Soluzioni IBM® Client Security

Password Manager Versione 1.4 - Guida per l'utente

Soluzioni IBM® Client Security

Password Manager Versione 1.4 - Guida per l'utente

Prima edizione (Ottobre 2004)

Indice

Prefazione

Questa guida contiene informazioni sul programma IBM Client Security Password Manager relative alla gestione e al richiamo delle informazioni di collegamento sensibili.

La guida è organizzata nel modo seguente:

Capitolo 1, “Introduzione a IBM Client Security Password Manager” contiene una panoramica delle funzioni di IBM Password Manager.

Capitolo 2, “Procedure” contiene le procedure relative all’impostazione, al richiamo e alla gestione delle informazioni sensibili mediante il programma IBM Client Security Password Manager.

La sezione Capitolo 3, “Limitazioni” contiene utili informazioni per conoscere i problemi e le limitazioni che si possono verificare durante l’utilizzo delle istruzioni, fornite in questa guida.

A chi si rivolge questa guida

Questa guida è specifica per gli utenti di Client Security Software Versione 4.0 o superiori che desiderano conservare traccia di tutti i relativi ID utente, tutte le password e le informazioni personali, utilizzati per la registrazione ed il collegamento ai siti Web o alle applicazioni.

IBM Client Security Password Manager Versione 1.4 supporta i sistemi operativi Windows 2000 e Windows XP.

Modalità di utilizzo di questa guida

Questa guida è stata progettata per aiutare l’utente ad utilizzare IBM Client Security Password Manager per semplificare le procedure di collegamento e la gestione delle password.

E’ possibile trovare questa guida e tutta la documentazione relativa a Client Security sul sito web IBM all’indirizzo http://www.pc.ibm.com/us/security/index.html.

Ulteriori informazioni

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

Capitolo 1. Introduzione a IBM Client Security Password Manager

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

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

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

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

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

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

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

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

  IBM Password Manager consente di generare password casuali per ciascun sito Web o per ciascuna applicazione. Ciò consente di implementare la protezione dei dati poiché a ciascuna applicazione sarà abilitata un'ulteriore protezione per password. Le password casuali sono molto più sicure delle password personalizzate poiché la maggior parte degli utenti utilizza le informazioni personali facili da ricordare per password facili da dimenticare.
- **Modificare le voci utilizzando l'interfaccia Password Manager**

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

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

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

- **Archiviare le informazioni di collegamento**

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

Capitolo 2. Procedure

In questa sezione sono descritte le principali funzioni di IBM Client Security Password Manager.

Creazione delle nuove voci

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

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

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

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

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

   Nota: Questa casella di controllo consente di selezionare il modo in cui viene visualizzato il testo in Password Manager. Una volta rilasciato il testo in un sito Web o in un'applicazione, le relative proprietà saranno controllate da tale applicazione.
5. Utilizzare l'icona di ″destinazione″ Seleziona campo per trascinare il testo dal programma di utilità Password Manager nel campo appropriato sul sito Web o nell'applicazione.

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

Nota: alcuni siti Web non utilizzano il tasto Invio per inoltrare le informazioni di collegamento. Se il collegamento non viene eseguito correttamente, disabilitare questa funzione.

10. Per completare la procedura, fare clic su **Salva nuova voce**.

Richiamo delle voci

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

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

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

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

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

Gestione delle voci

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

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

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

   Nota: Inoltre, è possibile accedere alla funzion Password Manager - Gestisci mediante i tasti di scelta rapida **Ctrl+Maiusc+B**.
2. Inserire la password UVM o completare i requisiti di accesso, specificati dalla politica di autenticazione utente UVM.
3. Modificare le informazioni. Selezionare le seguenti opzioni:
   - Informazioni sulla voce

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

– Aggiungi ″Invio″

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

– Elimina

Selezionare Elimina per eliminare la voce in modo completo.

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

- Informazioni sul campo Voce

Per modificare le informazioni sul campo Voce, completare la seguente procedura:

a. Fare clic con il tastino destro del mouse sul campo che si desidera modificare.

b. Selezionare le seguenti azioni:

– Campo Modifica voce

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

- Creando una voce casuale

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

- Modificando manualmente un campo di voce

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

– Elimina

Selezionare Elimina per eliminare completamente il campo relativo alla voce.

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

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

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

Esportazione delle informazioni di collegamento

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

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

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

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

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

Capitolo 3. Limitazioni

Questa sezione contiene informazioni sulle limitazioni del prodotto IBM Client Security Password Manager.

IBM Client Security Password Manager non supporta Netscape Navigator: per una completa funzionalità del programma IBM Password Manager, è necessario utilizzare Microsoft Internet Explorer. Il software Password Manager non supporta Netscape Navigator.

Appendice. Marchi e informazioni particolari

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

Informazioni particolari

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

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

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

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

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

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

Coloro che detengono la licenza su questo programma e desiderano avere informazioni su di esso allo scopo di consentire (1) uno scambio di informazioni tra programmi indipendenti ed altri (compreso questo) e (ii) l'uso reciproco di tali informazioni, dovrebbero rivolgersi a IBM Corporation, Department 80D,P.O. Box 12195, 3039 Cornwallis, Research Triangle Park, NC 27709 U.S.A. Queste

informazioni possono essere rese disponibili secondo condizioni contrattuali appropriate, compreso, in alcuni casi, il pagamento di un addebito.

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

Marchi

IBM e SecureWay sono marchi IBM Corporation.

Tivoli è un marchio Tivoli Systems Inc.

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

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

Stampato in Italia