

# ***PROTECTOR SUITE QL***

***versione 5.4***

***TouchChip***

## **Informazioni sul copyright e sulla proprietà**

Le informazioni fornite si suppongono essere accurate e affidabili. Tuttavia, UPEK<sup>®</sup>, Inc non si ritiene responsabile per qualsivoglia conseguenza d'uso di tali informazioni né per qualsiasi violazione di brevetti o di altri diritti di terze parti risultanti dall'uso stesso. Nessun diritto di licenza viene concesso, tacitamente, per preclusione o per qualsivoglia altro motivo, in base a qualsiasi brevetto o altro diritto di UPEK, Inc. Le informazioni contenute nella presente pubblicazione sono soggette a modifiche senza preavviso. Questa pubblicazione sostituisce tutte le informazioni fornite in precedenza. I prodotti di UPEK, Inc non sono autorizzati per l'uso in dispositivi o sistemi medicali di supporto vitale senza espressa approvazione scritta di UPEK, Inc.

Il logo UPEK è un marchio registrato di UPEK, Inc.

© 2004-2006 UPEK<sup>®</sup>, Inc – Tutti i diritti riservati

Tutti gli altri nomi sono proprietà dei rispettivi proprietari.

UPEK<sup>®</sup>, Inc

**<http://www.upek.com>**

Questo prodotto include il software sviluppato da OpenSSL Project da usare con OpenSSL Toolkit (<http://www.openssl.org/>).

Questo prodotto include software crittografico scritto da Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)).

## **Marchi registrati**

TouchChip<sup>®</sup>, Protector Suite<sup>™</sup> sono marchi registrati di UPEK, Inc. Tutti gli altri prodotti descritti nella pubblicazione sono marchi registrati dei rispettivi proprietari e devono essere trattati in quanto tali.

A close-up photograph of a person's hand touching a fingerprint sensor. The sensor is a circular device with a grid of small dots. The hand is positioned over the sensor, with the index finger making contact. The background is a soft, out-of-focus yellow and orange gradient.

## Capitolo 1

# Installazione

Benvenuti in Protector Suite QL. Il software viene utilizzato con Windows 2000 e Windows XP (con supporto speciale per la funzionalità Cambio rapido utente). Per offrire ulteriore praticità, Protector Suite QL introduce i metodi biometrici delle impronte digitali.

Registrate le vostre impronte digitali e sarete in grado di utilizzare le vostre dita per:

- *accedere e bloccare il computer,*
- *visualizzare e compilare le pagine Web preferite,*
- *compilare le finestre di dialogo utilizzate frequentemente,*
- *proteggere i file sensibili,*
- *eseguire le applicazioni preferite,*
- *utilizzare la funzione di scorrimento attraverso il sensore invece della rotellina del mouse.*

## Installazione

È possibile installare Protector Suite QL su qualsiasi computer equipaggiato con Windows 2000 o Windows XP, edizioni Home o Professional, e una porta USB libera. Per installare o disinstallare l'applicazione Protector Suite QL occorre disporre dei diritti di amministratore.

### Per installare Protector Suite QL:

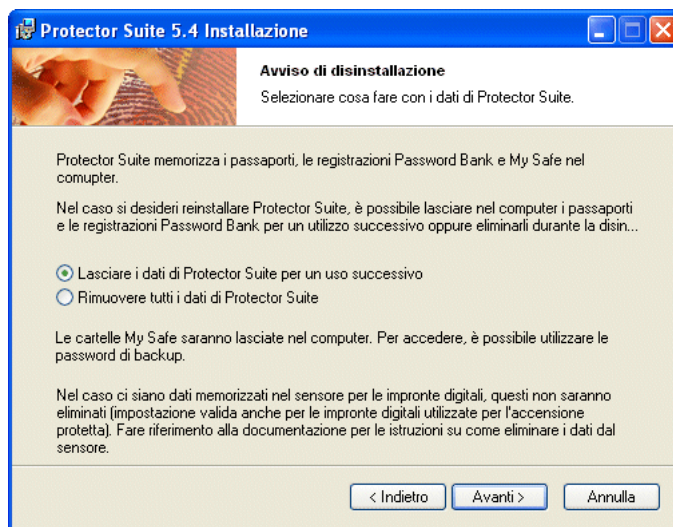
- 1 *È possibile che il software sia già pre-installato. Una procedura guidata all'installazione illustrerà il processo.*
- 2 *Leggere e confermare il contratto di licenza. Nel caso di non accettazione del contratto di licenza, l'installazione non potrà proseguire.*
- 3 *Inserire nome utente e società.*
- 4 *Selezionare la directory d'installazione di Protector Suite QL (la predefinita è Program Files\Protector Suite QL).*
- 5 *Alla fine dell'installazione, verrà richiesto di riavviare il computer. Protector Suite QL sarà attivo dopo il riavvio.*

Durante l'installazione, tutti i driver hardware necessari vengono pre-installati. Connettete l'hardware dopo il riavvio (se non si dispone di un lettore d'impronte digitali integrato) e potrete iniziare a utilizzare Protector Suite QL.

## Rimozione

Per disinstallare Protector Suite QL, selezionare **Start – Impostazioni – Pannello di controllo** e aprire **Installazione applicazioni**.

Selezionare Protector Suite QL e fare clic sul pulsante **Cambia**. Selezionare l'opzione **Rimuovi**.



Verrà richiesto cosa fare dei dati di Protector Suite QL memorizzati nel computer.

Esistono due opzioni:

È possibile lasciare tutti i dati nel computer. Questo significa che, nel caso si esegua una nuova installazione di Protector Suite QL successivamente, sarà possibile continuare a utilizzare le impronte digitali registrate e le registrazioni Password Bank.

OPPURE

È possibile rimuovere i dati di Protector Suite QL dal computer. Le impronte digitali registrate e le registrazioni Password Bank saranno eliminate in modo permanente.

**Nota:** se si è utilizzato l'opzione di registrazione sul proprio lettore d'impronte digitali, i dati rimarranno nella memoria del dispositivo. Le istruzioni su come cancellare la memoria del dispositivo da Protector Suite QL possono essere trovate nel capitolo 3.

I file e le cartelle memorizzati nelle cartelle **My Safe** non vengono eliminati durante la rimozione del programma. Sarà possibile utilizzarle successivamente se si esegue una nuova installazione di Protector Suite QL. Sarà possibile accedere utilizzando le password di backup inserite durante la creazione di **My Safe**. Comunque, se l'utente ha creato un'ampia cartella **My Safe** e non si è pianificato di utilizzarla successivamente, si raccomanda di eliminare tale cartella prima di disinstallare il prodotto. Per eliminare **My Safe**, fare clic sul pulsante **Elimina** nella finestra di dialogo **Control Center – Impostazioni – Impostazioni utente – My Safe**.





A hand is shown touching a fingerprint sensor on a device. The sensor is a circular area with a grid pattern. The hand is positioned over the sensor, with the index finger touching it. The background is a light yellow color with a subtle grid pattern.

## Capitolo 2

# Introduzione

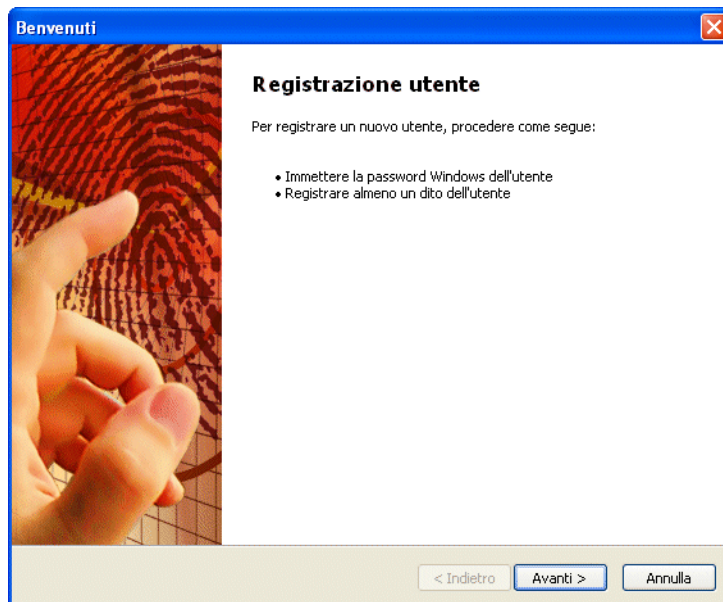
L'installazione di Protector Suite QL è stata appena completata oppure il prodotto è pre-installato sul computer. Questo capitolo vi guiderà attraverso i primi passi nell'utilizzo di Protector Suite QL. Per questo capitolo, supponiamo lo scenario più semplice: si è l'unico utente del computer, con diritti di amministratore ed è impostata la predefinita modalità pratica di Protector Suite QL.

Per una descrizione dettagliata delle funzionalità individuali di Protector Suite QL e delle differenze in altri scenari, consultare il prossimo capitolo.

## Primo utilizzo – Registrazione utente

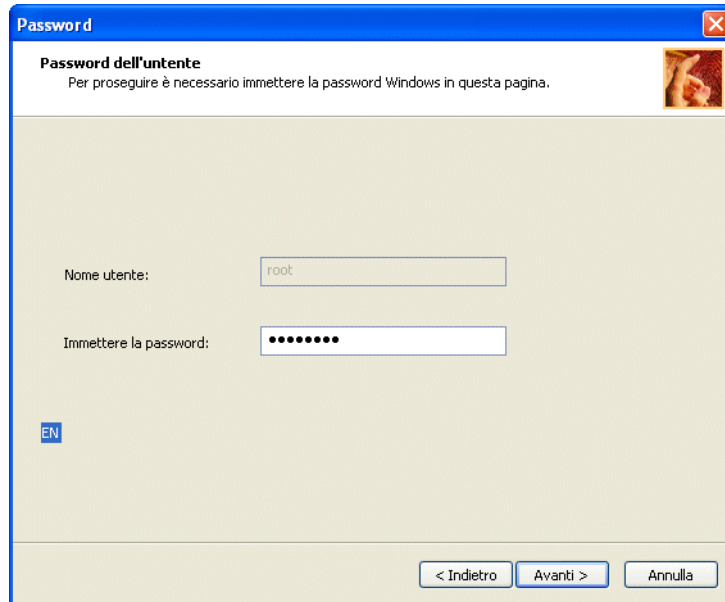
- 1 *Se desiderate utilizzare un sensore per le impronte digitali esterno, connettete la periferica. Tutti i driver necessari sono stati installati con Protector Suite QL. Nell'angolo inferiore destro dello schermo, viene visualizzato un messaggio informativo relativamente al fatto che il sensore è stato collegato ed è pronto all'uso. Nel caso di problemi con l'hardware, vedere il capitolo **Risoluzione dei problemi** di questa guida.*
- 2 *Avviare **Registrazione utente** dal menu **Start**. Verrà chiesto di selezionare il tipo di registrazione. Se la periferica supporta la registrazione nella memoria della periferica, è possibile selezionare se memorizzare i dati di autenticazione nella memoria della periferica oppure sul disco rigido. Se si seleziona la registrazione nella memoria della periferica, non è possibile accedere ai dati senza la periferica per le impronte digitali corrispondente. Questo significa che è possibile proteggere i propri dati con una chiave crittografica software generata dal software per le impronte digitali insieme a una chiave di crittografia hardware ottenuta direttamente dalla periferica.*

*Introduzione alla registrazione. È possibile utilizzare pienamente tutte le funzionalità di Protector Suite QL se si è registrato almeno un dito. La procedura guidata della registrazione illustrerà la procedura di registrazione.*





### 3 *Immettere la password Windows.*



The screenshot shows a Windows dialog box titled "Password". Inside, the text "Password dell'utente" is followed by the instruction "Per proseguire è necessario immettere la password Windows in questa pagina." Below this, there are two input fields: "Nome utente:" with the text "root" entered, and "Immettere la password:" with a masked password of seven dots. A small "EN" button is located at the bottom left. At the bottom right, there are three buttons: "< Indietro", "Avanti >", and "Annulla".

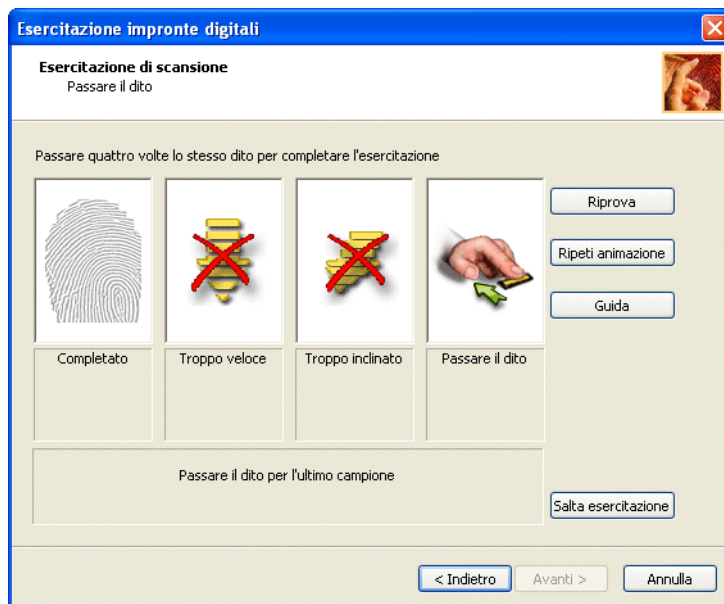
*Se non si utilizza la password Windows (la password Windows è vuota), se ne verrà informati e verrà richiesto se si desidera crearne una nuova.*  
**Suggerimento:** la creazione di una password Windows garantisce un maggiore protezione del proprio account utente di Windows.

