sicurezza relativa ai computer client IBM. Questa guida si integra con *Guida per l'utente e per il responsabile di Client Security Software*.

E' possibile scaricare questa guida e la relativa documentazione di Client Security dal sito web IBM all'indirizzo http://www.pc.ibm.com/us/security/secdownload.html.

Riferimenti al manuale *Guida per l'utente e per il responsabile di Client Security Software*

Riferimenti al manuale *Guida per l'utente e per i responsabile di Client Security Software* saranno forniti in questo documento. La *Guida per l'utente e per il responsabile* contiene informazioni sull'utilizzo di UVM (User Verification Manager) e della politica UVM e le informazioni sull'utilizzo di Administrator Utility e User Configuration Utility.

Dopo aver installato il software, utilizzare le istruzioni nella *Guida per l'utente e per il responsabile* per per impostare e conservare la politica di sicurezza per ciascun client.

Ulteriori informazioni

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

Capitolo 1. Introduzione

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

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

IBM Embedded Security Subsystem

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

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

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.

Capitolo 2. Introduzione

Questa sezione contiene i requisiti relativi alla compatibilità hardware e software da utilizzare con IBM Client Security Software. Inoltre, vengono fornite informazioni per scaricare IBM Client Security Software.

Requisiti hardware

Prima di scaricare ed installare il software, verificare che l'hardware dell'elaboratore sia compatibile con IBM Client Security Software.

Le informazioni più recenti relative ai requisiti hardware e software sono disponibili sul sito web IBM all'indirizzo http://www.pc.ibm.com/us/security/index.html.

IBM embedded Security Subsystem

IBM embedded Security Subsystem è un microprocessore di cifratura integrato nella scheda di sistema di un client IBM. Questo componente essenziale del Client Security IBM trasferisce le funzioni di sicurezza dal software non protetto all'hardware protetto, incrementando radicalmente la sicurezza del client locale.

Solo gli elaboratori e le stazioni di lavoro IBM che dispongono di IBM embedded Security Subsystem supportano IBM Client Security Software. Se si tenta di scaricare e installare questo software su un elaboratore che non dispone di IBM embedded Security Subsystem, tale software non verrà installato o non sarà eseguito correttamente.

Modelli IBM supportati

Client Security Software è un prodotto su licenza e supporta vari computer notebook e desktop IBM. Per un elenco completo dei modelli supportati, visitare il sito http://www.pc.ibm.com/us/security/index.html.

Requisiti software

Prima di scaricare ed installare il software, assicurarsi che il software dell'elaboratore ed il sistema operativo siano compatibili con IBM Client Security Software.

Sistemi operativi

IBM Client Security Software richiede uno dei sistemi operativi di seguito riportati:

- Windows XP
- Windows 2000 Professional

Prodotti compatibili con UVM

IBM Client Security viene fornito con il software UVM (User Verification Manager) che consente di personalizzare l'autenticazione per l'elaboratore desktop di cui si dispone. Questo primo livello di controllo basato sulla politica implementa la protezione e l'efficacia della gestione delle password. UVM, compatibile con programmi di politica di sicurezza per imprese, consente di utilizzare prodotti compatibili con UVM, inclusi:

- **Dispositivi biometrici, quali lettori di impronte digitali**

  UVM fornisce una interfaccia plug-and-play per dispositivi biometrici. E' necessario installare IBM Client Security Software *prima* di installare un sensore compatibile con UVM.

  Per utilizzare un sensore compatibile con UVM già installato su un client IBM, è necessario disinstallare il sensore compatibile con UVM, installare IBM Client Security Software, quindi reinstallare il suddetto sensore.
- **Tivoli Access Manager versione 5.1**

  Il software UVM semplifica e potenzia la gestione della politica integrandosi con una soluzione di controllo accessi centralizzata basata sulla politica, quale Tivoli Access Manager.

  Il software UVM potenzia la politica di sicurezza localmente se il sistema è in rete (desktop) o indipendente (standalone), creando in questo modo un modello di politica singolo e unificato.
- **Lotus Notes versione 4.5 o successive**

  UVM funziona con IBM Client Security Software per implementare la protezione del collegamento Lotus Notes (Lotus Notes versione 4.5 o successiva).
- **Entrust Desktop Solutions 5.1, 6.0 o 6.1**

  Entrust Desktop Solutions supporta potenziamenti alle funzioni di sicurezza per Internet, in modo che processi critici dell'impresa possano essere trasferiti su Internet. Entrust Entelligence fornisce un singolo livello di sicurezza che include un insieme completo delle esigenze di sicurezza potenziate dell'impresa, incluse l'identificazione, la riservatezza, la verifica e la gestione della sicurezza.
- **RSA SecurID Software Token**

  RSA SecurID Software Token abilita lo stesso record principale che viene utilizzato per i token hardware RSA tradizionali da integrare sulle piattaforme utente esistenti. Di conseguenza, gli utenti possono effettuare l'autenticazione per le risorse protette mediante l'accesso al software integrato invece di utilizzare dispositivi di autenticazione.
- **Programma di utilità per la lettura delle smart card Gemplus GemPC400**

  Il programma di utilità per la lettura delle smart card Gemplus GemPC400 consente alla politica di sicurezza di includere l'autenticazione mediante le smart card, aggiungendo un ulteriore livello di protezione a quella standard fornita dai passphrase.

Browser web

IBM Client Security Software supporta i browser web di seguito riportati per la richiesta dei certificati digitali:

- Internet Explorer 5.0 o successive
- Netscape 4.8 e Netscape 7.1

Informazioni sul livello di cifratura del browser

Se il supporto per la cifratura rigida è installato, utilizzare la versione a 128 bit del browser web. Per verificare il livello di codifica del browser web, fare riferimento alla guida fornita con il browser.

