Pagina iniziale di Dell Data Protection | Access

La pagina iniziale di **Dell Data Protection | Access** è il punto di partenza per accedere alle funzioni di questa applicazione. Da questa finestra è possibile accedere a:

System Access Wizard
Opzioni di accesso (Access Options)
Self-Encrypting Drive
Opzioni avanzate (Advanced Options)

Nell'angolo inferiore destro della finestra è presente il collegamento **avanzate** (advanced) che consente di accedere alle opzioni avanzate.

Dalla pagina delle opzioni avanzate è possibile fare clic sul collegamento **pagina iniziale** (home) nella parte inferiore destra della finestra per tornare alla pagina iniziale.

System Access Wizard

System Access Wizard si avvia automaticamente la prima volta che viene lanciata l'applicazione **Dell Data Protection | Access**. Questa procedura guidata aiuta l'utente a impostare tutti gli aspetti della sicurezza sul sistema, comprese le modalità (per esempio solo password o impronta digitale e password) e il momento (all'apertura di Windows, pre-Windows o entrambi) in cui si desidera eseguire l'accesso al sistema. Inoltre, la procedura guidata consente di configurare gli eventuali self-encrypting drive presenti nel sistema.

Funzioni dell'amministratore

Gli utenti per cui nel sistema sono stati impostati privilegi di amministratore in Windows sono autorizzati a eseguire le seguenti operazioni in **Dell Data Access | Protection**, che gli utenti standard non possono effettuare:

- Impostazione / modifica della password di sistema (pre-Windows)
- Impostazione / modifica della password disco rigido
- Impostazione / modifica della password amministratore
- Impostazione / modifica della password del proprietario TPM
- Impostazione / modifica della password amministratore ControlVault
- Reset del sistema
- Archiviazione e ripristino delle credenziali
- Impostazione / modifica PIN amministratore smart card
- Cancellazione / reimpostazione di una smart card
- Attivazione/ disattivazione di Accesso sicuro Dell (Dell Secure Login) a Windows
- Impostazione della policy di accesso a Windows
- Gestione dei self-encrypting drive, compreso quanto segue:
    - Attivazione / disattivazione del blocco dei self-encrypting drive
    - Attivazione / disattivazione della sincronizzazione delle password di Windows (WPS)
    - Attivazione / disattivazione del Single Sign On (SSO)
    - Esecuzione di una cancellazione crittografica

Gestione in remoto

La propria azienda può configurare un ambiente in cui le funzioni di sicurezza dell'applicazione **Dell Data Protection | Access** vengono gestite in modo centralizzato per più piattaforme (ovvero con la gestione in remoto). In casi del genere è possibile utilizzare l'infrastruttura di sicurezza di Windows (per esempio Active Directory) per gestire in modo sicuro funzioni specifiche di **Dell Data Protection | Access**.

Quando un computer è gestito in remoto (cioè "di proprietà" dell'amministratore remoto), l'amministrazione locale delle funzionalità di **Dell Data Protection | Access** è disattivata; la finestra di gestione dell'applicazione non è accessibile in locale. In remoto è possibile gestire le seguenti funzioni:

- Trusted Platform Module (TPM)
- ControlVault
- Accesso pre-Windows
- Reset del sistema (Reset System)
- Password del BIOS
- Policy di accesso a Windows
- Self-Encrypting Drive
- Registrazione di impronte digitali e smart card

Per richiedere ulteriori informazioni sull'utilizzo di Wave Systems EMBASSY® Remote Administration Server (ERAS) per la gestione in remoto, rivolgersi al rivenditore Dell o visitare il sito dell.com.

Opzioni di accesso (Access Options)

Dalla finestra Opzioni di accesso (Access Options) è possibile impostare le modalità di accesso al sistema.

Le eventuali opzioni impostate in **Dell Data Protection | Access** saranno visualizzate nella pagina iniziale insieme alle opzioni disponibili (per esempio modifica password di accesso pre-Windows). Le opzioni disponibili sono collegamenti sui quali è possibile fare clic per accedere alla finestra appropriata per l'esecuzione di una determinata operazione (per esempio modificare la password di accesso pre-Windows o registrare un'altra impronta digitale).

Generali
Innanzitutto è possibile specificare quando effettuare l'accesso (in Windows, pre-Windows o in entrambi i casi) e come effettuarlo (per esempio con impronta digitale e password). È possibile scegliere una o due opzioni per la modalità di accesso, tra cui combinazioni di impronte digitali, smart card e password. Le opzioni elencate si basano sulle policy di accesso adottate nell'ambiente in uso e sulle funzionalità supportate nella piattaforma.

Impronta digitale
Se il sistema è dotato di un lettore di impronte digitali, è possibile registrare o aggiornare le impronte digitali da utilizzare per l'accesso al sistema. Dopo avere registrato le impronte digitali è possibile passare le dita registrate sull'apposito sensore per accedere al sistema in Windows, pre-Windows o in entrambi i casi, a seconda delle opzioni impostate nelle Opzioni di accesso generali (General Access Options). Per ulteriori informazioni, vedere Registrazione delle impronte digitali dell'utente.

Accesso pre-Windows
Se è stato impostato l'accesso prima dell'apertura di Windows è necessario definire una password di sistema (detta anche password pre-Windows) per effettuare l'accesso prima dell'apertura di Windows. Una volta impostata, questa password può essere modificata in qualsiasi momento dall'amministratore.

Da questa schermata è possibile anche disattivare l'accesso pre-Windows: basta digitare la password di sistema corrente, verificare che sia corretta e fare clic sul pulsante **Disattiva**.

Smart card
Se è stato specificato che gli utenti devono effettuare l'accesso tramite smart card, è necessario registrare una o più smart card tradizionali (contact) o contactless. Fare clic sul collegamento **Registra un'altra smart card** per avviare la registrazione guidata di una smart card. Registrare una smart card significa impostarla per poterla utilizzare per accedere al sistema.

Dopo la registrazione è possibile modificare o impostare un PIN per la smart card mediante il collegamento **Modifica o imposta PIN smart card** (Change or setup my smartcard PIN).

