IBM® Client Security
Solutions

Guida all'installazione di Client Security Software versione 5.1

IBM® Client Security
Solutions

Guida all'installazione di Client Security Software versione 5.1

Prima edizione (aprile 2003)

Prima di utilizzare questo prodotto e le relative informazioni, consultare la sezione Appendice A, “Norme per l’esportazione di Client Security Software”, a pagina 43 e l’Appendice C, “**Marchi e informazioni particolari**”, a pagina 49.

Indice

Prefazione

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

Informazioni sulla guida

Questa guida contiene informazioni sull'installazione di Client Security Software su computer di rete IBM, anche definito come client IBM, che contiene Security Chips integrato IBM. Questa guida contiene anche istruzioni sull'abilitazione di Security Chip integrato IBM e sull'impostazione della password dell'hardware per il security chip.

La guida è organizzata nel modo seguente:

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

″Capitolo 2, "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 prerequisite per l'installazione di Client Security Software.

″Capitolo 4, "Installazione, aggiornamento e disinstallazione del 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, "Regole per password e passphrase",″ contiene i criteri della password che possono essere applicati alle regole e ad una passphrase UVM per le password di Security Chip.

″Appendice C, "**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 *Client Security Software Administrator, >Utilizzo di Client Security con Tivoli Access Manager*, e *Guida per l'utente di Client Security*.

Questa guida e tutte le altre documentazioni per Client Security possono essere scaricate dall'indirizzo http://www.pc.ibm.com/ww/security/secdownload.html sul sito Web IBM.

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

I riferimenti al manuale *Client Security Software Guida per il responsabile* vengono forniti in questo documento. La *Guida per il responsabile* contiene informazioni sull'uso di UVM (User Verification Manager) e della politica UVM e le informazioni su Administrator Utility e User Configuration Utility.

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

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

La *Guida per l'utente di Client Security* che si integra con la guida *Client Security Software Guida per il responsabile*, contiene informazioni sull'esecuzione delle attività utente di Client Security Software, quali l'utilizzo di una protezione per il collegamento UVM, la creazione di un certificato digitale e l'utilizzo di User Configuration Utility.

Ulteriori informazioni

E' possibile ottenere ulteriori informazioni e aggiornamenti del prodotto di sicurezza, quando sono disponibili, dall'indirizzo http://www.pc.ibm.com/ww/security/index.html sul sito Web IBM.

Capitolo 1. Introduzione a IBM Client Security Software

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

Applicazioni e componenti di Client Security Software

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

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

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

Funzioni PKI (Public Key Infrastructure)

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

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

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

Capitolo 2. Introduzione

Questa sezione contiene i requisiti relativi alla compatibilità hardware e software per utilizzare Client Security Software. Inoltre, vengono fornite informazioni relative alle procedure di download di Client Security Software.

Requisiti hardware

Prima di scaricare e installare il software, accertarsi che l'hardware del computer sia compatibile con Client Security Software.

Le informazioni più recenti sui requisiti hardware e software sono disponibili sul sito Web IBM all'indirizzo
http://www.pc.ibm.com/ww/security/secdownload.html.

Security Chip integrato IBM

Il Security Chip integrato IBM è un microprocessore di cifratura che viene incorporato sulla scheda di sistema del 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 i computer IBM e le stazioni di lavoro che contengono i Security Chip integrati IBM supportano Client Security Software. Se si tenta di scaricare e installare il software su un computer che non contiene un Security Chip integrato IBM, il software non verrà installato oppure non funzionerà 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, fare riferimento alla pagina Web
http://www.pc.ibm.com/ww/resources/security/secdownload.html.

Requisiti software

Prima di scaricare e installare il software, accertarsi che il software del computer e il sistema operativo siano compatibile con Client Security Software.

Sistemi operativi

Client Security Software richiede uno dei seguenti sistemi operativi:

- 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 la macchina desktop. 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 Client Security Software prima di installare un sensore compatibile con UVM.

Per utilizzare un sensore UVM già installato su un client IBM, è necessario disinstallare il sensore UVM, installare Client Security Software e, quindi, installare nuovamente il sensore UVM.

- **Tivoli Access Manager versioni 3.8 o 3.9**

  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 Client Security Software per migliorare la sicurezza di registrazione a Lotus Notes (Lotus Notes versione 4.5 o successive).

- **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 impronte digitali Targus**

  Il programma di utilità per la lettura delle impronte digitali Targus fornisce un'interfaccia semplice e rapida che consente alla politica di protezione di includere l'autenticazione mediante le impronte digitali.

- **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

Client Security Software supporta i browser Web riportati di seguito per la richiesta di certificati digitali:

- Internet Explorer 5.0 o successive
- Netscape 4.51 a Netscape 7

Informazioni sulla cifratura del browser Web

Se il supporto per la cifratura rigida è installato, utilizzare la versione a 128-bit del browser Web. Diversamente, utilizzare la versione a 40-bit del browser Web. Per verificare la severità della codifica del browser Web, fare riferimento alla guida fornita con il browser.