Servizi di cifratura

IBM Client Security Software supporta i servizi di cifratura di seguito riportati:

- **Microsoft CryptoAPI:** CryptoAPI è il servizio di cifratura predefinito per i sistemi operativi Microsoft e le applicazioni. Con il supporto integrato

CryptoAPI, IBM Client Security Software consente di effettuare operazioni di cifratura di IBM embedded Security Subsystem per la creazione di certificati digitali per le applicazioni Microsoft.

- **PKCS#11:** PKCS#11 è la cifratura standard per Netscape, Entrust, RSA e altri prodotti. Dopo aver installato il modulo PKCS#11 di IBM embedded Security Subsystem, è possibile utilizzare IBM embedded Security Subsystem per generare certificati digitali per Netscape, Entrust, RSA e altre applicazioni che utilizzano PKCS#11.

Applicazioni e-mail

IBM Client Security Software supporta i tipi di applicazione di seguito riportati che utilizzano e-mail protette:

- Le applicazioni e-mail che utilizzano Microsoft CryptoAPI per operazioni di cifratura, quali Outlook Express e Outlook (se utilizzate con una versione supportata di Internet Explorer)
- Le applicazioni e-mail che utilizzano PKCS#11 (Public Key Cryptographic Standard #11) per operazioni di cifratura, quali Netscape Messenger (se utilizzato con una versione supportata di Netscape)
- Supporto Lotus Notes tramite protezione autenticazione collegamento avanzata

Capitolo 3. Operazioni precedenti all'installazione del software

Questa sezione contiene le istruzioni sui prerequisiti necessari per eseguire il programma di installazione e la configurazione di IBM Client Security Software su client IBM.

Tutti i file richiesti per l'installazione di Client Security Software si trovano sul sito web IBM all'indirizzo http://www.pc.ibm.com/us/security/index.html. Sul sito web è possibile trovare informazioni che consentono di verificare che il sistema disponga di IBM embedded Security Subsystem e di selezionare l'offerta appropriata di IBM Client Security per il sistema di cui si dispone.

Operazioni precedenti all'installazione del software

Il programma di installazione consente di installare IBM Client Security Software su client IBM ed abilita IBM embedded Security Subsystem, tuttavia le specifiche di installazione variano in base a determinati fattori.

E' necessario che gli utenti si colleghino con i diritti di responsabile per installare IBM.

Installazione per utilizzare Tivoli Access Manager

Se si desidera utilizzare Tivoli Access Manager per controllare i requisiti di autenticazione dell'elaboratore, è necessario installare alcuni componenti di Tivoli Access Manager *prima* di installare IBM Client Security Software. Per ulteriori dettagli, fare riferimento alla guida *Utilizzo di Client Security con Tivoli Access Manager*.

Considerazioni sulle funzioni di avvio

Due funzioni di avvio IBM potrebbero condizionare il modo in cui si abilita IBM embedded Security Subsystem e si generano le chiavi di cifratura. Tali funzioni sono costituite dalla password del responsabile BIOS ed Enhanced Security ed è possibile accedervi da Configuration/Setup Utility di un computer IBM. IBM Client Security Software dispone di una password del responsabile a parte. Per evitare confusione, la password del responsabile impostata in Configuration/Setup Utility viene denominata *Password del responsabile di BIOS* nei manuali relativi a Client Security Software.

Password del responsabile di BIOS

La password del responsabile di BIOS impedisce agli utenti non autorizzati da modifica delle impostazioni di configurazione di un elaboratore IBM. LA password viene impostata utilizzando il programma Configuration/Setup Utility su elaboratori NetVista o ThinkCentre oppure il programma IBM BIOS Setup Utility su elaboratori ThinkPad. E' possibile accedere al programma appropriato premendo Invio o F1 durante la sequenza di avvio del computer. Questa password è denominata *password del responsabile* in the ThinkCentre Configuration/Setup Utility e *passwprd supervisore* in ThinkPad BIOS Setup Utility.

Enhanced Security

Enhanced Security fornisce un'ulteriore protezione per la password del responsabile di BIOS, oltre alle impostazioni della sequenza di avvio. E' possibile determinare se Enhanced Security viene abilitato o disabilitato utilizzando il

programma Configuration/Setup Utility, cui è possibile accedere premendo il tasto F1 durante la sequenza di avvio dell'elaboratore.

Per ulteriori informazioni relative alle password e a Enhanced Security, fare riferimento alla documentazione fornita con il computer.

Enhanced Security su modelli NetVista 6059, 6569, 6579, 6649 e tutti i modelli NetVista Q1x: Se è stata impostata la password del responsabile sui modelli NetVista (6059, 6569, 6579, 6649, 6646 e tutti i modelli Q1x), è necessario aprire Administrator Utility per abilitare IBM embedded Security Subsystem e generare le chiavi di cifratura.

Se Enhanced Security è abilitato su questi modelli, è necessario utilizzare Administrator Utility per abilitare IBM embedded Security Subsystem e generare le chiavi di cifratura *dopo* aver installato IBM Client Security Software. Se il programma di installazione rileva che Enhanced Security è abilitato, verrà notificato al termine del processo di installazione. Riavviare l'elaboratore, quindi aprire Administrator Utility per abilitare IBM embedded Security Subsystem e generare le chiavi di cifratura.

Enhanced Security su tutti gli altri modelli NetVista (diversi dai modelli 6059, 6569, 6579, 6649 e tutti i modelli NetVista Q1x): Se è stata impostata la password del responsabile su modelli NetVista, *non* viene richiesto di immettere la password del responsabile durante il processo di installazione.

Quando Enhanced Security viene abilitato sui modelli NetVista, è possibile utilizzare il programma di installazione per installare il software, ma è necessario utilizzare Configuration/Setup Utility per abilitare IBM embedded Security Subsystem. *Dopo* aver abilitato IBM embedded Security Subsystem, è possibile utilizzare Administrator Utility per generare le chiavi di cifratura.