- 4 *È estremamente raccomandato seguire l'Esercitazione Fingerprint. L'esercitazione può essere avviata dalla procedura guidata della registrazione oppure dal menu **Start**. L'esercitazione è costituita da tre pagine:*
- *La prima pagina illustra all'utente le finalità dell'esercitazione.*

- *La seconda pagina mostra la corretta procedura di scansione.*

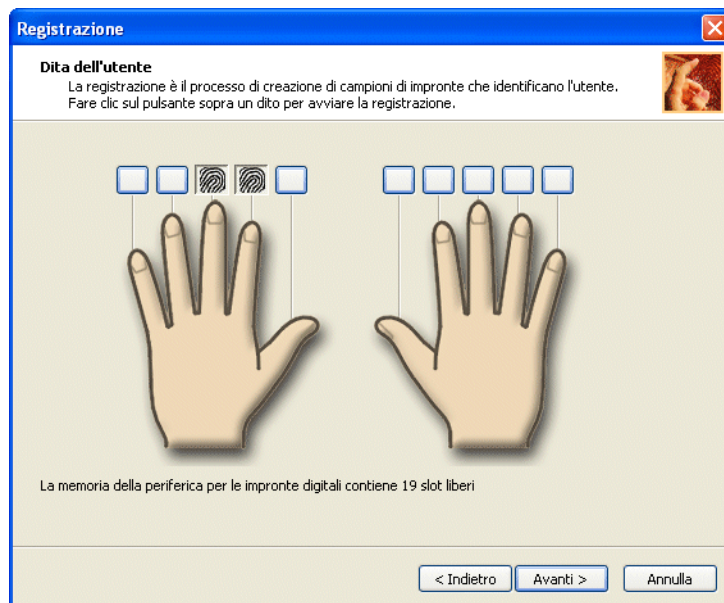


- Nella terza pagina, è possibile provare a creare quattro campioni delle proprie impronte digitali e farle corrispondere. Utilizzare il pulsante **Ripeti animazione** per richiamare il movimento corretto. Dopo aver creato correttamente i campioni, fare clic su **Fine** per chiudere l'esercitazione e tornare alla procedura guidata di registrazione

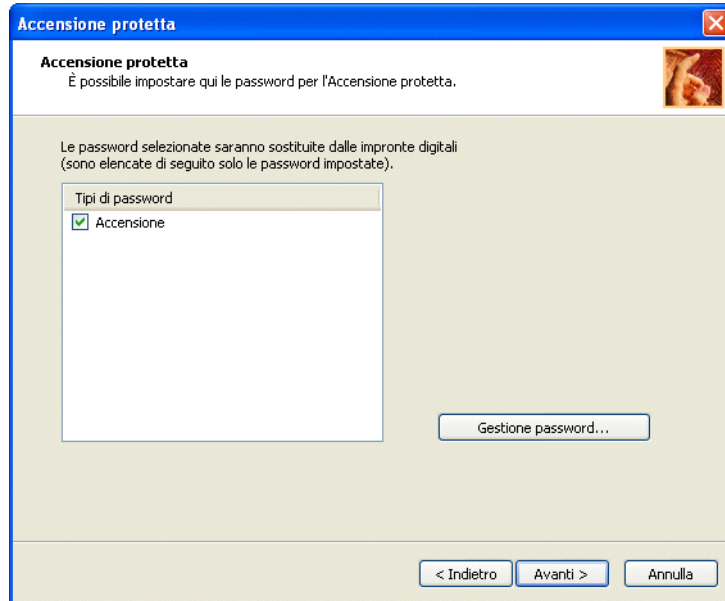


- 5 Fare clic sul pulsante sopra il dito per il quale si desidera eseguire la scansione. Creare tre campioni delle dita come illustrato nell'esercitazione. Da questi tre campioni verrà creato il modello finale. Nel caso in cui non si possa stabilire alcuna corrispondenza tra i tre campioni, verrà visualizzato un messaggio di avviso. In questo caso, si consiglia di ripetere l'esercitazione. È possibile registrare fino a dieci impronte digitali. **Si consiglia di registrare più di un dito nel caso in cui**

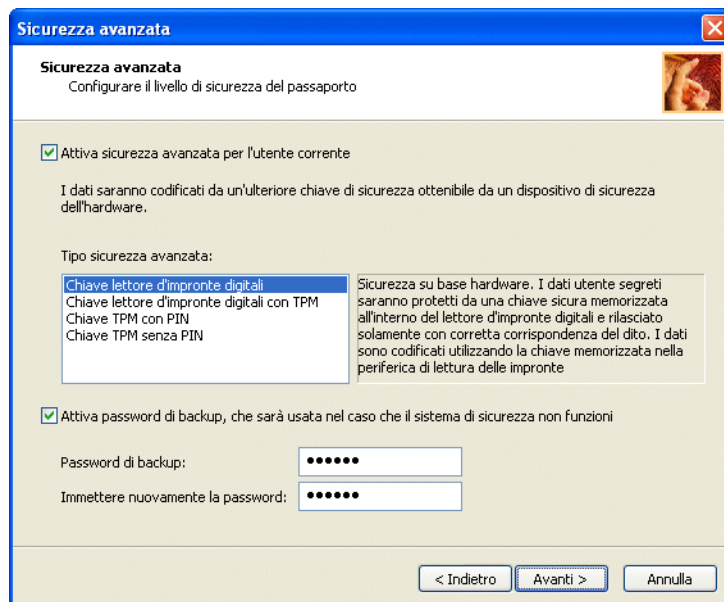
***si subisca una lesione; in questo modo sarà possibile superare la verifica biometrica necessaria per accedere alle funzionalità di Protector Suite QL.***



- 6 *Se il BIOS supporta password BIOS protette, verrà visualizzata una pagina di **accensione protetta**. Selezionare le password che saranno sostituite dalle impronte digitali. Verrà richiesto di immettere la password in seguito alla relativa selezione. La gestione delle password BIOS può essere effettuata dagli amministratori locali da qui. La selezione del pulsante **Gestione passaporto** consente di accedere alla finestra di dialogo **Password BIOS** in cui è possibile impostare, rimuovere l'impostazione o modificare i passaporti.*



- 7 Alcune configurazioni hardware forniscono una protezione supplementare dei dati tramite la crittografia. In tali configurazioni viene visualizzata una finestra di dialogo aggiuntiva con un tipo di Protezione avanzata. Selezionare il tipo di Protezione avanzata. Per ulteriori informazioni sulla protezione avanzata, vedere il capitolo 3. **Si raccomanda di impostare la password di backup.** Può rivelarsi utile nel caso in cui non sia possibile effettuare l'autenticazione biometrica.



- 8 *Una volta completata la procedura guidata della registrazione, una schermata di **Introduzione** visualizza le possibili modalità di utilizzo delle impronte digitali con Protector Suite QL.*

*Dopo aver registrato le impronte digitali, è possibile utilizzare il proprio dito:*

- *per accedere all'account del computer,*
- *per visualizzare il Biomenu con tutte le sue funzionalità (blocco del computer, registrazione di pagine, finestre di dialogo, accesso alla cartella My Safe, ecc.). È possibile eseguire la navigazione nel Biomenu muovendo il proprio dito sul sensore.*
- *per compilare finestre di dialogo o moduli Web registrati.*
- *per avviare le applicazioni preferite.*

**NOTA:** ogni utente Windows può avere un solo passaporto. Per creare un account utente, selezionare **Start – Impostazioni – Pannello di controllo** e fare clic su **Account utente**. Seguire le istruzioni visualizzate.



## Accesso alle principali funzioni di Biomenu

Una volta che le impronte digitali sono registrate, è possibile avviare l'inizializzazione delle varie azioni con il proprio dito. Passare il dito per visualizzare il **Biomenu**..

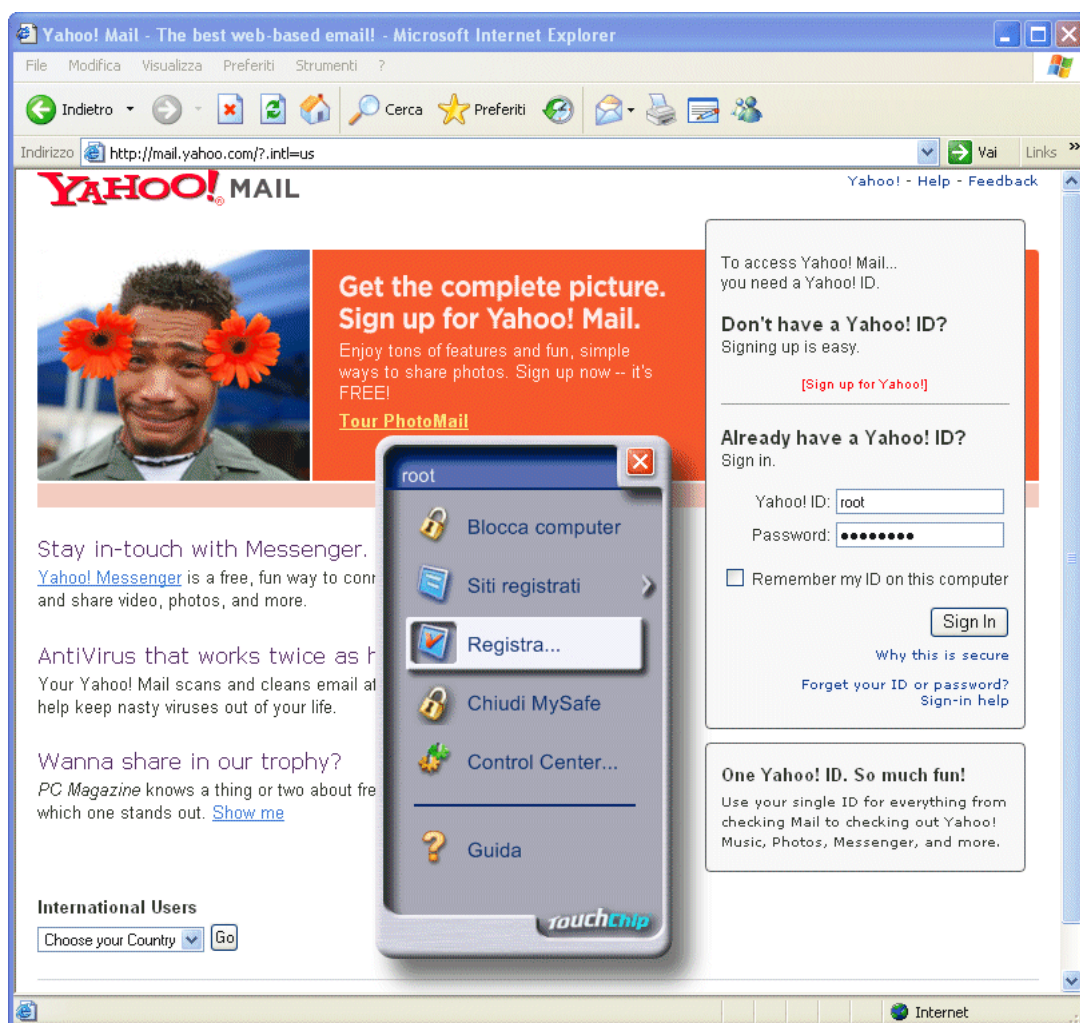


Il **Biomenu** fornisce l'accesso alle funzionalità di Protector Suite QL. Per forzare la visualizzazione di **Biomenu** in situazioni in cui il passaggio del dito si rivolge ad altre azioni (per esempio, una finestra registrata è attiva), tenere premuto il tasto **Maiusc** e passare il dito. **Biomenu** supporta la bio-navigazione. Questo significa che è possibile utilizzare il sensore invece del mouse per la navigazione. Muovere il dito per navigare all'interno del **Biomenu** e toccare l'elemento evidenziato per eseguire l'azione corrispondente.

## Registrazione di pagine web e finestre di dialogo in Password Bank

Molte pagine Web e altre applicazioni richiedono l'immissione di vari dati, nome utente, password e altre informazioni, ogni volta che vengono visualizzate. Password Bank è la soluzione giusta per tali situazioni. Si compilano le informazioni (o si impostano le opzioni necessarie) e si registra la finestra. Quando si accede alla pagina o alla finestra di dialogo in un secondo momento, è possibile riprodurre le informazioni memorizzate passando il dito sopra al sensore.

Aprire il browser e andare alla pagina che si desidera registrare (o visualizzare la finestra di dialogo che si desidera registrare). Inserire tutte le informazioni che si desidera avere nella registrazione. Passare il dito per visualizzare il **Biomenu**. Selezionare **Registra...**



Tutti i dati personali sono stati memorizzati. Viene visualizzato un messaggio che informa della riuscita creazione della registrazione.

È possibile accedere alla pagina Web registrata direttamente da **Biomenu – Siti registrati**.



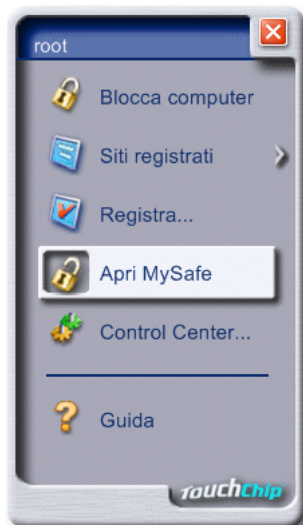
Per riprodurre le informazioni registrate in una finestra di dialogo o in un pagina Web, è sufficiente passare il dito sul sensore alla visualizzazione della finestra di dialogo o della pagina Web. I dati memorizzati nella registrazione saranno inseriti nel modulo in modo automatico.

