

Infineon Security Platform Solution



Benvenuti in Infineon Security Platform Solution

Security Platform Solution utilizza Trusted Platform Module per proteggere dati e applicazioni.

Per maggiori informazioni, consultare il sito Web Infineon:

<http://www.infineon.com/tpm/software>



©Infineon Technologies AG

Infineon Security Platform Solution

Introduzione

Il software Infineon Security Platform Solution è un insieme completo di strumenti che utilizzano un modulo specifico incorporato nel sistema, chiamato Trusted Platform Module. Questa soluzione offre i servizi necessari per creare e gestire facilmente i certificati digitali utilizzando Infineon Trusted Platform Module. I certificati possono essere utilizzati per eseguire le seguenti attività:

- Inviare e ricevere e-mail protette da client di posta elettronica come Microsoft Windows Mail/Outlook Express, Microsoft Outlook o Mozilla Thunderbird.
- Configurare browser (come Mozilla Firefox o Internet Explorer) e browser Web (come Microsoft Internet Information Server) per l'autenticazione del client.
- Firmare le macro di Microsoft Word.
- Crittografare file e cartelle.
- Proteggere le connessioni di rete.

I valori segreti degli utenti possono essere trasferiti ad altri computer per garantire la massima protezione di tutti i PC utilizzati.

Il software Infineon Security Platform Solution comprende i seguenti componenti:

- Tool di configurazione di Security Platform
- Inizializzazione Guidata Rapida di Infineon Security
- Inizializzazione guidata di Security Platform
- Inizializzazione utenti guidata di Security Platform
- Migrazione guidata di Security Platform
- Backup guidato di Security Platform
- Reimpostazione guidata password di Security Platform
- Importazione guidata PKCS #12 di Security Platform
- Visualizzatore certificati e Selezione certificati di Security Platform
- Icona TNA di Security Platform

- Servizi integrativi di Security Platform
- Servizi di Security Platform
- Server Integration Services
- Personal Secure Drive

Oltre a fornire informazioni sull'[installazione del software Infineon Security Platform Solution](#), il presente documento aiuta anche ad ottimizzare l'utilizzo del software stesso e di Infineon Trusted Platform Module per operazioni quali:

- [Richiesta di certificati digitali](#)
- [Crittografia di file e cartelle](#)
- [Configurazione dei client di posta elettronica per inviare e-mail crittografate con firma digitale](#)

Inoltre, questo documento è utile anche per gli amministratori dell'organizzazione, per assisterli durante operazioni come:

- [Mapping dei certificati con Internet Information Server e Active Directory](#)
- [Autenticazione dei client con Internet Explorer](#) o [Autenticazione dei client con Mozilla Firefox](#)
- [Utilizzo di certificati digitali per firmare elettronicamente le macro di Microsoft Word](#)

Un'altra attività molto importante che deve essere eseguita dagli amministratori è la gestione delle funzionalità di [backup e ripristino di emergenza](#). Queste funzionalità vengono definite in fase di inizializzazione di Security Platform e non influenzano le funzioni generali di protezione sopra descritte. Tali procedure sono essenziali per evitare la perdita di dati in caso di problemi del computer.



Infineon Security Platform Solution

Vantaggi dell'uso di Trusted Platform Module

La straordinaria diffusione di Internet e la tendenza all'espansione delle reti aziendali per consentire l'accesso a clienti e fornitori esterni al firewall della società pongono l'accento sul problema della sicurezza. Parallelamente alle forme di identificazione elettronica, che stanno sempre più sostituendo i metodi basati su documenti cartacei e sull'identificazione personale, le questioni associate alla sicurezza e alla privacy hanno assunto grande rilevanza. Queste problematiche sembrano essere state risolte con le applicazioni basate su chiavi pubbliche. La trasmissione sicura di informazioni tramite reti pubbliche, la firma digitale come garanzia di autenticità delle e-mail e l'autenticazione tra server e client sono solo alcuni esempi dei servizi possibili grazie alla tecnologia delle chiavi pubbliche.