Informazioni sull'aggiornamento di BIOS

Prima di installare il software, è necessario scaricare l'ultimo codice BIOS (basic input/output system) per il computer. Per determinare il livello BIOS utilizzato dal computer, riavviare la macchina e premere F1 per avviare il programma di utilità Configuration/Setup. Se si apre il menu principale per Configuration/Setup, selezionare Product Data per visualizzare le informazioni sul codice BIOS. Il livello del codice BIOS viene anche definito come livello di revisione EEPROM.

Per eseguire IBM Client Security Software 2.1 o versione successiva sui modelli NetVista (6059, 6569, 6579, 6649), è necessario utilizzare BIOS livello xxxx22axx o successivo; per eseguire IBM Client Security Software 2.1 o versione successiva sui modelli NetVista (6790, 6792, 6274, 2283), è necessario utilizzare BIOS livello xxxx20axx o successivo. Per ulteriori informazioni, consultare il file README incluso nel download del software.

Per ottenere gli aggiornamenti del codice BIOS per l'elaboratore di cui si dispone, visitare il sito web IBM all'indirizzo http://www.pc.ibm.com/support, immettere `bios` nel campo di ricerca, quindi selezionare download dall'elenco a discesa e premere Invio. Un elenco di aggiornamenti del codice BIOS vengono visualizzati. Fare clic sul numero di modello appropriato, quindi seguire le istruzioni visualizzate.

Utilizzo della coppia di chiavi del responsabile per archiviare le chiavi

La coppia di chiavi di archivio è semplicemente una copia della coppia di chiavi del responsabile memorizzata su un supporto esterno per il ripristino. Poiché Administrator Utility viene utilizzato per creare la coppia di chiavi di archivio, è necessario installare IBM Client Security Software su un client IBM prima di creare la coppia di chiavi del responsabile.

Capitolo 4. Scaricamento, installazione e configurazione software

Questa sezione contiene le istruzioni per lo scaricamento, l'installazione e la configurazione di IBM Client Security Software su client IBM. Questa sezione contiene inoltre, le istruzioni per la disinstallazione del software. Accertarsi di installare il programma IBM Client Security Software prima di installare qualsiasi programma di utilità che potenzia la funzionalità del programma Client Security.

Importante: se si aggiorna una versione precedente a IBM Client Security Software 5.0, è *necessario* decifrare tutti i file cifrati *prima* di installare Client Security Software 5.1 o versione successiva. IBM Client Security Software 5.1 o versione successiva non è in grado di decifrare i file cifrati utilizzando le versioni precedenti a Client Security Software 5.0 a causa delle modifiche effettuate nell'implementazione della cifratura dei file.

Download del software

Tutti i file richiesti per l'installazione di Client Security Software si trovano sul sito web IBM all'indirizzo http://www.pc.ibm.com/us/security/index.html. Sul sito web è possibile trovare informazioni che consentono di verificare che il sistema disponga di IBM Embedded Security Subsystem e di selezionare l'offerta appropriata di IBM Client Security per il sistema di cui si dispone.

Per scaricare i file appropriati per il sistema in uso, completare la seguente procedura:

1. Utilizzando un browser, visitare il sito web IBM all'indirizzo http://www.pc.ibm.com/us/security/index.html.
2. Nella casella Risorse, fare clic su **Supporto e download**.
3. Nella sezione della pagina web Embedded Security Subsystem e IBM Client Security Software, fare clic su **Download software**.
4. In Seleziona una casella di sistema, fare clic su **Detect my system & continue** o immettere il numero di sette cifre relativo al modello ed al tipo di macchina nel campo appropriato.
5. Immettere il proprio indirizzo e-mail nel campo appropriato e selezionare il proprio Paese/Regione dal menu a discesa.
6. Selezionare la casella di controllo appropriata considerando se si desidera ricevere informazioni sulle offerte.
7. Riesaminare l'Accordo di licenza facendo clic su **Visualizza licenza**; quindi fare clic su **Accetta licenza**.

   Viene visualizzata la pagina da cui è possibile scaricare IBM Client Security.
8. Trovare il collegamento per Client Security Software 5.4 e fare clic su **Scarica ora**.

   Nota: Consultare il file `css54readme.html` per aggiornamenti specifici ed informazioni sulle limitazioni.
9. Fare clic su **Salva** per salvare una copia del file eseguibile d'installazione sul disco fisso.

10. Specificare Salva come ubicazione e fare clic su **Salva**. Per iniziare l'installazione del software, fare clic su **Apri** una volta completato lo scaricamento o fare due volta clic con il tastino destro sull'icona del file eseguibile

    Viene visualizzata la finestra Benvenuti nella procedura guidata InstallShield per IBM Client Security Software.

Installazione software

Per installare i file appropriati per il sistema, completare la procedura seguente:

1. Fare due volta clic sul file eseguibile.

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

   Verrà visualizzato l'accordo di licenza di IBM Client Security Software.
3. Leggere i termini del contratto di licenza, selezionare il pulsante di opzione **Accetto i termini del contratto di licenza** e quindi fare clic su **Avanti**.

   Verrà visualizzato il pannello Selezione prodotti.
4. Selezionare uno dei seguenti pulsanti di opzione e fare clic su **Avanti**.
   - **IBM Client Security Software e IBM Password Manager.** Questa selezione installerà o aggiornerà IBM Client Security Software, IBM Password Manager e tutti driver dei dispositivi necessari.
   - **Solo IBM Client Security Software.** Questa selezione installerà o aggiornerà IBM Client Security Software e tutti i driver dei dispositivi necessari.

   Viene visualizzato il pannello Cartella di destinazione.
5. Fare clic su **Avanti** per accettare l'ubicazione di installazione predefinita o fare clic su **Modifica** per ricercare la cartella di destinazione desiderata.

