

PROTECTOR SUITE QL

versione 5.6

TouchChip

Informazioni sul copyright e sulla proprietà

Le informazioni fornite si suppongono essere accurate e affidabili. Tuttavia, UPEK[®], 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.

© 2001-2007 UPEK[®], Inc – Tutti i diritti riservati

Tutti gli altri nomi sono proprietà dei rispettivi proprietari.

UPEK[®], 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).

Marchi registrati

TouchChip[®], Protector Suite[™] 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

Indice

Capitolo 1 Installazione di Protector Suite QL	3
Installazione di Protector Suite QL	3
Disinstallazione Protector Suite QL	4
Capitolo 2 Procedure preliminari.....	7
Registrazione di impronte	8
Accesso alla funzionalità principali	9
Biomenu	9
Control Center	9
Icona sulla barra delle applicazioni	10
Utilizzo della Guida	11
Capitolo 3 Utilizzo di Protector Suite QL	13
Registrazione di impronte	14
Primo utilizzo	14
Esercitazione Fingerprint	21
Protezione avanzata	23
Accesso tramite impronte digitali	24
Cambio rapido utente	25
Modifica della password Windows (ripristino)	26
Password Bank	29
Registrazione di pagine web e finestre di dialogo	29
Registrazione di siti web e finestre di dialogo con vari moduli	32
Gestione delle registrazioni	33
Attivazione/disattivazione dei suggerimenti di Password Bank	35
Utilità di avvio dell'applicazione	37
File Safe	40
Crittografia dei file (aggiunta di file o cartelle a un archivio File Safe) ..	40
Blocco e sblocco di un archivio File Safe	43
Decrittografia di file da un archivio File Safe	45
Condivisione dell'accesso agli archivi File Safe	46
Gestione degli archivi File Safe	48
Capitolo 4 Gestione di Protector Suite QL	51
Control Center	52
Impronte digitali	53
Impostazioni	57
Guida	77
Biomenu	78

Icona sulla barra delle applicazioni	79
Infopanel lettore di impronte digitali	80
Capitolo 5 Risoluzione dei problemi di Protector Suite QL	81
Installazione	81
Registrazione di impronte	82
Cambio rapido utente	86
Accesso	86
Password Bank	87



Capitolo 1

Installazione di Protector Suite QL

Installazione di Protector Suite QL

Protector Suite QL può essere installato su qualsiasi computer equipaggiato con Windows 2000, Windows XP edizione Home o Professional o Windows Vista e una porta USB libera. Per installare o disinstallare l'applicazione occorre disporre dei diritti di amministratore. Protector Suite QL Se Protector Suite QL è già preinstallato sul computer, è possibile ignorare questo capitolo.

► Per eseguire l'installazione di Protector Suite QL:

- 1 *Se si dispone di un CD, inserirlo nell'unità CD-ROM; in caso contrario, eseguire Setup.exe e passare al punto 2.*
- 2 *Viene visualizzata la schermata di Protector Suite QL. Fare clic sull'icona Installazione. Se questa schermata non viene visualizzata, eseguire manualmente Setup.exe.*
- 3 *Viene visualizzata la schermata di benvenuto.*
- 4 *Scegliere **Avanti** per continuare.*
- 5 *Viene visualizzata la schermata Informazioni utente.*

- 6 *Immettere le informazioni utente, quindi scegliere **Avanti** per continuare.*
- 7 *Confermare o selezionare una directory d'installazione.*
- 8 *Scegliere **Avanti** per continuare l'installazione.*
- 9 *Al termine dell'installazione, riavviare il computer quando richiesto.*

L'installazione è ora completa. Dopo il riavvio del computer, viene visualizzata la schermata di accesso.

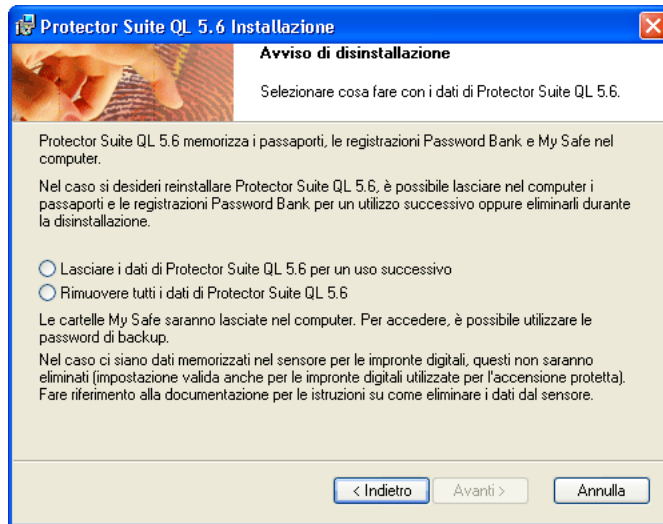


Nota: Durante l'installazione vengono installati i driver hardware necessari. Se si intende usare un sensore di impronte esterno, si raccomanda di collegarlo dopo aver completato l'installazione e riavviato il computer.

Disinstallazione Protector Suite QL

► Per eseguire la disinstallazione di Protector Suite QL:

- 1 *Fare clic su **Start > Pannello di controllo***
- 2 *Fare doppio clic sull'icona **Installazione applicazioni (Programmi e funzionalità in Windows Vista)**.*
- 3 *Selezionare **Protector Suite QL** e fare clic sul pulsante **Cambia**.*
- 4 *Fare clic sul pulsante **Rimuovi**.*



- 5 Verrà richiesto cosa fare dei dati di Protector Suite QL memorizzati nel computer. Esistono due possibilità:
- **Mantenere i dati di Protector Suite QL per un utilizzo futuro sul computer.** Ciò significa che se si reinstalla Protector Suite QL in seguito, è possibile continuare a utilizzare le impronte digitali registrate per accedere ai dati negli archivi File Safe crittografati, per accedere al computer e per accedere alle registrazioni Password Bank.
 - **Rimuovere tutti i dati Protector Suite QL dal computer.** Le impronte digitali registrate e le registrazioni Password Bank saranno eliminate in modo permanente.



Capitolo 2

Procedure preliminari

Protector Suite QL è un software biometrico che protegge la sicurezza dei dati tramite l'utilizzo della verifica delle impronte digitali. La verifica delle impronte avviene passando il dito sopra il sensore per impronte digitali.

Dopo aver installato il software e riavviato il computer, è necessario registrare le impronte per creare un'associazione tra nome utente, password e impronta digitale oltre a chiavi di sicurezza generate automaticamente. Tutti i dati vengono memorizzati nel *passaporto* dell'utente. Questa procedura viene chiamata **Registrazione di impronte**.

Dopo aver registrato le impronte, è possibile:

- *utilizzare il sensore per impronte digitali per gestire in totale sicurezza sia il livello di pre-avvio sia l'accesso al sistema operativo Windows (vedere "Accesso tramite impronte digitali" a pagina 24);*
- *registrare pagine web e applicazioni Windows per la sostituzione della password (vedere "Password Bank" a pagina 29);*
- *avviare le applicazioni preferite passando semplicemente un dito sopra il sensore (vedere "Utilità di avvio dell'applicazione" a pagina 37);*

- *archiviare informazioni confidenziali in forma crittografata in una cartella protetta (vedere “File Safe” a pagina 40).*

Questo capitolo offre una panoramica delle funzionalità e caratteristiche principali del software. Per una descrizione dettagliata di tutte le funzioni, vedere il Capitolo 3 “Utilizzo di Protector Suite QL” a pagina 13 e per una descrizione di come controllare e gestire Protector Suite QL, vedere il Capitolo 4 “Gestione di Protector Suite QL” a pagina 49.



Nota: Ogni utente Windows deve avere un Protector Suite QL passaporto unico.

Registrazione di impronte

Ogni identità utente in Protector Suite QL è rappresentata da un "passaporto" contenente i suoi dati biometrici delle impronte utilizzati per verificare l'identità dell'utente.

Prima di utilizzare il software per la prima volta, è necessario creare dei campioni di impronte digitali per il passaporto.

► Per avviare la procedura guidata di registrazione:

- *Selezionare il menu **Start > Programmi > Protector Suite QL > Registrazione utente.***

Seguire le istruzioni visualizzate. Per ulteriori informazioni, vedere il Capitolo 3 “Registrazione di impronte” a pagina 14.

Accesso alla funzionalità principali

Biomenu

Il **Biomenu** offre un rapido accesso alle funzionalità di Protector Suite QL, come il blocco del computer, l'avvio di siti registrati e la registrazione di siti web e finestre di dialogo, il blocco di file in archivi o la visualizzazione della **Guida**.

► Per visualizzare il Biomenu:

- *Dopo aver registrato almeno un'impronta digitale, passarla sopra il sensore: apparirà così il **Biomenu**.*

Per ulteriori informazioni sugli elementi del Biomenu, vedere il Capitolo 4 "Biomenu" a pagina 75.



Control Center

Dalla finestra di dialogo **Control Center** è possibile accedere alle **Impostazioni** generali di Protector Suite QL e alle funzionalità di gestione delle **Impronte digitali** (ad esempio la modifica o l'eliminazione di passaporti).

► Per visualizzare Control Center:

- *Scegliere **Start > Programmi > Protector Suite QL > Control Center**.*
- *o passare il dito per visualizzare il **Biomenu** e selezionare **Control Center**.*
- *o fare clic con il tasto destro sull'icona nella barra delle applicazioni e selezionare **Avvia Control Center...***

Viene visualizzata la schermata principale del Control Center. In questa schermata, vengono visualizzati le funzioni principali del software. Fare clic sul nome della funzione per visualizzare una schermata contenente un elenco delle azioni valide disponibili. Le funzioni includono **Impronte digitali**, **Impostazioni** ed **Guida**.



Per ulteriori informazioni su Control Center e sulle relative funzioni, vedere il Capitolo 4 “Control Center” a pagina 52.

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.

► Fare clic con il tasto destro sull'icona per visualizzare il menu:



Per ulteriori informazioni sugli elementi di menu dell'Icona sulla barra delle applicazioni, vedere il Capitolo 4 “Icona sulla barra delle applicazioni” a pagina 79.

Utilizzo della Guida

Protector Suite QL contiene un sistema di aiuto basato su HTML.

► Per visualizzare la guida HTML:

- Selezionare **Start > Programmi > Protector Suite QL > Guida**.
- o selezionare **Guida** dal **Biomenu**.
- o fare clic con il tasto destro sull'icona nella barra delle applicazioni e selezionare **Guida**.
- o fare clic sull'icona Guida nella finestra di dialogo Control Center.

Inoltre, in gran parte delle finestre di dialogo è possibile visualizzare l'aiuto contestuale.

► Per visualizzare l'aiuto contestuale:

- Premere **F1** per visualizzare la guida HTML nella finestra di dialogo per cui si necessita di aiuto.

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 be scanned or is demonstrating the process. The background is a light, textured surface.

Capitolo 3

Utilizzo di Protector Suite QL

Questo capitolo descrive nel dettaglio le funzionalità di Protector Suite QL:

“Registrazione di impronte” a pagina 14

“Accesso tramite impronte digitali” a pagina 24

“Password Bank” a pagina 29

“Utilità di avvio dell'applicazione” a pagina 37

“File Safe” a pagina 40

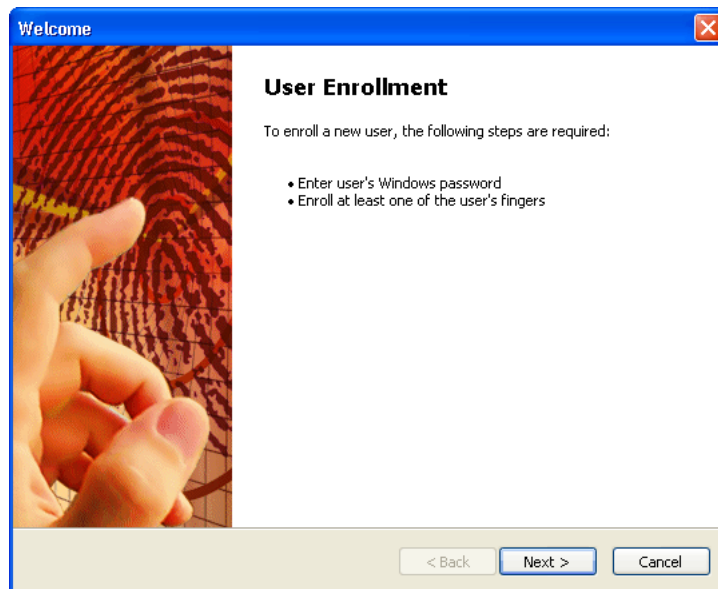
Registrazione di impronte

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

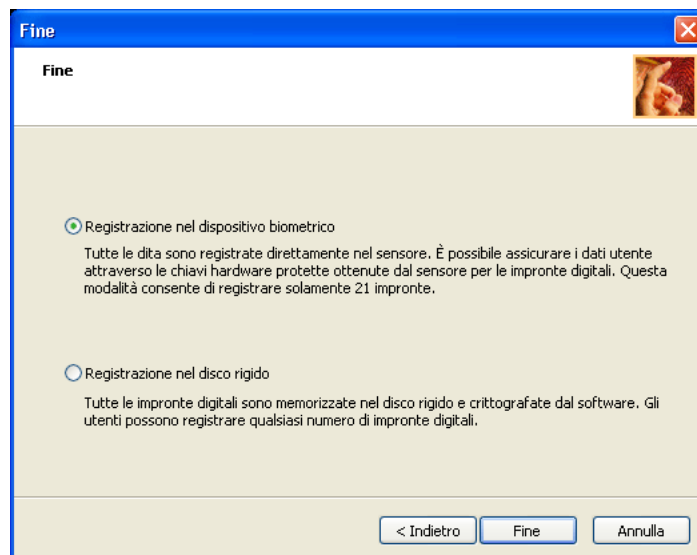
Primo utilizzo

► Per creare un nuovo passaporto (registrare impronte digitali):


- 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.*
- 2 *Viene visualizzato il Contratto di licenza. Leggere attentamente il Contratto di licenza.*
- 3 *Accettare il Contratto di licenza selezionando l'apposito pulsante di opzione. Per installare questo prodotto è necessario accettare tutti i termini del Contratto di Licenza. Se non si accettano i termini del Contratto di licenza, chiudere l'applicazione facendo clic su **Annulla**.*
- 4 *Per avviare la procedura guidata di registrazione, andare a Start > Programmi > **Protector Suite QL** > Registrazione utente.
o selezionare *Impronte digitali* > Registrazione o modifica delle impronte digitali in Control Center.
o fare clic sull'icona della barra delle applicazioni e selezionare **Modifica impronte....***