Per ulteriori informazioni su Password Bank e le possibili impostazioni, vedere “Password Bank” a pagina 28 e “Impostazioni” a pagina 42.

## Protezione dei file sensibili in My Safe

Se il computer è accessibile anche ad altri utenti, è possibile procedere alla creazione di un'area di memorizzazione crittografata. My Safe è il luogo in cui memorizzare i file sensibili che sono accessibili solamente attraverso l'utilizzo dell'impronta personale.

Per utilizzare My Safe, passare il dito e selezionare **Apri My Safe** da **Biomenu**.



Prima di utilizzarla per la prima volta, è necessario creare **My Safe**. Una procedura guidata illustrerà il processo.

Verrà chiesto di creare una password di backup per My Safe. È possibile utilizzare questa password per aprire **My Safe** in caso di guasto della periferica biometrica. È necessario che la password di backup sia lunga almeno 8 caratteri.

Crea My Safe

✕

**Password di backup**

La password di backup è lo strumento di emergenza per accedere a My Safe in caso di problemi.

Password backup (8 o più caratteri):

••••••••

Conferma password backup:

••••••••

Si raccomanda vivamente di trascrivere la password e conservarla in un luogo sicuro.  
In caso di problemi gravi, la password può risultare l'UNICO strumento per accedere ai dati in My Safe.

< Indietro

Avanti >

Annulla

Impostare le dimensioni di **My Safe**. La dimensione predefinita è di 50 MB. È possibile ridimensionare la cartella **My Safe** successivamente. Il ridimensionamento non influisce sui dati memorizzati.

È possibile posizionare qualsiasi file o cartella in **My Safe** proprio come in qualsiasi altra cartella. È possibile trovare **My Safe** in **Documenti**. Una volta completato il proprio lavoro, è sufficiente selezionare **Chiudi My Safe** da **Biomenu** e i file sensibili personali non saranno visibili né accessibili da nessun altro.

Per ulteriori informazioni su come lavorare con **My Safe**, vedere “**My Safe**” a pagina 33.



# Control Center

Il Control Center costituisce un'interfaccia utente comune per tutte le impostazioni di Protector Suite QL. L'elenco completo delle funzioni disponibili è riportato in pagina 36.

## Per utilizzare il Control Center di Protector Suite QL:

- *Selezionare **Start – Programmi – Protector Suite QL – Control Center**.*
- *oppure scegliere **Control Center** da **Biomenu**,*
- *oppure scegliere **Avvia Control Center...** dall'icona sulla barra delle applicazioni.*

## Avvio delle applicazioni

È possibile avviare un'applicazione (qualsiasi file eseguibile) sul proprio computer attraverso la scansione del dito assegnato. Per ulteriori informazioni sull'utilità di avvio dell'applicazione, vedere pagina 49.

**Per creare l'associazione tra il dito registrato e un'applicazione:**

- 1 *Aprire **Control Center**, selezionare **Impostazioni – Impostazioni utente**. Passare il dito per eseguire la verifica.*
- 2 *Selezionare la scheda **Applicazioni**.*
- 3 *Fare clic sul pulsante **Aggiungi**. Verrà visualizzata la finestra di dialogo **Applicazione**.*
- 4 *Selezionare un dito registrato dall'elenco.*
- 5 *Inserire il nome dell'applicazione. Tale nome è visualizzato nella pagina **Applicazioni in Impostazioni utente**.*
- 6 *Cercare l'applicazione che si desidera avviare: è necessario che tale file sia un file eseguibile.*
- 7 *A scelta, immettere qualsiasi parametro dell'applicazione necessario.*
- 8 *Scegliere **OK**.*

## Cambio rapido utente

È supportata anche la funzionalità Cambio rapido utente di Windows XP. Se un utente A è connesso e l'utente B (già registrato) passa un dito sul sensore, Protector Suite QL riconosce l'impronta digitale e passa da un utente all'altro.

Per attivare il supporto della funzionalità Cambio rapido utente, accedere a **Control Center – Impostazioni – Impostazioni del sistema**, quindi selezionare la casella di controllo **Abilita il supporto del cambio rapido utente**. L'opzione è visibile solo nel caso si stia utilizzando XP ed è disponibile solo in computer non membri di alcun dominio. Se il sistema non supporta la funzione di Cambio rapido utente, seguire le istruzioni visualizzate. In seguito a tale modifica può essere necessario riavviare il computer.





## Capitolo 3

# Riferimento

Questo capitolo descrive nel dettaglio tutte le funzionalità di Protector Suite QL.

**Registrazione**

**Biomenu**

**Accesso tramite impronte digitali**

**Password Bank**

**My Safe**

**Utilità di avvio dell'applicazione**

**Control Center**

**Icona sulla barra delle applicazioni**

# Registrazione

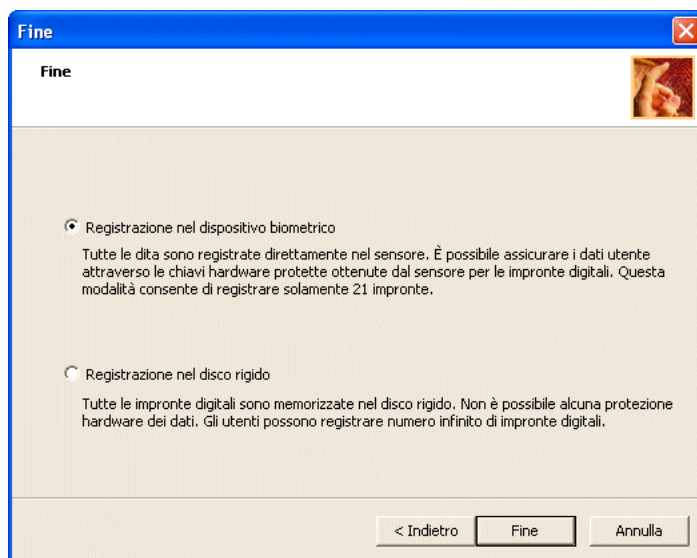
Prima di iniziare a utilizzare Protector Suite QL con tutte le funzionalità, è necessario *effettuare la registrazione*. La registrazione è il processo di creazione della corrispondenza tra nome utente e password e le impronte digitali (computerizzato in modo che sia impossibile ricostruire l'immagine originale) insieme con le chiavi di sicurezza generate automaticamente. Tutti i dati sono memorizzati nel *passaporto* personale.

Protector Suite QL si avvia automaticamente. Per accedere alle funzionalità e alle impostazioni, utilizzare i collegamenti del **menu di avvio (Start – Programmi – Protector Suite** contiene i collegamenti per accedere a **Control Center, Registrazione utente, Esercitazione Fingerprint e Guida), Biomenu** oppure l'icona sulla barra delle applicazioni.

## Tipo di registrazione

Protector Suite QL memorizza i dati di autenticazione derivati dai campioni di impronte digitali sia nella memoria della periferica oppure nel disco rigido. In entrambi i casi, i dati vengono memorizzati in un modulo crittografato.

Prima della prima registrazione successiva all'installazione, potrebbe essere necessario eseguire l'inizializzazione della periferica. Durante l'inizializzazione, verrà richiesto di selezionare un tipo di registrazione. Per alcuni tipi di periferica l'inizializzazione viene eseguita in modo automatico. Il processo di registrazione viene avviato subito dopo l'inizializzazione.





Se si seleziona la registrazione nella memoria della periferica, non è possibile accedere ai dati senza la periferica per le impronte digitali corrispondente. Questo significa che è possibile proteggere i propri dati con una chiave crittografica software generata dal software per le impronte digitali insieme a una chiave di crittografia hardware ottenuta direttamente dalla periferica.

L'unica limitazione è rappresentata dalla dimensione della memoria della periferica. In genere, la memoria della periferica consente di registrare fino a 21 impronte digitali, pertanto, se si desidera registrare un numero maggiore di impronte digitali per diversi utenti, è necessario effettuare la registrazione su disco rigido.

Se si seleziona la registrazione su disco rigido, i dati verranno crittografati mediante l'utilizzo di una chiave software. La verifica biometrica può essere eseguita mediante l'utilizzo di un lettore di impronte digitali.

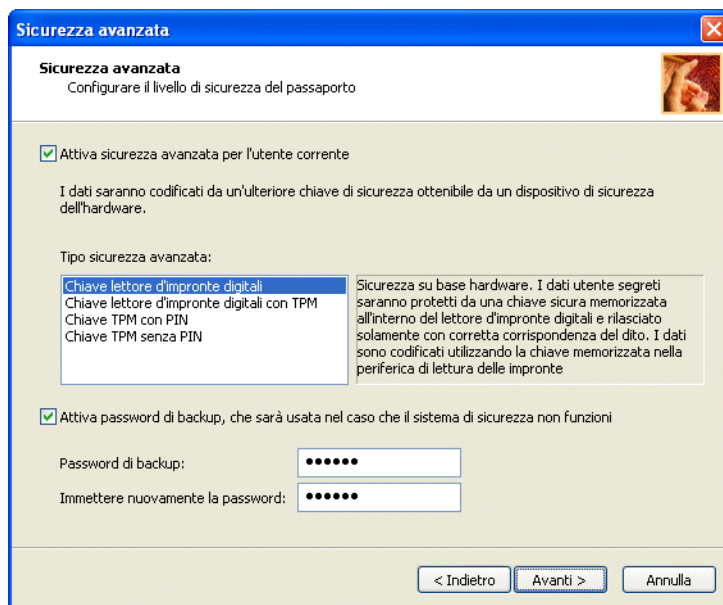
**ATTENZIONE:** non è possibile modificare il tipo di registrazione selezionata successivamente. Per apportare modifiche è necessario disinstallare e reinstallare Protector Suite QL.

Per una descrizione dettagliata sulle modalità di registrazione delle impronte digitali e di gestione del passaporto, vedere pagina 36.

### **Protezione avanzata**

È possibile aumentare la sicurezza in Protector Suite QL attraverso la crittografia supplementare. I tipi di crittografia supplementare disponibili variano a seconda dell'hardware. Ogni utente può attivare Protezione avanzata (o successivamente

disattivare) alla fine della procedura guidata per la registrazione e la modifica delle impronte digitali. In questa finestra di dialogo è possibile modificare i tipi di crittografia per regolare il livello di sicurezza necessario per la propria installazione.



### **Chiave lettore d'impronte digitali con TPM**

Offre sicurezza su base hardware avanzata. Un canale crittografato tra il TPM Security Chip e il lettore d'impronte digitali aumentano ulteriormente la sicurezza dei dati utente segreti. Raccomandato per la sicurezza massima.

### **Chiave lettore d'impronte digitali**

Offre sicurezza su base hardware avanzata. I dati utente segreti saranno protetti da una chiave sicura memorizzata all'interno del lettore d'impronte digitali e rilasciati solamente con corretta corrispondenza del dito. I dati sono codificati utilizzando la chiave memorizzata nella periferica per le impronte digitali.

### **Chiave TPM con PIN**

I dati utente segreti saranno protetti da un TPM Security Chip con PIN. Si richiede che l'utente inserisca il PIN durante ogni verifica d'identità. Raccomandato per maggiore sicurezza.

### **Chiave TPM senza PIN**

I dati utente segreti saranno protetti da un TPM Security Chip. Raccomandato per una maggiore praticità.

## Supporto per l'accesso

Protector Suite QL supporta l'accesso alla rete Novell. Affinché Protector Suite QL consenta l'accesso a una rete Novell in modo automatico, il nome utente e la password Windows devono corrispondere al nome utente e alla password Novell. Alcuni client Novell hanno problemi nel supporto di applicazioni di accesso di terze parti. Non sono supportate le seguenti versioni di client: 4.83, 4.90.

## Biomenu

**Biomenu** contiene i collegamenti alle funzionalità più utili di Protector Suite QL che necessitano della verifica biometrica. Una volta completata la registrazione, passare il dito per richiamare il **Biomenu**. A questo punto, sarà possibile accedere ai siti registrati, nonché registrare un nuovo modulo, un nuovo sito Web oppure una nuova finestra di dialogo (vedere **“Password Bank” a pagina 28**). È possibile aprire/chiusure **My Safe** (vedere **“My Safe” a pagina 33**). Inoltre, è possibile bloccare il computer, eseguire **Control Center** (vedere **“Control Center” a pagina 36**) oppure visualizzare la **Guida**.

## Accesso tramite impronte digitali

La sostituzione dell'accesso standard di Windows con l'accesso tramite impronte digitali consente di potenziare la sicurezza del computer e offre all'utente una maggiore praticità durante il processo di accesso. Inoltre, l'accesso biometrico garantisce una maggiore protezione dello screen saver (è necessario che nel sistema sia impostata l'opzione di protezione con password al ripristino dallo screen saver) e la riattivazione delle funzionalità di risparmio energetico (è necessario che nel sistema siano impostate le funzionalità di standby, sospensione – **Richiedi la password al termine della modalità di risparmio energetico**).

**Nota:** è necessario impostare una password Windows per proteggere il computer. In caso contrario, Protector Suite QL non può proteggere l'accesso al computer.

Per controllare il livello di protezione e praticità di Protector Suite QL, è necessario impostare una delle modalità di protezione.

In **modalità opportuna**, tutti gli utenti sono uguali e hanno gli stessi diritti. Questo significa che ciascun utente registra e gestisce il rispettivo passaporto.