Servizi di cifratura

Client Security Software supporta i seguenti servizi di cifratura:

- **Microsoft CryptoAPI:** CryptoAPI è il servizio di cifratura predefinito per i sistemi operativi Microsoft e le applicazioni. Con il supporto CryptoAPI incorporato, Client Security Software consente di utilizzare le operazioni di cifratura del Security Chip integrato IBM quando si creano 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 Security Chip integrato IBM, è possibile utilizzare Security Chip per creare certificati digitali per Netscape, Entrust, RSA ed altre applicazioni che utilizzano PKCS#11.

Applicazioni e-mail

Client Security Software supporta i seguenti tipi di applicazione 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)

Download del software

E' possibile eseguire il download di Client Security Software dal sito Web IBM http://www.pc.ibm.com/ww/security/secdownload.html.

Modulo di registrazione

Quando si esegue il download del software, è necessario completare un modulo di registrazione e un questionario ed aderire ai termini dell'accordo di licenza. Seguire le istruzioni fornite nel sito Web per il download del software.

I file di installazione per Client Security Software sono inclusi nel file a decompressione automatica csec51.exe.

Regole per l'esportazione

Client Security Software contiene un codice di cifratura che è possibile scaricare da Internet nell'America del Nord e in ambito internazionale. Se si è residenti in un paese in cui è proibito scaricare del software di cifratura da un sito Web, non è possibile scaricare Client Security Software. Per ulteriori informazioni sulle regole di esportazione relative a Client Security Software, consultare l'Appendice A, "Norme per l'esportazione di Client Security Software", a pagina 43.

Capitolo 3. Operazioni precedenti all'installazione del software

Questa sezione contiene le istruzioni prerequisite per l'esecuzione del programma di installazione e di configurazione di Client Security Software sui client IBM. Tutti i file richiesti per l'installazione vengono forniti nel file csec51.exe che è possibile scaricare dal sito Web IBM.

Operazioni precedenti all'installazione del software

Il programma di installazione installa Client Security Software sul client IBM e abilita il Security Chip integrato IBM; in ogni caso, le specifiche di installazione variano in base al numero di fattori.

Installazione sui client che eseguono Windows XP e Windows 2000

Gli utenti di Windows XP e Windows 2000 devono registrarsi con i privilegi del responsabile per installare Client Security Software.

Installazione per utilizzare Tivoli Access Manager

Se si desidera utilizzare Tivoli Access Manager per controllare i requisiti di autenticazione per il computer, è necessario installare alcuni componenti di Tivoli Access Manager prima di installare 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 possono interessare il modo in cui si abilitano i sistemi secondari di sicurezza (Security Chip integrato) e si creano le chiavi di codifica hardware. Tali funzioni sono la password del responsabile e Enhanced Security.

Password del responsabile (NetVista)

Le password del responsabile impediscono agli utenti non autorizzati di modificare le impostazioni sulla configurazione di un computer IBM. Tali password vengono impostate utilizzando il programma di utilità Configuration/Setup, a cui è possibile accedere premendo F1 in fase di avvio del sistema.

Password del supervisore (ThinkPad)

Le password del supervisore impediscono agli utenti non autorizzati di modificare le impostazioni sulla configurazione di un computer ThinkPad IBM. Tali password vengono impostate utilizzando il programma di utilità IBM BIOS Setup, a cui è possibile accedere premendo F1 in fase di avvio del sistema.

Enhanced Security

Enhanced Security fornisce una ulteriore protezione per la password del responsabile, come le impostazioni in fase di avvio. E' possibile verificare se Enhanced Security è abilitata o disabilitata, utilizzando il programma di utilità Configuration/Setup, a cui è possibile accedere premendo F1 in fase di avvio del sistema.

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 una password del responsabile è stata impostata sui modelli NetVista (6059, 6569, 6579, 6649, 6646 e tutti i modelli Q1x), è necessario aprire Administrator Utility per abilitare il chip e creare le chiavi hardware.

Se Enhanced Security è abilitato su questi modelli NetVista, è necessario utilizzare Administrator Utility per abilitare il Security Chip integrato e creare le chiavi di cifratura hardware dopo aver installato Client Security Software. Se il programma di installazione rileva che Enhanced Security è abilitato, verrà notificato al termine del processo di installazione. Riavviare il computer e aprire Administrator Utility per abilitare il chip e creare le chiavi hardware.

Enhanced Security su tutti gli altri modelli NetVista (diversi dai modelli 6059, 6569, 6579, 6649 e tutti i modelli NetVista Q1x): Se la password del responsabile è stata impostata su altri modelli NetVista, non è necessario immettere la password durante l'installazione.

Se Enhanced Security è abilitato su questi modelli NetVista, è possibile utilizzare il programma di installazione per installare il software, ma è necessario utilizzare il programma di utilità Configuration/Setup per abilitare il Security Chip integrato. Dopo aver abilitato il chip, è possibile utilizzare Administrator Utility per creare chiavi hardware.