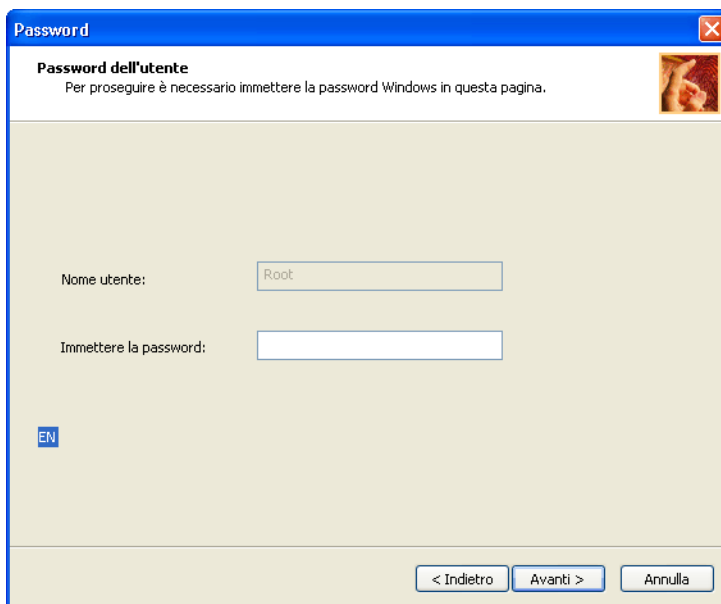
- 5 *Verrà chiesto di selezionare il tipo di registrazione. Se la periferica supporta la registrazione nella memoria della periferica, è possibile selezionare se memorizzare i dati di autenticazione nella memoria della periferica oppure sul disco rigido.*



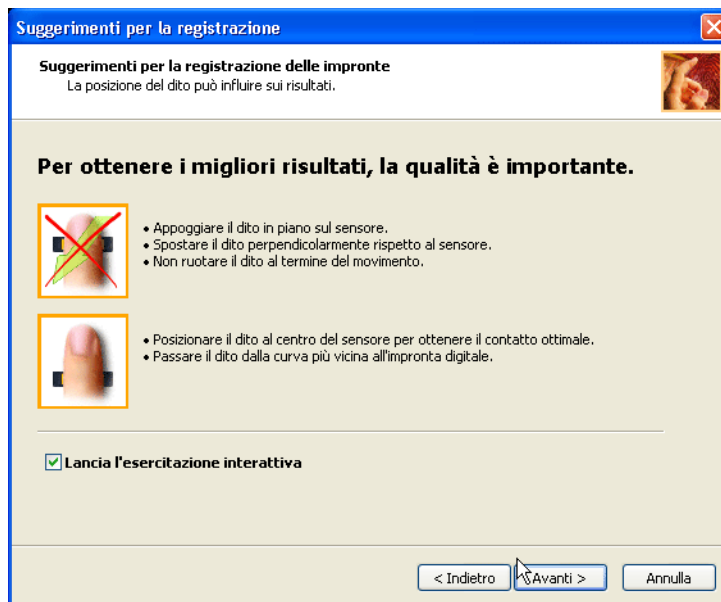
- *Se si seleziona la registrazione nella memoria della periferica, non è possibile accedere ai dati senza la periferica per le impronte digitali corrispondente. Questo significa che è possibile proteggere i propri dati con una chiave crittografica software generata dal software per le impronte digitali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

 **Importante:** Non è possibile modificare il tipo di registrazione selezionata successivamente. L'unico modo per modificarlo consiste nel disinstallare e reinstallare nuovamente Protector Suite QL.

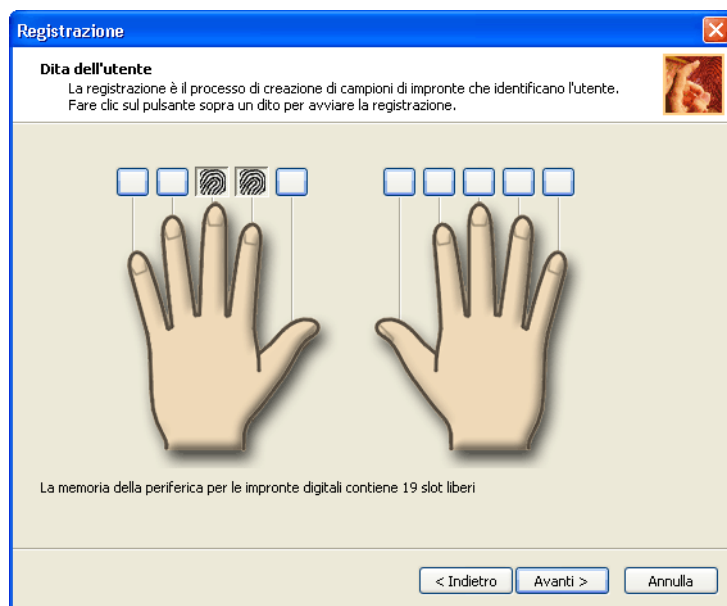
- 6 *Immettere il nome utente, la password, il dominio (se necessario) e fare clic su **Avanti**.*



- 7 Fare clic su **Avanti** per continuare con l'esercitazione sulle impronte digitali. O deselezionare la casella di controllo **Lancia l'esercitazione interattiva** e fare clic su **Avanti** per saltare l'esercitazione (per istruzioni sull'esercitazione, vedere "Esercitazione Fingerprint" a pagina 21).



- 8 *Fare clic sulla casella sopra il dito che si desidera registrare. Creare tre*



campioni del dito selezionato seguendo le istruzioni dell'esercitazione (vedere "Esercitazione Fingerprint" a pagina 21). Questi esempi verranno fusi in un'unica impronta nel passaporto. Nel caso in cui non si possa stabilire alcuna corrispondenza tra i tre campioni, verrà visualizzato un messaggio di avviso.

- 9 (Opzionale) *Se si è selezionata la registrazione sulla periferica e la configurazione di sistema supporta l'accensione protetta, tutte le impronte digitali registrate verranno utilizzate anche per l'accensione protetta.*
- 10 (Opzionale) *Se è stata selezionata la registrazione sul disco rigido e la configurazione di sistema supporta l'accensione protetta, le impronte digitali registrate verranno utilizzate anche per l'accensione protetta. Per via dei limiti di memoria della periferica, il numero massimo di impronte digitali registrabili è di 21. Se alcune delle impronte digitali registrate nei passaporti non sono assegnate all'accensione protetta nella periferica (ad esempio, è stata collegata un'altra periferica), sopra ogni dito appare il pulsante **Accensione**. Come impostazione predefinita, il pulsante Accensione viene visualizzato come "premuto". Il dito corrispondente verrà utilizzato per l'accensione protetta. Se non si*

desidera utilizzare il dito per l'accensione protetta ma solo per effettuare l'accesso, fare clic sul pulsante Accensione per eliminarlo dalla memoria della periferica.

- 11 (Opzionale) 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 o modificare i passaporti.



- 12 Selezionare un altro dito da registrare. È possibile registrare fino a dieci impronte digitali. **Si consiglia vivamente di registrare più di un'impronta, nell'eventualità di lesioni.** Fare clic su **Avanti** una volta terminata l'operazione.
- 13 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 l'opzione **Attiva sicurezza avanzata per l'utente corrente** per consentire ulteriori crittografie, ad esempio TMP.

- Impostare il tipo di **Protezione avanzata**. Per ulteriori informazioni, vedere “Protezione avanzata” a pagina 23.
 - Creare una password di backup. Questa password può essere utilizzata in caso di problema hardware del sensore per ignorare l'autenticazione tramite impronte digitali.
- 14** Per le dita aggiunte per l'accensione protetta, è necessario eseguire le operazioni descritte nella pagina finale:
- Spegnerne il computer.
 - Accendere il computer.
- 15** Quando richiesto, passare il dito Una volta terminato, fare clic su **Fine**.
- 16** 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 relative funzioni (blocco computer, registrazione pagine, finestre di dialogo ecc.); la navigazione nel Biomenu può avvenire spostando il dito sopra il sensore;
- per compilare finestre di dialogo o moduli Web registrati;
- per avviare le applicazioni preferite.



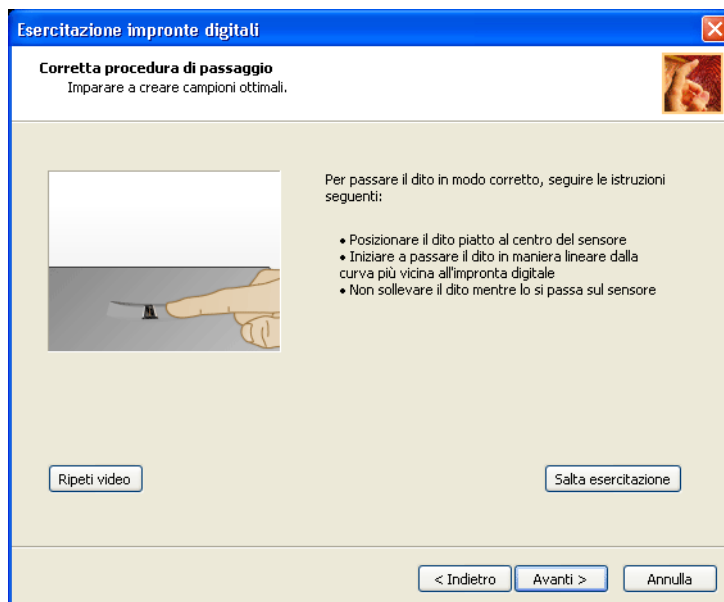
Nota: Ogni utente Windows può avere un solo passaporto. Per creare un account utente, selezionare **Start > Control Panel** e fare clic su **Account utente**. Seguire le istruzioni visualizzate.

Esercitazione Fingerprint

È estremamente raccomandato seguire l'Esercitazione Fingerprint. L'esercitazione mostrerà un breve filmato in cui verranno dimostrate 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.

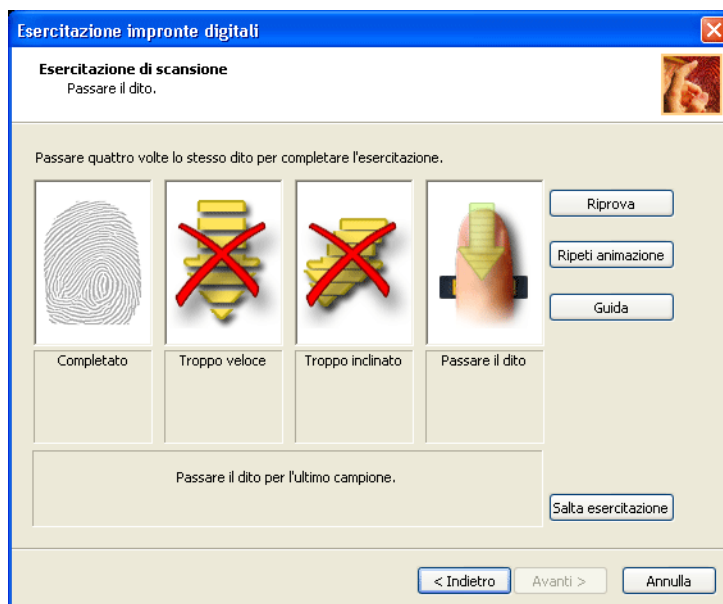
► Per eseguire l'esercitazione:

- 1 Per avviare l'esercitazione, andare a **Start > Programmi > Protector Suite QL > Esercitazione impronte digitali**.
o eseguirla dalla procedura guidata di registrazione delle impronte digitali.
o selezionare **Guida > Esercitazione** nella finestra di dialogo **Control Center**.
- 2 La pagina di apertura illustra le finalità dell'esercitazione.
- 3 La pagina successiva illustra la corretta procedura di scansione e mostra un breve video dimostrativo:



- Posizionare il dito piatto al centro del sensore.
- Iniziare a passare il dito in maniera lineare dalla curva più vicina all'impronta digitale.
- Non sollevare il dito mentre lo si passa sul sensore.

- 4 Nella pagina successiva, provare a creare quattro campioni dell'impronta digitale. Se i campioni non corrispondono, si consiglia di fare clic sul pulsante **Riprova** per ripetere la scansione. Utilizzare il pulsante **Ripeti video** per riprodurre nuovamente il video dimostrativo. Dopo aver creato correttamente i campioni, fare clic su **Fine** per chiudere l'esercitazione o per tornare alla procedura guidata di registrazione.



Nota: Le operazioni biometriche (registrazione, verifica, esercitazione) vengono messe in pausa dopo circa 2 minuti di inattività per prevenire un eccessivo consumo di energia. In caso di pausa, è sufficiente riavviare semplicemente il processo.

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. Il tipo di crittografia può essere modificato utilizzando questa finestra di dialogo per regolare il livello di sicurezza necessario per praticità dell'utente.

► Per attivare la sicurezza avanzata (opzionale):

- 1 Andare a **Start > Programmi > Protector Suite QL > Registrazione utente**
per avviare la procedura guidata di registrazione.
- 2 Nella finestra di dialogo **Protezione avanzata** dopo la registrazione, selezionare **Attiva sicurezza avanzata** attivare la sicurezza avanzata per l'utente corrente.
- 3 Impostare il tipo di **Protezione avanzata**.

Sicurezza avanzata
Configurare il livello di sicurezza del passaporto

☒ Attiva sicurezza avanzata per l'utente corrente

I dati saranno codificati da un'ulteriore chiave di sicurezza ottenibile da un dispositivo di sicurezza dell'hardware.

Tipo sicurezza avanzata:

Chiave lettore d'impronte digitali

Sicurezza su base hardware. I dati utente segreti saranno protetti da una chiave sicura memorizzata all'interno del lettore d'impronte digitali e rilasciati solamente con corretta corrispondenza dell'impronta digitale. I dati sono crittografati utilizzando la chiave memorizzata nella periferica per le impronte.

☒ Attiva password di backup, che sarà usata nel caso che il sistema di sicurezza non funzioni

Password di backup:

Immettere nuovamente la password:

< Indietro Avanti > Annulla

- **Chiave lettore d'impronte digitali con TPM** - offre una sicurezza migliorata basata su hardware. 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 basata su hardware. 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 crittografati dall'utente verranno protetti dal 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 segreti dell'utente verranno protetti dal TPM Security Chip. Raccomandato per una maggiore praticità.
- 4 **Impostare la password di backup.** È possibile utilizzare la password di backup nel caso di guasto hardware per superare la fase di autenticazione tramite impronte digitali. Si raccomanda di utilizzare una password complessa. Qualora non si definisca una password di backup, è possibile perdere i propri dati in caso di guasto dell'hardware di autenticazione.

Accesso tramite impronte digitali

Per attivare l'accesso tramite impronte digitali, è necessario registrare le impronte (vedere "Registrazione di impronte" a pagina 14). Durante la registrazione dell'utente, vengono analizzati i campioni di impronte digitali e viene creata la connessione tra i campioni di impronte digitali e l'account utente di Windows. Quando si riavvia il computer e si desidera accedervi nuovamente, la finestra di dialogo di accesso richiederà di passare il dito sopra il sensore o di premere **Ctrl + Alt + Canc** per accedere utilizzando la password Windows. Una volta passato il dito, l'impronta digitale registrata viene riconosciuta e l'utente è connesso.