La comunicazione tramite Internet è in costante crescita. Molte applicazioni, come quelle destinate all'e-commerce, si basano sulla fiducia nell'interlocutore e sull'affidabilità della connessione. Autenticità, correttezza, riservatezza e tutela della privacy sono principi fondamentali. Lo sviluppo dell'alleanza [TCG \(Trusted Computing Group\)](#) rappresenta una forte iniziativa commerciale la cui finalità è migliorare la fiducia nella sicurezza della Rete. TCG ha definito un dispositivo, conosciuto come **Trusted Platform Module** (TPM, Security Chip), che svolge molte funzioni importanti per la sicurezza.

Il Security Chip è la base di sicurezza di una determinata piattaforma (ad esempio i computer desktop o i notebook). Se integrato in un computer sul quale è installato un sistema operativo che riconosce il chip, Security Chip è in grado di controllare l'integrità del sistema e di autenticare utenti esterni che intendono accedere alle funzioni di sicurezza, pur restando sotto il completo controllo dell'utente principale. In questo modo privacy e riservatezza sono garantite. Le piattaforme basate su Security Chip consentono, per la prima volta, di creare i fondamenti per la definizione di un'infrastruttura di chiavi pubbliche globale (PKI, public key infrastructure). Questa garantisce soprattutto la sicurezza di molte applicazioni per ambienti privati e aziendali e rende possibili altri tipi di applicazioni non disponibili in passato.

Le attività dell'iniziativa TCG e lo standard di sicurezza che ne deriva sono una chiara dimostrazione dei requisiti ai quali deve rispondere la tecnologia di sicurezza odierna. L'architettura di Infineon Trusted Platform Module è stata progettata per fornire i più elevati standard di sicurezza disponibili, basati su una tecnologia di sicurezza verificata, e una facile integrazione dei sistemi grazie a

una soluzione di sicurezza completa. Infineon Trusted Platform Module offre le implementazioni di crittografia RSA e gli algoritmi hash (SHA-1 e MD-5) per assicurare le massime prestazioni possibili, nonché un generatore di numeri casuali (TRNG, true random number generator). Si tratta di un dispositivo protetto con i più alti livelli di sicurezza per l'analisi SPA (simple power analysis) e DPA (differential power analysis).

Fino a qualche tempo fa gli utenti di computer memorizzavano le chiavi private e i certificati sul disco rigido del PC, esponendo così le informazioni agli attacchi degli hacker e di tutti coloro che potevano avere accesso fisico al sistema. Trusted Platform Module fornisce invece un supporto di memorizzazione a prova di intrusione, garantendo la sicurezza delle informazioni.



©Infineon

Technologies AG

Soluzione Infineon Security Platform

Microsoft Windows

Questa pagina contiene informazioni specifiche per le versioni dei sistemi operativi Microsoft Windows.

Controllo dell'Account dell'Utente

Il Controllo dell'Account dell'Utente è una importante caratteristica offerta da Windows Vista e versioni successive. Con il Controllo dell'Account dell'Utente, gli amministratori IT possono gestire la maggior parte delle applicazioni, dei componenti e dei processi con un privilegio limitato, ma hanno "potenziale di elevazione" per attività amministrative specifiche e funzioni applicative. Quando gli utenti standard richiamano un'attività del sistema che richiede privilegi dell'amministratore, come ad esempio l'installazione di un'applicazione, Windows lo notificherà all'utente e richiederà l'autorizzazione dell'amministratore, ovvero nome utente e password di un account con privilegi amministrativi, per completare l'attività in questione. Inoltre, il Controllo dell'Account dell'Utente fa sì che anche gli account degli amministratori siano quasi sempre gestiti come account standard, e quando si tenta di svolgere un'attività a livello di amministratore, l'amministratore riceverà un sollecito per elevare temporaneamente i privilegi per il completamento di quella singola attività.

Windows utilizza un'icona scudo  per indicare che questa caratteristica particolare richiede privilegi amministrativi per eseguire l'attività (es. il ripristino di Security Platform mediante [Inizializzazione guidata di Security Platform Infineon](#)).



- In Windows 7, l'icona scudo non è visibile in modo permanente per impostazione predefinita, ma solo dopo una configurazione appropriata.
- L'aspetto di tale icona può variare leggermente, a seconda della versione di Windows.