La **modalità protetta** introduce il ruolo dell'amministratore per la gestione dei passaporti. Per impostazione predefinita, gli amministratori di Protector Suite QL fanno parte del gruppo di amministratori locali. Se si desidera aggiungere più utenti, accedere alla pagina **Modalità di protezione di Impostazioni del sistema** e fare clic sul pulsante **Gruppi amministratori**. Gli amministratori di Protector Suite QL creano e gestiscono i passaporti di tutti gli utenti. I membri che appartengono al gruppo degli amministratori

locali possono inoltre eseguire le impostazioni di sistema, le impostazioni comuni, per tutti. Di conseguenza, in modalità protetta, non tutte le funzionalità e le impostazioni descritte più avanti sono accessibili a ciascun utente.

**Nota:** per eseguire le seguenti operazioni, è necessario far parte del gruppo di amministratori di Protector Suite QL: registrazione utenti, eliminazione utenti (senza verifica), esportazione/importazione dei dati utente, gestione dell'accessione protetta, eliminazione delle impronte digitali di altri utenti mediante l'utilizzo di **Fingerprint storage inspector** (solo per le registrazioni nella periferica per le impronte digitali), accesso mediante nome utente e password.

Per una descrizione più dettagliata delle impostazioni di accesso mediante impronte digitali, vedere pagina 42

## Password Bank

Password Bank memorizza i dati immessi in una pagina Web o in una finestra di dialogo dell'applicazione in una registrazione e riproduce la registrazione memorizzata in un secondo momento. La registrazione può contenere un modulo Web (per esempio, una pagina di accesso contenente il nome utente e la password di accesso all'account di posta elettronica, i dati relativi all'internet banking, agli acquisti online) oppure una finestra di dialogo di Windows (per esempio, la finestra di dialogo di Windows Explorer per accedere ai dati relativi alle risorse che condividono la rete, la finestra di dialogo per accedere a un programma del database o a un client di posta elettronica). È necessario immettere i dati dell'accesso solo una volta, in fase di creazione delle registrazione; successivamente, è possibile memorizzarli nel passaporto mediante l'utilizzo delle impronte digitali. Quando la pagina Web o la finestra di dialogo verrà visualizzata nuovamente, sarà sufficiente passare il dito per immettere i dati in modo automatico.

Password Bank supporta i seguenti browser: Internet Explorer 5.0 o versione successiva, Mozilla 1.3 – 1.7, Netscape 7.0 – 8.0.4, Firefox 1.0 – 1.5. Il supporto di Internet Explorer viene installato in modo automatico. Quando Protector Suite QL rileva Mozilla/Firefox/Netscape, chiede all'utente se attivare il supporto. In alternativa, è possibile attivare il supporto di Mozilla/Firefox/Netscape psupport da **Control Center – Impostazioni – Impostazione utente – Password Bank**. Se si desidera attivare il supporto di Password Bank per un browser, selezionare la casella di controllo corrispondente. Solo gli amministratori locali possono visualizzare questa opzione e attivare più browser.

Quando è possibile eseguire un'azione (registrazione di una finestra di dialogo, riproduzione di una finestra di dialogo, ecc.), Password Bank visualizza dei suggerimenti per l'utente. Questi suggerimenti possono essere attivati o disattivati in **Impostazioni**

**utente** di Protector Suite QL. Tuttavia, questi suggerimenti non sono attivi nel caso in cui l'utente acceda tramite nome utente e password, senza autenticazione delle impronte, fino a quando la verifica delle impronte digitali non viene completata correttamente.

### **Per impostare la visualizzazione dei suggerimenti:**

- 1 Scegliere *Start – Programmi – Protector Suite QL – Control Center*.**
- 2 Selezionare *Impostazioni utente*.** L'autenticazione è obbligatoria.
- 3 Selezionare *Password Bank*.**
- 4 Selezionare i suggerimenti che si desidera visualizzare.**
  - ***Invia avviso quando la registrazione è riprodotta*** – Questo suggerimento informa l'utente che sta per iniziare la riproduzione della registrazione. Questo avviso è utile se si desidera creare più registrazioni dello stesso modulo o finestra di dialogo e non si desidera sovrascrivere i dati già immessi.
  - ***Invia avviso quando la registrazione è stata creata*** – Questo suggerimento informa l'utente che la creazione della registrazione è riuscita.
  - ***Invia avviso se il campo password viene modificato*** Questo suggerimento avverte l'utente che la password sarà visualizzata in un formato leggibile.
  - ***Invia avviso se è possibile riprodurre la finestra di dialogo*** – Questo suggerimento informa l'utente che è possibile riprodurre la registrazione.
  - ***Invia avviso se la finestra di dialogo è adatta alla registrazione*** – Questo suggerimento informa l'utente che la finestra di dialogo contiene un campo password che può essere registrato.
  - ***Invia avviso se la pagina Internet può essere riprodotta*** – Questo suggerimento informa l'utente che è possibile riprodurre la registrazione.
  - ***Invia avviso se la pagina Internet è adatta alla registrazione*** – Questo suggerimento informa l'utente che la pagina contiene un campo password che può essere registrato.

### **Registrazione delle pagine**

Aprire il browser Web e andare alla pagina che si desidera registrare. Immettere tutte le informazioni che si desidera avere nella registrazione, passare il dito e selezionare **Registra finestra** da **Biomenu**. Tutti i dati personali verranno memorizzati. È possibile accedere alla pagina registrata direttamente da **Biomenu – Siti registrati**.

Le registrazioni delle pagine Web utilizzano lo stesso formato per tutti i browser supportati. Le registrazioni create, ad esempio, in Internet Explorer possono essere successivamente riprodotte in Mozilla.

Password Bank registra moduli individuali. Se una pagina contiene diversi moduli, è necessaria una registrazione separata per ogni modulo. Questo significa che solamente il modulo attivo è registrato. Per registrare un modulo in una pagina per cui esiste già una registrazione (una pagina con moduli multipli), tenere premuto il tasto **Maiusc** e passare il dito per visualizzare il **Biomenu**. Se la pagina è già registrata, passando il dito sul sensore senza tenere premuto il tasto **Maiusc** provocherà la sostituzione della registrazione esistente.

In fase di registrazione di pagine con più moduli, procedere come segue:

- *Un modulo attivo è registrato.*
- *Se nessun modulo è attivo e si utilizza Internet Explorer 5.5 o versione successiva, viene chiesto all'utente di selezionare il modulo per la registrazione.*
- *Se nessuna delle affermazioni precedenti è vera, non viene eseguita alcuna azione.*

### **Scenari di esempio:**

Si supponga che non esistano registrazioni per una pagina. La pagina contiene il modulo A e il modulo B.

**A.** Il modulo A è stato compilato ed è ancora attivo. Passate il dito sul sensore. Il modulo A viene registrato.

**B.** Dopo avere compilato il modulo A, si passa al modulo B che prende lo stato attivo. Passate il dito sul sensore. Il modulo B viene registrato, ma è ancora vuoto.

**C.** Dopo avere compilato il modulo A, si fa clic all'esterno del modulo che perde lo stato attivo. Si sta utilizzando Internet Explorer 5.5 o versione successiva. Passate il dito sul sensore. Verrà chiesto di selezionare il modulo di destinazione per la registrazione.

**D.** La stessa situazione di C, ma si sta utilizzando una versione meno recente di IE, Mozilla, Mozilla o Netscape. Non viene eseguita alcuna azione.

### **Riprodurre una registrazione di pagina Web**

Una registrazione esistente viene riprodotta automaticamente se la pagina viene visualizzata da **Biomenu – Siti registrati**. Se la pagina è stata visualizzata manualmente e si desidera ora riprodurre la registrazione, passare il dito sul sensore.



Quando si riproducono registrazioni di pagine con moduli multipli:

- *Se esiste una sola registrazione per la pagina (indipendentemente dal numero totale di moduli esistenti), la registrazione viene riprodotta.*
- *Se esistono più moduli registrati e uno dei moduli registrati è attivo, viene riprodotto questo modulo.*
- *Se non esistono moduli attivi, è possibile riprodurre tutte le registrazioni esistenti per la pagina. Selezionare la registrazione che si desidera riprodurre.*

## **Registrazione e riproduzione di finestre di dialogo**

Password Bank è pensato principalmente per la registrazione di semplici finestre di dialogo contenenti un campo nome utente e password, di norma, finestre di dialogo per l'accesso a diverse applicazioni.

Finestre di dialogo più complesse potrebbero portare problemi. È sempre possibile registrare i campi di testo e i campi password. Le registrazioni salvano i controlli che non sono nascosti, disattivati o minimizzati. I pulsanti di opzione, le caselle di controllo, le caselle combinate e le selezioni nelle caselle di riepilogo vengono registrate per quelle applicazioni che utilizzano i controlli standard di Windows (per esempio, le finestre di dialogo di sistema). È possibile modificare qualsiasi informazione registrata, ad esempio, se è necessario modificare una password.

È possibile riscontrare problemi con le finestre di dialogo contenenti pagine multiple: in alcuni casi, tutte le pagine vengono registrate in un'unica registrazione. Password Bank non può maneggiare correttamente le finestre di dialogo in cui non si creano alcuni controlli prima dell'utilizzo ma solo il disegno. Esempi tipici sono alcune finestre di dialogo di Microsoft Office.

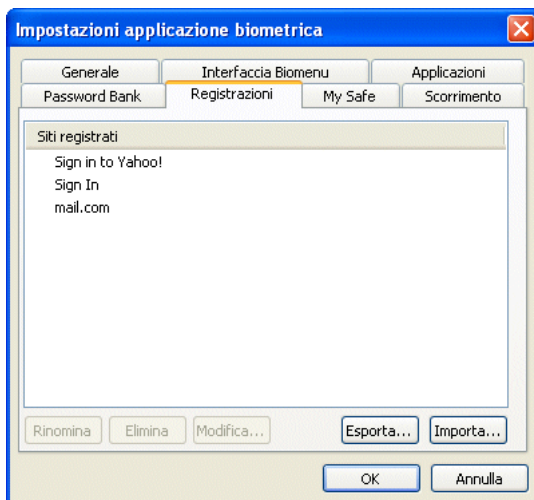
Durante la riproduzione di una finestra di dialogo registrata, nel caso qualche modifica del controllo richiami un'azione che richiede l'interazione dell'utente, Password Bank attende (con la finestra di dialogo) e la riproduzione sarà completata solamente dopo la fine dell'azione.

## **Gestione delle registrazioni**

Tutte le registrazioni possono essere visualizzate nella finestra di dialogo **Control Center – Impostazioni – Impostazioni utente – Registrazioni**. È possibile modificare il contenuto delle registrazioni personali per riflettere le eventuali modifiche dei dati o delle pagine registrate. È inoltre possibile attivare/disattivare l'invio automatico della registrazione riprodotta. Le registrazioni personali possono essere esportate, per l'utilizzo su un altro computer o come backup, o importate nel computer.

## Per gestire le registrazioni:

- 1 Scegliere **Start – Programmi – Protector Suite QL – Control Center**.
- 2 Selezionare **Impostazioni utente**. L'autenticazione è obbligatoria.
- 3 Selezionare **Registrazioni**.



- 4 Selezionare una registrazione con cui si desidera lavorare.
  - Fare clic sul pulsante **Rinomina** per modificare il nome della registrazione visualizzata in **Registrazioni**.
  - Fare clic sul pulsante **Elimina** per eliminare la registrazione.
  - Fare clic sul pulsante **Modifica** per modificare i dati memorizzati nella registrazione: per esempio, avete cambiato password o indirizzo e desiderate che questo si rifletta nelle registrazioni esistenti.
  - Selezionare la casella di controllo **Invio automatico** per inviare automaticamente la registrazione selezionata di un modulo dopo averla riprodotta. Selezionare la casella di controllo **Invio automatico** per inviare la registrazione selezionata di una finestra di dialogo facendo clic sul pulsante predefinito della finestra di dialogo (di solito **OK**).
  - Fare clic sul pulsante **Esporta** per esportare le registrazioni selezionate. Se non si seleziona alcuna registrazione, queste ultime verranno esportate tutte. Verrà richiesto di selezionare il file di destinazione e di inserire una password per la protezione delle registrazioni personali. L'estensione del file di Password Bank files è pb.

- Fare clic sul pulsante **Importa** per importare le registrazioni da un file password bank. Selezionare il file .pb di origine. Selezionare se si desidera sovrascrivere le registrazioni esistenti importando queste ultime oppure se si desidera aggiungere le registrazioni importate all'elenco delle registrazioni. Immettere la password creata durante l'esportazione.

## My Safe

**My Safe** è una cartella protetta dalle impronte digitali personali. È possibile modificarne le dimensioni in qualsiasi momento. **My Safe** è memorizzata nella cartella **Documenti**. Il suo contenuto non è visibile ad altri utenti (incluso altri utenti che hanno effettuato l'accesso nel caso di utilizzo della funzionalità di Cambio rapido utente).

Per una migliore accessibilità, viene creato un collegamento sia sul desktop sia in **Risorse del computer**.



È possibile accedere ai comandi **Chiudi/Apri** nel menu contestuale **My Safe** (o suo collegamento) e in **Biomenu**.

Prima di aprire **My Safe** per la prima volta, è necessario creare **My Safe**. In fase di creazione di MySafe è necessario definire la password di backup di **My Safe** e impostarne le dimensioni iniziali. In seguito, è possibile modificarle. Le dimensioni massime di **My Safe** sono 2 047 MB.