Accesso pre-Windows

Quando è impostato l'accesso pre-Windows è necessario autenticarsi (mediante password, impronte digitali o smart card) all'accensione del sistema, prima del caricamento di Windows. La funzionalità di accesso pre-Windows rafforza la sicurezza del sistema impedendo agli utenti non autorizzati di manomettere Windows e di accedere al computer (per esempio in caso di furto).

Dalla finestra Accesso pre-Windows (Pre-Windows Login), gli amministratori possono impostare l'accesso pre-Windows o creare e modificare una password pre-Windows (di sistema); se la password è già stata impostata, da questa finestra è possibile disattivare l'accesso pre-Windows. Se si configura l'accesso pre-Windows viene avviata una procedura guidata che esegue le seguenti operazioni:

- Password di sistema: imposta una password di sistema (detta anche password pre-Windows) per l'accesso pre-Windows. Questa password si utilizza anche come riserva nei casi in cui un utente disponga di altri fattori di autenticazione (per esempio per accedere al sistema in caso di problemi con il sensore per impronte digitali).
- Impronte digitali o smart card: imposta le impronte digitali o una smart card da utilizzare per l'accesso pre-Windows e specifica se questo fattore di autenticazione viene utilizzato in sostituzione o in aggiunta alla password pre-Windows.
- Single Sign On: per impostazione predefinita l'autenticazione pre-Windows (password, impronte digitali o smart card) sarà utilizzata anche per accedere automaticamente a Windows (il cosiddetto "Single Sign On"). Per disattivare questa funzione, selezionare la casella di controllo "Desidero effettuare nuovamente l'accesso a Windows" (I want to login again at Windows).
- Se oltre a una password pre-Windows è stata impostata una password disco rigido per il BIOS, sarà inoltre possibile modificare o disattivare la password disco rigido.

NOTA: non tutti i lettori di impronte digitali sono abilitati per l'autenticazione pre-Windows. Se il proprio lettore non è compatibile, sarà possibile registrare impronte digitali solo per l'accesso a Windows. Per verificare se un dispositivo specifico è compatibile, rivolgersi all'amministratore di sistema o visitare il sito support.dell.com per un elenco dei lettori di impronte digitali supportati.

Disattivazione dell'accesso pre-Windows
Da questa finestra è possibile anche disattivare l'accesso pre-Windows: basta digitare la password pre-Windows (di sistema) corrente, verificare che sia corretta e fare clic sul pulsante **Disattiva**. Tenere presente che, quando si disattiva l'accesso pre-Windows, tutte le impronte digitali o le smart card registrate restano registrate.

Registrazione / rimozione di impronte digitali

Gli utenti possono registrare o aggiornare le impronte digitali da utilizzare per l'autenticazione nel sistema per l'accesso a Windows o pre-Windows. Nella scheda Impronte digitali sono raffigurate delle mani che mostrano le dita eventualmente già registrate. Se si fa clic sul collegamento **Registra altre impronte** (Enroll another) viene aperta la Registrazione guidata impronta digitale che guida l'utente nella procedura di registrazione. "Registrare" significa salvare un'impronta digitale da utilizzare per accedere al sistema. Per effettuare la registrazione delle impronte digitali è necessario che nel sistema sia installato e opportunamente configurato un lettore di impronte digitali valido.

NOTA: non tutti i lettori di impronte digitali si possono utilizzare per l'accesso pre-Windows. Se si tenta di registrare un'impronta digitale per l'accesso pre-Windows su un lettore incompatibile, viene visualizzato un messaggio di errore. Per verificare se il dispositivo è compatibile, rivolgersi all'amministratore di sistema o visitare il sito support.dell.com per un elenco dei lettori di impronte digitali supportati.

Quando si registra un'impronta digitale, il sistema chiede di digitare la password di Windows per verificare l'identità dell'utente. Se la policy in uso lo prevede, il sistema chiederà di digitare anche la password pre-Windows (di sistema). La password pre-Windows si può utilizzare per accedere al sistema in caso di problemi con il lettore di impronte digitali.

NOTE:

- Si consiglia di registrare almeno due impronte digitali nel corso della procedura.
- Verificare che le impronte digitali siano state registrate correttamente prima di attivare l'autenticazione tramite impronta digitale.
- Se si cambia il lettore di impronte digitali di un sistema è necessario ripetere la registrazione delle impronte digitali sul nuovo lettore. Si sconsiglia di alternare continuamente l'uso di due dispositivi biometrici diversi sullo stesso PC.
- Se quando si registrano le impronte digitali viene visualizzato ripetutamente il messaggio "sensore non a fuoco", è possibile che il computer non riconosca il lettore di impronte digitali. Se questo è esterno, in molti casi il problema si risolve scollegandolo e ricollegandolo al sistema.

Cancellazione delle impronte digitali registrate
Per rimuovere le impronte digitali registrate, fare clic sul collegamento **Rimuovi impronta digitale** (Remove fingerprint) o fare clic (per deselezionarla) su un'impronta digitale registrata nella Registrazione guidata impronta digitale.

Per rimuovere un utente specifico che ha registrato le impronte digitali per l'autenticazione pre-Windows, l'amministratore può deselezionare tutte le impronte digitali registrate per quell'utente.

NOTA: in caso di errori durante la procedura di registrazione delle impronte digitali, visitare il sito wave.com/support/Dell per ulteriori informazioni.

Registrazione di smart card

Dell Data Protection | Access offre la possibilità di utilizzare una smart card tradizionale (contact) o contactless per l'accesso all'account di Windows o per l'autenticazione pre-Windows. Nella scheda Smart card, fare clic sul collegamento **Registra un'altra smart card** per lanciare la procedura guidata di registrazione della smart card che aiuta l'utente a completare la registrazione. "Registrare" significa impostare una smart card per poterla utilizzare per accedere al sistema.

Per effettuare la registrazione è necessario che nel sistema sia installato e opportunamente configurato un dispositivo di autenticazione per smart card valido.

NOTA: per verificare se un dispositivo specifico è compatibile, rivolgersi all'amministratore di sistema o visitare il sito support.dell.com per un elenco delle smart card supportate.