L'accesso biometrico protegge anche screen saver e riattivazione delle funzionalità di risparmio energetico (è necessario impostare sul sistema la richiesta della password dopo la riattivazione da screen saver e standby; andare a **Start > Pannello di controllo**, fare clic su **Schermo** e selezionare la scheda **Screen saver** per impostare lo screen saver).

► **Per disattivare l'Accesso tramite impronte digitali:**

- Scegliere **Start >Programmi > Protector Suite QL > Control Center**.
o passare il dito per visualizzare il **Biomenu** e selezionare **Control Center**.
- Selezionare **Impostazioni del sistema > Accesso**.
- Selezionare il pulsante di opzione Windows standard. L'accesso tramite impronte digitali verrà disattivato e sarà possibile accedere al sistema utilizzando l'accesso Windows standard.

► **Attivazione dell'accesso tramite impronte digitali:**

- Scegliere **Start >Programmi > Protector Suite QL > Control Center**.
o passare il dito per visualizzare il **Biomenu** e selezionare **Control Center**.
- Selezionare **Impostazioni > Impostazioni del sistema > Accesso**.
- Selezionare il pulsante di opzione Accesso tramite impronte digitali per attivare l'accesso al sistema tramite impronte anziché l'accesso tramite password Windows.

Per ulteriori informazioni sulle impostazioni di Accesso, vedere il Capitolo 4, Control Center "Accesso" a pagina 58.



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

Protector Suite QL opera anche in concomitanza con 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. I seguenti client Novell non funzionano con Protector Suite QL: 4.83, 4.90.

Cambio rapido utente

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

► **Per attivare Cambio rapido utente:**

- 1 Scegliere **Start >Programmi > Protector Suite QL > Control Center**.
- 2 o passare il dito per visualizzare il **Biomenu** e selezionare **Control Center**.
- 3 Selezionare **Impostazioni > Impostazioni del sistema**.
- 4 Selezionare la scheda **Accesso**.
- 5 Selezionare l'opzione **Abilita il supporto del cambio rapido utente**. Se l'opzione non è visibile, il sistema non supporta questa funzione (ad esempio, il computer è membro di un dominio. Per attivare il supporto Cambio rapido utente, è necessario rimuovere il computer dal dominio.).

► **Per rimuovere un computer da un dominio:**

- 1 Fare clic con il tasto destro su **Risorse del computer** sul desktop o, dal menu **Start**, selezionare **Proprietà**.
- 2 In Windows Vista, fare clic sul collegamento **Cambia impostazioni e autorizzarsi come amministratore**.
- 3 Selezionare la scheda **Nome computer**.
- 4 Fare clic sul pulsante **Cambia** (o **Rinomina**) e selezionare il pulsante di opzione **Gruppo di lavoro** nel riquadro **Membro di**.



Nota: Solo l'amministratore può rimuovere un computer da un dominio.

Modifica della password Windows (ripristino)

La password di accesso a Windows può essere modificata da un utente (tramite il pannello di controllo o la finestra di dialogo Ctrl+Alt+Canc) o da un amministratore (tramite il ripristino password). Non vi sono differenze tra i due tipi di modifica della password rispetto a Protector Suite QL. Gli scenari variano a seconda del tipo di account utente utilizzato e del modo in cui gli utenti accedono al computer.

Ciò vale per Windows 2000 e XP (in Windows Vista la funzionalità è simile ma viene visualizzata una GUI differente).

Quando si utilizza un account utente locale su un computer in un gruppo di lavoro o in un dominio, vi sono due possibili scenari.

- 1 *Un utente accede utilizzando nome utente e password Windows e successivamente la password viene modificata.*
 - *l'utente blocca il computer o si disconnette;*
 - *l'utente passa un'impronta digitale registrata;*
 - *viene visualizzato un messaggio indicante che si è utilizzato un nome utente o una password errati;*
 - *l'utente deve immettere una nuova password; questa password viene quindi memorizzata nel passaporto delle impronte digitali, il passaporto viene aggiornato e l'utente accede al computer; la volta successiva, l'accesso tramite impronte digitali verrà eseguito normalmente.*
- 2 *Un utente accede utilizzando un'impronta digitale registrata e successivamente la password viene modificata.*
 - *La password viene memorizzata nel passaporto delle impronte digitali; in seguito, non sarà necessario immettere nuovamente la nuova password.*
 - *L'utente blocca il computer o si disconnette.*
 - *L'utente passa un'impronta digitale registrata.*
 - *Il computer viene sbloccato o l'utente esegue l'accesso.*

Quando si utilizza un account utente di dominio in un dominio.

L'utente accede utilizzando nome utente e password Windows o un'impronta digitale registrata. La password viene successivamente modificata.

- *l'utente blocca il computer o si disconnette;*
- *l'utente passa un'impronta digitale registrata;*
- *viene visualizzato un messaggio indicante che si è utilizzato un nome utente o una password errati;*
- *l'utente deve immettere una nuova password; questa password viene quindi memorizzata nel passaporto delle impronte digitali, il passaporto viene aggiornato e l'utente accede al computer; la volta successiva, l'accesso tramite impronte digitali verrà eseguito normalmente.*

Casi particolari.

Viene impostata l'opzione per cui l'utente dovrà modificare la password all'accesso successivo oppure la scadenza della password è definita nel dominio.

- *Su un computer client un utente esegue l'accesso utilizzando un'impronta digitale registrata.*
- *Appare una finestra di dialogo che richiede all'utente di modificare la password; questa password viene quindi memorizzata nel passaporto delle impronte digitali, il passaporto viene aggiornato e l'utente accede al computer; la volta successiva, l'accesso tramite impronte digitali verrà eseguito normalmente.*

Password Bank

Password Bank è una funzionalità opzionale di Protector Suite QL. Quando installata, Password Bank archivia le registrazioni (nomi utente, password e altre impostazioni) dei siti web e delle finestre di dialogo delle applicazioni per consentire agli utenti di accedere ai siti web e alle applicazioni visitati o utilizzati più di frequente (webmail, conti bancari, e-commerce, ecc.) in assoluta sicurezza, senza la preoccupazione di dover immettere nuovamente nomi utente e password o compilare moduli. Si immettono le informazioni necessarie una sola volta, durante la registrazione della pagina Web o della finestra di dialogo con password. Quando la finestra sarà visualizzata nuovamente, sarà possibile riprodurre tutti i dati utilizzando il sensore. È inoltre possibile accedere ai siti Web registrati direttamente dal Biomenu.

Password Bank supporta i seguenti browser: Internet Explorer 5.0 e successivo, Firefox 1.0 - 1.5. Il supporto per Internet Explorer viene installato automaticamente. Quando Protector Suite QL rileva Firefox, chiede all'utente se attivare il supporto. In alternativa, è possibile attivare il supporto di Firefox da **Control Center > Impostazioni > Impostazioni 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.

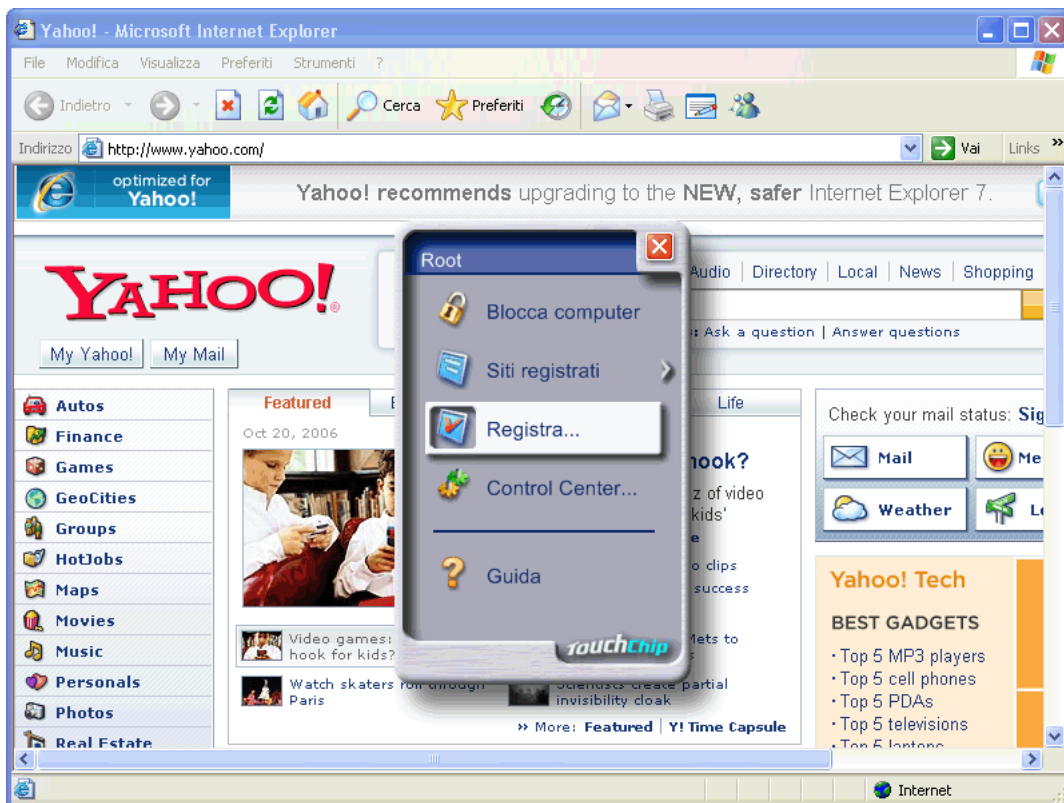
La registrazione di applicazioni a 32 bit eseguite su sistemi a 64 bit non è supportata.

Registrazione di pagine web e finestre di dialogo

Affinché sia possibile riprodurli in seguito, ad esempio completando automaticamente un modulo semplicemente passando il dito sopra il sensore, è necessario prima registrare siti web e finestre di dialogo per memorizzarne le informazioni (nomi utente, password e altre impostazioni).

► Per creare una nuova registrazione:

- 1 *Visualizzare la pagina Web o la finestra di dialogo che si desidera registrare.*
- 2 *Popolare i campi relativi a nome utente, password e qualsiasi altro campo necessario.*
- 3 *Passare il dito per visualizzare il **Biomenu**.*
- 4 *Selezionare **Registra...***



Tutti i dati personali sono stati memorizzati. Dopo aver creato una registrazione, viene visualizzato un suggerimento nell'angolo del browser a conferma dell'avvenuta creazione. (Per ulteriori informazioni su come attivare/disattivare questi suggerimenti, vedere "Attivazione/disattivazione dei suggerimenti di Password Bank" a pagina 35). Fare clic su **Modifica** per modificare i dettagli della registrazione direttamente dalla finestra di dialogo del suggerimento.

Riproduzione delle registrazioni

Se si riproduce una registrazione, il sito Web registrato verrà avviato e l'utente vi accederà in automatico utilizzando le credenziali registrate.

► Per riprodurre una registrazione:

- 1 *Visualizzare la finestra di dialogo o il sito web registrato.*
- 2 *Passare il dito sul sensore per le impronte digitali.*
- 3 *(facoltativo) Se viene visualizzato il suggerimento relativo alla riproduzione delle finestre di dialogo, confermare che si desidera riprodurre la registrazione.*
- 4 *Verrà riprodotta la registrazione.*

► Per avviare un sito web registrato è possibile utilizzare anche il Biomenu.

- *Passare il dito per visualizzare il **Biomenu**.*
- *Selezionare **Siti registrati**. Appare un elenco di siti registrati.*
- *Fare clic su un sito e il sito verrà aperto nel browser e la registrazione riprodotta oppure fare clic su **Indietro** per tornare al **Biomenu**.*



Registrazione di siti web e finestre di dialogo con vari moduli

Registrazione di siti web con vari moduli

Password Bank registra moduli individuali. Se un sito contiene diversi moduli, è necessaria una registrazione separata per ogni modulo. Ciò significa che è possibile registrare solamente un modulo attivo.

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.

- *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. Dopo aver compilato il modulo A, si fa clic all'esterno del modulo che perde lo stato attivo, ma si utilizza una versione precedente di IE. Non viene eseguita alcuna azione.

Riproduzione delle registrazioni di siti web con vari moduli:

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.

- *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.*

Registrazione e riproduzione di finestre di dialogo complesse

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 non essere supportate. È sempre possibile registrare i campi di testo e i campi password. Le registrazioni salvano i controlli non nascosti, disabilitati, ridotti ecc. I pulsanti di opzioni, le caselle di selezione, le caselle combinate e le selezioni in caselle elenco vengono registrati per le applicazioni che utilizzano i controlli Windows standard (ad 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 controlli prima dell'utilizzo ma solo il disegno. Esempi tipici sono alcune delle 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

Talvolta può essere utile modificare la registrazione esistente, ad esempio se la mailbox della società è cambiata e si desidera aggiornare le registrazioni. Inoltre, è possibile eliminare la registrazione o attivare/disattivare l'invio automatico della registrazione riprodotta. È possibile esportare la registrazione per utilizzarla su un altro computer. Una registrazione esportata è un file con estensione ***.pb** che può essere importato successivamente.

► **Per gestire le registrazioni:**

- 1 Selezionare **Start > Programmi > Protector Suite QL > Control Center**.
o passare il dito per visualizzare il **Biomenu** e selezionare **Control Center**.
- 2 Selezionare **Impostazioni > Impostazioni utente**. Selezionare **Impostazioni > Impostazioni utente**. È necessaria l'autenticazione.
Passare il dito sul sensore per le impronte digitali quanto richiesto.
- 3 Selezionare la scheda **Registrazioni**.



- 4 Selezionare una registrazione con cui si desidera lavorare.
 - Fare clic sul pulsante **Rinomina** per modificare il nome predefinito archiviato con la registrazione. Il nome immesso è solamente una descrizione visualizzata nel **Biomenu**; non influisce sulle informazioni memorizzate con la registrazione.
 - Fare clic sul pulsante **Elimina** per eliminare la registrazione.
 - Fare clic sul pulsante **Modifica** per modificare i dettagli della registrazione archiviata (ad esempio, il nome utente o la password sono stati modificati e si desidera che tale cambiamento venga rispecchiato nella registrazione esistente). La casella di controllo **Invio automatico del modulo** consente di inviare automaticamente il modulo dopo la

riproduzione della registrazione. Se si seleziona questa opzione, la registrazione verrà riprodotta automaticamente dopo il passaggio del dito. In caso contrario, appare una finestra di dialogo che richiede all'utente di confermare la riproduzione. Ciò avviene ogni volta che si accede a una finestra di dialogo o a un sito web registrato.

- Fare clic sul pulsante **Esporta** per esportare la registrazione, ad esempio per utilizzarla su un altro computer. Scegliere le registrazioni da esportare o se esportare tutte le registrazioni esistenti automaticamente. Per selezionare più registrazioni, tenere premuto il tasto **Ctrl** o **Maiusc** mentre si esegue la selezione. Quindi selezionare un file di destinazione e immettere una password. Questa password verrà richiesta durante l'importazione delle registrazioni. L'estensione del file di Password Bank è ***.pb**.