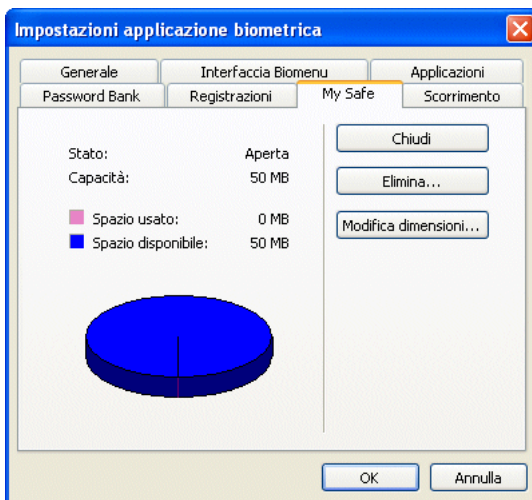
### Password di backup

Quando si crea **My Safe**, verrà richiesto l'inserimento di una password di backup. Questa password potrà essere utilizzata per accedere ai dati memorizzati in **My Safe** in caso di guasto al sensore per le impronte digitali o se non è possibile utilizzare l'impronta digitale registrata. Provate ad accedere a **My Safe** come in precedenza. Una finestra di dialogo informerà del problema e chiederà di inserire la password di backup.

**SUGGERIMENTO:** se avete dimenticato la password di backup, è possibile eliminare il vecchio **My Safe** da questa finestra di dialogo e crearne uno nuovo. Tutti i dati memorizzati nel MySafe esistente andranno persi.

## Per gestire MySafe:

- 1 Scegliere **Start – Programmi – Protector Suite QL – Control Center**.
- 2 Selezionare **Impostazioni utente**. L'autenticazione è obbligatoria.
- 3 Selezionare **My Safe**.



Vengono visualizzate le informazioni sullo stato di **My Safe** (chiuso/aperto) e sulle dimensioni (o sullo spazio libero/occupato se **My Safe** è aperto). Alcuni pulsanti non sono disponibili in tutte le situazioni. Modificare lo stato di **My Safe** per rendere disponibili le altre opzioni.

- Fare clic sul pulsante **Crea** per creare **My Safe**. Questo pulsante è disponibile solamente quando non esiste una cartella **My Safe**.
- Fare clic sul pulsante **Apri** per aprire **My Safe**. Questo pulsante è disponibile solamente quando **My Safe** è aperto. È possibile accedere ai dati memorizzati in **My Safe** solo se è aperto.
- Fare clic sul pulsante **Chiudi** per chiudere **My Safe**. Questo pulsante è disponibile solamente quando **My Safe** è chiuso.
- Fare clic sul pulsante **Elimina** per eliminare **My Safe**. Tutti i dati memorizzati in **My Safe** verranno eliminati in modo permanente e non potranno essere ripristinati.
- Fare clic sul pulsante **Modifica dimensioni** per modificare le dimensioni di **My Safe**. Questa operazione non ha alcun effetto sui dati memorizzati in **My Safe**.

Non bisogna dimenticare che tutti i file memorizzati in **My Safe** sono accessibili se **My Safe** rimane chiuso e l'utente ha effettuato l'accesso. **My Safe** verrà automaticamente chiusa al termine della sessione, ovvero alla disconnessione. In altri casi, chiudere **My Safe** manualmente per proteggere i file sensibili personali.

## Utilità di avvio dell'applicazione

È possibile avviare un'applicazione (qualsiasi file eseguibile) sul proprio computer attraverso la scansione del dito assegnato. È necessario lasciare almeno un dito registrato senza assegnazione per permettere la visualizzazione di **Biomenu**. Se si desidera ignorare l'avvio dell'applicazione e richiamare il **Biomenu**, tenere premuto **Maiusc** mentre si passa il dito.

Per creare o modificare l'associazione tra il dito registrato e l'applicazione, aprire **Control Center**, selezionare **Impostazioni – Impostazioni utente** quindi la scheda **Applicazioni**.



**Per creare l'associazione tra un dito registrato e un'applicazione:**

- 1 Fare clic sul pulsante **Aggiungi**. Verrà visualizzata la finestra di dialogo **Applicazione**.
- 2 Selezionare una delle dita registrate libere.
- 3 Inserire il nome dell'applicazione. (tale nome appare nella finestra di dialogo **Applicazioni** in **Impostazioni utente**).
- 4 Cercare il file che si desidera avviare: è necessario che tale file sia un file eseguibile.

- 5 *A scelta, se l'applicazione richiede parametri supplementari, digitarli nel campo **Parametri applicazione**.*
- 6 *Scegliere **OK**.*

**Per modificare successivamente la combinazione impronta/applicazione:**

- 1 *Selezionare un'applicazione nella finestra di dialogo **Applicazioni**.*
- 2 *Scegliere il pulsante **Modifica**.*
- 3 *Nella finestra di dialogo **Applicazione** apportare le modifiche necessarie.*
- 4 *Scegliere **OK**.*

**Per eliminare la combinazione impronta/applicazione:**

- 1 *Selezionare un'applicazione nella finestra di dialogo **Applicazioni**.*
- 2 *Fare clic sul pulsante **Elimina**.*

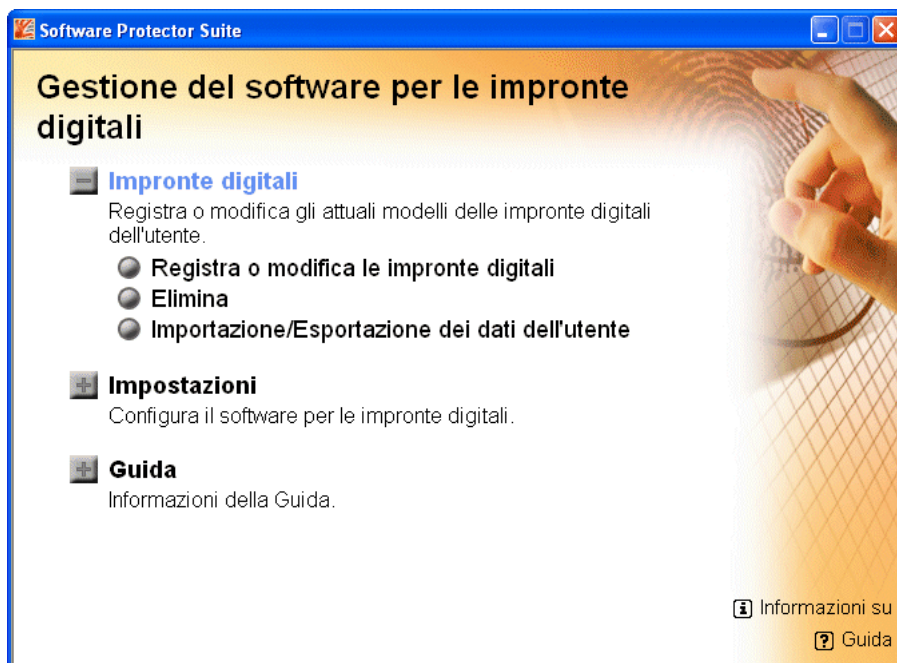
Le modifiche effettuate nella scheda **Applicazioni** vengono salvate solo dopo aver fatto clic sul pulsante **OK** nella finestra di dialogo **Impostazioni utente**.

## Control Center

Viene visualizzata la schermata principale del Control Center. Nella schermata vengono visualizzati gli argomenti. Fare clic sull'argomento desiderato per visualizzare l'elenco delle azioni valide disponibili per l'argomento in questione. Gli argomenti disponibili sono **Impronte digitali**, **Impostazioni** e la **Guida**.

### Impronte digitali

La sezione relativa alle impronte digitali consente all'utente di registrare, modificare ed eliminare i passaporti, nonché di eseguirne l'esportazione o l'importazione. L'elenco di azioni disponibili può variare in base all'hardware di autenticazione, ai passaporti esistenti e ai privilegi di accesso dell'utente corrente.



Ogni identità utente in Protector Suite QL è rappresentata da un passaporto contenente i suoi dati biometrici delle impronte usati per autenticare l'utente sul computer. Ogni utente Windows può avere un solo passaporto. Due passaporti non possono contenere la stessa impronta digitale.

### Registrazione o modifica delle impronte digitali

**Nota:** in modalità protetta gli amministratori di Protector Suite QL possono registrare i passaporti per tutti gli utenti, in alternativa, è possibile attivare l'autoregistrazione dell'utente all'accesso. In modalità opportuna, gli utenti possono registrare o modificare solo i rispettivi passaporti.

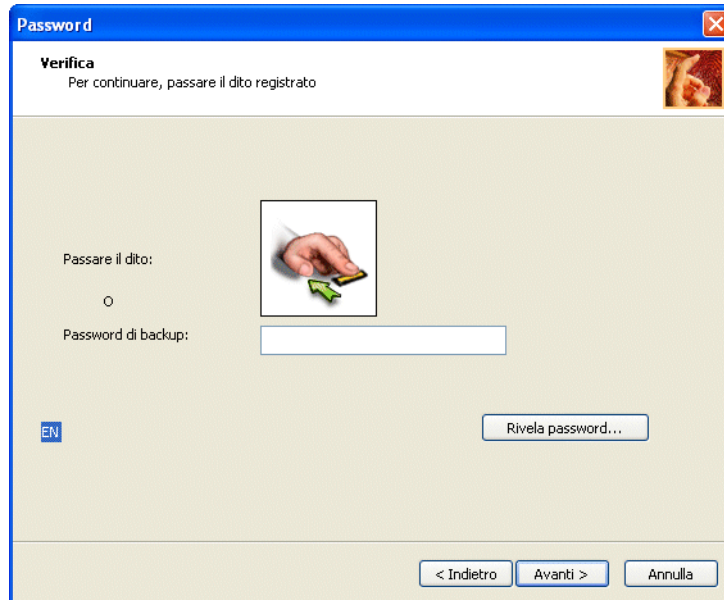
**Per creare un nuovo passaporto e registrare impronte digitali, procedere come segue:**

- 1 Scegliere **Start – Programmi – Protector Suite QL – Control Center**.
- 2 Scegliere **Impronte digitali**.
- 3 Fare clic su **Registra o modifica le impronte digitali**. Dopo l'installazione ma prima della registrazione del primo utente, in questa sezione viene visualizzata solo la procedura guidata **Inizializza**. Una volta selezionato il tipo di registrazione, la relativa procedura guidata viene

*avviata in modo automatico.*

*In modalità protetta, viene visualizzato un elenco di passaporti esistenti. Fare clic sul pulsante **Registrazione** per iniziare la registrazione di un nuovo utente.*

- 4 *Immettere la password Windows dell'utente e scegliere **Avanti**. In modalità protetta è inoltre possibile immettere il nome utente manualmente.*



- 5 *Leggere le istruzioni sulla modalità di creazione dei campioni di impronte digitali. Fare clic su **Avanti** per continuare con l'esercitazione Fingerprint. L'esercitazione è altamente raccomandata per gli utenti che utilizzano per la prima volta questa tecnologia.*
- 6 *L'esercitazione mostrerà un breve filmato in cui verranno illustrate le modalità corrette e non corrette per l'esecuzione della scansione delle impronte digitali. Successivamente, sarà possibile provare a creare i primi campioni di impronte digitali. A tal fine, è sufficiente seguire le istruzioni visualizzate. Una volta completata correttamente l'esercitazione, fare clic su **Avanti** per continuare con il processo di registrazione.*
- 7 *Verrà visualizzata una pagina raffigurante due mani. Fare clic sul dito che si desidera registrare per selezionarlo e avviare la scansione delle impronte digitali.*



- 8 *È necessario eseguire la scansione del dito selezionato tre volte. I campioni creati vengono combinati in un campione finale di impronte digitali.*  
*È possibile registrare fino a dieci dita.*  
*Se il sistema supporta la funzionalità di accensione protetta, per impostazione predefinita le impronte digitali vengono aggiunte all'autenticazione all'accensione. Se è impostata la registrazione su disco rigido, è possibile che venga visualizzato un pulsante di **accensione** su ogni dito nel caso in cui la memoria della periferica sia piena. Per selezionare le impronte digitali per l'accensione protetta, utilizzare questi pulsanti.*
- 9 *Eseguire una delle seguenti procedure:*
- *Selezionare un altro dito da registrare. Si raccomanda la registrazione di almeno due dita.*
  - *Scegliere **Avanti**.*
- 10 *Se il BIOS supporta password BIOS protette, verrà visualizzata una pagina di **accensione protetta**. Selezionare le password che saranno sostituite dalle impronte digitali. Verrà richiesto di immettere la password in seguito alla relativa selezione.*  
*La gestione delle password BIOS può essere effettuata dagli amministratori locali da qui. La selezione del pulsante **Gestione passaporto** consente di accedere alla finestra di dialogo **Password BIOS** in cui è possibile impostare, rimuovere l'impostazione o modificare i passaporti.*
- 11 *Alcune periferiche per le impronte digitali consentono di proteggere i dati attraverso la crittografia supplementare. Se si utilizzano periferiche del genere, selezionare il tipo di protezione avanzata. Per ulteriori informazioni sulla protezione avanzata, vedere il capitolo 3. **Si raccomanda di impostare la password di backup**. Può rivelarsi utile nel caso in cui non sia possibile effettuare l'autenticazione delle impronte digitali.*
- 12 *Una volta terminato, scegliere **Fine**.*

**Per modificare passaporto e impronte digitali, procedere come segue:**

- 1 **Scegliere Start – Programmi – Protector Suite QL – Control Center.**

- 2 Scegliere **Impronte digitali**.
- 3 Fare clic su **Registra o modifica le impronte digitali**.  
*In modalità protetta, viene visualizzato un elenco di passaporti esistenti. Selezionare l'utente da modificare, quindi fare clic sul pulsante **Modifica**.*
- 4 Verrà visualizzata la schermata **Apertura del passaporto dell'utente**.
- 5 Passare il dito sul sensore per le impronte digitali oppure immettere la password Windows o di backup della protezione avanzata, quindi fare clic su **Avanti**.
- 6 Eseguire una delle seguenti procedure:
  - Per registrare una nuova impronta digitale, procedere come segue:
    - Selezionare un dito da registrare facendo clic sull'immagine corrispondente.
    - Passare il dito selezionato sul sensore per le impronte digitali. Sono necessarie tre immagini valide per registrare un'impronta digitale.
  - Per eliminare un'impronta digitale, procedere come segue:
    - Selezionare un dito da eliminare facendo clic sull'immagine corrispondente.