   Verrà visualizzato il pannello di installazione del programma.
6. Fare clic su **Installa** per iniziare l'installazione o fare clic su **Indietro** per rivedere o modificare le impostazioni di installazione.

   Una barra di stato visualizzerà il progresso dell'installazione e verrà quindi visualizzato il pannello di completamento della procedura guidata InstallShield.
7. Fare clic su **Fine** per uscire dalla procedura guidata.

E' necessario riavviare il computer perché le modifiche apportate all'istallazione siano valide.

Selezione di un'opzione di configurazione

Il primo pannello della procedura guidata di IBM Client Security Setup consente di selezionare un'opzione di configurazione. E' importante selezionare l'opzione di configurazione appropriata. Prima di selezionare un'opzione di configurazione, verificare attentamente le informazioni di seguito riportate. Per gli utenti non esperti, si consiglia di selezionare l'opzione *configurazione tipica*.

Configurazione tipica

Quando si seleziona la configurazione tipica di IBM Client Security Software utilizzando la procedura guidata di Client Security Setup, si configurano le seguenti funzioni di Client Security:

- IBM Password Manager (se selezionato all'installazione)
- Cifratura file con il tastino destro del mouse

- Autenticazione con passphrase e impronte digitali
- Supporto firma digitale

L'utilizzo dell'opzione consigliata *configurazione tipica* nella procedura guidata di Client Security Setup rende semplice il processo di configurazione. Tuttavia, alcune funzioni avanzate di Client Security Software vengono disabilitate quando viene selezionata questa configurazione, rendendo non disponibili alcune funzioni di CSS.

Impostazioni predefinite della configurazione tipica

Le impostazioni predefinite cifrate della configurazione tipica sono:

- **Ubicazione archivio:** C:\documents and settings\all users\application data\ibm\security\archive
- **Ubicazione coppia chiavi del responsabile:** C:\documents and settings\all users\application data\ibm\security\keys

  La chiave privata del responsabile non viene divisa e viene cifrata con il passphrase del responsabile di CSS.

Le altre impostazioni includono quanto segue:

- Il supporto di IBM Password Manager è abilitato
- La politica di protezione è media: ciascun metodo di autenticazione disponibile verrà richiesto solo la prima volta che verrà utilizzata una funzione di CSS.
- L'autenticazione passphrase viene sempre richiesta.
- L'autenticazione mediante le impronte digitali viene richiesta quando è rilevato un lettore per le impronte digitali.
- Il passphrase UVM dell'utente che ha impostato CSS è anche la *password del responsabile* di CSS. Se si modifica il passphrase UVM verrà modificata anche la password del responsabile CSS. Il passphrase del responsabile di CSS non scade mai.

Limitazioni componente di configurazione tipica

Alcune funzioni di Client Security Software abilitate in seguito alla configurazione avanzata vengono disabilitate quando viene selezionata la configurazione tipica. Queste funzioni non possono essere utilizzate se si seleziona la configurazione tipica di CSS. Per abilitare queste funzioni, è necessario convertire la configurazione tipica in avanzata. Di seguito sono riportate le differenze funzionali in seguito ad una configurazione tipica:

- **Administrator Utility**

  Le azioni seguenti non sono consentite in una configurazione tipica:

  – Reimpostazione utente
  – Rimozione utente
  – Modifica della password del responsabile utilizzando il pulsante Impostazioni chip
  – Funzioni relative alla configurazione delle chiavi

  Se un utente tenta di effettuare una delle operazioni di seguito riportate, verrà richiesto di convertire la configurazione tipica di CSS in avanzata. Il processo di conversione decifra la chiave privata del responsabile e sposta la coppia di chiavi del responsabile in una posizione specificata dall'utente.
- **Administrator Console**

  Le seguenti differenze di utilizzo di applicano in una configurazione tipica:

– La directory di archivio, l'ubicazione della chiave privata e quella della chiave pubblica vengono cifrate ed è impossibile modificarle. L'archivio può essere solo modificato sul computer locale.
– L'opzione per configurare il roaming delle credenziali non è disponibile per la configurazione tipica. Se si seleziona la configurazione tipica, e si desidera impostare una rete di roaming delle credenziali, è necessario prima convertire le configurazione tipica in una configurazione avanzata.
– Non è possibile ignorare un passphrase UVM per il responsabile di CSS.

• **User Configuration Utility**

Le seguenti differenze di utilizzo si applicano in una configurazione tipica:

– Il passphrase UVM dell'utente che ha configurato CSS è anche la password del responsabile. Se si modifica il passphrase UVM, verrà modificata anche la password del responsabile.
– L'utente responsabile di CSS non può essere reimpostato.
– L'opzione per configurare il roaming delle credenziali non è disponibile per la configurazione tipica.

Conversione di una configurazione tipica in una configurazione avanzata

Per convertire una configurazione tipica di Client Security Software in una configurazione avanzata, completare la procedura qui indicata:

1. Avviare Administrator Utility.
2. Immettere la password del responsabile di CSS.
3. Fare clic sul pulsante **Configurazioni chiavi**.
4. Per continuare, fare clic su **OK**.
5. Immettere la posizione in cui si desidera memorizzare la coppia di chiavi del responsabile decifrate. Non memorizzare la coppia di chiavi decifrate sul disco fisso locale. Il processo di conversione è ora completo.
6. Modificare la posizione di archivio. Non memorizzare l'archivio sul disco fisso locale.

Una volta convertito Client Security Software in una configurazione avanzata, non è possibile convertirlo nuovamente in una configurazione tipica.