- Fare clic sul pulsante **Importa** per importare le registrazioni da un file Password Bank. Selezionare il file ***.pb** di origine. Se una o più registrazioni tra quelle che si stanno importando esistono già, scegliere se sovrascrivere le registrazioni esistenti con quelle importate o aggiungere le registrazioni importate all'elenco di registrazioni. (Se si conservano le registrazioni e si importano altre registrazioni con lo stesso nome, al nome delle nuove registrazioni importate dal file ***.pb** verrà aggiunto un numero.) Immettere la password creata durante l'esportazione.

Attivazione/disattivazione dei suggerimenti di Password Bank

Password Bank visualizza dei suggerimenti per l'utente, quando è possibile eseguire un'azione (registrazione di una finestra di dialogo, riproduzione di una finestra di dialogo, ecc....). Questi suggerimenti possono essere attivati o disattivati nella finestra di dialogo **Impostazioni utente**. Se l'utente accede a Windows utilizzando nome utente e password, i suggerimenti non vengono attivati finché non si esegue una corretta verifica delle impronte digitali.

► Per attivare/disattivare i suggerimenti:

- 1 Selezionare **Start > Programmi > Protector Suite QL > Control Center**.
o passare il dito per visualizzare il **Biomenu** e selezionare **Control Center**.
- 2 Selezionare **Impostazioni > Impostazioni utente**. È necessaria l'autenticazione. Passare il dito sul sensore per le impronte digitali quanto richiesto.

- 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. Fare clic su **Modifica** per modificare la registrazione direttamente da questa finestra di dialogo.
 - **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.

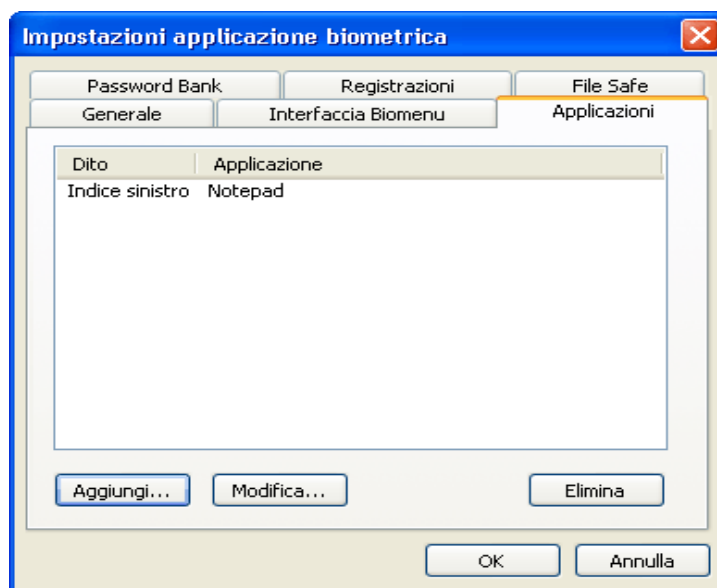
Utilità di avvio dell'applicazione

L'Utilità di avvio dell'applicazione è una funzionalità opzionale di Protector Suite QL.

Se installata, consente di avviare le applicazioni registrate passando semplicemente il dito sopra il sensore.

È necessario lasciare almeno un dito registrato senza assegnazione per permettere la visualizzazione del Biomenu. Il numero massimo di applicazioni avviabili in questo modo è pari al numero di dita registrate -1.

Se si desidera ignorare l'avvio dell'applicazione e richiamare il **Biomenu**, tenere premuto **Maiusc** mentre si passa il dito.



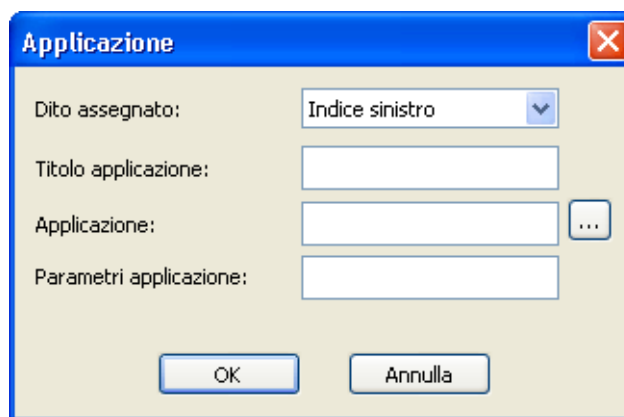
► Per creare l'associazione tra un dito registrato e un'applicazione:

- 1 Selezionare **Start > Programmi > Protector Suite QL > Control Center**.
o passare il dito per visualizzare il **Biomenu** e selezionare **Control Center**.
- 2 Selezionare **Impostazioni > Impostazioni utente**. È necessaria l'autenticazione. Passare il dito sul sensore per le impronte digitali quanto richiesto.
- 3 Selezionare la scheda **Applicazioni**.

- 4 Fare clic sul pulsante **Aggiungi**. Verrà visualizzata la finestra di dialogo **Applicazione**.
- 5 Selezionare una delle dita registrate libere. Appare una finestra che richiede la registrazione di più dita se non ve ne sono disponibili.
- 6 Inserire il nome dell'applicazione. (Tale nome Appare nella scheda **Applicazioni in Impostazioni utente**.)
- 7 Cercare il file che si desidera avviare: Può essere qualsiasi file eseguibile (ad esempio, *explorer.exe*).
- 8 Facoltativamente, è possibile immettere parametri aggiuntivi nel campo Parametri applicazione. Se non si è sicuri, lasciare il campo vuoto. Di seguito sono riportati alcuni esempi di parametri applicazione.
- 9 Fare clic su **OK**.

Esempi di parametri applicazione

- È possibile aprire un sito Web avviando un browser Web come Internet Explorer. Digitare l'indirizzo di un sito Web (come *www.upek.com*) nel campo dei parametri applicazione e il sito verrà visualizzato ogni volta che si passerà il dito assegnato e si avvierà il browser.



- È possibile aprire un file tramite un'applicazione, come avviene per i documenti di Microsoft Word. Digitare il percorso del file tra virgolette (ad esempio "*C:\Documents and Settings\account.personale\Documenti\documento.doc*"). Il file *documento.doc* si aprirà in Word ogni volta che si passerà il dito. È possibile utilizzare più parametri per una applicazione.

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

- 1 *Selezionare un'applicazione nella scheda **Applicazioni**.*
- 2 *Scegliere il pulsante **Modifica**.*
- 3 *Apportare le modifiche necessarie nella scheda **Applicazioni**.*
- 4 *Fare clic su **OK**.*

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

- 1 *Selezionare un'applicazione nella scheda **Applicazioni**.*
- 2 *Scegliere il pulsante **Elimina**.*

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

File Safe

File Safe è una funzionalità opzionale di Protector Suite QL.

File Safe consente di memorizzare i file in un archivio crittato sul disco rigido. Gli archivi crittati possono contenere file o cartelle e sono protetti tramite verifica delle impronte digitali o password, se impostata al momento della creazione dell'archivio. Quando un archivio File Safe è sbloccato, è possibile lavorare con il file dell'archivio come se fosse una cartella standard (eliminare, copiare o assegnare un nuovo nome ai file, ecc.). Anche il drag-and-drop è supportato. È possibile copiare e incollare o trascinare i file nell'archivio sbloccato; quando lo si bloccherà nuovamente, i file verranno crittati. Quando solamente un file è crittografato in un archivio ed è sbloccato, è sufficiente un clic su di esso per aprirlo. È inoltre possibile condividere gli archivi crittati con altri utenti dotati di impronte digitali registrate.

Crittografia dei file (aggiunta di file o cartelle a un archivio File Safe)

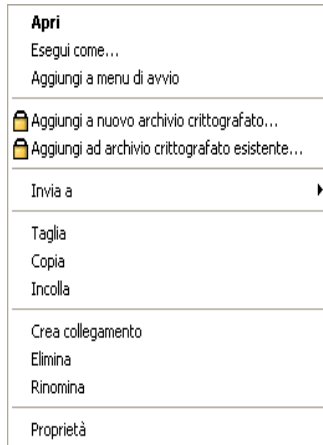
L'utente ha avuto accesso al computer e desidera aggiungere dei file a un archivio crittografato.



Nota: Prima di creare un archivio, è necessario registrare le impronte digitali. In caso contrario, apparirà un avviso indicante che nessun utente è stato selezionato. Per informazioni su come registrare le impronte digitali, vedere Registrazione di impronte.

► Per aggiungere file o cartelle a un nuovo archivio File Safe:

- 1 *Visualizzare i file o le cartelle che si desidera crittografare (utilizzando Esplora risorse o un'altra finestra di dialogo di Windows).*
- 2 *Selezionare i file e/o le cartelle (utilizzando il mouse e i tasti Maiusc o Ctrl) e fare clic con il tasto destro per visualizzare il menu contestuale.*
- 3 *Selezionare **Aggiungi a nuovo archivio crittografato**.*



- 4 *Appare una finestra di dialogo che chiede all'utente di*
 - *Scegliere una cartella di destinazione (fare clic su ... per sfogliare e selezionare una cartella).*
 - *Scegliere una password. Per ulteriori informazioni, vedere di seguito.*
 - **Avanzate >>** *Selezionare gli utenti che hanno accesso ai file crittografati.*
 - *Premere **OK**. Verrà richiesto di passare il dito sopra il sensore per verificare l'identità dell'utente.*
- 5 *Dopo la crittografia dei file, una finestra di dialogo chiederà quale operazione eseguire con i file originali:*
 - **Conserva i file originali** *non elimina i file originali, che verranno salvati sia nell'archivio crittografato sia nel percorso originale, non crittografati.*
 - **Elimina i file originali** *elimina i file originali e ne mantiene unicamente la forma crittografata nell'archivio.*
 - *Selezionare la casella di controllo **Pulire i file prima di eliminare** per sovrascrivere i file che si desidera eliminare con un contenuto casuale prima di eliminarli. In tal modo sarà impossibile recuperare i file eliminati.*
- 6 *Viene ora creato l'archivio crittografato (con estensione ***.uea** oppure ***.ueaf** se è stato crittografato unicamente un file).*

Tipi di password:

- **Nessuna password di backup**, per lasciare l'archivio protetto unicamente tramite impronte digitali. Non vi è modo di accedere ai file archiviati nell'archivio File Safe quando non è possibile effettuare la verifica delle impronte digitali (in caso di lesioni alle dita, problemi della periferica, ecc.).
- **Utilizza password di backup globale**, per impostare una password globale, ovvero una password di backup comune a tutti gli archivi. Si tratta di un'opzione utile se si desidera evitare l'utilizzo di password diverse ogni volta che si crea un archivio. Se non è stata ancora impostata la password di backup globale, questa opzione sarà disattivata. Informazioni su come impostare o modificare la password di backup globale in "Gestione degli archivi File Safe" a pagina 48.
- **Utilizza la password di backup seguente**, per creare una nuova password per l'archivio File Safe corrente.

Si consiglia di utilizzare una password di backup perché in caso contrario non sarebbe possibile sbloccare gli archivi qualora non fosse possibile effettuare la verifica delle impronte digitali (lesioni alle dita, problemi della periferica, ecc.). Utilizzare una password complessa, di almeno otto caratteri, che includa caratteri non alfanumerici, ecc.

Nei casi in cui la verifica delle impronte digitali non è possibile, appare una finestra di dialogo che richiede una password di backup. È possibile forzare la visualizzazione di questa finestra di dialogo e ignorare la verifica delle impronte digitali chiudendo la finestra di dialogo che richiede all'utente di passare il dito.



Nota: Se non si imposta una password di backup e le impronte digitali registrate vengono eliminate, non sarà possibile aprire gli archivi File Safe bloccati. Sbloccare gli archivi File Safe e spostare i file prima di eliminare le impronte digitali o impostare una password di backup.

► Per aggiungere file o cartelle a un archivio File Safe esistente:

- 1 Visualizzare i file o le cartelle che si desidera crittografare (utilizzando Esplora risorse o un'altra finestra di dialogo di Windows).
- 2 Selezionare i file e/o le cartelle (utilizzando il mouse e i tasti Maiusc o Ctrl) e fare clic con il tasto destro per visualizzare il menu contestuale.

- 3 Selezionare **Aggiungi ad archivio crittografato esistente**.
- 4 Sfogliare e selezionare l'archivio cui si desidera salvare i file (il file ha l'estensione ***.uea**).
- 5 Selezionare **Apri**.
- 6 Passare il dito sul sensore quanto richiesto.
- 7 Dopo la crittografia dei file, una finestra di dialogo chiederà quale operazione eseguire con i file originali:
 - **Conserva i file originali** non elimina i file originali, che verranno salvati sia nell'archivio crittografato sia nel percorso originale, non crittografati.
 - **Elimina i file originali** elimina i file originali e ne mantiene unicamente la forma crittografata nell'archivio.
 - Selezionare la casella di controllo **Pulire i file prima di eliminare** per sovrascrivere i file che si desidera eliminare con un contenuto casuale prima di eliminarli. In tal modo, nessuno potrà recuperare i file eliminati. I file sono ora aggiunti all'archivio File Safe crittografato.

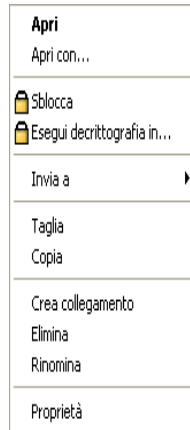
Blocco e sblocco di un archivio File Safe

L'utente ha eseguito l'accesso al computer e desidera bloccare o sbloccare un archivio File Safe crittato.

Quando un archivio File Safe è sbloccato, è possibile lavorare con il file dell'archivio come se fosse una cartella standard (eliminare, copiare o assegnare un nuovo nome ai file, ecc.). Anche il drag-and-drop è supportato. Quando solamente un file è crittografato in un archivio ed è sbloccato, è sufficiente un clic su di esso per aprirlo. Sbloccarlo procedendo come per gli archivi File Safe standard.

► Per sbloccare e aprire un archivio File Safe:

- 1 Selezionare il file d'archivio (***.uea** o ***.ueaf**) che si desidera aprire e fare clic con il tasto destro per visualizzare il menu contestuale.
- 2 Scegliere **Apri** o **Sblocca**.