*Scegliere **OK** per confermare l'operazione di eliminazione.*

*Se è impostata la registrazione su disco rigido, è possibile che venga visualizzato un pulsante di **accensione** su ogni dito nel caso in cui la memoria della periferica sia piena. Per selezionare le impronte digitali per l'accensione protetta, utilizzare questi pulsanti.*
- 7 Terminato di registrare o eliminare eventuali impronte, scegliere **Avanti**.

## **Elimina**

**Nota:** in modalità protetta, solo gli amministratori possono eliminare i passaporti.

### **Per eliminare un passaporto esistente:**

- 1 Scegliere **Start – Programmi – Protector Suite QL – Control Center**.
- 2 Scegliere **Impronte digitali**.
- 3 Scegliere **Elimina**.  
*In modalità opportuna, passare il dito per eseguire l'autenticazione e confermare l'eliminazione del passaporto corrente.*  
*In modalità protetta, viene visualizzato un elenco di passaporti esistenti. Selezionare il passaporto che si desidera eliminare e confermare l'eliminazione.*

## Importa o esporta dati utente

L'esportazione consente di creare una copia di backup del passaporto. Se è selezionata la registrazione nella periferica, il passaporto esportato può rivelarsi utile nel caso in cui sia necessario effettuare la sostituzione del sensore.

### Per esportare un passaporto esistente:

- 1 Scegliere **Start – Programmi – Protector Suite QL – Control Center**.
- 2 Scegliere **Impronte digitali**.
- 3 Scegliere **Importa o esporta dati utente**.  
*In modalità protetta, viene visualizzato un elenco di passaporti esistenti. Selezionare il passaporto che si desidera esportare e scegliere **Esporta**.*
- 4 Selezionare il file di destinazione con estensione *vtp*.
- 5 Creare la password che proteggerà i dati esportati.
- 6 Verificare l'impronta digitale contenuta nel passaporto appena esportato.

### Per importare un archivio di passaporti, procedere come segue:

- 1 Scegliere **Start – Programmi – Protector Suite QL – Control Center**.
- 2 Scegliere **Impronte digitali**.
- 3 Scegliere **Importa o esporta dati utente**.
- 4 Cercare il file del passaporto con estensione *vtp*.
- 5 Immettere la password creata durante l'esportazione.

# Impostazioni



## Impostazioni del sistema

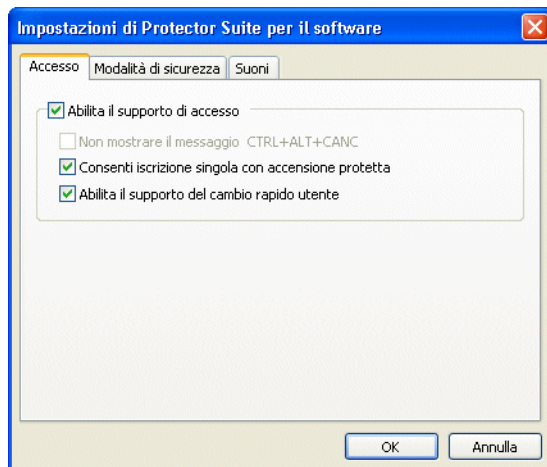
La finestra di dialogo Impostazioni del sistema è costituita da più pagine a seconda della configurazione del sistema. Non tutte le pagine descritte possono essere visualizzate nell'installazione dell'utente.

### Generale

La casella di controllo **Mostra Control Center all'avvio di Windows** attiva e disattiva la visualizzazione della schermata principale all'avvio del sistema.

## Accesso

**Nota:** le impostazioni di accesso possono essere modificate solo dagli amministratori. Per l'attivazione di alcune modifiche verrà richiesto di riavviare il computer.



**Per modificare le impostazioni di accesso, procedere come segue:**

- 1 Scegliere **Start – Programmi – Protector Suite QL – Control Center**.
- 2 Scegliere **Impostazioni**.
- 3 Scegliere **Impostazioni del sistema**. Andare alla pagina **Accesso**.
- 4 Selezionare o deselezionare le caselle di controllo relative alle opzioni richieste:

**Sostituire la procedura di accesso di Windows con quella protetta da impronte digitali**

Quando questa casella di controllo è selezionata, è possibile accedere al computer usando l'autenticazione dell'impronta digitale. Quando questa casella di controllo è deselezionata, è necessario accedere al computer usando la password di Windows.

**Non mostrare il messaggio CTRL+ALT+CANC**

Il messaggio standard di Windows CTRL+ALT+CANC non verrà visualizzato se si seleziona questa opzione. Verrà mostrato solamente il suggerimento di passare il dito. È possibile richiamare la finestra di dialogo d'accesso in cui inserire nome utente/dominio/password premendo CTRL+ALT+CANC in modo che l'utente sia in grado di accedere utilizzando nome utente e password.

**Esegui l'accesso automatico di utenti verificati da Accensione protetta,**

*disponibile solo nelle configurazioni che supportano l'accensione protetta. Questa casella di controllo limita l'autenticazione all'accensione all'autenticazione Windows. Se un'impronta digitale utilizzata per la funzionalità di accensione protetta corrisponde a un'impronta di un passaporto esistente, l'utente corrispondente accede automaticamente a Windows. Quando questa casella di controllo è deselezionata e l'autenticazione all'accensione è attivata, è necessario fornire l'impronta digitale per l'autenticazione BIOS e l'accesso a Windows.*

#### **Abilita il supporto del cambio rapido utente**

*Questa casella di controllo attiva e disattiva la funzionalità di cambio rapido utente di Windows XP, se supportata dal computer in uso. Quando il cambio rapido utente è supportato ma non attivato, verrà chiesto di attivarlo sul sistema.*

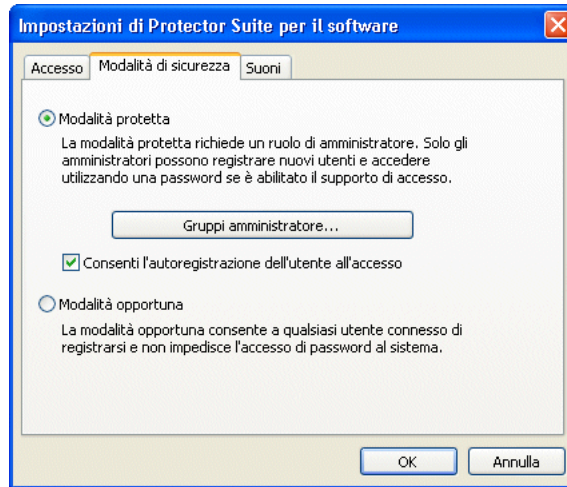
### **5 Scegliere *Fine*.**

#### **Modalità di protezione**

**Nota:** la modalità di protezione può essere modificata solo dagli amministratori.

La schermata Modalità di protezione permette di determinare chi possa accedere ai controlli di gestione della protezione tramite impronte digitali. Le modalità di protezione sono due: opportuna e protetta. In modalità opportuna, tutti gli utenti hanno gli stessi privilegi. Ad esempio, ciascun utente può creare il proprio passaporto oppure accedere utilizzando il nome utente e la password di Windows.

Se però la sicurezza viene impostata sulla modalità protetta, la situazione cambia. Solo l'amministratore avrà un accesso illimitato alle funzioni amministrative. Gli utenti standard (non amministratori) dovranno ottenere il passaporto dall'amministratore, a meno che non sia abilitata l'autoregistrazione dell'utente all'accesso. Gli utenti standard potranno solo modificare il proprio passaporto.



**Per impostare una modalità di protezione, procedere come segue:**

- 1 Scegliere **Start – Programmi – Protector Suite QL – Control Center**.
- 2 Scegliere **Impostazioni**.
- 3 Scegliere **Impostazioni del sistema**. Andare alla pagina **Modalità di protezione**.
- 4 Selezionare la modalità di protezione desiderata. Le opzioni sono le seguenti:

- **Modalità protetta:** la modalità protetta introduce un ruolo di amministratore per le operazioni di gestione di Protector Suite QL. Il computer sarà più protetto se alcune funzioni più delicate, come la gestione dei passaporti, saranno gestibili esclusivamente dagli amministratori. Gli utenti standard (non amministratori) non possono effettuare l'accesso utilizzando il nome utente e la password di Windows corrispondente.

Fare clic sul pulsante **Gruppi amministratore** per modificare l'elenco di utenti che dispongono di diritti di amministratore di Protector Suite QL. Selezionare **Consenti l'autoregistrazione dell'utente all'accesso** per consentire la registrazione delle impronte digitali durante l'accesso

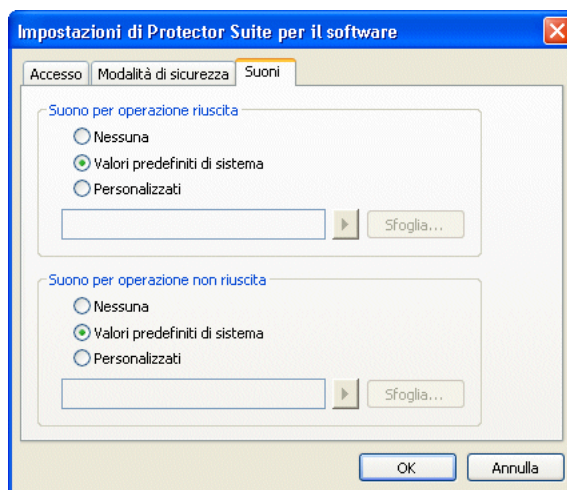
*direttamente agli utenti che non dispongono dei diritti di amministratore di Protector Suite QL. In questo caso, gli utenti standard (non amministratori) immettono il nome utente e la password di Windows al primo accesso, provvedendo alla registrazione del proprio passaporto prima dell'esecuzione dell'effettivo accesso. Questo significa che l'accesso non verrà eseguito correttamente fino a quando le impronte digitali dell'utente non vengono registrate.*

- **Modalità opportuna:** sviluppata principalmente per l'utilizzo domestico, dove la praticità d'uso è più importante della protezione.

## Suoni

**Nota:** le impostazioni di accesso possono essere modificate solo dagli amministratori.

Il suono selezionato è utilizzato quando le operazioni relative alle impronte digitali sono state completate correttamente o non sono riuscite. È possibile utilizzare i suoni predefiniti del sistema, disabilitare i suoni o cercare i propri file audio preferiti (formato wav).



## TPM

**Nota:** il modulo TPM può essere inizializzato solo da un amministratore.

Questa pagina viene visualizzata quando è rilevata un'applicazione di gestione TPM di terze parti. L'inizializzazione TPM abilita l'utilizzo del modulo di protezione TPM da parte della funzionalità Protector Suite QL Advanced Security.



## Per inizializzare il modulo TPM:

- 1 Fare clic sul pulsante **Inizializza TPM** per avviare la procedura guidata dell'inizializzazione TPM.
- 2 Scegliere **Avanti** nella schermata di **benvenuto**. Verrà eseguita l'inizializzazione.
- 3 Successivamente, verrà visualizzato il risultato dell'operazione. Se l'operazione viene completata correttamente, Protector Suite QL sarà in grado di utilizzare la protezione TMP supplementare. Scegliere **Fine** per chiudere la procedura guidata.

## Impostazioni utente

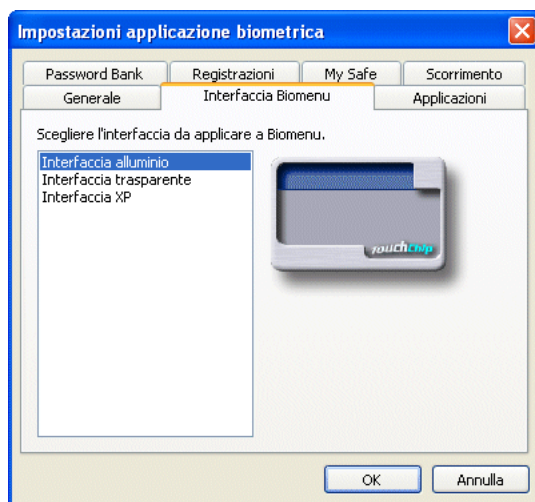
**Nota:** l'accesso alle **Impostazioni utente** richiede l'esecuzione della verifica biometrica.

### Generale

Selezionare la casella **Mostra icona nella barra delle applicazioni** per visualizzare l'icona sulla barra delle applicazioni che fornisce accesso rapido ad alcune delle funzionalità di Protector Suite. Per una descrizione dettagliata dell'icona sulla barra delle applicazioni, vedere pagina 52.

### Interfaccia di Biomenu

È possibile visualizzare Biomenu con diverse interfacce. Selezionate la vostra preferita.



### Password Bank

Questa pagina è costituita da due parti.

**Suggerimenti** è visibile a tutti gli utenti. Questa parte contiene le impostazioni che controllano la visualizzazione dei suggerimenti per informare un utente delle possibili azioni.

La seconda parte è visibile solo per gli amministratori. Viene visualizzata solo se è installato Mozilla, Netscape o Firefox. Quando Protector Suite QL rileva Mozilla/Netscape/Firefox, chiede all'utente se attivare il supporto. In alternativa, il supporto per Mozilla/Netscape/Firefox può essere attivato qui. Se si desidera attivare il supporto di Password Bank per un browser, selezionare la casella di controllo corrispondente.