Registrazione
Quando si registra una smart card, il sistema chiede di digitare la password di Windows per verificare l'identità dell'utente. Se la policy in uso lo prevede, il sistema chiederà di digitare anche la password pre-Windows (di sistema). La password pre-Windows si può utilizzare per accedere al sistema in caso di problemi con il lettore di smart card.

Durante la registrazione verrà richiesto l'inserimento del PIN della smart card eventualmente impostato. Se la policy in uso richiede un PIN e questo non è stato impostato, il sistema richiederà di crearne uno.

NOTE:

- Un utente registrato per l'utilizzo della smart card per l'accesso pre-Windows non può essere rimosso.
- Gli utenti standard possono modificare il PIN utente di una smart card e l'amministratore può modificare sia il PIN amministratore che il PIN utente.
- L'amministratore può inoltre reimpostare una smart card; una volta reimpostata, questa non può essere utilizzata per autenticarsi durante l'accesso a Windows o pre-Windows fino a quando non viene nuovamente registrata.

NOTA: per l'autenticazione dei certificati TPM, gli amministratori possono registrare i certificati TPM mediante la procedura di registrazione delle smart card di Microsoft Windows. Per la compatibilità con questa applicazione, gli amministratori devono selezionare "Wave TCG-Enabled CSP" come CSP (fornitore di servizi di crittografia) al posto di un CSP smart card. Inoltre è necessario abilitare l'Accesso sicuro Dell (Dell Secure Login) con la policy del tipo di autenticazione per il client adeguata.

NOTA: se un messaggio di errore avverte che il servizio smart card non è in esecuzione, è possibile avviare / riavviare il servizio nel modo seguente:

- Dal Pannello di controllo, accedere alla finestra Strumenti di amministrazione, selezionare Servizi, fare clic con il pulsante destro del mouse su smart card e selezionare Avvia o Riavvia.
- Per informazioni più dettagliate su un messaggio di errore specifico, visitare il sito wave.com/support/Dell.

Self-Encrypting Drive

Dell Data Protection | Access gestisce le funzioni di sicurezza hardware dei self-encrypting drive, in cui la crittografia dei dati è incorporata nell'hardware dell'unità. Questa funzionalità si utilizza per garantire che solo gli utenti autorizzati possano accedere ai dati crittografati (quando il drive è in modalità di blocco).

Alla finestra Self-Encrypting Drive si accede facendo clic sulla scheda **Self-Encrypting Drive**. La scheda è visualizzata solo quando nel sistema sono presenti uno o più self-encrypting drive (SED).

Fare clic sul collegamento **Configura** (Setup) per avviare la configurazione guidata del self-encrypting drive. Questa procedura consente di impostare la password per l'amministratore del drive, farne il backup e applicare le impostazioni di crittografia del drive. Solo gli amministratori di sistema possono accedere alla configurazione guidata del self-encrypting drive.

Importante! Una volta configurato il drive, la protezione dei dati e il blocco del drive sono "attivati". Quando un drive è bloccato, il suo comportamento è il seguente:

- Il drive entra in modalità di *blocco* ogni volta che viene spento.
- Il drive non si avvia finché non vengono immessi il nome utente e la password (o l'impronta digitale) corretti nella schermata di autenticazione pre-Windows. Quando il blocco del drive non è attivato, i relativi dati sono accessibili per chiunque utilizzi il computer.
- Il drive è protetto anche se viene collegato a un altro computer come unità secondaria; per accedere ai dati è necessario autenticarsi.

Una volta configurato il drive, la finestra Self-Encrypting Drive mostra i drive installati e un collegamento che permette agli utenti di modificare le password di accesso al drive. Da questa finestra, l'amministratore del drive potrà inoltre aggiungere o rimuovere gli utenti del drive. Se è stato configurato un drive esterno, sarà visualizzato in questa finestra e potrà essere sbloccato.

NOTA: per poter bloccare un drive secondario esterno è necessario che il drive venga spento indipendentemente dal computer.

L'amministratore del drive può gestirne le impostazioni in **Avanzate>Dispositivi** (Advanced > Devices). Per ulteriori informazioni, vedere Gestione dispositivi (Device Management) - Self-Encrypting Drive.

Configurazione del drive

La configurazione guidata del self-encrypting drive consente di eseguire la configurazione dei drive. Quando si esegue questa procedura è importante tenere presenti i concetti elencati di seguito.

Amministratore del drive
Il primo utente con privilegi di amministratore di sistema che imposta l'accesso al drive (e la password amministratore del drive) diventa amministratore del drive; questo è l'unico utente autorizzato a modificare le impostazioni di accesso al drive. Per garantire che il primo utente venga impostato deliberatamente come amministratore del drive, è necessario selezionare la casella di controllo "Confermo" (I understand) per continuare la procedura.

Password amministratore del drive
La procedura guidata chiede di creare una password amministratore del drive e di digitarla nuovamente per confermarla. Per poter creare la password amministratore del drive è necessario

digitare la password di Windows per identificarsi. L'utente corrente di Windows deve disporre di privilegi di amministratore per creare questa password.

Backup delle credenziali di accesso al drive
Digitare un percorso o fare clic sul pulsante **Sfoglia** per selezionarne uno e salvarvi una copia di backup delle credenziali di amministratore del drive.

IMPORTANTE

- Si consiglia vivamente di eseguire il backup di queste credenziali e di salvarle in un'unità diversa dal disco rigido principale (per esempio su un supporto rimovibile). In caso contrario, se non è più possibile accedere al drive non sarà possibile nemmeno accedere al backup di questi dati.
- Una volta terminata la configurazione del drive, al successivo riavvio del sistema tutti gliutenti dovranno inserire il nome utente e la password (o le impronte digitali) corretti prima del caricamento di Windows per accedere al sistema.

Aggiunta di utenti del drive
L'amministratore del drive può aggiungere al drive altri utenti che siano utenti validi di Windows. Durante questa operazione, l'amministratore ha la possibilità di richiedere all'utente di reimpostare la password al primo accesso. Per sbloccare il drive, l'utente dovrà reimpostare la password nella schermata di autenticazione pre-Windows.