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

Per gli ultimi aggiornamenti del codice BIOS, visitare il sito Web IBM http://www.pc.ibm.com/support, immettere bios nel campo di ricerca e selezionare downloads dall'elenco a discesa; quindi, premere Invio. Un elenco di aggiornamenti del codice BIOS vengono visualizzati. Fare clic sul numero del modello NetVista appropriato e seguire le istruzioni sulla pagina Web.

Utilizzo della coppia di chiavi dell'archivio

La coppia di chiavi dell'archivio, che include la chiave pubblica di gestione e la chiave privata, consente di creare chiavi di cifratura dell'hardware per un client IBM e tiene traccia dei dati di chiavi per il ripristino.

Poiché Client Security Administrator Utility consente di creare la coppia di chiavi dell'archivio, è necessario installare Client Security Software sul primo client IBM e, quindi, creare la coppia di chiavi dell'archivio. Le istruzioni per l'installazione e la configurazione del software sul primo client IBM sono fornite di seguito.

Nota: se si desidera utilizzare la politica UVM che può essere utilizzata su client remoti, è necessario utilizzare lo stessa coppia di chiavi dell'archivio quando si installa il software su quei client.

Capitolo 4. Installazione, aggiornamento e disinstallazione del software

Questa sezione contiene le istruzioni per lo scaricamento, l'installazione e la configurazione di Client Security Software sui 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 pecedente a Client Security Software 5.0, è necessario decifrare tutti i file cifrati prima di installare Client Security Software 5.1. Client Security Software 5.1 non può decifrare i file cifrati con le versioni precedenti a Client Security Software 5.0, a causa delle modifiche dovute all'implementazione per la cifratura dei file.

Scaricamento ed installazione del software

Tutti i file richiesti per l'installazione del programma Client Security Software sono forniti all'interno del file csec51.exe da scaricare dall'indirizzo http://www.pc.ibm.com/ww/security/secdownload.html sul sito Web IBM. Il sito Web fornisce le informazioni che consentono di verificare che il sistema disponga di IBM embedded Security Chip e di selezionare l'offerta appropriata di Client Security per il sistema in uso.

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

1. Utilizzando un browser Web, passare all'indirizzo http://www.pc.ibm.com/ww/security/secdownload.html sul sito Web IBM
2. Utilizzando le informazioni sul sito Web, verificare che IBM security chip integrato sia presente sul sistema e che il numero del modello corrisponda a quello fornito nella tabella per i requisiti del sistema; quindi, fare clic su **Continua**.
3. Selezionare il pallino che corrisponde al Tipo di macchina e fare clic su **Continua**.
4. Creare un ID utente, effettuare la registrazione presso la IBM compilando il modulo in linea e consultare l'Accordo di licenza; quindi, fare clic su **Accetto la licenza**.

   Verrà visualizzata la pagina per lo scaricamento del programma Client Security in modo automatico.
5. Seguire la procedura presente nella pagina di scaricamento per scaricare i driver di periferica necessari, i file README, il software, i documenti di riferimento ed i programmi di utilità aggiuntivi che costituiscono IBM Client Security Software. Seguire la sequenza di scaricamento specificata sul sito Web.
6. Dal desktop di Windows fare clic su **Start > Esegui**.
7. Nel campo Esegui, immettere `d:\directory\csec51.exe`, dove `d:\directory\` è la lettera relativa all'unità e la directory in cui è ubicato il file.
8. Fare clic su **OK**.

   Viene visualizzata la finestra Welcome to the InstallShield Wizard for IBM Client Security Software.

9. Fare clic su **Avanti**.

   La creazione guidata estrae i file ed installa il software. Una volta completata l'installazione, verrà fornita l'opzione per riavviare l'elaboratore in questo momento oppure successivamente.

10. Selezionare l'opzione per riavviare l'elaboratore e fare clic su **OK**.

    La Creazione guidata all'installazione di IBM Client Security Software viene visualizzata quando viene riavviato l'elaboratore.

Utilizzo della creazione guidata all'installazione di IBM Client Security

La creazione guidata all'installazione di IBM Client Security fornisce una interfaccia di supporto durante l'installazione di Client Security Software ed abilita il Security Chip integrato IBM. La creazione guidata all'installazione di IBM Client Security Software guida gli utenti tramite le attività necessarie implicate nell'installazione di una politica di sicurezza sul client IBM.

Di seguito viene riportata tale procedura:

- **Impostazione di una password di Security Administrator**

  La password di Security Administrator consente di controllare l'accesso al programma IBM Client Security Administrator Utility, che viene utilizzato per modificare le impostazioni di sicurezza per questo elaboratore.