- 3 *Verrà richiesto di passare un dito o immettere la password di backup per verificare l'identità dell'utente (a seconda delle opzioni impostate al momento della creazione dell'archivio).*
- 4 *L'archivio viene ora sbloccato ed è possibile lavorarci come con qualsiasi altra cartella standard (eliminare, copiare o assegnare un nuovo nome ai file, ecc.). Se è un archivio con un solo file (*.ueaf), verrà aperto il file nell'archivio (ad esempio, si aprirà un documento di testo).*



Nota: Se si fa doppio clic su un archivio:

- *se è bloccato, verrà richiesta l'autorizzazione (passare il dito o immettere la password), quindi la cartella d'archivio verrà sbloccata e aperta;*
- *se è già sbloccato, la cartella d'archivio verrà aperta;*
- *se vi è un solo file crittato ed è bloccato, verrà richiesta l'autorizzazione, quindi il file verrà avviato;*
- *se vi è un solo file crittato ed è sbloccato, il file verrà avviato..*

► Per bloccare un archivio File Safe:

- 1 *Selezionare un file d'archivio sbloccato (*.uea o *.ueaf) e fare clic con il tasto destro per visualizzare il menu contestuale.*
- 2 *Scegliere **Blocca**. Non viene richiesta alcuna verifica in questa fase.*
- 3 *L'archivio viene ora bloccato.*

► **Per bloccare tutti gli archivi File Safe:**

- 1 *Per visualizzare il **Biomenu**, passare il proprio dito sopra il sensore.*
- 2 *Selezionare **Blocca tutti gli archivi** dal menu. Non viene richiesta alcuna verifica in questa fase.*
- 3 *Tutti gli archivi sbloccati vengono ora bloccati.*

Decrittografia di file da un archivio File Safe

L'utente ha avuto accesso al computer e desidera decrittare file o cartelle da un archivio File Safe. L'utente può selezionare l'intero archivio File Safe e decrittare tutti i file in esso contenuti oppure selezionare diversi file da un archivio e decrittarli.

► **Per decrittare tutti i file o cartelle in un archivio File Safe contemporaneamente**

- 1 *Selezionare il file d'archivio (***.uea** o ***.ueaf**) che si desidera decrittare e fare clic con il tasto destro per visualizzare il menu contestuale.*
- 2 *Scegliere **Esegui decrittografia in...***
- 3 *Scegliere un percorso di destinazione dove salvare i file decrittati.*
- 4 *Verrà richiesto di passare un dito o immettere una password per verificare l'identità dell'utente (a seconda delle opzioni impostate al momento della creazione dell'archivio).*
- 5 *I file sono decrittati al percorso selezionato.*

Per eseguirne nuovamente la crittografia o creare un nuovo archivio, vedere “Crittografia dei file (aggiunta di file o cartelle a un archivio File Safe)” a pagina 40.


► **Per eseguire la decrittografia dei file o delle cartelle selezionati da un archivio File Safe:**

- 1 *Selezionare il file d'archivio (***.uea**) che si desidera decrittare e aprirlo (fare doppio clic e se bloccato eseguire la verifica).*
- 2 *Selezionare il o i file da decrittare (utilizzando il mouse e i tasti **Maiusc** o **Ctrl**) e fare clic con il tasto destro per visualizzare il menu contestuale.*
- 3 *Selezionare **Esegui decrittografia in...***
- 4 *Scegliere un percorso di destinazione dove salvare il o i file decrittati.*

- 5 *Scegliere quale operazione eseguire con i file originali nell'archivio:*
Elimina i file originali - i file decrittati verranno eliminati dall'archivio.
Conserva i file originali - i file nell'archivio crittografato verranno conservati.
- 6 *I file sono vengono quindi decrittati al percorso selezionato.*
Per eseguire nuovamente la crittografia dei file o creare un nuovo archivio, vedere “Crittografia dei file (aggiunta di file o cartelle a un archivio File Safe)” a pagina 40.

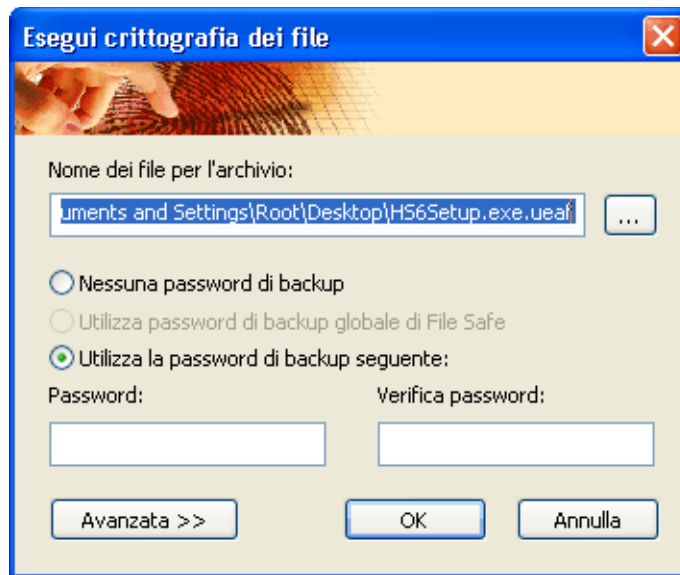
Condivisione dell'accesso agli archivi File Safe

Gli utenti possono condividere l'accesso agli archivi File Safe. Quando si crea un archivio, è possibile scegliere gli utenti che potranno disporre di un accesso condiviso a tale archivio utilizzando impronte digitali registrate. Inoltre, è possibile concedere (o negare) agli utenti l'accesso in un secondo momento, nelle **Proprietà** File Safe. Chiunque, e non solamente gli utenti con privilegi di condivisione dell'archivio, può accedere all'archivio utilizzando una password di backup valida.

 **Importante:** Tutti gli utenti che condividono un archivio dispongono degli stessi privilegi d'accesso, tra cui la capacità di eliminare e aggiungere file, modificare la password di accesso all'archivio, negare l'accesso ad altri utenti, ecc.

► Per concedere l'accesso agli utenti quando si crea un archivio:

- 1 *Fare clic con il tasto destro sui file che si desidera crittografare e selezionare **Aggiungi a nuovo archivio crittografato** dal menu.*
- 2 *Scegliere una password di backup. Tutti gli utenti utilizzeranno la stessa password di backup.*
- 3 *Fare clic su **Avanzate >>**.*



- 4 **Apparirà la finestra Esegui crittografia per utenti** contenente un elenco di utenti registrati. Fare clic sugli utenti che condivideranno l'archivio.
- 5 Fare clic su **OK**. Tutti gli utenti selezionati potranno sbloccare l'archivio passando un dito sopra il sensore.

► **Per concedere o negare l'accesso agli utenti nelle Proprietà File Safe:**

- 1 Selezionare un file d'archivio (*.uea o *.ueaf
- 2) e fare clic con il tasto destro, quindi selezionare **Proprietà**.
- 3 Se l'archivio è bloccato, fare clic su **Sblocca** per poter accedere alle opzioni delle proprietà. Identificarsi tramite impronta digitale o password di backup.
- 4 A questo punto è possibile modificare la password per l'archivio. In tal modo la password verrà modificata per tutti gli utenti. Nella finestra **Concedi l'accesso agli utenti** selezionare gli utenti cui si desidera concedere o negare l'accesso. Tutti gli utenti selezionati potranno sbloccare l'archivio passando un dito sopra il sensore.
- 5 Se si desidera blocca un archivio, fare clic su **Blocca**.

Se si utilizza la **password di backup globale**, viene impostata la password configurata nelle **Impostazioni utente** dell'utente che ha creato l'archivio. La modifica di questa password non interessa gli archivi File Safe creati in precedenza.

Se si desidera che altri utenti possano accedere a File Safe, il file d'archivio deve essere collocato in una cartella condivisa sul computer.



Nota: Quando un utente connesso sblocca un archivio e in seguito viene operato un cambio utente senza che vi sia disconnessione né riavvio del computer, l'utente attualmente connesso non potrà accedere all'archivio anche se l'accesso è condiviso. Se si desidera condividere l'archivio, bloccarlo prima di operare un cambio utente.

Gestione degli archivi File Safe

► Per accedere alla proprietà degli archivi File Safe

- 1 *Selezionare un file d'archivio (*.uea o *.ueaf*
- 2 *) e fare clic con il tasto destro, quindi selezionare **Proprietà**.*
- 3 *Selezionare la scheda **File Safe**.*
- 4 *Se l'archivio è bloccato, fare clic su **Sblocca** per poter accedere alle opzioni delle proprietà. Identificarsi tramite impronta digitale o password di backup.*
A questo punto è possibile modificare il tipo di password utilizzata per l'archivio e consentire o negare l'accesso ad altri utenti.
- 5 *Fare clic su **Blocca** per bloccare nuovamente l'archivio.*



Nota: L'archivio deve essere sbloccato per poter accedere alle proprietà. Se si desidera sbloccare l'archivio, fare clic su Sblocca nelle Proprietà o vedere Sblocco/blocco degli archivi.

► Per cambiare la password di backup per File Safe:


- 1 *Selezionare un file d'archivio (*.uea o *.ueaf*
- 2 *) e fare clic con il tasto destro, quindi selezionare **Proprietà**.*
- 3 *Selezionare la scheda **File Safe**.*
- 4 *Se l'archivio è bloccato, fare clic su **Sblocca** per poter accedere alle opzioni delle proprietà. Identificarsi tramite impronta digitale o password di backup.*
- 5 *Scegliere:*

- **Elimina password di backup** per eliminare la password di backup.

OPPURE

- **Imposta password di backup** per impostare una nuova password o modificarla se è già stata impostata. Selezionare:

- **Utilizza la password di backup globale** per utilizzare una password di backup comune per tutti gli archivi selezionati come protetti dalla Password di backup globale. Questa password può essere modificata in Impostazioni utente.
- **Utilizza la password di backup seguente** per creare una nuova password per l'archivio.

 **Importante:** In tal modo viene modificata la password di backup per l'archivio, ovvero per tutti gli utenti che condividono l'archivio. Tutti gli utenti che hanno accesso all'archivio possono modificarne la password.

► **Per impostare/cambiare la password di backup globale nelle Impostazioni utente:**

- 1 Selezionare **Start > Programmi > Protector Suite QL > Control Center**.
o passare il dito per visualizzare il **Biomenu** e selezionare **Control Center**.
- 2 Selezionare **Impostazioni > Impostazioni utente**. Selezionare **Impostazioni > Impostazioni utente**. È necessaria l'autenticazione.
Passare il dito sul sensore per le impronte digitali quanto richiesto.
- 3 Selezionare la scheda **File Safe**.
- 4 A questo punto è possibile modificare o impostare la **password di backup globale**. Questa password è comune a tutti gli archivi selezionati come protetti dalla **password di backup globale** (al momento della creazione di un archivio o impostata nelle **Proprietà**).

La modifica di questa password non influisce sugli archivi File Safe già creati. Gli archivi attualmente bloccati continueranno a essere protetti dalla password precedente.



Capitolo 4

Gestione di Protector Suite QL

Vi sono tre modi per gestire le funzioni e le impostazioni di Protector Suite QL: tramite la finestra di dialogo Control Center, la barra delle applicazioni e il Biomenu (visualizzato dopo aver passato un dito registrato sopra il sensore). Questo capitolo illustra le relative funzioni.

Protector Suite QL presenta delle funzioni accessibili anche tramite il menu **Start** di Windows. Selezionare **Start > Programmi > Protector Suite QL** per un elenco di funzionalità disponibili.

Control Center

Control Center contiene diverse funzionalità per la gestione delle impronte digitali e l'impostazione del software. Tra di esse vi sono **Impronte digitali**, **Impostazioni** ed **Guida**. Le opzioni disponibili dipendono dallo stato del software, dall'hardware utilizzato e dalle applicazioni installate.

► Visualizzazione di Control Center:

- Scegliere **Start > Programmi > Protector Suite QL > Control Center**.
- o passare il dito per visualizzare il **Biomenu** e selezionare **Control Center**.
- o fare clic con il tasto destro sull'icona nella barra delle applicazioni e selezionare **Avvia Control Center...**



Aumenta privilegi amministrativi per l'utente (solo Windows Vista).

Se si desidera accedere e apportare modifiche alle Impostazioni del sistema o gestire e modificare altri account utente (ad esempio poter registrare o eliminare le impronte digitali di altri utenti) è necessario aumentare i propri privilegi amministrativi, ovvero identificarsi come utente autorizzato.

- 1 Fare clic su **Aumenta privilegi amministrativi per l'utente**.
- 2 Quando appare la finestra di dialogo Vista Control User Account, immettere le proprie credenziali per l'autenticazione da parte del sistema (se si è già effettuato l'accesso come amministratore, continuare secondo le indicazioni del programma).
- 3 La finestra di dialogo Control Center apparirà nuovamente senza l'icona dello scudo. I diritti amministrativi vengono così aumentati. Ora è possibile accedere a **Impostazioni > Impostazioni del sistema** e apportare modifiche.

Ripetere questa procedura ogni volta che si esegue la finestra di dialogo Control Center.

Impronte digitali

È possibile registrare, modificare ed eliminare le impronte digitali degli utenti e, se è implementata l'accensione protetta, anche gestire le impronte digitali presenti nella memoria della periferica. L'elenco di funzionalità disponibili varia in base alla versione installata di Protector Suite QL, al sensore di impronte digitali, ai passaporti esistenti e ai privilegi amministrativi dell'utente corrente.



Nota: Le funzionalità variano a seconda dei privilegi amministrativi dell'utente. In modalità Protetta, gli utenti definiti come amministratori di impronte digitali (vedere "Modalità di protezione" a pagina 62) possono registrare o modificare i passaporti per tutti gli utenti registrati. In modalità Opportuna, gli utenti possono registrare o modificare solo i rispettivi passaporti.

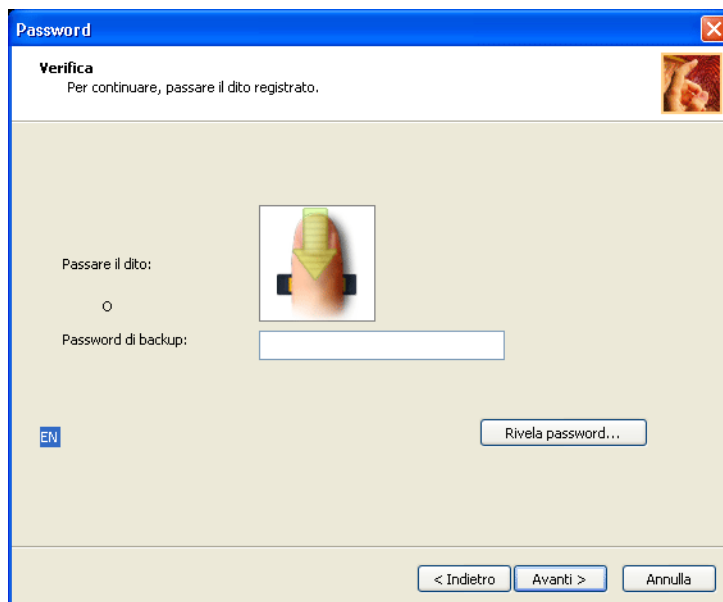
Registrazione o modifica delle impronte digitali

La registrazione delle impronte digitali è il processo di creazione della corrispondenza tra nome utente, password e impronte digitali (computerizzato in modo che non sia possibile ricostruire l'immagine originale) insieme con le chiavi di sicurezza generate automaticamente. Tutti i dati vengono memorizzati nel passaporto di impronte di un utente.