Impostazioni avanzate

- *Single Sign On* - Per impostazione predefinita, la password del self-encrypting drive inserita prima dell'avvio di Windows per autenticarsi sul drive sarà utilizzata automaticamente anche per accedere a Windows (questa funzione è detta "Single Sign On"). Per disattivare questa funzione, selezionare la casella di controllo "Desidero accedere nuovamente all'avvio di Windows" (I want to login again when Windows starts) quando si configurano le impostazioni del drive.
- *Accesso tramite impronta digitale* - Sulle piattaforme supportate è possibile specificare che si desidera autenticarsi sul self-encrypting drive con un'impronta digitale anziché con una password.
- *Supporto per la modalità sospensione/standby (S3)* (se supportata dalla piattaforma) - Se il supporto è attivato, il self-encrypting drive si può tranquillamente mettere in modalità Sospensione/Standby (detta anche modalità S3); per uscire da questa modalità, richiederà l'autenticazione pre-Windows.

NOTE:

- Quando è attivato il supporto S3, le password di crittografia del drive sono soggette a ogni eventuale limitazione esistente delle password del BIOS. Per ulteriori informazioni sulla presenza di eventuali limitazioni specifiche relative alle password del BIOS, consultare il produttore dell'hardware del sistema.
- Non tutti i self-encrypting drive supportano la modalità S3. La presenza o meno del supporto per la modalità Standby/Sospensione sarà verificata in sede di configurazione del drive. Per i drive che non supportano questa modalità, le richieste S3 di Windows saranno convertite automaticamente in richieste di ibernazione, se questa modalità è attivata (si consiglia vivamente di attivare la modalità di sul computer).
- Al primo accesso dopo l'impostazione dell'opzione Single Sign On (SSO), il processo si interromperà alla schermata di accesso a Windows. L'utente dovrà inserire il proprio modulo di autenticazione per Windows, che verrà archiviato in modo sicuro per i futuri tentativi di accesso a Windows. Al successivo riavvio del sistema, l'utente accederà automaticamente a Windows tramite il SSO. Lo stesso procedimento è necessario in caso di modifica della modalità di autenticazione a Windows di un utente (password, impronta digitale, PIN di una smart card). Se il computer fa parte di un dominio in cui si applica una

policy che richiede di premere i tasti ctrl+alt+canc per accedere a Windows, la policy sarà rispettata.

ATTENZIONE: se occorre disinstallare l'applicazione **Dell Data Protection | Access**, è necessario prima disattivare la protezione dati del self-encrypting drive e sbloccare il drive.

Funzioni utente Self-Encrypting Drive

La gestione della sicurezza e degli utenti dei self-encrypting drive sono affidate agli amministratori. Gli utenti dei drive diversi dall'amministratore possono eseguire solo le operazioni seguenti:

- Modificare la propria password per il drive
- Sbloccare un drive

Questa operazioni si possono eseguire accedendo alla scheda **Self-Encrypting Drive** in **Dell Data Protection | Access**.

Cambia password
Consente agli utenti registrati di creare una nuova password di autenticazione del drive. Per poter impostare la password del drive su un nuovo valore è necessario digitare la password corrente per il Self-Encrypting Drive.

NOTE:

- Se abilitate, vengono applicate le policy relative alla lunghezza e alla complessità delle password di Windows. Se le policy relative alle password di Windows non sono abilitate, la lunghezza massima della password di un Self-Encrypting Drive è di 32 caratteri. Tenere presente che se non è abilitata la modalità S3 (Sospensione/Standby) la lunghezza massima è di 127 caratteri.
- La password utente di un Self-Encrypting Drive è separata dalla password di Windows. Quando una password utente di Windows viene modificata o reimpostata, l'operazione non influisce sulla password utente del drive a meno che non sia stata abilitata la sincronizzazione delle password di Windows. Per ulteriori informazioni, consultare Dispositivi: Self-Encrypting Drive.
- Su alcune tastiere non inglesi è presente un set di caratteri riservati che non si può utilizzare per le password dei self-encrypting drive. Se la password di Windows contiene uno di questi caratteri ed è abilitata la sincronizzazione delle password di Windows, la sincronizzazione non andrà a buon fine e verrà visualizzato un messaggio di errore.

Sblocco drive
Sblocco drive consente a un utente del drive registrato di sbloccare un drive bloccato. Se è abilitato il blocco del drive, lo stato del drive passa a bloccato ogni volta che viene spento il computer. Quando il sistema viene riacceso è necessario autenticarsi nel drive digitando la password nella schermata di autenticazione pre-Windows.

NOTE:

- Talvolta può essere impossibile entrare in una modalità di risparmio energia (sospensione/standby o ibernazione) se su uno stesso computer sono attivi contemporaneamente più account utente di self-encrypting drive.
- Nelle versioni dell'applicazione localizzate in cinese, giapponese, coreano e russo, "User 1", "User 2" ecc. vengono sostituiti dai nomi utente dei drive nella schermata di autenticazione pre-Windows.

Opzioni avanzate (Advanced Options)

Le Opzioni avanzate (Advanced options) di **Dell Data Protection | Access** consentono a un utente dotato di privilegi di amministratore di gestire i seguenti aspetti dell'applicazione:

Manutenzione
Password
Dispositivi (Devices)

NOTA: solo gli utenti con privilegi di amministratore possono apportare modifiche nelle Opzioni avanzate (Advanced options); gli utenti standard possono visualizzare queste impostazioni ma non le possono modificare.

Manutenzione

La finestra Manutenzione si può utilizzare per impostare le preferenze di accesso a Windows, per eseguire il reset di un sistema per predisporlo a una diversa destinazione o archiviare o ripristinare le credenziali utente memorizzate nei dispositivi hardware di sicurezza del sistema. Per informazioni, consultare i seguenti argomenti:

Preferenze di accesso (Access Preferences)
Reset del sistema (Reset System)
Archiviazione e ripristino delle credenziali

Preferenze di accesso (Access Preferences)

La finestra Preferenze di accesso (Access Preferences) consente agli amministratori di specificare le preferenze di accesso a Windows per tutti gli utenti del sistema.