- **Creazione delle chiavi di sicurezza del responsabile**

  Le chiavi di sicurezza del responsabile sono una serie di chiavi digitali memorizzate in un file dell'elaboratore. E' preferibile salvare tali chiavi di sicurezza su un'unità o un disco amovibile. Quando viene apportata una modifica alla politica di sicurezza nel programma Security Administrator Utility, verrà richiesto questo file per dimostrare l'autorizzazione della modifica di politica.

  Le informazioni di sicurezza di backup sono salvate nel caso in cui è necessario sostituire la scheda di sistema o l'unità disco fisso dell'elaboratore in uso. Tali informazioni di backup devono essere memorizzate in qualche unità esterna al sistema.

- **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 degli 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.

- **Selezione di un livello di sicurezza 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.

Per utilizzare la creazione guidata all'installazione di IBM Client Security Software, completare la procedura seguente:

1. Se non è stata visualizzata la creazione guidata, fare clic su **Start > Programmi > Access IBM > IBM Client Security Software > IBM Client Security Setup Wizard**.

La finestra di benvenuto della creazione guidata all'installazione di IBM client Security visualizza una panoramica dei passi della creazione guidata.

Nota: se si desidera utilizzare l'autenticazione delle impronte digitali, è necessario installare il software ed il lettore delle impronte digitali prima di proseguire.

2. Fare clic su **Avanti** per iniziare ad utilizzare la creazione guidata.

   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. Procedere nel modo seguente:
   - **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 le nuove chiavi di sicurezza**.
     b. Specificare dove si desidera salvare le chiavi di administrator security immettendo il percorso nel campo fornito oppure facendo clic su **Sfoglia** e selezionando la cartella appropriata.
     c. Se si desidera dividere la chiave della sicurezza per aumentare la protezione, fare clic sulla casella di spunta **Suddividi la chiave di sicurezza di backup per la sicurezza crescente** 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 dove 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 appropriata.
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 collegamento normale di Windows con il collegamento protetto di Client Security**

  Selezionare questa casella per sostituire il normale collegamento di Windows con il collegamento protetto di Client Security. Ciò consente di incrementare la protezione del sistema e di collearsi solo dopo l'autenticazione con IBM Embedded Security Chip e le periferiche opzionali, come i dispositivi di lettura per le impronte digitali.
- **Abilita la cifratura della cartella e del file**

  Selezionare questa casella se si desidera proteggere i file sul disco fisso con Security Chip integrato IBM. (E' richiesto lo scaricamento di IBM Client Security File e Folder Encryption utility).
- **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. (E' richiesto il download dell'applicazione IBM Client Security Password Manager).
- **Sostituisci il collegamento Lotus Notes con il Collegamento di IBM Client Security**

  Selezionare questa casella se si desidera che Client Security esegua l'autenticazione degli utenti di Lotus Notes mediante Security Chip integrato IBM.
- **Abilita supporto Entrust**

  Selezionare questa casella se si desidera abilitare l'integrazione con i prodotti software di sicurezza Entrust.
- **Protezione di Microsoft Internet Explorer**

  Questa protezione consente di proteggere le comunicazioni via e-mail e sfogliare il 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 degli utenti non autorizzati.
     b. Fare clic su **Utenti autorizzati**.
     c. Immettere e confermare il passphrase di IBM Client Security nei campi forniti e fare clic su **Fine**.
     d. 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 degli utenti autorizzati.
     b. Fare clic su **Utenti non autorizzati**.
     c. Immettere e confermare il passphrase di IBM Client Security nei campi forniti e fare clic su **Fine**.
     d. Fare clic su **Avanti**.

Viene visualizzata la finestra Seleziona livello di sicurezza del sistema.

9. Selezionare un livello di sicurezza del sistema utilizzando la seguente procedura:
   a. Selezionare i requisiti di autenticazione che si desidera utilizzare facendo clic sulle caselle di spunta appropriate. E' possibile selezionare più di un requisito di autenticazione.
   b. Selezionare un livello di sicurezza del sistema trascinando il selettore sul livello di sicurezza desiderato e fare clic su **Avanti**.

   Nota: è inoltre possibile definire una politica di sicurezza personalizzata utilizzando IBM Client Security Policy Editor.
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 il Security Chip integrato IBM. Viene visualizzato un messaggio che conferma la protezione dell'elaboratore da parte IBM Client Security.
11. Fare clic su **OK**.

    E' possibile installare e configurare IBM Client Security Password Manager e i programmi di utilità IBM Client Security File e Folder Encryption.

Abilitazione di IBM Security Chip

E' necessario che IBM Security Chip sia abilitato prima di poter 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 Chip utilizzando Administrator Utility, completare la seguente procedura:

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

   Una finestra visualizza un messaggio che indica che IBM Security Chip non è stato abilitato e che richiede se si desidera abilitare il chip.
2. Fare clic su **Sì**.

   Viene visualizzato un messaggio che indica se è stata abilitata una password del responsabile, è necessario disabilitarla nel BIOS Setup prima di proseguire.
3. Procedere nel modo seguente:
   - 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 Client Security Subsystem** per visualizzare Administrator Utility.