Microsoft BitLocker

[BitLocker](#) della Microsoft, fornito con alcune edizioni di Windows Vista e versioni successive, può essere utilizzato per crittografare un intero disco rigido, rendendo più difficile l'accesso ai dati del computer nel caso in cui venisse perso o rubato. La Crittografia unità BitLocker, con o senza il Trusted Platform Module, fornisce la crittografia di tutto il disco. Il Trusted Platform Module rende la crittografia del drive ancora più sicura perchè utilizza il chip per generare chiavi di crittografia basate sugli scan dei file di sistema di base, in aggiunta a una chiave per l'hard drive stesso. Per configurare questa caratteristica, controllare la [l'Inizializzazione guidata dell'Infineon Security Platform](#) e gli [Tool di Configurazione di Infineon Security Platform](#).

Gestione Trusted Platform Module (TPM)

L'applicazione Microsoft *Gestione Trusted Platform Module (TPM)* è una nuova funzionalità offerta da Windows Vista e versioni successive. Questa applicazione può essere usata per impostare e gestire la proprietà del Trusted Platform Module. Informazioni più dettagliate sono disponibili nel Microsoft TechNet. Fare riferimento a Microsoft TechNet.

Errori

Se vi sono errori TPM o TSS inaspettati con Windows Vista o con sistemi operativi successivi, controllare che i comandi TPM siano bloccati con le impostazioni dei Criteri del Gruppo Windows.



©Infineon

Technologies AG

Infineon Security Platform Solution - Modalità operative

Modalità operative

Modalità Server

In modalità server, i Server Integration Services integrano la Security Platform in un Trust Domain con gestione centralizzata.

 Consultare *Guida Tecnica per Trusted Computing Management Server* per informazioni più dettagliate sulla modalità server.

Condizioni preliminari in modalità server per iscrizione piattaforma e iscrizione utente

	Informazioni
Iscrizione alla piattaforma	<p>L'iscrizione piattaforma viene eseguita automaticamente senza alcuno intervento dell'utente.</p> <p>Condizioni preliminari:</p> <ul style="list-style-type: none">• Trust Domain Platform è un membro del gruppo di iscrizione piattaforme (Per ulteriori informazioni consultare la <i>Guida Tecnica per Trusted Computing Management Server</i>.)• Trusted Platform Module è stato abilitato e attivato.• Trusted Platform Module non è configurato ancora (non da Infineon TPM Professional Package in modalità autonoma, da Server Dominio Trusted in modalità Server o da altro software come Windows <i>Trusted Platform Module (TPM) Management</i>).• Trust Domain Platform è online, ciò significa che, Trust Domain Platform ha una connessione di rete al Trust Domain Server.
Iscrizione dell'utente	<p>L'iscrizione dell'utente sarebbe eseguita interattivamente come in modalità autonoma se le seguenti condizioni preliminari sono soddisfatti:</p> <p>Condizioni preliminari:</p> <ul style="list-style-type: none">• L'utente Trust Domain è un membro del gruppo di iscrizione utente (Per ulteriori informazioni consultare <i>Guida Tecnica per Trusted Computing Management</i>

Server.)

- Trusted Platform Module della piattaforma utente è stato abilitato e attivato.
- Trust Domain Platform è online, ciò significa che, Trust Domain Platform ha una connessione di rete al Trust Domain Server.
- L'utente è connesso al dominio.

Modalità Autonoma

In modalità autonoma la Security Platform non è integrata in un Trust Domain con gestione centralizzata.

Differenze fra le Modalità Operative:

La seguente tabella elenca il comportamento dei diversi componenti di interfaccia utente nelle Modalità Operative:

Componente	Modalità Autonoma	Modalità Server
<u>Tool di configurazione</u>	Questo componente è designato come Applet del Pannello di controllo. Gli amministratori e gli utenti possono eseguire l'inizializzazione, la configurazione della Security Platform Caratteristiche e gestire tutte le funzionalità della Security Platform.	La configurazione di tutte le impostazioni di autenticazione e di Proprietario della Security Platform sono automaticamente gestite dal Trusted Computing Management Server. La pagina Avanzata e la pagina di Migrazione non sono disponibili.
<u>Inizializzazione Guidata Rapida</u>	Unisce l'inizializzazione della piattaforma e dell'utente con impostazioni predefinite (consigliato per la maggior parte degli utenti).	Le attività specifiche della piattaforma sono ignorate, poiché se ne occupa il Server di Gestione Elaborazione Trust.
<u>Assistente di inizializzazione</u>	Inizializzazione, Abilitazione e Ripristino delle Funzionalità della Security Platform (passi amministrativi). Questa procedura guidata è completamente funzionale in questa modalità.	L'Inizializzazione, l'Abilitazione e il Ripristino avvengono automaticamente una volta che il sistema cliente è integrato in un Trust Domain con gestione centralizzata, ovvero l'amministratore non deve eseguire questo compito. La Procedura Guidata della Security Platform non è funzionale se la piattaforma è membro del gruppo di

		iscrizione piattaforme.
Inizializzazione utenti guidata	La Procedura Guidata di Inizializzazione Utente supporta l'inizializzazione degli Utenti della Security Platform e la configurazione delle Funzionalità della Security Platform . Questa procedura guidata è completamente funzionale in questa modalità.	L'inizializzazione dell'utente è possibile solo se l'utente attuale è un membro dell'enrollment group utenti specificato nel Trusted Computing Management Server. Anche questa procedura guidata è completamente funzionale in questa modalità.
Migrazione guidata	La migrazione di chiavi e certificati specifici per utenti da una piattaforma di origine ad una piattaforma di destinazione include azioni utente e amministrative. Questa procedura guidata è completamente funzionale in questa modalità.	Questa procedura guidata non è funzionale poiché la migrazione di chiavi e certificati specifici per utenti è eseguita automaticamente dal Trusted Computing Management Server, ovvero l'amministratore e l'utente non devono eseguire questa attività.
Backup guidato	Il Backup e il Ripristino automatico e manuale comprendono passi dell'utente e amministrativi. Inoltre, se il Personal Secure Drive (PSD) è stato configurato, il Backup e il Ripristino manuali di questo drive possono essere eseguiti.	Il Backup e il Ripristino sono eseguiti dal Server Integration Services. Se il Personal Secure Drive (PSD) è stato configurato, il Backup e il Ripristino manuali possono essere eseguiti.
Reimpostazione guidata password	La reimpostazione della Password Utente di Base comprende passi amministrativi e utente. L'amministratore prepara la	Il Trusted Computing Management Server si occupa di preparare e fornire il Codice di Autorizzazione per la Reimpostazione della

	reimpostazione della password per un utente e fornisce il Codice di Autorizzazione per la Reimpostazione della Password. L'utente reimposta la sua Password Utente di Base.	Password per l'utente e l'amministratore specifico. C'è un'opzione aggiuntiva per ottenere il Codice di Autorizzazione di Reimpostazione dal server.
Importazione guidata PKCS #12	Questa procedura guidata viene utilizzata per importare file di Scambio Informazioni Personali nella Security Platform ed è completamente funzionale in questa modalità.	Nessun cambiamento nel funzionamento di questa procedura guidata ed è anche completamente funzionale in questa modalità.
Icona TNA	Eseguire attività amministrative della Security Platform e ottenere informazioni relative allo stato. Questa applicazione è completamente funzionale in questa modalità.	Le attività eseguite dal server senza interazione dell'utente non sono disponibili in questa modalità.



Soluzione Infineon Security Platform

Soluzione Installazione del software Infineon Security Platform

Nel caso in cui nel sistema sia già installata una versione del software Soluzione Infineon Security Platform, non occorre disinstallarla. L'installazione esistente può essere sovrascritta in un'unica operazione.



Aggiornamento: La procedura di aggiornamento delle versioni precedenti del prodotto è descritta nel file *ReadmeUpgrade.txt*.

1. Eseguire il programma di installazione.

Nota: se il software Infineon Security Platform è già installato nel sistema, apparirà una finestra di dialogo in cui è possibile scegliere se modificare, aggiornare o eliminare l'installazione esistente.