Attiva Accesso sicuro Dell (Enable Dell Secure Login)
La possibilità di sostituire la normale schermata ctrl-alt-canc di Windows consente di utilizzare altri fattori di autenticazione al posto della password per l'accesso a Windows o in aggiunta a questa. Per aumentare la sicurezza della procedura di accesso a Windows, si può decidere di aggiungere un'impronta digitale come secondo fattore di autenticazione. È possibile aggiungere anche altri fattori di autenticazione per l'accesso a Windows, per esempio una smart card o un certificato TPM.

NOTE:

- L'attivazione di Accesso sicuro Dell (Dell Secure login) influisce su tutti gli utenti del sistema.
- Si consiglia di attivare questa opzione solo DOPO che gli utenti abbiano registrato le rispettive impronte digitali o smart card.
- Al primo accesso dopo l'impostazione di questa opzione, il sistema chiede di autenticarsi in Windows secondo la policy standard; al successivo avvio sarà necessario utilizzare i nuovi fattori di autenticazione.

Disattiva Accesso sicuro Dell (Disable Dell Secure login)
Questa opzione disattiva tutte le funzioni di accesso a Windows di **Dell Data Protection | Access**. Quando è selezionata, il sistema torna alle policy di accesso a Windows standard.

NOTE:

- Se durante un tentativo di accesso viene visualizzato un messaggio di errore relativo all'Accesso sicuro a Windows, disattivare e riattivare l'opzione Accesso sicuro Dell (Dell Secure login).
- Per informazioni più dettagliate su un messaggio di errore specifico, visitare il sito wave.com/support/Dell.

Reset del sistema (Reset System)

La funzione Reset del sistema (Reset System) si utilizza per cancellare tutti i dati degli utenti dai dispositivi hardware di sicurezza della piattaforma, per esempio in caso di destinazione di un computer a un uso diverso. Questa opzione cancella tutte le password presenti nel sistema tranne le password utente di Windows, nonché tutti i dati presenti nei dispositivi hardware (ControlVault, TPM e lettori di impronte digitali). Per i SED, questa funzione disattiva anche la protezione dei dati in modo da renderli accessibili sul drive.

Dopo avere confermato che si desidera reimpostare il sistema, fare clic su **Avanti**. Per eseguire il reset sarà necessario digitare la password eventualmente impostata per ogni singolo dispositivo di sicurezza:

- Proprietario TPM
- Amministratore ControlVault
- Amministratore BIOS
- Di sistema per il BIOS (pre-Windows)
- Disco rigido (BIOS)
- Amministratore Self-Encrypting Drive

NOTA: per i self-encrypting drive non è necessario digitare tutte le password utente del drive, ma solo la password amministratore del drive.

Importante: l'unico modo per recuperare i dati cancellati dal reset del sistema è ripristinarli da un archivio creato in precedenza. Se non si dispone di un archivio, i dati non sono recuperabili. Per i self-encrypting drive vengono eliminati solo i dati di configurazione, ma non i dati personali presenti sull'unità.

Archiviazione e ripristino delle credenziali

La funzionalità di archiviazione e ripristino delle credenziali si utilizza per il backup e il ripristino di tutte le credenziali utente (dati di accesso e di crittografia) archiviate nei dispositivi ControlVault e Trusted Platform Module (TPM). Il backup di questi dati è importante in caso di reinstallazione dei sistemi di un computer o per il ripristino dei dati in seguito a guasti dei componenti hardware. In casi del genere è sufficiente ripristinare sul nuovo computer tutte le credenziali da un file di archivio precedentemente salvato.

È possibile decidere di archiviare o ripristinare le credenziali per un solo utente o per tutti gli utenti del sistema.

Le credenziali utente sono costituite dai dati utilizzati per l'accesso pre-Windows, quali impronte digitali e dati di smart card registrati, e dalle chiavi memorizzate nel TPM. TPM creerà le chiavi su richiesta delle applicazioni di sicurezza: per esempio, la generazione di un certificato digitale determina la creazione di chiavi in TPM.

NOTA: per stabilire se le chiavi TPM sono idonee per l'archiviazione con **Dell Data Protection | Access**, consultare la documentazione dell'applicazione di sicurezza. In linea di massima, per la generazione delle chiavi sono supportate le applicazioni che utilizzano “Wave TCG-Enabled CSP”.

Archiviazione delle credenziali
Per archiviare le credenziali, procedere nel modo seguente:

- Specificare se le credenziali da archiviare sono per sé o per tutti gli utenti del sistema.
- Autenticarsi sui componenti hardware di sicurezza digitando la password di sistema (pre-Windows), la password amministratore ControlVault e la password del proprietario TPM.
- Creare una password per il backup delle credenziali.
- Specificare un percorso per l'archivio con il pulsante **Sfoglia**. Il percorso dell'archivio deve puntare a un supporto rimovibile, per esempio un'unità flash USB o un'unità di rete, per evitare problemi in caso di guasti del disco rigido.

Note importanti:
- Prendere nota del percorso dell'archivio per essere in grado di ripristinare le credenziali all'occorrenza.
- Prendere nota della password per il backup delle credenziali per garantire il ripristino dei dati. Questo è importante, poiché la password non si può recuperare.
- Se non si conosce la password del proprietario TPM, rivolgersi all'amministratore del sistema o consultare le istruzioni di impostazione TPM del computer.

Ripristino delle credenziali
Per ripristinare le credenziali, procedere nel modo seguente:

- Specificare se le credenziali da ripristinare sono per sé o per tutti gli utenti del sistema.
- Accedere alla posizione di archiviazione e selezionare il file dell'archivio.
- Digitare la password per il backup delle credenziali definita quando è stato creato l'archivio.
- Autenticarsi sui componenti hardware di sicurezza digitando la password di sistema (pre-Windows), la password amministratore ControlVault e la password del proprietario TPM.

NOTE:
- Se dopo svariati tentativi di ripristino un messaggio di errore avverte che il ripristino delle credenziali non è riuscito, provare a eseguirlo per un file di archivio diverso. Se

l'operazione non riesce, creare un altro archivio per le credenziali e provare a eseguire il ripristino dal nuovo archivio.