   Viene visualizzato un messaggio che indica che IBM Security Chip non è stato configurato oppure è stato annullato. Viene richiesta una nuova password.

6. Immettere e confermare una nuova password di IBM Security Chip nei campi appropriati e fare clic su **OK**.

   Nota: è necessario che la lunghezza della password sia di otto caratteri.

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

Installazione del software su altri client IBM quando la chiave pubblica di gestione è disponibile - solo per le installazioni non presidiate

Se è stato installato il software sul primo client IBM e creata una coppia di chiavi pubbliche di gestione, è possibile installare il software ed abilitare il sistema secondario di sicurezza su altri client IBM utilizzando il programma di installazione.

Durante l'installazione, è necessario selezionare una ubicazione per la chiave pubblica admin, la chiave privata admin e l'archivio delle chiavi. Se si desidera utilizzare una chiave pubblica di gestione che risiede su una directory condivisa oppure salvare l'archivio delle chiavi in una directory condivisa, è necessario prima mappare una lettera unità alla directory di destinazione prima di poter utilizzare il programma di installazione. Per informazioni sulla mappatura di una lettera unità ad una risorsa di rete condivisa, consultare la documentazione del sistema operativo di Windows.

Esecuzione di un'installazione non presidiata

Un'installazione non presidiata consente al responsabile di installare Client Security Software su un client IBM remoto senza dover essere vicini fisicamente al computer client.

Prima di eseguire un'installazione non presidiata, consultare il Capitolo 3, "Operazioni precedenti all'installazione del software", a pagina 9. Nessun messaggio di errore viene visualizzato durante l'installazione non presidiata. Se un'installazione non presidiata termina prematuramente, è necessario eseguire su una installazione presidiata per visualizzare ogni messaggio di errore.

Nota: gli utenti devono registrarsi con i privilegi dell'utente responsabile per installare Client Security Software.

Per le informazioni complete su come eseguire un'installazione non presidiata, completare la seguente procedura, consultare il file css51readme disponibile all'indirizzo http://www.pc.ibm.com/ww/security/secdownload.html sul sito Web IBM

Distribuzione di massa

La distribuzione di massa consente ai responsabili di sicurezza di iniziare la politica di sicurezza su più elaboratori contemporaneamente. Questa operazione rende più semplice la gestione e la distribuzione delle misure di sicurezza e verifica l'implementazione corretta delle politiche di sicurezza.

E' necessario che i seguenti driver di periferica siano installati prima di completare la procedura di distribuzione di massa:

- Il driver di periferica bus SM

- Il driver di periferica bus LPC (per sistemi TCPA)

Sono presenti due passi principali per la distribuzione di massa:

- Installazione di massa
- Configurazione di massa

Installazione di massa

E' necessario eseguire un'installazione non presidiata per installare IBM Client Security Software su più client contemporaneamente. E' necessario utilizzare il parametro di installazione non presidiata durante l'avvio della distribuzione di massa.

Per cominciare un'installazione di massa, completare la seguente procedura:

1. Creare il file CSS.ini.

   Tale passo viene richiesto solo se si desidera eseguire una configurazione di massa.
2. Estrarre il contenuto del pacchetto di installazione CSS mediante Winzip utilizzando i nomi della cartella.
3. Modificare le voci `szIniPath` e `szDir`, richieste per la configurazione di massa, che si trovano nel file setup.iss.

   Il contenuto completo di questo file viene elencato di seguito. Il parametro `szIniPath` viene richiesto solo se si desidera eseguire una configurazione di massa.
4. Copiare i file sul sistema di destinazione.
5. Creare l'istruzione della riga comandi `\setup -s`.

   E' necessario che questa istruzione della riga comandi sia eseguita dal desktop di un utente che ha i diritti del responsabile. Il gruppo del programma StartUp o il tasto Esegui si trova in un'ottima posizione per eseguire tale operazione.
6. Rimuovere l'istruzione della riga comandi al successivo avvio.

l contenuto completo del file setup.iss viene elencato di seguito con poche descrizioni: [InstallShield Silent] Version=v6.00.000 File=Response File szIniPath=d:\csssetup.ini (Il parametro sopra riportato indica il nome e la posizione del file .ini, richiesto per la configurazione di massa. Se si tratta di un'unità di rete, è necessario che sia mappata. Quando non viene utilizzata una configurazione di massa con un'installazione presidiata, rimuovere questa voce.) [File Transfer] OverwrittenReadOnly=NoToAll [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-DlgOrder] Dlg0={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdLicense-0 Count=4 Dlg1={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdAskDestPath-0 Dlg2={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdSelectFolder-0 Dlg3={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdFinishReboot-0 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdLicense-0] Result=1 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdAskDestPath-0] szDir=C:\Program Files\IBM\Security (Il parametro sopra riportato indica la directory utilizzata per installare Client Security. E' necessario che sia una directory locale del computer.) Result=1 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdSelectFolder-0] szFolder=IBM Client Security Software (Il parametro sopra riportato indica il gruppo del programma per Client Security.) Result=1 [Application] Name=Client Security Version=5.00.002f Company=IBM Lang=0009 [{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdFinishReboot-0] Result=6 BootOption=3