Per ulteriori informazioni, vedere pagina 28.

## Registrazioni

Questa finestra di dialogo elenca tutte le registrazioni personali esistenti. Vengono visualizzate sia le pagine che le finestre di dialogo registrate.

Per ulteriori informazioni, vedere pagina 28.

## Scorrimento

È possibile utilizzare il sensore per scorrere attraverso le diverse finestre, per esempio documenti lunghi.

Quando si desidera utilizzare lo scorrimento tramite impronte digitali, per esempio in documenti lunghi, premere il tasto di scelta rapida per Scroll Switch selezionato per consentire lo scorrimento. Tale tasto non è impostato per impostazione predefinita, pertanto è necessario impostarlo prima di utilizzarlo per la prima volta. Quando si utilizza la funzionalità di scorrimento, non è possibile utilizzare il sensore per richiamare contemporaneamente il **Biomenu**. Per attivare il comportamento standard di Protector Suite QL, è necessario premere nuovamente il tasto di scelta rapida al termine dello scorrimento.

La pagina **Scorrimento** consente di regolare la velocità e l'accelerazione dello scorrimento, nonché di impostarne il tasto di scelta rapida. Questo tasto di scelta rapida attiva e disattiva la funzionalità di scorrimento. Per impostazione predefinita, non viene utilizzato alcun tasto.

- *Spostare il cursore **Velocità** per regolare la velocità del movimento, più velocemente si riuscirà a muovere il dito, più velocemente avrà luogo lo scorrimento. Questa impostazione controlla la velocità di scorrimento.*

- *Spostare il cursore **Accelerazione** per regolare l'accelerazione. Quanto più il dito si muoverà nella stessa direzione, tanto più veloce sarà lo scorrimento. Questa impostazione controlla la velocità di scorrimento.*
- *Provare le impostazioni. Fare clic sul pulsante **Verifica velocità** e provare le impostazioni.*
- *Se si desidera impostare o modificare il tasto di scelta rapida predefinito per Scroll Switch, attivare il campo corrispondente e premere la combinazione di tasti selezionata. I tasti di scelta rapida disponibili sono elencati nella finestra di dialogo.*

## **My Safe**

Questa pagina contiene le opzioni per la gestione di **My Safe**. Vengono visualizzate le informazioni sullo stato di **My Safe** (chiuso/aperto) e sulle dimensioni (o sullo spazio libero/occupato se **My Safe** è aperto).

Per ulteriori informazioni, vedere pagina 33.

## **Utilità di avvio dell'applicazione**

Vengono visualizzate le applicazioni che possono essere avviate tramite impronte digitali. L'Utilità di avvio dell'applicazione può contenere fino a numero di impronte registrate - 1 applicazioni.

Per ulteriori informazioni, vedere pagina 35.

## **Accensione protetta**

La funzionalità facoltativa di accensione protetta utilizza il BIOS del computer per impedire l'accesso non autorizzato al computer. I computer in cui è attivata la funzionalità di accensione protetta non caricheranno il sistema operativo se l'impronta non viene autenticata a livello BIOS.

Il computer attiverà la funzionalità di accensione protetta solo se l'impronta digitale acquisita corrisponde a un'impronta registrata per l'utente corrente. Al termine della verifica, il processo di attivazione dell'accensione protetta continuerà normalmente. Se l'autenticazione dell'impronta digitale non riesce per un numero specificato di volte in una riga (a seconda del BIOS), l'accesso viene bloccato e il computer deve essere riavviato.

## **Attivazione dell'accensione protetta in Fingerprint Software**

La funzionalità di accensione protetta può essere attivata in Fingerprint Software mediante la procedura guidata dell'accensione protetta solo se tale funzionalità è supportata dal sistema. L'accensione protetta è attivata per impostazione predefinita.

**Per attivare/disattivare la funzionalità di accensione protetta usando l'interfaccia di Protector Suite QL, procedere come segue:**

- 1 *Scegliere **Start – Programmi – Protector Suite QL – Control Center.***
- 2 *Scegliere **Impostazioni.***
- 3 *Scegliere **Accensione protetta.***
- 4 *Selezionare la casella di controllo **Sostituisci le password di accensione e del disco rigido con il lettore d'impronte digitali.***
- 5 *L'implementazione della funzionalità di accensione protetta variano a seconda del disco rigido. Per ulteriori informazioni, fare clic sul collegamento **Ulteriori informazioni.***
- 6 *Scegliere **Fine.***

Se è impostata la registrazione su disco rigido, nella finestra di dialogo **Accensione protetta** sono disponibili più opzioni. Le impronte digitali presenti nella memoria di accensione protetta sono elencate nella finestra **Impronte digitali autorizzate per l'accensione protetta**. È possibile rimuovere le impronte digitali dalla memoria di accensione protetta da qui.

**Nota:** modificando un passaporto (cioè aggiungendo o eliminando un'impronta digitale) vengono automaticamente aggiunte o rimosse le impronte digitali da utilizzare per l'accensione protetta.

#### **Attivazione dell'accesso automatico di utenti verificati dall'accensione protetta**

La funzionalità di accensione protetta può essere impostata anche per l'accesso dell'utente a Windows. Quando questa funzionalità è attivata, se un'impronta digitale utilizzata per la funzionalità di accensione protetta corrisponde a un'impronta di un passaporto esistente, l'utente corrispondente accede automaticamente a Windows. Questa funzionalità evita all'utente di autenticarsi due volte all'accensione del computer, e cioè una volta per la funzionalità di accensione protetta e un'altra per accedere a Windows.

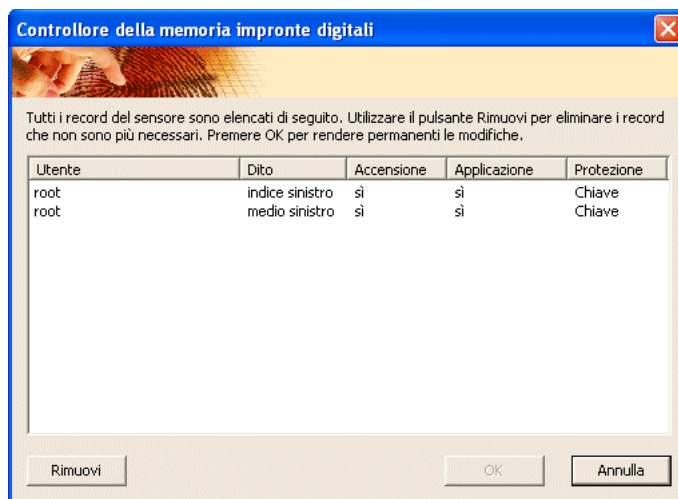
**Per attivare l'accesso automatico a Windows di utenti verificati dall'accensione protetta, procedere come segue:**

- 1 *Scegliere **Start – Programmi – Protector Suite QL – Control Center.***
- 2 *Scegliere **Impostazioni.***
- 3 *Scegliere **Impostazioni del sistema** e andare alla pagina **Accesso.***
- 4 *Selezionare la casella di controllo **Consenti iscrizione singola con accensione protetta.***

## Fingerprint Storage Inspector

Fingerprint Storage Inspector è uno strumento per la visualizzazione e la modifica del contenuto memorizzato nella periferica per la lettura delle impronte digitali. Vengono mostrati tutti i record memorizzati nella periferica.

Per ogni impronta viene mostrata una descrizione con le informazioni sull'utilizzo per accensione protetta (autenticazione pre-avvio), applicazioni (per esempio Logon) e stato della protezione avanzata (TPM o nessuna protezione avanzata).



### Per rimuovere le impronte digitali dalla periferica:

- 1 *Selezionare il record che si desidera eliminare quindi fare clic sul pulsante **Rimuovi**. L'elenco dei record sarà aggiornato per riflettere le modifiche.*
- 2 *Dopo aver rimosso i record non necessari, fare clic sul pulsante **OK** per rendere permanenti le modifiche oppure scegliere **Annulla** per rinunciare alle modifiche.*

**Nota:** in modalità protetta, solo gli amministratori possono rimuovere i record. In modalità opportuna, gli utenti possono rimuovere le proprie impronte digitali oppure quelle non incluse in alcun passaporto esistente. Per ogni passaporto, è necessario che rimanga almeno un'impronta. Per gestire o eliminare l'intero passaporto, utilizzare la procedura guidata **Registra o modifica le impronte digitali**.

# Guida

## Introduzione

Tutte le funzionalità di base di Protector Suite QL sono riepilogate nella schermata **Introduzione**. I collegamenti visualizzati nella finestra di dialogo consentiranno all'utente di accedere direttamente agli argomenti della guida corrispondenti.

## Esercitazione

Per aiutare l'utente a utilizzare correttamente la periferica per le impronte digitali, è disponibile un'esercitazione che consente all'utente di esercitarsi e apprendere la tecnica di scansione delle impronte digitali corretta.

Questa esercitazione può essere eseguita in qualsiasi momento dal menu **Control Center** oppure dal menu **Start, Programmi – Protector Suite QL – Esercitazione Fingerprint**.

Questa esercitazione mostra un breve filmato in cui vengono illustrati campioni di esecuzioni della scansione delle impronte digitali corrette e non corrette. L'utente avrà modo di imparare alcuni suggerimenti su come ottenere la migliore qualità possibile di campioni di impronte digitali analizzati.

È possibile provare a creare i primi campioni di impronte digitali e osservare le immagini risultanti. In questo modo sarà possibile imparare a posizionare più correttamente le dita sul sensore, esercitare la pressione, la velocità e la scorrevolezza della scansione.

## Icona sulla barra delle applicazioni

L'icona Protector Suite QL nella barra delle applicazioni indica che il programma è in esecuzione e consente l'accesso alle funzioni che non richiedono l'autenticazione tramite impronta.



## Modifica impronte...

Apri la procedura guidata per registrare ulteriori impronte. È possibile avviare questa procedura guidata anche da **Biomenu** selezionando **Impostazioni – Dita**.

## **Avvia Control Center...**

Avvia il Control Center di Protector Suite QL.

## **Non usare il sensore/Usa il sensore**

**Nota:** questa funzionalità è disponibile solo per gli utenti avanzati, per esempio gli sviluppatori di altre applicazioni biometriche.

Questa funzionalità consente all'utente di scollegare Protector Suite QL dalla periferica per le impronte digitali. Questo comando rende temporaneamente disponibile la periferica solo per la sessione utente corrente. La periferica può essere utilizzata esclusivamente da una sola applicazione per volta. Questa opzione è specifica per i casi in cui si pianifica di sviluppare oppure di utilizzare un'applicazione biometrica diversa e si desidera che Protector Suite QL sblocchi la periferica.

Se si seleziona l'opzione **Non usare il sensore**, Protector Suite QL non eseguirà alcuna verifica delle impronte digitali.

## **Guida**

Visualizza la guida.

## **Informazioni su**

Visualizza le informazioni sul programma e sulla versione.





A hand is shown pointing at a fingerprint on a document. The fingerprint is a latent print, and the hand is positioned as if it is about to lift it. The background is a light yellow color with a subtle grid pattern.

## Capitolo 4

# Risoluzione dei problemi

Questo capitolo fornisce le informazioni per gli utenti che hanno difficoltà nell'utilizzo di Protector Suite QL.

## Installazione

### Non riesco a installare Protector Suite QL.

- *Controllare i privilegi di cui si dispone. L'utente che installa Protector Suite QL deve godere dei privilegi di amministratore.*
- *Controllare di disporre di spazio libero sufficiente nel computer in uso. Per procedere all'installazione di Protector Suite QL, è necessario disporre di circa 40 MB.*
- *Controllare il sistema. Sono supportati solo Windows 2000 e Windows XP.*

### Protector Suite QL non funziona dopo la relativa installazione.

- *Una volta completata l'installazione di Protector Suite QL, è necessario riavviare il computer.*

## Registrazione di impronte

### La periferica non funziona.

- *Controllare la connessione della periferica.*
- *Controllare se il driver è installato correttamente. I driver sono generalmente installati durante l'installazione di Protector Suite QL. Tuttavia, se si verificano problemi, i driver necessari possono essere trovati nella sottocartella **Driver** all'interno della cartella di installazione. Per informazioni relative all'installazione dei driver specifiche sulla periferica, consultare il file *Leggimi.txt* nella cartella **Driver**. Per controllare lo stato della periferica, fare clic con il tasto destro su **Risorse del computer**, selezionare **Proprietà – Hardware** e aprire **Gestione periferiche**.*

### Non riesco a registrare le mie impronte digitali. Le impronte digitali non sono riconosciute correttamente.

- *Seguire l'esercitazione Fingerprint per imparare come creare correttamente campioni di impronte digitali. L'esercitazione Fingerprint può essere eseguita come parte della registrazione delle impronte digitali oppure separatamente dal menu **Start**.*
- *Provare a esercitare una maggiore o una minore pressione sul sensore.*
- *Provare a modificare la velocità di passaggio del dito.*

- *Pulire il sensore. Utilizzare un panno umido, che non rilasci fibre e pelucchi, unitamente ad acqua oppure a una lozione idratante, che non contenga agenti profumanti, e strofinare delicatamente il panno sul sensore. Non utilizzare tessuti e sostanze abrasive e corrosive.*
- *Tentare di passare il proprio dito. (Soprattutto ad alte temperature.)*
- *Provare a utilizzare un altro dito. Di solito, è più semplice effettuare la registrazione del dito indice piuttosto che la registrazione del dito mignolo.*

**Non riesco a utilizzare l'autenticazione delle impronte digitali poiché mi sono prodotto una ferita all'unico dito registrato. Desidero registrare un altro dito.**

Per poter utilizzare pienamente tutte le funzionalità di Protector Suite QL, è necessario disporre di impronte digitali registrate che possono essere utilizzate. Si consiglia di registrare almeno due dita per evitare di incorrere in problemi di questo tipo.