2. All'avvio dell'installazione guidata, vengono visualizzate la versione del software Infineon Security Platform e altre informazioni di tipo legale.
3. Cliccare su **Avanti** per continuare la procedura di installazione. Viene visualizzato il Contratto di Licenza con l'utente finale (EULA).
4. Leggere attentamente il contratto. Accettare i termini del contratto di licenza. Fare clic su **Avanti** per continuare la procedura di installazione.
5. Successivamente, è necessario fornire alcune informazioni generali per l'installazione. Immettere i propri dati e quelli della società nelle caselle di testo corrispondenti.
6. Cliccare su **Avanti** per continuare la procedura di installazione.
7. Nella finestra **Tipo Setup**, selezionare il tipo di setup desiderato:
 - Selezionare **Completo** se si desidera installare tutti I componenti nella directory di installazione predefinita.
 - Altrimenti selezionare **Personalizzato**.
8. Selezionare i componenti da installare. Sul lato destro dello schermo, viene visualizzata la descrizione di ciascun componente. È possibile scegliere se installarlo subito o in un secondo tempo oppure non installarlo affatto. Alcuni componenti sono obbligatori e non possono essere deselezionati. Inoltre, è possibile scegliere la directory in cui si vuole installare il software

Soluzione Infineon Security Platform.

9. Cliccare su **Avanti** per continuare la procedura di installazione.
10. Scegliere **Installa** per completare la procedura di installazione.
11. L'installazione guidata provvede ad installare il software Soluzione Infineon Security Platform.

In base alle opzioni selezionate, verranno installati nel sistema i seguenti componenti:

- Tool di configurazione di Security Platform
 - Inizializzazione Guidata Rapida di Infineon Security
 - Inizializzazione guidata di Security Platform
 - Inizializzazione utenti guidata di Security Platform
 - Migrazione guidata di Security Platform
 - Backup guidato di Security Platform
 - Reimpostazione guidata password di Security Platform
 - Importazione guidata PKCS #12 di Security Platform
 - Visualizzatore certificati e Selezione certificati di Security Platform
 - Icona TNA di Security Platform
 - Personal Secure Drive
 - Infineon TPM Cryptographic Service Provider
 - Stack del software Security Platform
 - Software del driver di Trusted Platform Module
 - Server Integration Services
12. La procedura di installazione del software Soluzione Infineon Security Platform è completata.
 13. Selezionare **Preparazione Iscrizione TPM** per [attivare](#) il Trusted Platform Module, se desiderato (solo su sistemi con Trusted Platform Module disattivato e supporto Interfaccia Presenza Fisica). Ciò consentirà di inizializzare successivamente la piattaforma, senza dover riavviare nuovamente il sistema.
 14. Se necessario, selezionare l'opzione **Visualizza il file Readme**.
 15. Scegliere **Fine** per completare l'installazione.



Infineon Security Platform Solution

Installazione e amministrazione di Infineon Security Platform

Nello stato iniziale, Infineon Security Platform è disabilitato per impostazione predefinita. Tale condizione assicura che in questa fase non vi sia un flusso di informazioni da Infineon Security Platform al costruttore della piattaforma, in quanto non esistono dati segreti condivisi, in qualsiasi forma.

Lo stato corrente di Infineon Security Platform non è mai influenzato dall'installazione di Infineon Security Platform Solution.

Prima di poter utilizzare Infineon Security Platform è necessario:

- Abilitare Infineon Security Platform seguendo la procedura descritta nella documentazione del prodotto:

- Impostazione Infineon Security Platform e Utente avviando l'Inizializzazione Guidata Rapida



In [modalità server](#), la Security Platform è inizializzata automaticamente se il sistema cliente è integrato in un Trust Domain con gestione centralizzata, ovvero l'amministratore non deve eseguire questo compito.

Per informazioni dettagliate sulle procedure guidate e sui tool di amministrazione, vedere [Tool di Infineon Security Platform Solution](#).

Dopo aver installato Infineon Security Platform e configurato un utente, è possibile [ottenere un certificato basato su Trusted Platform Module](#).

Le operazioni che possono essere eseguite sono controllate dallo stato corrente di Infineon Security Platform. La [panoramica dello stato](#) elenca i possibili valori di stato.