Configurazione di massa

Il seguente file è fondamentale durante l'avvio di una configurazione di massa. Il file può essere nominato in qualsiasi modo, affinché abbia un'estensione .ini. Di seguito viene riportato l'aspetto del file. Nella parte laterale è riportata una breve descrizione che non deve essere inclusa nel file. Il seguente comando esegue questo dalla riga comandi quando la configurazione di massa non viene effettuata con un'installazione di massa:

```
<CSS installation folder>\acamucli /ccf:c:\csec.ini
```

Nota: se qualsiasi file o percorso si trovano su un'unità di rete, è necessario mappare l'unità ad una lettera.

[CSSSetup]	Intestazione della sezione per l'installazione CSS.
suppw=bootup	Password del responsabile. Lasciare lo spazio vuoto se non richiesto.
hwpw=11111111	Password hardware CSS. E' necessario che sia costituita da otto caratteri. Viene sempre richiesta. E' necessario che sia corretta se la password hardware è stata già impostata.
newkp=1	1 per creare una nuova coppia di chiavi admin 0 per utilizzare una coppia di chiavi admin esistente.
keysplit=1	Quando newkp è 1, determina il numero dei componenti delle chiavi private. **Nota:** se la coppia di chiavi esistente utilizza più parti della chiave privata, è necessario che tutte le parti siano memorizzate nella stessa directory.
kpl=c:\jgk	Posizione della coppia di chiavi admin quando newkp è 1, se si tratta di un'unità di rete mappata.
kal=c:\jgk\archive	Posizione dell'archivio di chiavi dell'utente, se si tratta di un'unità di rete mappata.
pub=c:\jk\admin.key	Posizione della chiave pubblica admin quando si utilizza una coppia di chiavi admin esistente, se si tratta di un'unità di rete mappata.
pri=c:\jk\private1.key	Posizione della chiave privata admin quando si utilizza una coppia di chiavi admin esistente, se si tratta di un'unità di rete mappata.
clean=0	1 per eliminare il file .ini in seguito all'inizializzazione. 0 per lasciare il file .ini in seguito all'inizializzazione.
[UVMEnrollment]	Intestazione della sezione per la registrazione dell'utente.
enrollall=0	1 per registrare tutti gli account utente locali in UVM, 0 per registrare account specifici dell'utente in UVM.
defaultuvmpw=top	Quando enrollall è 1, esso indica il passphrase UVM per tutti gli utenti.
defaultwinpw=down	Quando enrollall è 1, esso indica la password di Windows registrata con UVM per tutti gli utenti.
enrollusers=2	Quando enrollall è 0, esso indica il numero degli utenti registrati in UVM.
user1=joseph	Numerare gli utenti da registrare iniziando con il numero 1, è necessario che i nomi utenti siano i nomi account. Per reperire il nome account corrente in XP, procedere nel modo seguente 1. Avviare Gestione computer (Gestione periferiche). 2. Espandere il nodo Utenti e gruppi locali. 3. Aprire la cartella Utenti. Gli elementi elencati nella colonna Nome sono i nomi account.
user1uvmpw=chrome	Numerare gli utenti da registrare con il passphrase UVM iniziando con il numero 1.

user1winpw=spinning	Numerare gli utenti daregistrare con il passphrase di Windows registrati in UVM, iniziando con il numero 1.
user1domain=0	0 per indicare che questo account è locale. 1 per indicare che questo è presente sul dominio.
user2=hallie	
user2uvmpw=left	
user2winpw=right	
user2domain=0	
[UVMAppConfig]	Intestazione della sezione per l'installazione del modulo e l'installazione di applicazioni, compatibili con UVM.
uvmlogon=0	1 per utilizzare la protezione del collegamento UVM, 0 per utilizzare il collegamento di Windows.
entrust=0	1 per utilizzare UVM per l'autenticazione entrust, 0 per utilizzare l'autenticazione entrust.
notes=0	1 per utilizzare la protezione UVM per lotus notes, 0 per utilizzare la protezione di password di Notes.
passman=0	1 per utilizzare Password Manager, 0 per non utilizzare Password Manager
folderprotect=0	1 per utilizzare File e Folder Encryption, 0 per non utilizzare File e Folder Encryption.

Aggiornamento della versione di Client Security Software

E' necessario che i client su cui sono installate le versioni precedenti di Client Security aggiornino il relativo software con Client Security Software versione 5.1 per disporre delle nuove funzioni di Client Security.