Per aggiornare le impronte digitali registrate, è necessario immettere la procedura guidata **Registra o modifica le impronte digitali**.

- *Se non si utilizza la funzionalità di Protezione avanzata, è possibile effettuare l'accesso utilizzando la password Windows.*
- *Se invece si utilizza la funzionalità di Protezione avanzata con la password di backup, è possibile effettuare l'accesso utilizzando la password di backup.*
- *Se si utilizza la funzionalità di Protezione avanzata senza la password di backup, non esiste in alcun modo la possibilità di aggiungere un'altra impronta digitale. In questo caso, si consiglia di attendere fino a che non sia possibile riutilizzare il dito (per esempio la guarigione del dito) oppure di eliminare il passaporto (eseguendo la procedura guidata di **eliminazione** del passaporto) e di registrare nuove impronte digitali. Si noti che in questo caso tutti i dati segreti memorizzati (password, chiavi di crittografia e così via) andranno perduti. Per eseguire l'operazione di eliminazione è necessario annullare l'operazione di verifica delle impronte digitali al fine di accedere alla finestra di dialogo della password e immettere la password Windows.*
- *Se il tipo di protezione avanzata impostato è **Chiave lettore d'impronte digitali** o **Chiave lettore d'impronte digitali con TPM**, al termine della registrazione verrà chiesto di passare il dito originale per sbloccare i dati utente segreti sulla periferica. Dal momento che non è possibile eseguire tale operazione, è necessario disattivare la funzionalità di Protezione avanzata prima di uscire dalla procedura guidata. Una volta abbandonata la procedura guidata, è possibile accedere nuovamente utilizzando il nuovo dito registrato e*

*riattivare la funzionalità di Protezione avanzata. Questi passaggi sono obbligatori per procedere alla creazione di un nuovo set di chiavi collegate alla nuova impronta digitale.*

**Al termine del processo di registrazione mi è stato chiesto di passare nuovamente il mio dito. Per quale motivo?**

Questo messaggio viene visualizzato nel caso in cui sia stata utilizzata la password di backup della protezione avanzata per immettere la procedura guidata **Registra o modifica le impronte digitali**, nel caso in cui sia stato impostato il tipo di Protezione avanzata **Chiave lettore d'impronte digitali** o **Chiave lettore d'impronte digitali con PIN** e nel caso in cui si sia aggiunta una nuova impronta digitale al passaporto.

- *Questo comportamento è normale. Questa verifica è obbligatoria per procedere alla creazione di un nuovo set di chiavi collegate alla nuova impronta digitale.*

**Non riesco a registrare un utente in modalità opportuna.**

- *Controllare se esiste il passaporto dell'utente. È possibile che l'utente sia già registrato. Ciascun utente può avere un solo passaporto.*

**L'importazione degli utenti non funziona.**

- *Controllare se esiste il passaporto dell'utente. Se si desidera importare i dati di un utente esistente, è necessario aver eliminato il passaporto precedente.*
- *Controllare la memoria della periferica in **Fingerprint Storage Inspector (Control Center – Impostazioni – Fingerprint Storage Inspector)**. Valido solo se viene utilizzata la registrazione nella periferica.*

**Per quale motivo è consigliabile esportare il passaporto dell'utente?**

I dati esportati contengono le informazioni relative alle impronte digitali, le credenziali di accesso, le registrazioni Password Bank, nonché le informazioni di crittografia di My Safe, ma non i dati My Safe.

- *Esportare i dati utente regolarmente come backup di tutte queste informazioni.*

**Ho perso la password di backup della Protezione avanzata.**

- *Per modificare la password di backup della Protezione avanzata, andare alla procedura guidata **Registra o modifica le impronte digitali**, passare il dito e seguire la registrazione delle impronte digitali. Nella pagina Protezione avanzata è possibile modificare la password di backup.*

## Ho la necessità di sostituire il sensore.

Se si ha la necessità di sostituire un lettore o un sensore per le impronte digitali non funzionale, seguire la procedura riportata di seguito:

### Registrazione su disco rigido:

- *Se è impostata la registrazione su disco rigido, Protector Suite QL non memorizza alcun dato nella periferica; di conseguenza, non è necessario effettuare alcuna azione in seguito alla sostituzione del sensore. Nel caso in cui si utilizzi la funzionalità di accensione protetta (l'autenticazione pre-boot), è possibile che sia necessario utilizzare la procedura guidata **Registra o modifica le impronte digitali** per eseguire l'aggiornamento dei relativi dati.*

### Registrazione nella periferica:

- *Esiste una connessione tra il passaporto dell'utente e la periferica per le impronte digitali che richiede la sostituzione del passaporto corrente con quello precedentemente esportato.*

## È possibile ripristinare il passaporto importando il relativo backup nella nuova periferica:

- 1 *Eliminare la propria password.*
- 2 *Connettere la nuova periferica funzionale.*
- 3 *Importare il passaporto da un file di backup.*

### Cambio dei lettori esterni:

- *La procedura descritta sopra è valida anche nel caso in cui si tenti di utilizzare i lettori per le impronte digitali con Protector Suite QL, per esempio un lettore interno e uno esterno oppure lo scambio tra due lettori esterni. Se si utilizza la registrazione su disco rigido, in genere non si riscontrano problemi con le possibili eccezioni della funzionalità di accensione protetta (autenticazione pre-boot). Se si utilizza invece la registrazione nella periferica, non è possibile effettuare lo scambio dei lettori a meno che non esistano buoni motivi ed è necessario eliminare, nonché creare nuovamente il passaporto.*

Se è impostata la registrazione nella periferica e il lettore contiene dati, provenienti da un'installazione precedente o diversa di Protector Suite QL, di un utente che esiste nel computer ma che non è ancora registrato, viene visualizzato un messaggio in cui viene chiesto se riutilizzare tali dati.

In caso contrario, ovvero se il nuovo lettore contiene i dati di un utente già registrato, non è possibile riutilizzare tali dati. Le impronte digitali vengono invece eliminate dalla periferica per motivi di sicurezza, per esempio per evitare di inserire impronte digitali che appartengono a utenti non sottoposti a verifica.

### **Il modulo TPM non funziona.**

Se si utilizza la Protezione avanzata con TMP (Trusted Platform Module) e il modulo TPM è danneggiato, cancellato o disattivato, la funzionalità di Protezione avanzata non funzionerà.

**Se si imposta la password di backup per la protezione avanzata, è possibile seguire questi passaggi:**

- 1 *Immettere la procedura guidata **Registra o modifica le impronte digitali** utilizzando la password di backup.*
- 2 *Disattivare la funzionalità di Protezione avanzata e scegliere fine.*
- 3 *Una volta che il TPM è stato ripristinato, attivato oppure nel caso in cui sia stato eliminato, è possibile immettere nuovamente la procedura guidata **Registra o modifica le impronte digitali** utilizzando il proprio dito e riattivare la funzionalità di Protezione avanzata con TPM.*

## **Cambio rapido utente**

### **Impossibile attivare il Cambio rapido utente.**

Questa opzione è visibile solamente su computer con in esecuzione Windows XP. La funzionalità Cambio rapido utente può essere utilizzata solamente su computer che non sono membri di un dominio.

- *Controllare se il computer non appartiene a un dominio.*
- *L'installazione di altri software, per esempio il client Novell, può impedire l'attivazione del Cambio rapido utente.*

## **Accesso**

### **Non riesco ad accedere utilizzando nome utente e password.**

- *Controllare la modalità di protezione. L'accesso tramite nome utente e password può essere effettuato da tutti gli utenti solo in modalità pratica. In modalità opportuna, solo gli amministratori dispongono di questa opzione.*

**Non riesco a modificare le impostazioni di Protector Suite QL System benché siano visibili in Control Center.**

- *Controllare i privilegi dell'utente. Le **Impostazioni del sistema** possono essere modificate solo dagli amministratori. Essere l'amministratore locale non equivale a essere membro del **gruppo di amministratori** di Protector Suite QL. I membri di questo gruppo possono gestire i passaporti, le impronte digitali, l'accensione protetta, nonché effettuare l'accesso tramite nome utente e password.*

## Password Bank

**Le pagine registrate vengono riprodotte in Internet Explorer dopo un intervallo prestabilito.**

Le registrazioni vengono riprodotte (e possono essere create) solamente dopo il completamento del caricamento della pagina. Sfortunatamente, Internet Explorer, a volte, visualizza in modo incorretto il completamento del caricamento (l'animazione nell'angolo in alto a destra viene interrotta), benché la pagina non sia ancora completamente caricata. Se l'utente preme Termina per finire il caricamento, IE, a volte, ignora il comando e non si arresta. In tali situazioni, attendere fino al completamento del caricamento. È possibile che lo stesso problema occorra con le pagine in cui il mouse, passando sopra ad alcuni elementi attivi (per esempio, animazioni Flash), avvii il caricamento di un oggetto benché la pagina sia stata già caricata.

- *Attendere fino al completamento del caricamento.*

**Non riesco a registrare una pagina già registrata. Il passaggio del dito attiva la riproduzione.**

- *Invece di riprodurre la registrazione, quando si passa il dito per registrare una pagina o una finestra di dialogo già registrata, premere il tasto MAIUSC.*

**Password Bank non è in grado di registrare la mia finestra di dialogo.**

Password Bank non è in grado di gestire correttamente le finestre di dialogo che non contengono controlli standard. Gli esempi includono finestre di dialogo di Microsoft Office.

- *Password Bank è pensata principalmente per la registrazione di finestre di dialogo semplici e standard, contenenti nome utente e password. Finestre di dialogo complesse e non standard potrebbero causare problemi.*

### **La mia registrazione non viene riprodotta correttamente.**

- *La riproduzione di Password Bank suppone che la pagina utilizzata per la riproduzione corrisponda con esattezza alla pagina utilizzata in fase di creazione della registrazione. Di conseguenza, è possibile che si riscontrino problemi con le pagine create in modo dinamico con JavaScript oppure con i moduli che sembrano equivalere ma che in realtà differiscono all'interno.*

## **My Safe**

### **Non riesco a lavorare con My Safe.**

La creazione di My Safe non può essere completata se sono attivi programmi antivirus. Questo problema esiste, per esempio, con Norton AntiVirus o Sophos.

- *Impostare il programma antivirus in modo da ignorare il file con estensione fdp di My Safe. **My Safe** è memorizzato in forma codificata e quindi la scansione del contenuto non avrebbe senso.*

### **Non riesco ad accedere a My Safe tramite impronte digitali.**

- *È possibile accedere in qualsiasi momento a **My Safe** tramite l'utilizzo della password di backup di **My Safe**.*

### **My Safe è rimasto aperto (sbloccato).**

La cartella **My Safe** viene automaticamente chiusa alla disconnessione oppure allo spegnimento del computer. Tuttavia, se si blocca il computer, si chiude il browser del file oppure si rimuove la periferica biometrica, la cartella **My Safe** rimane aperta.

- *È consigliabile chiudere sempre, ovvero bloccare, **My Safe** una volta completato il proprio lavoro con i dati memorizzati.*

### **Desidero utilizzare My Safe in una diversa installazione di Protector Suite QL.**

- *È possibile copiare MySafe.fdp in un altro computer. Tuttavia, dal momento che le informazioni di autenticazione, per esempio impronte digitali, chiavi di crittografia e così via, sono univoche per ciascuna installazione, è necessario utilizzare la password di backup di **My Safe**. Questa password è stata definita durante la creazione di **My Safe**.*

### **Ho perso la password di backup di My Safe.**

La password di backup di My Safe non può essere modificata direttamente. È necessario creare una nuova **My Safe**.



**Per crearne una nuova senza perdere alcun dato:**

- 1 *Aprire **My Safe**.*
- 2 *Copiare i dati di **My Safe** in un'altra cartella.*
- 3 *Eliminare **My Safe** da **Control Center – Impostazioni – Impostazioni utente – My Safe**.*
- 4 *Creare una nuova cartella **My Safe** e definire la nuova password di backup di **My Safe**.*
- 5 *Copiare i dati nella nuova cartella **My Safe**.*

**Dopo aver aperto My Safe utilizzando la password di backup di My Safe, non riesco a utilizzare alcune funzionalità di My Safe.**

- *L'utilizzo della password di backup offre all'utente solo un accesso di emergenza ai dati. Non è da intendersi come metodo standard di apertura di **My Safe**. Effettuare l'accesso a **My Safe** utilizzando la verifica delle impronte digitali oppure, nel caso non sia possibile procedere in questo modo, eseguire il backup dei dati e creare una nuova cartella **My Safe**, come descritto sopra per il precedente problema.*

**Il computer si è bloccato. Desidero ripristinare i dati My Safe.**

Nel caso un computer oppure un sistema operativo si blocchi in modo anomalo, è ancora possibile accedere ai dati My Safe, ammesso che il file di dati My Safe data file possa essere ripristinato. Il file di dati viene salvato in “C:\Documents and Settings\<nome utente>\Application Data\Protector Suite\My Safe.fdp”.

- *Su un sistema di ripristino di destinazione, posizionare il file My Safe.fdp nella stessa cartella e procedere all'installazione di Protector Suite QL. Se si dispone di un passaporto esportato, importarlo ora; sarà così possibile accedere a **My Safe** direttamente tramite impronte digitali. In alternativa, è possibile accedere a **My Safe** utilizzando la password di backup di My Safe; **My Safe** sarà in grado di riconoscere la variazione dell'installazione e consentirà all'utente di utilizzare la password di backup.*