Configurazione avanzata

La *configurazione avanzata* di IBM Client Security Software configura le seguenti funzioni *aggiuntive* di Client Security:

• **Protezione collegamento UVM**
• **Selezione posizione di memorizzazione della chiave**
• **Supporto applicazione:** Entrust, File and Folder Encryption, Lotus Notes

Utilizzo della procedura guidata di IBM Client Security Setup

La procedura guidata di IBM Client Security Setup fornisce un'interfaccia di supporto all'installazione di Client Security Software ed abilita l'IBM Embedded Security Chip. La procedura guidata all'installazione di IBM Client Security guida gli utenti tramite le attività necessarie implicate nell'installazione di una politica di sicurezza su un client IBM.

I passi generali indicati dalla procedura guidata IBM Client Security Setup sono i seguenti. I passaggi specifici si diversificano a seconda dell'opzione di configurazione selezionata.

- **Impostare una password di Security Administrator**

  La password del responsabile della protezione, denominata in questo manuale password del responsabile, è utilizzata per controllare l'accesso a IBM Client Security Administrator Utility, che consente di modificare le impostazioni di sicurezza per il relativo elaboratore.

- **Creazione chiavi chiavi di protezione del responsabile**

  Le chiavi di protezione del responsabile sono costituite da una serie di chiavi digitali memorizzate in un file dell'elaboratore. Tali file sono anche denominati come chiavi del responsabile, coppia di chiavi del responsabile o coppia di chiavi di archivio. Si consiglia di salvare queste chiavi di protezione importantissime su un supporto o un'unità rimovibile. Quando viene effettuata una modifica alla politica di protezione in Administrator Utility, viene richiesta una chiave del responsabile per dimostrare che tale modifica della politica è autorizzata.

  Inoltre, la copia di backup delle informazioni di protezione viene salvata nel caso in cui è necessario sostituire la scheda di sistema o l'unità disco fisso dell'elaboratore. Memorizzare tali informazioni di backup nel sistema locale.

- **Protezione delle applicazioni con IBM Client Security**

  Selezionare le applicazioni che si desidera proteggere con IBM Client Security. E' possibile che alcune opzioni non siano disponibili se non devono essere installate ulteriori applicazioni necessarie.

- **Autorizzazione utenti**

  E' necessario che gli utenti siano autorizzati prima di poter accedere all'elaboratore. Quando si autorizza un utente, è necessario specificare tale passphrase dell'utente. Gli utenti non autorizzati non possono utilizzare l'elaboratore.

- **Selezionare un livello di protezione del sistema**

  La selezione di un livello di sicurezza del sistema consente di stabilire una politica di sicurezza di base in modo facile e rapido. E' possibile definire una politica di sicurezza personalizzata nel programma IBM Client Security Administrator Utility successivamente.

Utilizzo della procedura guidata all'installazione per completare una configurazione tipica

Per utilizzare la procedura guidata d'installazione di IBM Client Security per completare una configurazione tipica, completare la procedura di seguito indicata:

1. Fare clic su **Start > Programmi > Access IBM > IBM Client Security Software > IBM Client Security Setup Wizard**.

   Il pannello di benvenuto della procedura guidata per l'installazione di IBM Client Security consente di selezionare un'opzione di configurazione.

2. Selezionare i pulsanti d'opzione della configurazione tipica (consigliata) e fare clic su **Avanti**.

   Questa selezione abilita IBM Password Manager e richiede l'immissione solo di pochi parametri. Quando si seleziona la configurazione tipica, CSS memorizza le informazioni di backup e le chiavi di sicurezza sul disco fisso. Per gli utenti non esperti, si consiglia di utilizzare la configurazione tipica. Questa è l'impostazione predefinita.

   Viene visualizzato il pannello Immissione passphrase.

3. Completare le seguenti attività:
   a. Immettere un passphrase nel campo appropriato. Se necessario, fare clic sul pulsante **Visualizza requisiti passphrase** per un supporto nel definire un passphrase valido.

      Nota: All'installazione iniziale o dopo l'eliminazione di IBM Embedded Security Chip, sarà richiesta la conferma del passphrase nel campo relativo. Inoltre, è possibile che sia fornita la password del responsabile, se valida.
   b. Immettere una parola o una frase nel campo di suggerimento passphrase.
   c. Fare clic su **Avanti**.

   Se viene rilevato sul computer un lettore di impronte digitali, verrà visualizzato il pannello di memorizzazione impronte digitali. La casella **Sì, memorizza ora le impronte digitali** viene selezionata per impostazione predefinita.
4. Effettuare una delle seguenti operazioni:
   - Aggiornare la casella di controllo **Sì, memorizza ora le impronte digitali** quindi fare clic su **Avanti**.
   - Fare clic su **Avanti** e seguire le istruzioni sullo schermo per iniziare la registrazione delle impronte digitali.

   Viene visualizzato il pannello di autorizzazione utenti aggiuntivi.
5. Effettuare una delle seguenti operazioni:
   - Selezionare la casella di controllo **Seleziona utenti aggiuntivi da autorizzare ora (Facoltativo)** quindi fare clic su **Avanti**.
   - Fare clic su **Ignora** per ignorare questa attività.

   Viene visualizzato il pannello di riepilogo delle funzioni e delle impostazioni di protezione.
6. Fare clic su **Fine** per implementare le impostazioni di protezione selezionate. Questa operazione potrebbe richiedere alcuni minuti. Viene visualizzato un messaggio che indica che il computer adesso è protetto da IBM Client Security.
7. Fare clic su **OK**.

Utilizzo della procedura guidata d'installazione per completare una configurazione avanzata

Per utilizzare la procedura guidata d'installazione di IBM Client Security per completare una configurazione tipica, completare la procedura di seguito indicata:

1. Fare clic su **Start > Programmi > Access IBM > IBM Client Security Software > IBM Client Security Setup Wizard**.

   Il pannello di benvenuto della procedura guidata per l'installazione di IBM Client Security consente di selezionare un'opzione di configurazione.
2. Selezionare il pulsante di opzione **Configurazione avanzata** e fare clic su **Avanti**.