Importante: i sistemi TCPA dotati di IBM Client Security Software Versione 4.0x installato devono eliminare il chip prima di installare IBM Client Security Software Versione 5.1. 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. Eliminare IBM embedded Security Chip nel BIOS utility.
4. Riavviare il sistema.
5. Installare Client Security Software Release 5.1 e configurarlo utilizzando la procedura guidata all'installazione di IBM Client Security Software.

Aggiornamento di Client Security versione 5.1 mediante i dati di sicurezza esistenti

Se si desidera aggiornare un rilascio di Client Security Software precedente alla versione 5.0 utilizzando i dati di protezione esistenti, completare la procedura di seguito riportata:

1. Aggiornare l'archivio completando la seguente procedura:
   a. Fare clic su **Start > Programmi > Access IBM > IBM Client Security Software > Client Utility**.

b. Fare clic sul pulsante **Aggiorna archivio** per verificare che siano aggiornate le informazioni di backup.

   Annotarsi la directory di archivio.

c. Uscire dal programma IBM Client Security Software Client Utility.

2. Rimuovere la versione esistente del programma Client Security Software completando la seguente procedura:
   a. Individuare le chiavi private e pubbliche del responsabile, create quando è stata configurata la versione precedente di Client Security Software.
   b. Fare clic su **Start > Impostazioni > Pannello di controllo > Installazione applicazioni** e selezionare per rimuovere IBM Client Security Software.
   c. Selezionare **No** quando viene richiesto il riavvio.
   d. Spegnere il sistema.
3. Eliminare Embedded Security Chip completando la seguente procedura:
   a. Accendere il sistema.
   b. Premere il tasto F1 per attivare BIOS Setup utility.
   c. Passare alle impostazioni di Security Chip ed eliminare il chip di sicurezza.
   d. Uscire dal BIOS Setup utility.

      Il sistema continua il riavvio.
4. Eseguire il programma di installazione Client Security Software Versione 5.0.
5. Riavviare quando richiesto.

   Una volta eseguito il riavvio, la creazione guidata di Client Security Software verrà avviata automaticamente. NON eseguire la creazione guidata all'installazione.
6. Premere **Annulla** per uscire dalla creazione guidata all'installazione.
7. Eseguire il backup della politica di sicurezza predefinita completando la seguente procedura:
   a. Utilizzando Windows Explorer, passare alla directory di installazione di IBM Client Security Software (la directory predefinita è c:\program files\ibm\security).
   b. Fare clic con il tastino destro del mouse sulla cartella Politica_UVM e selezionare **Copia**.
   c. Fare clic con il tastino destro del mouse sul desktop di Windows e fare clic su **Incolla**.

      Verrà creato un backup temporaneo sul desktop di Windows.

      Nota: le impostazioni della politica di sicurezza esistenti saranno sostituite con quelle nuove predefinite.
8. Ripristinare le impostazioni da IBM Client Security Software Versione 4.0x completando la seguente procedura:
   a. Fare clic su **Start > Impostazioni > Pannello di controllo > IBM Client Security Subsystem**.

      Viene visualizzata la finestra principale IBM Client Security Software Administrator Utility.
   b. Fare clic sul pulsante **Configurazioni chiavi**.
   c. Selezionare **Sì** per ripristinare le chiavi dall'archivio delle chiavi.
9. Fornire la posizione della directory dell'archivio precedente.
10. Fornire la posizione dei file della chiave privata e pubblica del responsabile, creati nel release precedente.

Sarà notificato l'aggiornamento dell'archivio per il nuovo release.

11. Fare clic su **OK**.
12. Fornire la posizione per creare le nuovi chiavi del responsabile. Creare le chiavi in una posizione diversa dalla posizione delle chiavi del responsabile esistenti. Se si dispongono di chiavi del responsabile create per Release 5.0 su un altro sistema, è possibile selezionare **Utilizza una chiave doppio dell'archivio CSS esistente** e fornire la posizione delle chiavi esistenti.
13. Fare clic su **Avanti**.

    L'archivio sarà convertito e ripristinato.
14. Una volta terminato, uscire dall'applicazione.
15. Ripristinare le impostazioni della politica completando la seguente procedura:
    a. Utilizzando Windows Explorer, passare alla directory di installazione di IBM Client Security Software (la directory predefinita è c:\program files\ibm\security).
    b. Utilizzando il tastino sinistro del mouse, trascinare la cartella Politica_UVM dal desktop alla directory di installazione di IBM Client Security Software.
    c. Fare clic su **Sì** a tutti i messaggi di avvertenza.

    I dati di sicurezza sono stati migrati a Client Security Software Release 5.0.

Nota: se la politica di sicurezza è stata modificata precedentemente in Client Security Software Versione 4.0x, è possibile inoltrare di nuovo le impostazioni della politica di sicurezza completando la seguente procedura:

1. Fare clic su **Start > Impostazioni > Pannello di controllo > IBM Client Security Subsystem**.
2. Fare clic sul pulsante **Configura politica e supporto dell'applicazione**.
3. Fare clic sul pulsante **Politica applicativa**.
4. Fare clic sul pulsante **Modifica politica**.