- Se un messaggio di errore avverte che non è stato possibile ripristinare le chiavi TPM, creare un archivio per le credenziali e quindi cancellare il TPM nel BIOS. Per cancellare il TPM, riavviare il computer, premere il tasto **F2** all'inizio del riavvio per accedere alle impostazioni del BIOS e quindi accedere a Sicurezza>Sicurezza TPM. Impostare nuovamente la proprietà di TPM e riprovare a ripristinare le credenziali.
- Per informazioni più dettagliate su un messaggio di errore specifico, visitare il sito wave.com/support/Dell.

Gestione password

Dalla finestra Gestione password, l'amministratore può creare o modificare tutte le password di sicurezza del sistema:

- Di sistema (nota anche come pre-Windows)*
- Amministratore*
- Disco rigido*
- ControlVault
- Proprietario TPM
- Principale TPM
- Cassaforte password TPM
- Self-Encrypting Drive

NOTE:

- Poiché sono visualizzate solo le password valide per la configurazione corrente della piattaforma, la finestra può cambiare a seconda della configurazione e dello stato del sistema.
- Le password contrassegnate da un * sono password del BIOS e si possono modificare anche dal BIOS del sistema.
- Le password del BIOS non si possono creare né modificare se l'amministratore del BIOS non consente di modificare le password.
- Se si fa clic sul collegamento **configurazione** (setup) di un self-encrypting drive viene avviata la configurazione guidata del Self-Encrypting Drive; se si fa clic su **gestione** (manage) è possibile modificare le password di uno o più Self-Encrypting Drive.
- Se si fa clic sul collegamento **gestione** (manage) della cassaforte password TPM, viene visualizzata una finestra in cui è possibile visualizzare o modificare le password che proteggono le chiavi TPM. Quando si crea una chiave TPM che richiede una password, questa viene generata in modo casuale e memorizzata nella cassaforte. Non è possibile gestire la cassaforte password TPM se non si è prima creata una password principale TPM.

Regole di complessità delle password di Windows

Dell Data Protection | Access garantisce che la password seguente è conforme alle regole di complessità delle password di Windows per il computer:

- Password del proprietario TPM

Per determinare la complessità della password di Windows per un computer, seguire queste istruzioni:

1. Accedere al Pannello di controllo.
2. Fare doppio clic su Strumenti di amministrazione.
3. Fare doppio clic su Criteri di protezione locali.
4. Espandere Criteri account e selezionare Criterio password.

Dispositivi (Devices)

La finestra Dispositivi (Devices) è utilizzata dagli amministratori per la gestione di tutti i dispositivi di sicurezza installati nel sistema. Per ogni dispositivo sono visualizzati lo stato e informazioni dettagliate aggiuntive, per esempio la versione del firmware. Fare clic su **mostra** (show) per visualizzare le informazioni dei singoli dispositivi o su **nascondi** (hide) per comprimere quella sezione. I dispositivi che è possibile gestire sono i seguenti, a seconda di quelli installati sulla piattaforma in uso:

Trusted Platform Module (TPM)
ControlVault®
Self-Encrypting Drive
Informazioni sui dispositivi di autenticazione (Authentication Device Information)

Trusted Platform Module (TPM)

Per utilizzare le funzioni di sicurezza avanzate disponibili nell'applicazione **Dell Data Protection | Access** e nel TPM, è necessario avere attivato il chip di sicurezza TPM e avere definito la proprietà TPM.

La finestra Trusted Platform Module di **Gestione dispositivi** (Device Management) è visualizzata solo quando nel sistema viene rilevata la presenza di un TPM.

Gestione TPM (TPM Management)

Queste funzioni consentono all'amministratore di sistema di gestire il TPM.

Stato
Visualizza lo stato *attivo* o *inattivo* del TPM. Lo stato "Attivo" indica che il TPM è stato attivato nel BIOS ed è pronto per essere configurato (ovvero è possibile assegnargli una proprietà). Se il TPM non è attivo (abilitato) non può essere gestito e non è possibile accedere alle relative funzioni di sicurezza.

Se nel sistema viene rilevato un TPM non attivo (non abilitato), è possibile attivarlo facendo clic sul collegamento **attiva** (activate) in questa finestra, senza accedere al BIOS del sistema. Dopo l'attivazione di TPM con questa funzione, è necessario riavviare il computer. Durante il riavvio, il sistema potrebbe chiedere all'utente di confermare le modifiche.

NOTA: la possibilità di abilitare (attivare) il TPM da questa applicazione potrebbe non essere supportata in tutte le piattaforme. Se non è supportata è necessario abilitarla nel BIOS del sistema . Per eseguire questa operazione, riavviare il sistema, premere il tasto **F2** prima dell'avvio di Windows e accedere al BIOS, quindi spostarsi su Sicurezza>Sicurezza TPM e attivare il TPM.

Da questa finestra è possibile anche *disattivare* il TPM facendo clic sul link **disattiva** (deactivate); con la disattivazione, il TPM non è più disponibile per le funzioni avanzate di sicurezza. Tuttavia, la disattivazione non modifica in alcun modo le impostazioni del TPM, né elimina o modifica le informazioni o le chiavi in esso memorizzate.

Con proprietario
Mostra lo stato di proprietà (cioè "con proprietario") e consente di definire o modificare il proprietario TPM. Affinché le funzioni di sicurezza del TPM siano disponibili è necessario stabilire la proprietà TPM. Prima di stabilire la proprietà è necessario abilitare (attivare) il TPM.

La procedura di definizione della proprietà prevede che l'utente (dotato di privilegi di amministratore) crei una password del proprietario TPM. Una volta definita la password, la proprietà è stabilita e il TPM può essere utilizzato.

NOTA: la password del proprietario TPM deve rispettare le regole di complessità delle password di Windows definite per il sistema.

Importante: è importante non perdere o dimenticare la password del proprietario TPM in quanto essa è necessaria per accedere alle funzioni di sicurezza avanzate del TPM in **Dell Data Protection | Access**.

Bloccato (Locked)
Visualizza lo stato *bloccato* o *sbloccato* del TPM. Il "blocco" è una funzione di sicurezza del TPM; il TPM entra in modalità di blocco dopo un numero prestabilito di tentativi di accesso con una password del proprietario TPM errata. Il proprietario TPM può sbloccare il TPM da questa finestra; è necessario digitare la password del proprietario TPM.