   Questa seleziona richiede di specificare le informazioni sulla configurazione, come ad esempio l'ubicazione di memorizzazione delle chiavi ed un livello di protezione e consente di abilitare la protezione di collegamento CSS, Lotus Notes e IBM Password Manager.

   Il pannello Impostare la password di Security Administrator viene visualizzato.
3. Immettere la password di Security Administrator nel campo Inserisci password del responsabile e fare clic su **Avanti**.

Nota: all'installazione iniziale o in seguito all'eliminazione di IBM embedded Security Chip, sarà richiesta la conferma di Security Administrator Password nell'area Conferma password del responsabile. Inoltre, è possibile che sia fornita la password del responsabile, se valida.

Viene visualizzato il pannello Creare le chiavi di Administrator Security.

4. Effettuare una delle seguenti operazioni:
   - **Creare le nuove chiavi di sicurezza**

     Per creare le nuove chiavi di sicurezza, utilizzare la seguente procedura:

     a. Fare clic sul pulsante di opzione **Crea nuove chiavi**.
     b. Specificare dove si desidera salvare le chiavi di protezione del responsabile immettendo il percorso nel campo fornito oppure facendo clic su **Sfoglia** e selezionando la cartella appropriata.
     c. Se si desidera dividere la chiave di sicurezza per aumentare la protezione, fare clic sulla casella di controllo **Dividi chiave di archivio per aumentare la protezione** in modo da visualizzare un contrassegno nella casella e, quindi, utilizzare le frecce per selezionare il numero desiderato nella casella di scorrimento **Numero di suddivisioni**.
   - **Utilizzare una chiave di sicurezza esistente**

     Per utilizzare una chiave di sicurezza esistente, utilizzare la seguente procedura:

     a. Fare clic sul pallino **Utilizza una chiave di sicurezza esistente**.
     b. Specificare la posizione della Chiave pubblica immettendo il nome del percorso nel campo fornito oppure facendo clic su **Sfoglia** e selezionando la cartella appropriata.
     c. Specificare la posizione della Chiave privata immettendo il nome del percorso nel campo fornito oppure facendo clic su **Sfoglia** e selezionando la cartella appropriata.
5. Specificare l'ubicazione di archivio delle chiavi in cui si desidera salvare le copie di backup delle informazioni di sicurezza immettendo il nome del percorso nel campo fornito oppure facendo clic su **Sfoglia** e selezionando la cartella selezionata.
6. Fare clic su **Avanti**.

   Viene visualizzato il pannello Proteggere le applicazioni con IBM Client Security.
7. Abilitare la protezione IBM Client Security selezionando le caselle appropriate in modo da rendere visibile un segno di spunta in ciascuna casella selezionata e facendo clic su **Avanti**. Di seguito sono riportate le selezioni disponibili di Client Security:
   - **Proteggere l'accesso al sistema sostituendo il normale collegamento Windows con il collegamento protetto di Client Security**

     Selezionare questa casella per sostituire il collegamento normale di Windows con il collegamento protetto di Client Security. Questa procedura implementa la protezione del sistema e consente il collegamento solo dopo l'autenticazione con IBM Embedded Security Chip e dispositivi opzionali, come ad esempio i dispositivi di lettura per le impronte digitali o le smart card.
   - **Abilita la cifratura della cartella e del file**

     Selezionare questa casella se si desidera proteggere i file sul disco fisso con IBM Embedded Security Chip. (E' richiesto lo scaricamento di IBM Client Security File e Folder Encryption).
   - **Abilita il supporto IBM Client Security Password Manager**

Selezionare questa casella se si desidera utilizzare IBM Password Manager per memorizzare in modo appropriato e sicuro le password di collegamento al sito web e alle applicazioni.

- **Sostituisci il collegamento Lotus Notes con il Collegamento di IBM Client Security**

  Selezionare questa casella se si desidera che il programma Client Security autentichi gli utenti Lotus Notes mediante IBM embedded Security Chip.

- **Abilita supporto Entrust**

  Selezionare questa casella se si desidera abilitare l'integrazione con i prodotti software di protezione Entrust.

- **Protezione di Microsoft Internet Explorer**

  Questa protezione consente di rendere più sicure le comunicazioni via e-mail e navigare sul web con Microsoft Internet Explorer (è richiesto un certificato digitale). Per impostazione predefinita è abilitato il supporto per Microsoft Internet Explorer.

Una volta selezionate le caselle appropriate, viene visualizzata la finestra Autorizzazione degli utenti.

8. Completare il pannello Utenti autorizzati completando una delle seguenti procedure:
   - Per autorizzare gli utenti ad eseguire le funzioni di IBM Client Security:
     a. Selezionare un utente nell'area Utenti non autorizzati.
     b. Fare clic su **Utenti autorizzati**.
     c. Immettere e confermare il passphrase di IBM Client Security nel campo fornito, quindi fare clic su **Avanti**.

        Viene visualizzato il pannello relativo alla scadenza del passphrase UVM.
     d. Impostare la scadenza del passphrase utente, quindi fare clic su **Fine**.
     e. Fare clic su **Avanti**.
   - Per annullare l'autorizzazione degli utente dall'esecuzione delle funzioni IBM Client Security, procedere nel modo seguente:
     a. Selezionare un utente nell'area Utenti non autorizzati.
     b. Fare clic su **Utenti non autorizzati**.

        Viene visualizzato il messaggio, "Si è sicuri di non voler autorizzare ?"
     c. Fare clic su **Sì**.
     d. Fare clic su **Avanti**.