Dopo la registrazione, sarà possibile utilizzare le proprie impronte invece di nome utente e password.

► **Per registrare o modificare un passaporto (registrare o modificare impronte digitali):**

- 1 Scegliere **Start > Programmi > Protector Suite QL > Control Center**.
o passare il dito per visualizzare il **Biomenu** e selezionare **Control Center**.
- 2 Fare clic su **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 (vedere "Modalità di protezione" a pagina 62), viene visualizzato un elenco di passaporti esistenti. Selezionare l'utente e fare clic sul pulsante **Modifica** per modificare l'impronta di un utente esistente o su **Registra** per registrare un nuovo utente.
- 4 Appare la finestra della **registrazione guidata**.
- 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:*
 - *Selezionare un dito da registrare facendo clic sulla casella sopra il dito.*
 - *Passare il dito selezionato sul sensore per le impronte digitali. Sono necessarie tre immagini corrette per registrare un'impronta digitale (vedere Capitolo 3, "Registrazione di impronte", a pagina 14 per ulteriori istruzioni).*
 - *Per eliminare un'impronta digitale:*
 - *selezionare un dito da eliminare facendo clic sulla casella sopra il dito.*
 - *Fare clic su **OK**.*
- 7 *(Opzionale) Se si è selezionata la registrazione sulla periferica e la configurazione di sistema supporta l'accensione protetta, tutte le impronte digitali registrate verranno utilizzate anche per l'accensione protetta.*
- 8 *(Opzionale) Se è stata selezionata la registrazione sul disco rigido e la configurazione di sistema supporta l'accensione protetta, le impronte digitali registrate verranno utilizzate anche per l'accensione protetta.*
- 9 *Per via dei limiti di memoria della periferica, il numero massimo di impronte digitali registrabili è di 21. Se alcune delle impronte digitali registrate nei passaporti non sono assegnati all'accensione protetta nella periferica (ad esempio, è stata collegata un'altra periferica), sopra ogni dito appare il pulsante **Accensione**. Come impostazione predefinita, il pulsante Accensione viene visualizzato come "premuto". Il dito corrispondente verrà utilizzato per l'accensione protetta. Se non si desidera utilizzare il dito per l'accensione protetta ma solo per effettuare l'accesso, fare clic sul pulsante Accensione per eliminarlo dalla memoria della periferica.*
- 10 *Fare clic su **Avanti** per terminare la registrazione o configurare altre impostazioni opzionali (come Sicurezza avanzata) come descritto in "Registrazione di impronte" a pagina 14.*

Elimina

Le funzionalità variano a seconda dei privilegi amministrativi dell'utente. In modalità Protetta (vedere "Modalità di protezione" a pagina 62), solamente gli utenti definiti amministratori di impronte digitali possono eliminare i passaporti utente.

► **Per eliminare un passaporto esistente (tutti i dati dell'utente):**

- 1 Scegliere **Start >Programmi > Protector Suite QL > Control Center.**
o passare il dito per visualizzare il **Biomenu** e selezionare **Control Center**.
- 2 Fare clic su **Impronte digitali**.
- 3 Fare clic su **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.

Importazione o esportazione di un passaporto utente

I dati utente esistenti (inclusi impronte digitali, chiavi di crittografia e credenziali d'accesso) possono essere esportati in un file *.vtp (file passaporto) e importati nuovamente nel software di impronte digitali. Il file *.vtp è codificato e protetto da una password definita durante l'esportazione. È possibile importare un passaporto di un utente esistente ma In questo caso, è necessario innanzi tutto eliminare il passaporto utente.



Suggerimento: Si raccomanda di esportare il proprio passaporto per ragioni di backup.

► **Per esportare un passaporto esistente:**

- 1 Scegliere **Start >Programmi > Protector Suite QL > Control Center.**
o passare il dito per visualizzare il **Biomenu** e selezionare **Control Center**.
- 2 Fare clic su **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 (***.vtp**).
- 5 Creare la password che proteggerà i dati esportati.
- 6 Verificare il dito (contenuto nel passaporto che si sta esportando).

► **Per importare un passaporto:**

- 1 Scegliere **Start >Programmi > Protector Suite QL > Control Center.**
o passare il dito per visualizzare il **Biomenu** e selezionare **Control Center**.
- 2 Fare clic su **Impronte digitali**.
- 3 Scegliere **Importa o Esporta Dati Utente**. In modalità Protetta, viene visualizzato un elenco di passaporti esistenti. Fare clic su **Importa**.
- 4 Cercare il file del passaporto (*.vtp).
- 5 Immettere la password creata durante l'esportazione.

Impostazioni


La finestra di dialogo Protector Suite QL Impostazioni contiene varie opzioni di configurazione Protector Suite QL. Non tutte le funzioni della finestra di dialogo Impostazioni qui descritte saranno visibili: le funzioni disponibili variano a seconda della versione installata di Protector Suite QL e dei privilegi amministrativi dell'utente corrente.



Impostazioni del sistema

Impostazioni del sistema contiene le impostazioni comuni per tutti gli utenti. L'accesso a queste impostazioni sono limitate all'amministratore. Le seguenti funzionalità possono essere configurate in Impostazioni del sistema:

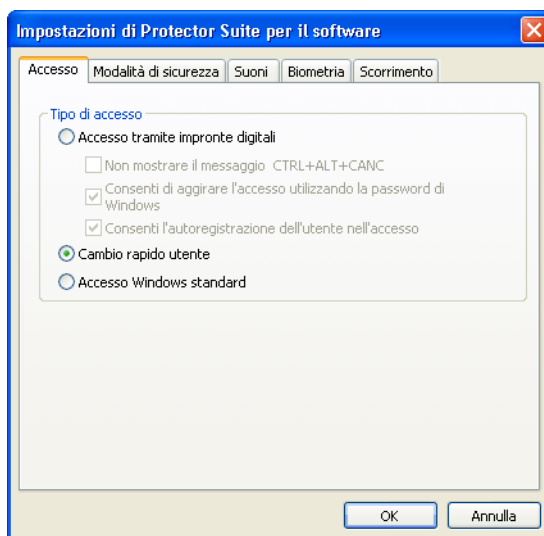
Accesso, Modalità di protezione, Suoni, Biometria, TMP (opzionale), Scorrimento.

 Se si utilizza Windows Vista, fare clic su **Aumenta privilegi amministrativi per l'utente** in Control Center per ottenere i diritti amministrativi per apportare modifiche alle Impostazioni del sistema e ad altri account utente.

Accesso

le impostazioni di accesso possono essere modificate solo dagli amministratori. Per l'attivazione di alcune modifiche verrà richiesto di riavviare il computer. La schermata delle Impostazioni di accesso consente di:

- *Sostituire l'accesso a Windows con l'accesso protetto tramite impronte digitali*
- *Eseguire l'accesso automatico di utenti verificati da Accensione protetta (facoltativo)*
- *Consentire il Cambio rapido utente (facoltativo).*



► **Per modificare le impostazioni di accesso:**

- 1 Scegliere **Start >Programmi > Protector Suite QL > Control Center.**
o passare il dito per visualizzare il **Biomenu** e selezionare **Control Center**.
- 2 Andare a **Impostazioni > Impostazioni del sistema > Accesso.**
- 3 Selezionare:

- **Accesso tramite impronte digitali**

Quando si seleziona questa opzione, l'accesso tramite impronte digitali al computer è attivato.


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

Il messaggio predefinito di Windows, CTRL+ALT+CANC, non verrà visualizzato. Verrà mostrata solamente la richiesta 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.

- **Consenti di aggirare l'accesso utilizzando la password di Windows.** Se si seleziona questa opzione, è possibile


utilizzare l'accesso Windows standard. Se non la si seleziona, solamente gli amministratori di impronte digitali potranno accedere tramite nome utente e password.

- **Consenti l'autoregistrazione dell'utente all'accesso.** Gli utenti possono registrare le proprie dita all'accesso al computer.

 • Se si utilizza Windows Vista, fare clic su **Dettagli** per visualizzare le impostazioni dei provider di credenziali ovvero come viene gestita l'autenticazione degli utenti dal sistema. Vedere "Provider di credenziali in Windows Vista" di seguito per ulteriori informazioni.

- **Cambio rapido utente**

Se si seleziona questa opzione, viene attivato il cambio utente rapido biometrico controllato tramite impronte digitali (se supportato dal sistema). Quando il cambio rapido utente è supportato ma non attivato, verrà chiesto di attivarlo sul sistema. Non è possibile abilitare il Cambio rapido utente quando il computer è membro di un dominio.

 Se si utilizza Windows Vista, questa opzione è sempre attivata come impostazione predefinita e non può essere modificata.

- **Accesso Windows standard** Quando si seleziona questa opzione, l'accesso tramite impronte digitali è disattivato e viene utilizzato l'accesso Windows standard.

- **Consenti iscrizione singola con accensione protetta**

Selezionare questa opzione per eseguire l'autenticazione all'accensione e dell'impronta digitale in un unico passo. Gli utenti verificati a livello di BIOS hanno automaticamente accesso a Windows.

- 4 Fare clic su **OK** e riavviare il computer.

Provider di credenziali in Windows Vista

I provider di credenziali consentono diversi modi con cui autenticarsi nel sistema. Il Provider di password Microsoft richiede nome utente e password, mentre il Provider di impronte digitali richiede di passare un dito sopra il sensore. L'elenco di provider di credenziali varia a seconda della configurazione di un particolare sistema.

► **Per visualizzare le impostazioni di un provider:**

- 1 Scegliere **Start > Programmi > Protector Suite QL > Control Center**.
o passare il dito per visualizzare il **Biomenu** e selezionare **Control Center**.
- 2 Scegliere **Impostazioni > Impostazioni del sistema > Accesso**.
- 3 Fare clic su **Dettagli**.
- 4 Le seguenti funzionalità sono definiti dai provider di credenziali:
 - **Accesso** definisce il modo in cui gli utenti eseguono l'autenticazione al momento dell'accesso al sistema (ad esempio, tramite impronte digitali, tramite nome e password, ecc.).
 - **Sblocca** definisce il modo in cui gli utenti eseguono l'autenticazione al momento dello sblocco del computer.
 - **Esegui come amministratore** è una funzionalità di Windows Vista. Un utente connesso come utente con privilegi limitati può eseguire l'autenticazione come amministratore ed eseguire un'applicazione riservata agli amministratori.
 - **Modifica password** definisce il tipo di autenticazione richiesta per modificare la password utente (ad esempio, verifica tramite impronte digitali, nome utente e password).
- 5 Selezionare:
 - **Contrassegna immagine affiancata utente registrato** per visualizzare un'icona dell'impronta sopra l'immagine della miniatura dell'account utente per contrassegnare quell'utente come registrato: l'accesso verrà gestito da un'impronta digitale. Se non si seleziona questa opzione, la miniatura dell'account apparirà normalmente. In tal mondo si imposta il Provider di password Microsoft in stato "allineato" (vedere di seguito).
 - **Consenti l'autoregistrazione dell'utente all'accesso** per consentire agli utenti con password valida ma senza impronta registrata di registrare da soli un'impronta digitale quando accedono al computer.

- 6 *Per modificare le impostazioni di un provider, selezionare un provider dall'elenco e fare clic su **Dettagli...** (o fare doppio clic sul provider).*



Nota: Il Provider di impronte digitali e il Provider di password Microsoft non possono essere impostati dall'utente. Tali impostazioni sono predefinite.

- 7 *Appare una finestra di dialogo che consente di visualizzare le impostazioni per il provider selezionato. Le opzioni sono le seguenti:*
- **On** attiva il Provider. Ad esempio, quando si imposta On per il Provider di impronte digitali nella sezione Accesso, gli utenti dovranno eseguire l'autenticazione passando un dito sopra il sensore per accedere al computer.
 - **Off** disattiva il Provider. Ad esempio, quando nella sezione Accesso si imposta Provider di password Microsoft su Off e Provider di impronte digitali su On, sarà consentita unicamente l'autenticazione tramite impronte digitali all'accesso.
 - **Allineato** - per gli utenti, il provider allineato sembra essere impostato su On, ma il controllo delle relative funzioni verrà condotto dal Provider di impronte digitali.



Nota: Il Provider di impronte digitali non può essere impostato come allineato ma può allineare gli altri provider (come il Provider di password Microsoft).

Modalità di protezione

Protector Suite QL può operare in tre modalità di protezione:

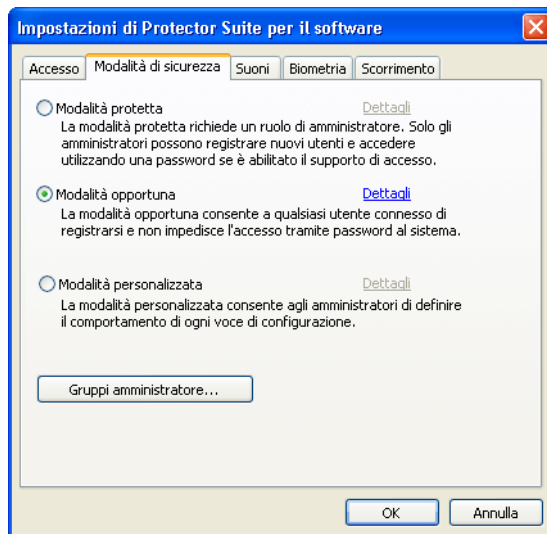
Modalità protetta, Modalità pratica e Modalità personalizzata.

Le modalità di sicurezza variano per privilegi concessi agli utenti. Questi privilegi includono, ad esempio, la possibilità di registrare altri utenti, di eliminare o modificare le impronte digitali, ecc.

Fare clic su **Dettagli** per vedere le impostazioni dei criteri di sicurezza di ogni modalità. Solamente i criteri nella Modalità personalizzata possono essere modificati.

Gruppi di amministratori di impronte digitali

Contiene un elenco di gruppi di utenti di sicurezza locali o di dominio definiti "amministratori di impronte digitali". Questi utenti dispongono di privilegi amministrativi per la gestione di Protector Suite QL. I loro privilegi sono definiti nei criteri della Modalità di sicurezza (vedere di seguito).



► **Per scegliere una modalità di sicurezza:**

- 1 Scegliere **Start > Programmi > Protector Suite QL > Control Center**.
o passare il dito per visualizzare il **Biomenu** e selezionare **Control Center**.
- 2 Selezionare **Impostazioni > Impostazioni del sistema**
- 3 Selezionare la scheda **Modalità di sicurezza**. Scegliere:
 - **Modalità protetta.** Nella Modalità protetta solamente gli amministratori di impronte digitali dispongono di accesso illimitato a tutte le funzioni di gestione delle impronte digitali (ad esempio, creazione o eliminazione di passaporti di impronte per tutti gli utenti), tra cui l'amministrazione di *Fingerprint Storage Inspector* e *Accensione protetta*.
 - **Modalità pratica.** In Modalità pratica, tutti gli utenti hanno gli stessi privilegi. Ad esempio, tutti gli utenti possono creare, modificare o eliminare i propri passaporti di impronte digitali.

