IBM® Client Security
Solutions

Utilizzo di Client Security Software versione 5.1 con Tivoli® Access Manager

IBM® Client Security
Solutions

Utilizzo di Client Security Software versione 5.1 con Tivoli® Access Manager

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 31 e l’Appendice D, “**Marchi e informazioni particolari**”, a pagina 39.

© Copyright International Business Machines Corporation 2002. Tutti i diritti riservati.

Indice

© Copyright IBM Corp. 2002

Prefazione

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

Questa guida è organizzata nel modo seguente:

″Capitolo 1, "**Introduzione 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. Installazione del componente Client Security su un server di Tivoli Access Manager″, contiene i prerequisiti e le istruzioni per l'installazione del supporto Client Security sul server Tivoli Access Manager.

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

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

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

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

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

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

A chi si rivolge questa guida

Questa guida si rivolge agli amministratori di aziende che utilizzeranno Tivoli Access Manager versione 3.8 e versione 3.9 per gestire gli oggetti di autenticazione impostati dalla politica di sicurezza UVM (User Verification Manager) su un client IBM.

Gli amministratori devono essere a conoscenza dei seguenti concetti e procedure:

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

© Copyright IBM Corp. 2002

Modalità di utilizzo di questa guida

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

Questa guida e 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 *Guida all'installazione di Client Security Software*

I riferimenti al manuale *Guida all'installazione di Client Security Software* vengono forniti in questo documento. Dopo aver impostato e configurato il server di Tivoli Access Manager ed installato l'ambiente di esecuzione sul client, utilizzare le istruzioni contenute nella *Guida all'installazione di Client Security Software* per installare Client Security Software sui client IBM. Per ulteriori informazioni, consultare il Capitolo 3, "Configurazione dei client IBM", a pagina 9.

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

I riferimenti al manuale *Client Security Software Guida per il responsabile* vengono forniti in questo documento. *La guida per il responsabile di Client Security Software* contiene informazioni su come impostare l'autenticazione utente e la politica UVM per il client IBM. Una volta installato Client Security Software, utilizzare il manuale *Guida per il responsabile di Client Security Software* per impostare l'autenticazione utente e la politica della sicurezza. Per ulteriori informazioni, consultare il Capitolo 3, "Configurazione dei client IBM", a pagina 9.

Ulteriori informazioni

E' possibile ottenere ulteriori informazioni e aggiornamenti del prodotto di sicurezza, se disponibili, in
http://www.pc.ibm.com/ww/security/securitychip.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.

© Copyright IBM Corp. 2002

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

L'autenticazione degli utenti finali a livello di client è un problema di politica di 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 principale componente di Client Security Software.

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

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

Prima di poter utilizzare Client Security con Tivoli Access Manager, è necessario installare il componente Client Security di Tivoli Access Manager. Questo componente può essere scaricato dal sito web IBM http://www.pc.ibm.com/ww/security/secdownload.html.

Prerequisiti

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

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

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

Scaricamento e installazione del componente Client Security

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

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

1. Utilizzando le informazioni sul sito Web, verificare che IBM 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**.
2. Selezionare il pallino che corrisponde al Tipo di macchina e fare clic su **Continua**.
3. Creare un ID utente, effettuare la registrazione presso la IBM compilando il modulo in linea e consultare l'Accordo di licenza; quindi, fare clic su **Accetto la licenza**.

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

© Copyright IBM Corp. 2002

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

      Viene visualizzata la finestra Welcome to the InstallShield Wizard for IBM Client Security Software.
   d. Fare clic su **Avanti**.

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

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

Aggiunta del componente Client Security sul server di Tivoli Access Manager

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

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

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

Il comando di seguito riportato è un esempio per creare l'object space IBM Solutions, le azioni di Client Security e le singole voci ACL sul server di Tivoli Access Manager:

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

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

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

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

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

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

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

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

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

E' necessario inserire i seguenti parametri:

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

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

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

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

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

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

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

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

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

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

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

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

Capitolo 3. Configurazione dei client IBM

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

Prerequisiti

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

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

Configurazione delle informazioni di impostazione di Tivoli Access Manager

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

- Selezione del percorso completo del file di configurazione
- Selezione dell'intervallo di aggiornamento della cache locale

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

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

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

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

© Copyright IBM Corp. 2002

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

6. Fare clic sul pulsante **Politica applicativa**.
7. Fare clic sul pulsante **Modifica politica**.

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

   Viene visualizzato il pannello IBM UVM Policy.
9. Selezionare le azioni da controllare da Tivoli Access Manager nel menu a discesa Azioni.
10. Selezionare la casella Access Manager controlla l'oggetto selezionato in modo da rendere visibile un segno di spunta nella casella.
11. Fare clic sul pulsante **Applica**.

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

Impostazione ed uso della funzione di cache locale

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

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

1. Fare clic su **Avvio > Programmi > Client Security Software > Administrator Utility**.
2. Immettere la password per l'hardware e fare clic su **OK**.

   Viene visualizzata la finestra Administrator Utility. Per informazioni complete sull'uso di Administrator Utility, consultare la *guida alla gestione di Client Security Software*.
3. In Administrator Utility fare clic sul pulsante **Configura politica e supporto dell'applicazione**.

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

Abilitazione di Access Manager per controllare gli oggetti del client IBM

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

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

Importante: l'attivazione di Tivoli Access Manager per il controllo di un oggetto fornisce il controllo dell'object space di Tivoli Access Manager. In tal caso, è necessario installare di nuovo Client Security Software per ristabilire il controllo locale su quell'oggetto.

Modifica di una politica UVM locale

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

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

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

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

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

   Viene visualizzato il pannello Modifica configurazione politica di Client Security.
2. Fare clic sul pulsante **Modifica politica**.

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

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

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

   Importante: l'attivazione di Tivoli Access Manager per il controllo di un oggetto fornisce il controllo dell'object space di Tivoli Access Manager. In tal caso, è necessario installare di nuovo Client Security Software per ristabilire il controllo locale su quell'oggetto.

   Nota: durante la modifica della politica UVM, è possibile visualizzare le informazioni di riepilogo della politica facendo clic su **Riepilogo della politica**.
6. Fare clic su **Applica** per salvare le modifiche apportate.

7. Fare clic su **OK** per uscire.

Modifica e utilizzo della politica UVM per i client remoti

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

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

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

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

Capitolo 4. Risoluzione dei problemi

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

Funzioni del responsabile

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

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.

© Copyright IBM Corp. 2002

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).

© Copyright IBM Corp. 2002

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 numerici 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)

© Copyright IBM Corp. 2002

Ad esempio, quando è stabilito,aaabcdefghijk è una password non valida.

- Stabilire se consentire che il passphrase termini 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. Regole sull'uso della protezione UVM per il collegamento del sistema

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

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

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

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

© Copyright IBM Corp. 2002

Appendice D. Marchi e informazioni particolari

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

Informazioni particolari

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

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

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

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

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

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

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

© Copyright IBM Corp. 2002

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
Utilizzo di Client Security Software versione 5.1 con Tivoli® Access
Manager

Numero parte 59P7643

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: 59P7643

Printed in Denmark by IBM Danmark A/S

(1P) P/N: 59P7643