NOTE:

- Se un messaggio di errore avverte che non è stato possibile stabilire la proprietà del TPM, cancellare il TPM nel BIOS del sistema e riprovare a stabilire la proprietà. Per cancellare il TPM, riavviare il computer, premere il tasto **F2** all'inizio del riavvio per accedere alle impostazioni del BIOS e quindi accedere a Sicurezza>Sicurezza TPM.
- Se un messaggio di errore avverte che è stato impossibile modificare la password del proprietario TPM, archiviare i dati del TPM (archiviazione delle credenziali), cancellare il TPM nel BIOS, stabilirne nuovamente la proprietà e ripristinare i dati del TPM (ripristino delle credenziali).
- Per informazioni più dettagliate su un messaggio di errore specifico, visitare il sito wave.com/support/Dell.

Dell ControlVault®

Dell ControlVault® (CV) è un dispositivo hardware di archiviazione protetto per le credenziali utente utilizzate nell'accesso pre-Windows (per esempio password utente o impronte digitali registrate). La finestra ControlVault di **Gestione dispositivi** (Device Management) è visualizzata solo quando nel sistema viene rilevata la presenza di un dispositivo ControlVault.

Gestione di ControlVault

Queste funzioni permettono all'amministratore del sistema di gestire il dispositivo ControlVault presente nel sistema.

Stato

Visualizza lo stato *attivo* o *inattivo* di ControlVault. Lo stato "Inattivo" significa che il dispositivo ControlVault non è disponibile per l'archiviazione nel sistema. Consultare la documentazione del sistema Dell per determinare se il sistema è dotato di un dispositivo ControlVault.

Password

Indica se è stata impostata una password amministratore ControlVault e consente di impostare una password o di modificarla se ne è già stata impostata una. Solo gli amministratori di sistema possono impostare o modificare questa password. La password amministratore ControlVault deve essere impostata per eseguire le seguenti operazioni:

- Archiviazione o ripristino delle credenziali.
- Cancellazione dei dati degli utenti (per tutti gli utenti).

NOTA: se si tenta di eseguire un'operazione di archiviazione o ripristino senza avere prima impostato la password amministratore ControlVault, il sistema chiede all'utente di crearne una (se l'utente è un amministratore).

Utenti registrati

Indica se gli utenti hanno registrato credenziali di accesso (per esempio password, impronte digitali o dati di smart card) che sono memorizzate nel dispositivo ControlVault.

Cancellazione dei dati degli utenti (Clear User Data)

Periodicamente può essere necessario cancellare i dati memorizzati nel dispositivo ControlVault; per esempio, se gli utenti incontrano problemi nell'utilizzo o nella registrazione delle credenziali pre-Windows per l'autenticazione. Da questa finestra è possibile cancellare tutti i dati memorizzati nel dispositivo ControlVault, per un singolo utente o per tutti gli utenti.

Per cancellare tutti i dati degli utenti presenti sulla piattaforma è necessario digitare la password amministratore ControlVault. Se sono state registrate credenziali pre-Windows, il sistema chiederà di digitare anche la password di sistema (pre-Windows). Quando si cancellano i dati di tutti gli utenti, la password amministratore ControlVault e la password di sistema vengono reimpostate; tenere presente che questo è l'unico modo per cancellare la password amministratore ControlVault.

NOTA: quando tutti i dati degli utenti sono stati cancellati, viene richiesto il riavvio del computer. Il riavvio è importante per il corretto funzionamento del sistema.

Non è necessario impostare la password amministratore ControlVault per cancellare le credenziali di un singolo utente. Quando si fa clic su **cancella dati utente** (clear user data), il sistema chiede di selezionare l'utente di cui si desidera cancellare le credenziali sul dispositivo ControlVault. Dopo che è stato selezionato un utente, viene richiesto l'inserimento della password di sistema (solo se sono state registrate credenziali pre-Windows).

NOTE:

- Se un messaggio di errore avverte che è impossibile creare la password amministratore ControlVault, archiviare le proprie credenziali, cancellare tutti i dati degli utenti dal dispositivo ControlVault, riavviare il computer e riprovare a creare la password.
- Se un messaggio di errore avverte che è impossibile cancellare le credenziali di un singolo utente dal dispositivo ControlVault, archiviare le proprie credenziali, provare a cancellare i dati di tutti gli utenti e quindi riprovare a cancellare i dati di quel singolo utente.
- Se un messaggio di errore avverte che è stato impossibile cancellare le credenziali di tutti gli utenti dal dispositivo ControlVault, verificare se sia opportuno eseguire un reset del sistema. **Importante:** prima di eseguire il reset del sistema, consultare l'argomento della guida "Reset del sistema" in quanto l'operazione cancellerà TUTTI i dati di sicurezza degli utenti.
- Se un messaggio di errore avverte che non è stato possibile eseguire il backup dei dati di ControlVault e del TPM, disattivare il TPM nel BIOS del sistema. Per eseguire questa operazione, riavviare il computer, premere il tasto **F2** al riavvio per accedere alle impostazioni del BIOS e quindi accedere a Sicurezza>Sicurezza TPM. Riattivare quindi il TPM e riprovare ad archiviare i dati ControlVault.
- Per informazioni più dettagliate su un messaggio di errore specifico, visitare il sito wave.com/support/Dell.

Self-Encrypting Drive: funzioni avanzate

Dell Data Protection | Accessgestisce le funzioni di sicurezza hardware dei self-encrypting drive, in cui la crittografia dei dati è incorporata nell'hardware dell'unità. Questa gestione garantisce che solo gli utenti autorizzati possano accedere ai dati crittografati quando il drive è in modalità di blocco.

La finestra Self-Encrypting Drive in **Gestione dispositivi** (Device Management) è visualizzata solo se nel sistema sono presenti uno o più self-encrypting drive (SED).

Importante! Una volta configurato il drive, la protezione dei dati e il blocco del self-encrypting drive sono "attivati".

Gestione dei drive (Drive Management)
Queste funzioni consentono all'amministratore del drive di gestire le impostazioni di sicurezza del drive. Le modifiche alle impostazioni di sicurezza del drive diventano effettive una volta spento il drive.