• **Modalità personalizzata.** Le impostazioni dei criteri della Modalità personalizzata possono essere configurate diversamente da parte degli amministratori e utenti con privilegi limitati.

4 Scegliere **OK** per chiudere le finestre di dialogo.

Criteri delle modalità di sicurezza

I criteri nelle Modalità protetta e pratica sono preimpostati e non possono essere modificati. Solamente i criteri nella Modalità personalizzata possono essere modificati. Selezionare e fare doppio clic su un criterio per visualizzarne i dettagli.

Criteri di protezione		
Criterio di protezione	Amministratore	Utente limitato
Accensione protetta: Aggiungi impronte digitali all'accensione protetta	Sì	Sì
Accensione protetta: Attiva/Disattiva accensione protetta	Sì	Sì
Fingerprint Storage Inspector: Elimina impronte digitali di altri utenti	No	No
Fingerprint Storage Inspector: Elimina impronte digitali inutilizzate	Sì	Sì
Fingerprint Storage Inspector: Elimina tutte le impronte digitali	No	No
Fingerprint Storage Inspector: Usa Fingerprint Storage Inspector	Sì	Sì
Registrazione: Elimina altri utenti	No	No
Registrazione: Elimina utente corrente	Sì	Sì
Registrazione: Esporta altri utenti	No	No
Registrazione: Esporta utente corrente	Sì	Sì
Registrazione: Importa altri utenti	No	No
Registrazione: Importa utente corrente	Sì	Sì
Registrazione: Modifica altri utenti	No	No
Registrazione: Modifica utente corrente	Sì	Sì
Registrazione: Registra altri utenti	No	No
Registrazione: Registra utente corrente	Sì	Sì
Registrazione: Registra utenti senza scansione delle impronte digitali	No	No
Registrazione: Rivela password	Sì	Sì

► Per modificare i criteri nella Modalità personalizzata:

- 1 Scegliere **Start > Programmi > Protector Suite QL > Control Center.** o passare il dito per visualizzare il **Biomenu** e selezionare **Control Center**.
- 2 Selezionare **Impostazioni > Impostazioni del sistema**
- 3 Selezionare la scheda **Modalità di sicurezza**.
- 4 Fare clic sul pulsante di opzione **Personalizzata**, quindi fare clic su **Dettagli**. Appare la finestra dei criteri. Vedere di seguito i dettagli dei criteri.
- 5 Fare clic sul pulsante **Cambia** (o doppio clic) per modificare le impostazioni dei criteri.
- 6 Scegliere **OK** per chiudere le finestre di dialogo.

I criteri possono essere definiti in maniera diversa per un account amministratore di impronte digitali e un account utente con privilegi limitati. Selezionare **Consenti/Non consentire** per impostare i privilegi di ciascun gruppo di utenti.

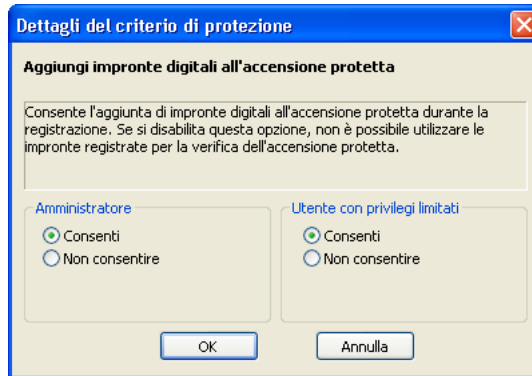
È possibile copiare le impostazioni dei criteri dalla Modalità pratica o protetta alla Modalità personalizzata e quindi apportare ulteriori modifiche. Si tratta di un'opzione utile quando si desidera apportare solamente poche modifiche alle impostazioni dei criteri.

► **Per copiare i criteri dalla Modalità pratica o protetta:**

- 1 Scegliere **Start > Programmi > Protector Suite QL > Control Center**.
*o passare il dito per visualizzare il **Biomenu** e selezionare **Control Center**.*
- 2 Selezionare **Impostazioni > Impostazioni del sistema**
- 3 Selezionare la scheda **Modalità di sicurezza**.
- 4 Fare clic sul pulsante di opzione **Personalizzata**, quindi fare clic su **Dettagli**. Appare la finestra dei criteri. Vedere di seguito i dettagli dei criteri.
- 5 Fare clic sul pulsante **Copia** per copiare le impostazioni dei criteri.
- 6 Scegliere la Modalità **protetta** o **pratica** e le impostazioni dei criteri verranno copiate dalla modalità selezionata.
- 7 Ora è possibile modificare i criteri utilizzando il pulsante **Modifica**.
- 8 Scegliere **OK** per chiudere le finestre di dialogo.

Dettagli dei criteri:

Selezionare e fare doppio clic su un criterio per visualizzarne i dettagli.



Registrazione:

- *Elimina altri utenti: consente di eliminare un passaporto di impronte digitali per qualsiasi utente registrato sul computer. Non viene richiesta alcuna verifica prima dell'eliminazione dei passaporti.*
- *Elimina utente corrente: dopo la verifica, consente di eliminare un passaporto di impronte digitali per l'utente attualmente connesso.*
- *Modifica altri utenti: consente di modificare un passaporto di impronte digitali per qualsiasi utente registrato sul computer, ad esempio aggiungere o eliminare delle impronte registrate.*
- *Modifica utente corrente: consente di modificare un passaporto di impronte digitali per l'utente attualmente connesso, ad esempio aggiungere o eliminare delle impronte registrate.*
- *Registra altri utenti: consente ad altri utenti di registrare impronte digitali. Solamente gli utenti con account Windows valido possono essere registrati.*
- *Registra utente corrente: consente all'utente attualmente connesso di registrare impronte digitali.*
- *Registra utenti senza scansione delle impronte digitali: consente agli utenti di essere registrati senza scansione delle impronte digitali. Agli utenti verrà richiesto di eseguire la scansione delle impronte digitali al prossimo accesso.*
- *Esporta altri utenti: consente di esportare un passaporto di impronte digitali per qualsiasi utente registrato sul computer.*

- *Esporta utente corrente: consente di esportare un passaporto di impronte digitali per l'utente attualmente connesso.*
- *Importa altri utenti: consente di importare un passaporto di impronte digitali per qualsiasi utente registrato sul computer.*
- *Importa utente corrente: consente di importare un passaporto di impronte digitali per l'utente attualmente connesso.*
- *Rivela password: consente di rivelare la password Windows dell'utente durante la registrazione delle impronte digitali.*

Fingerprint Storage Inspector:

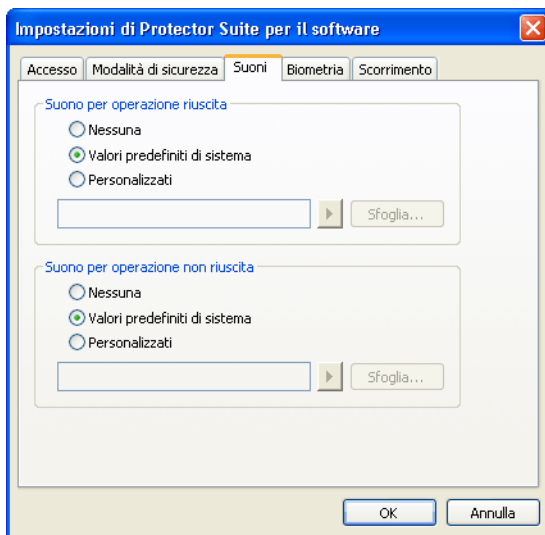
- *Elimina tutte le impronte digitali: consente di eliminare tutte le impronte digitali dalla periferica. (Il criterio di utilizzo di Fingerprint Storage Inspector deve essere abilitato affinché questo criterio abbia effetto.)*
- *Elimina impronte digitali di altri utenti: consente di eliminare le impronte digitali di altri utenti. Tuttavia, deve essere mantenuta almeno un'impronta registrata per ogni utente. (Il criterio di utilizzo di Fingerprint Storage Inspector deve essere abilitato affinché questo criterio abbia effetto.)*
- *Elimina impronte digitali inutilizzate: consente di eliminare i record di impronte digitali che non appartengono ad alcun utente registrato localmente, ad esempio utenti di una precedente installazione. (Il criterio di utilizzo di Fingerprint Storage Inspector deve essere abilitato affinché questo criterio abbia effetto.)*
- *Usa Fingerprint Storage Inspector: consente l'utilizzo di Fingerprint Storage Inspector, ovvero gli utenti possono eliminare solamente le proprie impronte digitali (ad eccezione dell'ultima; deve essere mantenuta almeno un'impronta registrata).*

Accensione protetta:

- *Aggiungi impronte digitali all'accensione protetta: consente di aggiungere le impronte digitali all'accensione protetta durante la registrazione. Se disattivata, le impronte digitali registrati non possono essere utilizzare per la verifica dell'accensione protetta.*
- *Attiva/Disattiva accensione protetta: consente di attivare o disattivare l'accensione protetta sul computer.*

Suoni

Il suono selezionato viene riprodotto in caso di buona o cattiva riuscita di un'operazione con impronta digitale. È possibile utilizzare i suoni predefiniti del sistema, disabilitare i suoni o cercare i propri file audio preferiti (formato wav).



Biometria

Queste impostazioni consentono di modificare il livello di impostazioni di sicurezza del sensore per impronte digitali. È necessario riavviare il computer ogni volta che si apportano modifiche.

► Per modificare le Impostazioni biometriche:

- 1 Scegliere **Start > Programmi > Protector Suite QL > Control Center**.
o passare il dito per visualizzare il **Biomenu** e selezionare **Control Center**.
- 2 Fare clic su **Impostazioni > Impostazioni del sistema** e andare a **Modalità di sicurezza > Biometria**.
 - **Blocco intruso**

- **Conteggio di blocco:** imposta il numero di tentativi di verifica non riusciti (passaggi di dita) consentiti prima del blocco della periferica.
- **Tempo di blocco:** imposta il tempo per cui la periferica rimarrà bloccata. Allo scadere di questo tempo, sarà nuovamente possibile utilizzare il sensore per impronte digitali.

- **Prestazioni biometriche** imposta il livello di accuratezza con cui la scansione di un'impronta digitale deve corrispondere ai campioni registrati. Si noti che l'utilizzo del livello inferiore può compromettere la sicurezza della periferica. Il livello superiore, tuttavia, richiede una corrispondenza perfetta con il campione registrato e potrebbe comportare ripetute verifiche non riuscite per gli utenti autorizzati. Si raccomanda di impostare il livello predefinito (medio).

TPM (opzionale)

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 Protezione avanzata. Vedere "Protezione avanzata" a pagina 23.

► Per inizializzare il modulo TPM:

- 1 Fare clic Sul pulsante **Inizializza TPM** per avviare la procedura guidata dell'inizializzazione TPM.
- 2 Fare clic su **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 TPM supplementare.
- 4 Fare clic su **Fine** per chiudere la procedura guidata.

Scorrimento

È possibile utilizzare il sensore per impronte digitali per scorrere all'interno del **Biomenu** (vedere page 80) e di qualsiasi applicazione Windows, al posto della rotella del mouse.

Attivare o disattivare lo scorrimento selezionando o deselezionando l'opzione **Funzionalità di scorrimento del sensore** dall'icona nella barra delle applicazioni (fare clic con il tasto destro del mouse sull'icona nella barra delle applicazioni e selezionare la funzionalità) oppure premendo il tasto di scelta rapida per Scroll Switch.

Quando l'opzione Funzionalità di scorrimento del sensore è selezionata, l'icona nella barra delle applicazioni viene modificata e la funzionalità di scorrimento è attiva. Il tasto di scelta rapida non è definito per impostazione predefinita dopo l'installazione di Protector Suite QL e deve essere pertanto impostato (vedere di seguito).

► **Per impostare lo scorrimento e il tasto di scelta rapida per Scroll Switch:**

- 1 Scegliere **Start >Programmi > Protector Suite QL > Control Center.**
o passare il dito per visualizzare il **Biomenu** e selezionare **Control Center**.
- 2 Selezionare la scheda **Scorrimento**.
 - Fare clic sul pulsante **Verifica velocità** per verificare lo scorrimento con i valori selezionati.
 - **Velocità** - Spostare il cursore per regolare la velocità di scorrimento. Si imposta così il movimento del cursore quando si sposta il dito sopra il sensore.
 - **Accelerazione** - Spostare il cursore per impostare l'accelerazione dello scorrimento. Più veloce si passa il dito sopra il sensore e più veloce sarà lo scorrimento.
 - **Livello** - imposta i livelli di sensibilità del sensore: un numero basso indica una maggiore sensibilità del sensore al movimento del dito nella data direzione, il che significa che il sensore reagirà più velocemente al movimento del dito.
 - **Ripetizione** - Imposta il ritardo dopo il quale il sensore inizierà a reagire quando si lascia il dito posato su di esso: un numero basso indica una maggiore velocità di reazione del sensore.
 - Per impostare il tasto di scelta rapida per Scroll Switch, attivare il campo **Tasto di scelta rapida per Scroll Switch**. Premere i tasti che si desidera utilizzare per attivare/disattivare la funzionalità di scorrimento.
- 3 Scegliere **OK** per chiudere la finestra di dialogo.

Impostazioni utente

Impostazioni utente contengono impostazioni specifiche per l'utente. Queste impostazioni sono protette tramite le impronte digitali.

Le seguenti funzionalità possono essere configurate in Impostazioni utente:

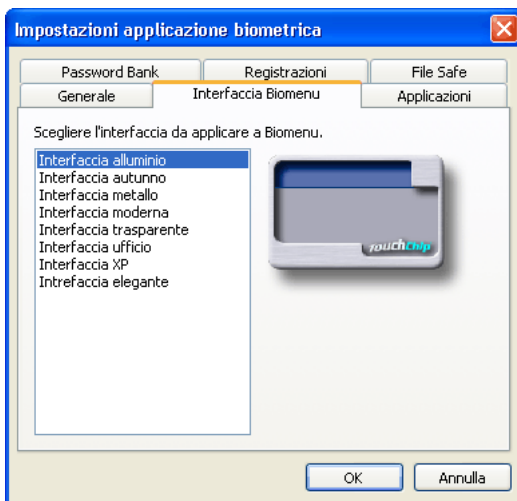
Generale, Interfaccia di Biomenu, Password Bank, Registrazioni, File Safe e Applicazioni.

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 QL. Vedere "Icona sulla barra delle applicazioni" a pagina 79 per ulteriori informazioni sulle funzioni disponibili nella barra delle applicazioni.

Interfaccia di Biomenu

Selezionare un'interfaccia (aspetto) per il Biomenu di Protector Suite QL. Viene visualizzato un campione a destra della finestra di dialogo. L'anteprima delle interfacce non è supportata in Windows 2000.