   Viene visualizzata la finestra Seleziona livello di protezione del sistema.
9. Selezionare i requisiti di autenticazione desiderati facendo clic sulle caselle di controllo appropriate. E' possibile selezionare più requisiti di autenticazione.
   - La casella di controllo **Utilizza passphrase UVM** è l'impostazione predefinita.
   - E' necessario installare i driver di periferica per la lettura delle impronte digitali e per la smart card prima di avviare la procedura guidata all'installazione di IBM Client Security, affinché tali periferiche siano disponibili al momento della procedura guidata all'installazione.
   - Selezionare un livello di sicurezza del sistema trascinando il selettore sul livello di sicurezza desiderato e fare clic su **Avanti**.

     Nota: E' possibile definire una politica di protezione personalizzata utilizzando Policy Editor in Administrator Utility.

Viene visualizzato il pannello Impostazione completata - Rivedere le impostazioni di protezione.

10. Controllare le impostazioni della sicurezza ed eseguire una delle seguenti operazioni:
    - Per accettare le impostazioni, fare clic su **Fine**.
    - Per modificare le impostazioni, fare clic su **Indietro**, apportare le modifiche appropriate; quindi ritornare a questa finestra e fare clic su **Fine**.

    IBM Client Security Software configura le impostazioni mediante IBM Embedded Security Chip. Viene visualizzato un messaggio che conferma la protezione dell'elaboratore da parte IBM Client Security.
11. Fare clic su **OK**.

Abilitazione di IBM Security Subsystem

E' necessario abilitare IBM Security Subsystem prima di utilizzare Client Security Software. Se il chip non è stato abilitato, è possibile abilitarlo utilizzando Administrator Utility. Le istruzioni sull'utilizzo della creazione guidata all'installazione sono contenute nella sezione precedente.

Per abilitare IBM Security Subsystem utilizzando Administrator Utility, completare la procedura di seguito riportata:

1. Fare clic su **Start > Impostazioni > Pannello di controllo > IBM Embedded Security Subsystem**.

   Viene visualizzato un pannello con un messaggio indicate che IBM Security Subsystem non è stato abilitato e che richiede se si desidera abilitarlo.
2. Fare clic su **Sì**.

   Viene visualizzato un messaggio indicante che se è stata abilitata una password per il supervisore o una password per il responsabile del BIOS, è necessario disabilitarla in BIOS Setup Utility prima di continuare.
3. Effettuare una delle seguenti operazioni:
   - Se è stata abilitata una password del responsabile, fare clic su **Annulla**, disabilitare la password del responsabile poi completare questa procedura.
   - Se non è stata abilitata una password del responsabile, fare clic su **OK** per continuare.
4. Chiudere tutte le applicazioni attive e fare clic su **OK** per riavviare l'elaboratore.
5. Una volta riavviato il sistema, fare clic su **Start > Impostazioni > Pannello di controllo > IBM Embedded Security Subsystem** per aprire Administrator Utility.

   Viene visualizzato un messaggio indicante che IBM Security Subsystem non è stato configurato oppure è stato annullato. Viene richiesta una nuova password.
6. Immettere e confermare la nuova password del responsabile nei campi appropriati, quindi fare clic su **OK**.

   L'operazione è completa e viene visualizzata la finestra principale di Administrator Utility.

Aggiornamento della versione di Client Security Software

E' necessario che i client su cui sono installate le versioni precedenti di Client Security Software aggiornino il software con la versione più recente per disporre delle nuove funzioni di Client Security.

Importante: E' necessario che i sistemi che dispongono di IBM Client Security Software Versione 4.0x disinstallino IBM Client Security Software versione 4.0x ed azzerino il chip prima di installare questa versione di IBM Client Security Software. E' possibile che si verifichi un errore durante un errore di installazione o mentre il software non è operativo.

Aggiornamento dell'utilizzo dei nuovi dati di sicurezza

Se si desidera rimuovere Client Security Software ed effettuare l'avvio, completare la seguente procedura:

1. Disinstallare la versione precedente di Security Software utilizzando l'applet Installazione applicazioni del Pannello di controllo.
2. Riavviare il sistema.
3. Azzerare IBM embedded Security Chip in BIOS Setup Utility.
4. Riavviare il sistema.
5. Installare la versione più recente di Client Security Software e configurarlo utilizzando la procedura guidata d'installazione di IBM Client Security.

Aggiornamento da CSS 5.0 o versioni successive utilizzando i dati di sicurezza esistenti

Se si desidera aggiornare Client Security Software Versione 5.0 o le versioni successive del software utilizzando i dati di sicurezza esistenti, completare la procedura seguente:

1. Aggiornare l'archivio completando la seguente procedura:
   a. Fare clic su **Start > Programmi > Access IBM > IBM Client Security Software > Modifica impostazioni di protezione**.
   b. Fare clic sul pulsante **Aggiorna archivio delle chiavi** per assicurarsi che le informazioni di backup siano aggiornate.

      Annotarsi la directory di archivio.
   c. Uscire dal programma IBM Client Security Software User Configuration Utility.
2. Aggiornare la versione esistente di Client Security Software completare i passi seguenti:
   a. Dal desktop di Windows fare clic su **Start > Esegui**.
   b. Nel campo Esegui, immettere `d:\directory\csec5xxus_00yy.exe`, dove `d:\directory\` è la lettera unità e la directory in cui è ubicato il file eseguibile. `xx` e `yy` sono caratteri alfanumerici.
   c. Selezionare **Aggiorna**.
   d. Riavviare il sistema.

Disinstallazione di Client Security Software

Assicurarsi che siano disinstallati i vari programmi di utilità (IBM Client Security Password Manager, IBM Client Security File and Folder Encryption (FFE)) che potenziano le funzioni di Client Security, prima di disinstallare IBM Client Security Software. Gli utenti devono collegarsi con i privilegi dell'utente responsabile per disinstallare Client Security Software.

Nota: è necessario disinstallare tutti i programmi di utilità di IBM Client Security Software o il software del sensore UVM prima di disinstallare IBM Client Security Software. Per disinstallare Client Security Software viene richiesta la password del responsabile.