Aggiornamento da Release 5.1 a versioni successive utilizzando i dati di sicurezza esistenti

Se si desidera aggiornare Client Security Software Versione 5.0 a versioni successive mediante i dati di sicurezza esistenti, completare la seguente procedura:

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

      Annotarsi la directory di archivio.
   c. Uscire dal programma IBM Client Security Software User Configuration Utility.
2. Rimuovere la versione esistente del programma Client Security Software completando la seguente procedura:
   a. Individuare le chiavi private e pubbliche del responsabile, create quando è stata configurata la versione precedente di Client Security Software.
   b. Eseguire il file csec51.exe.
   c. Selezionare **Aggiorna**.
   d. Riavviare il sistema.

Disinstallazione di Client Security Software

Accertarsi di disinstallare i vari programmi di utilità che potenziano la funzionalità 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, 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 **Sì** per disinstallare il software.
8. Procedere nel modo seguente:
   - Se è stato installato Security Chip integrato IBM modulo PKCS#11 per Netscape, viene visualizzato un messaggio in cui viene richiesto di avviare il processo per disattivare il modulo PKCS#11 di Security Chip integrato IBM. 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 Security Chip integrato IBM 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.
9. Fare clic su **OK** dopo aver eliminato 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. Tuttavia, l'archivio della chiave non è influenzato quando Client Security Software è disinstallato.

Capitolo 5. Risoluzione dei problemi

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

Funzioni del responsabile

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

Impostazione di una password responsabile (ThinkCentre)

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

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

Attenzione:

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

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

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

Per impostare una password di responsabile:

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

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

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

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

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

Impostazione di una password del supervisore (ThinkPad)

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

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

Attenzione:

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

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

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

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

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

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

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

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

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

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

Protezione di una password per l'hardware

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

Annullamento di IBM embedded Secutity Chip (ThinkCentre)

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

Attenzione:

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

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

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

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

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

Annullamento di IBM embedded Security Chip (ThinkPad)

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

Attenzione:

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

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

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

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

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

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

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

Administrator Utility

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

Rimozione di utenti

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

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

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

Limiti

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

Utilizzo di Client Security Software con sistemi operativi Windows

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

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

Utilizzo di Client Security Software con applicazioni Netscape

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

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

- SHA-1
- MD5

Certificato IBM embedded Security Chip e algoritmi di cifratura

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

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

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

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

Utilizzo della protezione UVM per un ID utente Lotus Notes

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

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

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

Limiti di User Configuration Utility

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

Windows XP Professional

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

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

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

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

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

Windows XP Home

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

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

Messaggi di errore

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

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

Prospetti per la risoluzione dei problemi

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

Informazioni sulla risoluzione dei problemi relativi all'installazione

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

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

Informazioni sulla risoluzione dei problemi del programma Administrator Utility

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

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

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

Informazioni sulla risoluzione dei problemi del programma User Configuration Utility

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

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

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

Informazioni sulla risoluzione dei problemi specifici al ThinkPad

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

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

Informazioni sulla risoluzione dei problemi della Microsoft

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

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

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

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

Informazioni sulla risoluzione dei problemi dell'applicazione Netscape

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

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

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

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

Informazioni sulla risoluzione dei problemi relativi al certificato digitale

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

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

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

Informazioni sulla risoluzione dei problemi di Tivoli Access Manager

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

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

Informazioni sulla risoluzione dei problemi relativi a Lotus Notes

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

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

Informazioni sulla risoluzione dei problemi relativi alla cifratura

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

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

Informazioni sulla risoluzione dei problemi relativi all'unità UVM

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

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

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

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

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

Appendice B. Regole per password e passphrase

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

Regole per la password hardware

Le seguenti regole si applicano alla password hardware:

Lunghezza
Le password devono essere costituite esattamente da otto caratteri.

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

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

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

Regole per passphrase UVM

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

  Quando viene selezionata questa opzione, il passphrase non scade.

La politica 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 inserisce il passphrase UVM in modo non corretto per più volte

durante una sessione, il computer non viene bloccato. Non è presente alcun limite sul numero dei tentativi errati.

Appendice C. Marchi e informazioni particolari

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

Informazioni particolari

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

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

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

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

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

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

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

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

Marchi

IBM e SecureWay sono marchi IBM Corporation.

Tivoli è un marchio Tivoli Systems Inc.

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

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

Riservato ai commenti del lettore

IBM® Client Security
Solutions
Guida all'installazione di Client Security Software versione 5.1

Numero parte 59P7641

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

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

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

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

Commenti:

Si ringrazia per la collaborazione.

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

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

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

Nome

Indirizzo

Società

Numero di telefono

Indirizzo e-mail

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

Selfin S.p.A.
Translation Assurance

Via F. Giordani, 7

80122 NAPOLI

Numero parte: 59P7641

Printed in Denmark by IBM Danmark A/S

(1P) P/N: 59P7641