Protezione dei dati (Data Protection)
Visualizza lo stato *attivato* o *disattivato* per la protezione dati del self-encrypting drive. Lo stato "attivato" significa che la protezione del drive è stata configurata; tuttavia, fino a quando non viene impostato il *blocco* del drive, gli utenti non dovranno eseguire l'autenticazione pre-Windows per accedere al drive.

Da questa schermata è possibile disattivare la protezione dei dati del self-encrypting drive. Quando questa è disattivata, tutte le funzioni di sicurezza avanzate del self-encrypting drive sono disattivate ed esso si comporta come una normale unità. La disattivazione della protezione dati elimina anche tutte le impostazioni di sicurezza, comprese le credenziali degli amministratori e degli utenti del drive. Invece, questa funzione non altera né rimuove alcun dato dell'utente sul drive.

Blocco (Locking)
Visualizza lo stato *attivato* o *disattivato* dei self-encrypting drive. Per informazioni sul comportamento dei drive bloccati, consultare l'argomento Self-Encrypting Drive.

Se è necessario disattivare temporaneamente il blocco dei drive, è possibile farlo in questa schermata. Si sconsiglia di eseguire questa operazione poiché quando il blocco dei drive è disattivato non sono richieste credenziali per accedere al drive e quindi qualsiasi utente della piattaforma può accedere ai dati presenti sul drive. La disattivazione del blocco dei drive nonelimina in alcun modo le impostazioni di sicurezza (comprese le credenziali dell'amministratore e degli utenti del drive), né i dati di qualsiasi utente.

ATTENZIONE: se occorre disinstallare l'applicazione **Dell Data Protection | Access**, è necessario prima disattivare la protezione dati del self-encrypting drive e sbloccare il drive.

Amministratore drive

Mostra l'amministratore corrente del drive. Da questa schermata, l'amministratore del drive può modificare l'utente impostato come amministratore del drive. Il nuovo amministratore deve essere un utente Windows del sistema valido e disporre dei privilegi di amministratore. Nel sistema può esistere un solo amministratore del drive.

Utenti del drive

Mostra gli utenti del drive registrati e il numero di utenti registrati in quel momento. Il numero massimo di utenti supportati dipende dal self-encrypting drive (attualmente 4 utenti per i drive Seagate e 24 per i drive Samsung).

Sincronizzazione delle password di Windows

La funzione di sincronizzazione delle password di Windows (WPS) imposta automaticamente le password utente dei self-encrypting drive sulle password utente di Windows. Questa funzione non è obbligatoria per l'amministratore del drive, ma solo per gli utenti. La funzione WPS si può utilizzare negli ambienti aziendali in cui le password devono essere modificate periodicamente (per esempio ogni 90 giorni); con questa opzione attivata, tutte le password utente dei self-encrypting drive vengono aggiornate automaticamente quando vengono modificate le password di Windows degli utenti corrispondenti.

NOTA: quando è attivata la sincronizzazione delle password di Windows (WPS), le password utente dei self-encrypting drive non si possono modificare; per aggiornarle automaticamente è necessario modificare le password di Windows degli utenti corrispondenti.

Ricorda ultimo nome utente

Quando questa opzione è attivata, l'ultimo nome utente digitato viene visualizzato per impostazione predefinita nel campo **Nome utente** della schermata di autenticazione pre-Windows.

Selezione nome utente (Username Selection)

Quando questa opzione è attivata, gli utenti possono visualizzare tutti i nomi utente dei drive nel campo **Nome utente** della schermata di autenticazione pre-Windows.

Cancellazione crittografica

Questa opzione si può utilizzare per "cancellare" tutti i dati presenti sul self-encrypting drive. I dati non vengono effettivamente cancellati, ma vengono eliminate le chiavi utilizzate per la crittografia dei dati che risultano così inutilizzabili. Dopo una cancellazione crittografica non è più possibile recuperare i dati; inoltre, la protezione dati del self-encrypting drive è disattivata e l'unità è pronta per essere adibita a un uso diverso.

NOTE:

- Se vengono visualizzati messaggi di errore relativi alle funzioni di gestione dei self-encrypting drive, spegnere il computer e riavviarlo (non limitarsi al semplice riavvio).
- Per informazioni più dettagliate su un messaggio di errore specifico, visitare il sito wave.com/support/Dell.

Informazioni sui dispositivi di autenticazione (Authentication Device Information)

La finestra Informazioni sui dispositivi di autenticazione (Authentication Device Information) di **Gestione dispositivi** (Device Management) visualizza le informazioni e lo stato di tutti i dispositivi di autenticazione (lettori di impronte digitali, lettori di smart card tradizionali o contactless) connessi al sistema.

Assistenza tecnica

Per l'assistenza tecnica relativa al software **Dell Data Protection | Access**, visitare il sito http://www.wave.com/support.dell.com.

Wave TCG-Enabled CSP

Wave Systems Trusted Computing Group (TCG)-enabled Cryptographic Service Provider (CSP) è fornito con l'applicazione **Dell Data Protection | Access** ed è disponibile per l'uso ogniqualvolta sia necessario un CSP, chiamato direttamente da un'applicazione o selezionabile da un elenco dei CSP installati. Se possibile, selezionare "Wave TCG-Enabled CSP" in modo che TPM possa generare le chiavi e che **Dell Data Protection | Access** possa gestire le chiavi e le relative password.

Wave Systems TCG-enabled CSP consente alle applicazioni di utilizzare le funzioni disponibili sulle piattaforme compatibili con TCG direttamente tramite MSCAPI. Un modulo CSP MSCAPI ottimizzato per TCG che fornisce la funzionalità di chiave asimmetrica su TPM e sfrutta le avanzate caratteristiche di sicurezza fornite dal modulo TPM, indipendentemente dagli specifici requisiti dei fornitori in relazione al provider TSS (Trusted Software Stack).

NOTA: se le chiavi TPM generate da Wave TCG-enabled CSP richiedono una password e l'utente ha creato una password principale TPM, le singole password chiave saranno generate in modo casuale e memorizzate nella cassaforte delle password TPM.