Per disinstallare Client Security Software, completare la seguente procedura:

1. Chiudere tutti i programmi Windows.
2. Dal desktop Windows, fare clic **Start > Impostazioni > Pannello di controllo**.
3. Fare clic sull'icona **Aggiungi/Rimuovi**.
4. Nell'elenco del software che può essere eliminato automaticamente, selezionare **IBM Client Security**.
5. Fare clic su **Aggiungi/Rimuovi**.
6. Selezionare il pallino **Rimuovi**.
7. Fare clic su **Avanti** per disinstallare il software.
8. Fare clic su **OK** per confermare l'operazione.
9. Immettere la password del responsabile nell'interfaccia appropriata, quindi fare clic su **OK**.
10. Effettuare una delle seguenti operazioni:
    - Se è stato installato il modulo IBM Embedded Security Chip PKCS#11 per Netscape, viene visualizzato un messaggio in cui viene richiesto di avviare il processo per disattivare il modulo PKCS#11 di IBM Embedded Security Chip. Fare clic su **Sì** per continuare.

      Una serie di messaggi viene visualizzata. Fare clic su **OK** per ogni messaggio fino all'eliminazione del modulo PKCS#11 di Security Chip.
    - Se non è stato installato il modulo PKCS#11 di IBM Embedded Security Chip per Netscape, viene visualizzato un messaggio in cui viene chiesto se se si desidera cancellare i file DLL condivisi installati con Client Security Software.

      Fare clic su **Sì** per disinstallare questi file oppure fare clic su **No** per lasciare i file installati. Lasciare i file installati non interessa il normale funzionamento del computer.

    Se al messaggio ″Si desidera rimuovere le informazioni sul sistema dall''archivio?″ ?″ si seleziona **No**, è possibile ripristinare le informazioni quando viene reinstallata la versione più aggiornata di IBM Client Security Software.
11. Fare clic su **Fine** una volta rimosso il software.

    E' necessario riavviare il computer prima di disinstallare Client Security Software.

Quando si disinstalla Client Security Software, rimuovere tutti i componenti software installati di Client Security con tutte le chiavi dell'utente, i certificati digitali, le impronte digitali registrate e le password memorizzate.

Regole per l'esportazione

IBM Client Security Software contiene il codice di cifratura che può essere scaricato da Internet in America del Nord e in ambito internazionale. Se si è residenti in un paese in cui è proibito scaricare i software di cifratura da un sito web, non è possibile scaricare IBM Client Security Software. Per ulteriori informazioni sulle norme di esportazione relative a IBM Client Security Software, consultare l'Appendice A, "Norme per l'esportazione di Client Security Software", a pagina 35.

Capitolo 5. Risoluzione dei problemi

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

Funzioni del responsabile

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.

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

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

6. Immettere di nuovo la password e premere freccia giù.
7. Selezionare **Modifica password responsabile** e premere Invio; premere di nuovo Invio.
8. Premere **Esc** per uscire e salvare le impostazioni.

Dopo aver impostato la password del responsabile 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 il computer.
2. Quando viene visualizzata la finestra Setup Utility, premere il tasto F1.
   Viene aperto il menu principale di Setup Utility.
3. Selezionare **Password**.
4. Selezionare **Password supervisore**.
5. Immettere la password e premere Invio.
6. Immettere di nuovo la password e premere Invio.
7. Fare clic su **Continua**.
8. Premere F10 per salvare e uscire.

Esempio 2

1. Chiudere e riavviare il computer.
2. Quando viene visualizzato il messaggio "To interrupt normal startup, press the blue Access IBM button", premere il pulsante blu Access IBM.
   Viene aperta Access IBM Predesktop Area.
3. Fare doppio clic su **Start setup utility**.

4. Selezionare **Protezione** utilizzando i tasti di spostamento cursore per spostarsi nel menu.
5. Selezionare **Password**.
6. Selezionare **Password supervisore**.
7. Immettere la password e premere Invio.
8. Immettere di nuovo la password e premere Invio.
9. Fare clic su **Continua**.
10. Premere F10 per salvare e uscire.

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

Importante: conservare la password del supervisore in un luogo sicuro. Se si perde o si dimentica la password del supervisore, non è possibile accedere al programma di utilità di impostazione IBM BIOS e non è possibile modificare o cancellare la password. Per ulteriori informazioni, consultare la documentazione sull'hardware fornita con il computer.

Annullamento di IBM embedded Security Subsystem (ThinkCentre)

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

Attenzione:

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

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

1. Chiudere e riavviare il computer.
2. Quando viene visualizzata la finestra Setup Utility, premere il tasto F1.
   Viene aperto il menu principale di Setup Utility.
3. Selezionare **Security**.
4. Selezionare **IBM TCPA Security Feature** e premere Invio.
5. Selezionare **Sì**.
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 il computer.
2. Quando viene visualizzata la finestra Setup Utility, premere il tasto F1.
   Viene aperto il menu principale di Setup Utility.
3. Selezionare **Security**.
4. Selezionare **IBM 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 durante l'installazione o la configurazione di Client Security Software Versione 5.4.

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.

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.

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.
Viene visualizzato un messaggio di errore quando si tenta di utilizzare determinate funzioni del responsabile di Client Security	**Azione**
Viene visualizzato un messaggio di errore durante l'esecuzione di una funzione da responsabile di Client Security.	E' necessario che la password supervisore ThinkPad o la password del responsabile BIOS ThinkCentre vengano disabilitate per creare la coppia di chiavi hardware su un sistema Crypto 1 (disverso da TCG). Il processo di installazione CSS non è in grado di abilitare IBM Embedded Security Subsystem fino a che non viene disabilitata la password appropriata.

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

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

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

Appendice B. Informazioni sulle password e i passphrase

L'appendice contiene informazioni sulle password e i passphrase.

Regole per password e passphrase

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

Regole per la password del responsabile

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. 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