Password Bank

Questa finestra di dialogo è costituita da due parti. La prima contiene le impostazioni dei suggerimenti visualizzati per informare un utente delle azioni di Password Bank. Selezionare o deselezionare la casella di controllo accanto a ogni suggerimento per visualizzare o nascondere il suggerimento nel browser.



La seconda parte contiene informazioni sull'utilizzo di Password Bank.

Selezionando la casella di controllo della la finestra di dialogo di Windows verrà attivato l'utilizzo di Password Bank per memorizzare le credenziali delle applicazioni standard di Windows. Il supporto delle credenziali web in Internet Explorer è sempre presente, la casella di controllo consente di abilitare o disabilitare l'utilizzo del browser per l'utente corrente. Per il browser Firefox è necessario installare un plug-in. Facendo clic sul collegamento verrà avviata una finestra del browser predefinito. In questo caso Firefox deve essere impostato come browser predefinito. L'installazione può essere avviata anche direttamente da Firefox come un'installazione standard di plug-in.

Per ulteriori informazioni su Password Bank, vedere Capitolo 3, "Password Bank", a pagina 29.

Registrazioni

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

Selezionare una registrazione dall'elenco e fare clic su uno dei pulsanti - **Rinomina** per rinominare la registrazione, **Modifica** per modificare la registrazione, **Elimina** per eliminare la registrazione. Fare clic su **Esporta** per esportare le registrazioni per utilizzarle su un altro computer o per eseguirne il backup e su **Importa** per importare le registrazioni da un file di esportazione.

Per ulteriori informazioni, vedere Capitolo 3, "Gestione delle registrazioni", a pagina 33.

File Safe

È possibile impostare o modificare la protezione tramite password dei file memorizzati negli archivi File Safe crittati. Questa password protegge tutti gli archivi impostati per la protezione tramite Password di backup globale. Si raccomanda di utilizzare una password di backup perché, in caso contrario, non vi è altro modo per accedere ai file memorizzati nell'archivio File Safe quando la verifica delle impronte digitali non è possibile (ad esempio, per una lesione alle dita, un problema del dispositivo, ecc.). Utilizzare una password complessa, di almeno otto caratteri, che includa caratteri non alfanumerici, ecc.



Nota: La modifica di questa password non interessa gli archivi File Safe creati in precedenza.

Per ulteriori informazioni su password e File Safe, vedere Capitolo 3, "Crittografia dei file (aggiunta di file o cartelle a un archivio File Safe)", a pagina 40

Applicazioni

Vengono visualizzate le applicazioni che possono essere avviate tramite impronte digitali.

È necessario lasciare almeno un dito registrato senza assegnazione per permettere la visualizzazione del Biomenu. Il numero massimo di applicazioni che è possibile avviare è pari al numero di dita registrate meno uno, ad esempio se si desidera avviare due applicazioni è necessario avere almeno tre dita registrate.

► Per avviare un'applicazione tramite un'impronta registrata:

- 1 Fare clic sul pulsante **Aggiungi**. Verrà visualizzata la finestra di dialogo *Applicazione*.
- 2 Selezionare una delle dita registrate libere. Appare una finestra che richiede la registrazione di più dita se non ve ne sono disponibili.
- 3 Inserire un nome dell'applicazione.

- 4 Cercare il file che si desidera avviare: Può essere qualsiasi file eseguibile (ad esempio, *lexplore.exe*) .
- 5 Facoltativamente, è possibile immettere parametri aggiuntivi nel campo **Parametri applicazione** (vedere page 37).
- 6 Fare clic su **OK**.

Per ulteriori informazioni sull'Utilità di avvio delle applicazioni e sui Parametri applicazione, vedere Capitolo 3, "Utilità di avvio dell'applicazione" , a pagina 37.

Accensione protetta (facoltativo)

La funzionalità di accensione protetta impedisce l'accesso da parte di utenti non autorizzati al computer dell'utente a livello di BIOS. I computer in cui è attivata l'accensione protetta non caricheranno il sistema operativo dal disco rigido nel caso l'impronta non venga autenticata.

I campioni di impronte sono archiviati nella memoria della periferica per le impronte digitali. Durante l'avvio del computer, viene richiesta l'autenticazione delle impronte digitali. L'utente ha a disposizione un tempo limitato per passare un dito sopra il sensore. Il computer verrà avviato solo se l'impronta digitale analizzata corrisponde a un campione archiviato nella memoria della periferica. Al termine della verifica, il processo di avvio continua normalmente.

Attivazione dell'accensione protetta in Protector Suite QL

Le opzioni per l'accensione protetta vengono visualizzate solamente se il computer supporta questa funzionalità (principalmente supportata dai portatili). Nella maggior parte delle configurazioni, l'accensione protetta è abilitata automaticamente dopo la registrazione del primo utente.

► Per attivare/disattivare l'accensione protetta:

- 1 Scegliere **Start >Programmi > Protector Suite QL > Control Center**.
o passare il dito per visualizzare il **Biomenu** e selezionare **Control Center**.
- 2 Selezionare **Impostazioni > Accensione protetta**.
- 3 Selezionare la casella di controllo **Sostituisci le password** di accensione e del disco rigido con il lettore d'impronte digitali.
- 4 Fare clic su **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.

Per aggiungere impronte digitali all'accensione protetta, vedere Capitolo 3, "Registrazione di impronte", a pagina 14.

Iscrizione singola con accensione protetta

L'accensione protetta può essere configurata per interagire con l'accesso tramite impronte digitali. Se un'impronta digitale utilizzata per la funzionalità di accensione protetta del BIOS corrisponde a un'impronta di un passaporto esistente, l'utente corrispondente viene automaticamente connesso senza dover immettere la password di Windows o passare nuovamente il dito.

► Per abilitare l'accesso a Windows automatico per gli utenti verificati tramite l'accensione protetta:

- 1 Scegliere **Start > Programmi > Protector Suite QL > Control Center**.
o passare il dito per visualizzare il **Biomenu** e selezionare **Control Center**.
- 2 Fare clic su **Impostazioni > Impostazioni del sistema**
- 3 Selezionare la scheda **Accesso**.
- 4 Selezionare la casella di controllo **Consenti iscrizione singola con accensione protetta**.



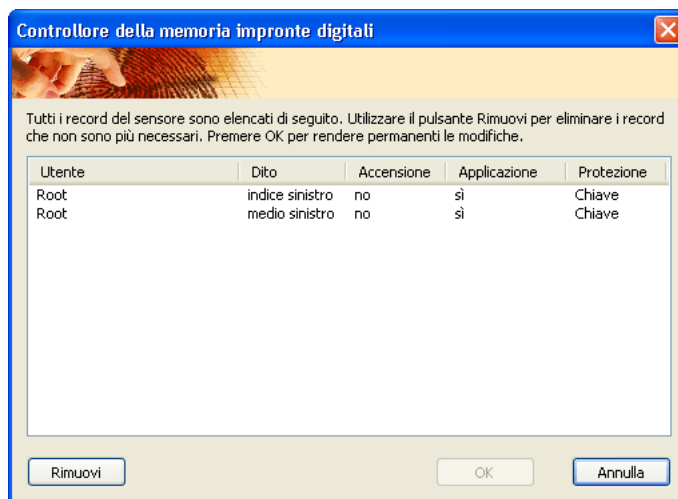
Nota: L'hardware deve supportare l'accensione protetta affinché sia possibile utilizzare questa funzionalità di iscrizione singola e l'utente deve disporre dei privilegi amministrativi per modificare le impostazioni.

Fingerprint Storage Inspector (opzionale)

Questa funzionalità è disponibile solamente quando Si utilizza la registrazione nella periferica.

Fingerprint Storage Inspector è uno strumento per la visualizzazione e la modifica del contenuto memorizzato nella periferica per 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.



► **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.*

*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** o **Elimina** (vedere "Registrazione o modifica delle impronte digitali" a pagina 53).*



Nota: L'autorizzazione a rimuovere le impronte digitali è definita nelle impostazioni della Modalità di sicurezza (vedere "Modalità di protezione" a pagina 62). Alcuni privilegi potrebbero essere limitati ai soli amministratori di impronte digitali.

Guida

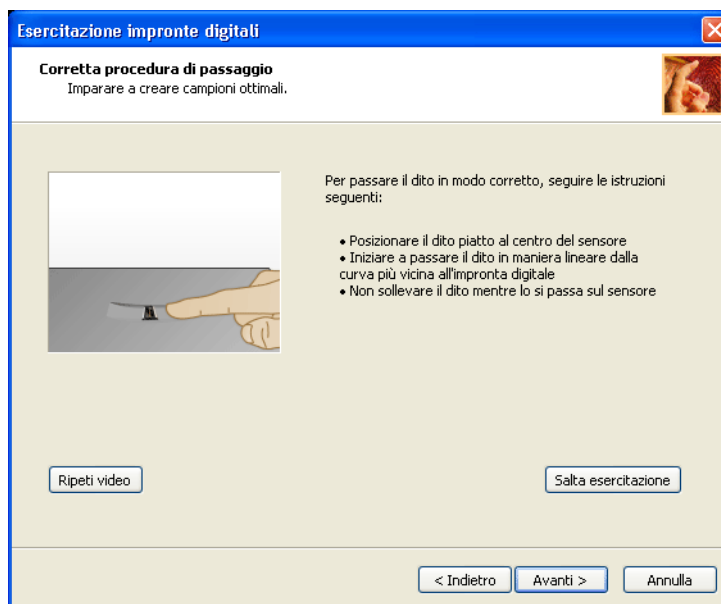
Introduzione

Le funzioni 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

In tal modo verrà avviata l'Esercitazione impronte digitali.

L'esercitazione mostrerà un breve filmato in cui verranno dimostrate 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.



Per ulteriori informazioni, vedere Capitolo 3, "Esercitazione Fingerprint", a pagina 21.



Nota: per visualizzare la guida basata su HTML selezionare **Start >Programmi > Protector Suite QL > Guida** o fare clic sull'icona **Guida** nella finestra di dialogo principale Control Center. Per visualizzare l'aiuto contestuale HTML, premere F1 nella finestra di dialogo per cui si necessita di aiuto.

Biomenu

Il **Biomenu** consente di accedere alle funzionalità e alle impostazioni di Protector Suite QL. Gli elementi disponibili variano a seconda dei componenti installati.

► Per visualizzare il Biomenu:

- *passare un dito registrato sopra il sensore per impronte digitali.*
*Per visualizzare il Biomenu nei casi in cui la verifica del dito richiama un'altra azione (ad esempio la riproduzione di una pagina registrata), tenere premuto **Maiusc** mentre si passa il dito sopra il sensore.*

Utilizzare il mouse o il sensore per navigare. Se si utilizza il sensore, muovere il dito per navigare all'interno del **Biomenu** e toccare l'elemento evidenziato per eseguire l'azione corrispondente. È possibile configurare le impostazioni di scorrimento nella finestra di dialogo Impostazioni del sistema (vedere "Scorrimento" a pagina 69).

Il Biomenu è disponibile in diverse interfacce. Per visualizzare o modificare un'interfaccia, aprire **Control Center > Impostazioni > Impostazioni dell'utente**, passare il dito per conferma e passare alla scheda **Interfaccia Biomenu**.

- **Blocca computer**

*La prima voce del menu contiene il comando **Blocca computer** con cui è possibile bloccare il computer. Per sbloccare nuovamente il computer, passare il dito sopra il sensore*

- **Siti registrati** (opzionale)

Mostra un elenco delle pagine Web registrate tramite Password Bank. Per visualizzare e compilare una pagina registrata nel browser Web predefinito, selezionarne il nome nell'elenco.

- **Registra...** (opzionale)

Registra una nuova finestra (pagina web o finestra di dialogo). Per ulteriori informazioni sulla registrazione di Password Bank, vedere Capitolo 3, "Registrazione di pagine web e finestre di dialogo", a pagina 29.

- **Blocca tutti gli archivi** (opzionale)



Blocca tutti gli archivi File Safe attualmente aperti. Questo elemento viene visualizzato unicamente quando almeno due archivi sono sbloccati.

- **Control Center...**

Visualizza la finestra di dialogo Control Center (vedere “Control Center” a pagina 52).

- **Guida**

Visualizza la guida HTML. Per visualizzare l’aiuto contestuale HTML, premere F1 nella finestra di dialogo per cui si necessita di aiuto.

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 l'esercitazione sulla registrazione delle impronte.

È possibile avviare questa procedura guidata anche da Control Center selezionando **Impostazioni > Registra o modifica delle impronte digitali**. Vedere **Capitolo 3, “Registrazione di impronte”**, a pagina 14 per ulteriori informazioni su come registrare le impronte.

Avvia Control Center...

Avvia Control Center di Protector Suite QL (vedere page 52).

Non usare il sensore/Usa il sensore

Consente di scollegare temporaneamente la periferica per impronte digitali da Protector Suite QL per utilizzarla con un'altra applicazione. Questo comando rende disponibile la periferica solo per la sessione utente corrente. La periferica può essere utilizzata da una sola applicazione per volta.

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



Importante: Questa funzionalità è disponibile solo per gli utenti avanzati, per esempio gli sviluppatori di altre applicazioni biometriche.

Guida

Visualizza la guida HTML. Per visualizzare l'aiuto contestuale HTML, premere F1 nella finestra di dialogo per cui si necessita di aiuto.

Informazioni su

Visualizza le informazioni di prodotto di Protector Suite QL.

Infopanel lettore di impronte digitali

Infopanel lettore di impronte digitali contiene informazioni sul sensore e una finestra di prova per la scansione delle impronte digitali. È possibile utilizzare questa finestra di dialogo per ottenere informazioni sul sensore in caso di problemi con l'hardware per comunicazioni con il supporto tecnico.

► Per visualizzare Infopanel lettore di impronte digitali

- 1 Selezionare **Start > Pannello di controllo**.
- 2 Fare clic sull'icona **Sensore di impronte digitali**. Apparirà la finestra di dialogo **Infopanel lettore di impronte digitali**.
 - Selezionare la scheda **Versione** per visualizzare le informazioni sul sensore (quali tipo di periferica, nome, versione, ecc.).
*Per esportare le informazioni in un file di testo, fare clic su **Salva** e scegliere un percorso per il salvataggio del file (come impostazione predefinita `FingerprintSensorVersion.txt`).*
 - Selezionare la scheda **Test dito** per vedere immagini di prova delle impronte digitali acquisite quando si è passato il dito sopra il sensore.
- 3 Fare clic su **Chiudi** per chiudere la finestra di dialogo.

A hand is shown pointing at a fingerprint scanner, which is a common security measure for accessing sensitive information.

Capitolo 5

Risoluzione dei problemi 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 esclusivamente Windows 2000, 2003, Windows XP e Windows Vista.*

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 le 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. Ogni 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 un 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 File Safe, ma non i dati File 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 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 poiché 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.

Se 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. Al contrario, le impronte digitali vengono eliminate dalla periferica per motivi di sicurezza (per evitare l'aggiunta di impronte non verificate).

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 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 solo dopo che la pagina sarà interamente caricata. 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.*