Le risposte alle domande più frequenti sull'uso di Security Platform sono riportate nella sezione [domande frequenti](#).



TPM

©Infineon Technologies AG

Infineon Security Platform Solution

Ruoli utente

Security Platform Solution consente di utilizzare diversi ruoli utente.

- Tutti i ruoli degli utenti di Security Platform sono basati sugli account utente di Windows (utenti locali o del dominio). Questi account sono stati autenticati dalla funzione di accesso a Windows.
- Ogni ruolo utente ha uno scopo specifico.
- I membri dei vari ruoli utente vengono inizializzati durante la configurazione di Security Platform.
- Per operare con un ruolo utente specifico è richiesta un'autenticazione particolare (es.: un'apposita password).
- Ogni utente può operare con più ruoli.

La tabella seguente elenca tutti i possibili ruoli utente.

Ruolo utente	Basato su...	Scopo e attività	Inizializzazione	Autenticazione
Proprietario di Security Platform	Account utente di Windows (locale o di dominio), membro del gruppo di amministratori	Esegue attività amministrative importanti, quali il ripristino di Security Platform.	L'inizializzazione del software abilita un utente Windows ad operare come proprietario di Security Platform.	Password propria
Amministratore di Security Platform (o semplicemente "amministratore")	Account utente di Windows (locale o di dominio), membro del gruppo di amministratori	Esegue attività amministrative che richiedono i diritti di amministrazione di Windows.	Non è necessaria nessuna inizializzazione particolare.	Oltre all'autenticazione come Amministratore di Windows, alcune attività amministrative richiedono l'accesso token protetto con password dedicata.

<p>Utente di Security Platform (o semplicemente "utente")</p>	<p>Account utente di Windows (locale o di dominio)</p>	<p>Utilizza le funzionalità di Security Platform, come la crittografia di file e cartelle o la protezione della posta elettronica.</p> <p>Inoltre, configura le funzioni del software ed esegue altre attività specifiche degli utenti di Security Platform.</p>	<p>L'inizializzazione del software abilita un utente Windows ad operare come utente di Security Platform.</p>	<p>Passw di bas</p>
<p>Agente di ripristino EFS/PSD (o semplicemente "utente")</p>	<p>Utilizzo di un certificato di ripristino dedicato e di una chiave privata</p>	<p>Ripristino dei dati di un utente di EFS o PSD, nel caso in cui le credenziali originali EFS/PSD siano andate perdute.</p>	<p>Il ripristino di EFS/PSD è abilitato mediante la registrazione degli agenti di ripristino.</p>	<p>Chiaav dell'ag riprist</p>



Infineon Security Platform Solution

Autenticazione utente

Per motivi di sicurezza, l'accesso alle funzionalità di protezione richiede l'autenticazione dell'utente in Infineon Security Platform. Ad esempio, è necessario specificare la chiave utente di base, protetta da password, per poter crittografare i file. Digitando questa password viene eseguita l'autenticazione in Security Platform. L'utilizzo della chiave utente di base è possibile soltanto se l'autenticazione è stata completata correttamente.

Infineon Security Platform Solution dispone di due livelli di autenticazione per proteggere la chiave utente.

Autenticazione password

La chiave utente di base è protetta dalla relativa *password utente di base* che deve essere immessa manualmente.

Autenticazione avanzata

La chiave utente di base è protetta da una *frase password* che viene memorizzata dal dispositivo di autenticazione, ad esempio una smart card, un token USB protetto, un lettore di impronte digitali o un altro dispositivo biometrico di autenticazione. La frase password è accessibile unicamente dal dispositivo di autenticazione in uso (ad esempio, inserendo la smart card e digitando il PIN corrispondente oppure appoggiando un dito sul lettore di impronte digitali).

Password e frasi password

L'**autenticazione password** richiede l'utilizzo di una normale password come "password utente di base". Sebbene sia tecnicamente possibile utilizzare password lunghe e complesse, la maggior parte di esse è piuttosto breve, dal momento che devono essere memorizzate.

Con l'**autenticazione avanzata** non è necessario memorizzare le password poiché vengono gestite dal dispositivo di autenticazione. La password è infatti sostituita da un codice PIN o da un'autenticazione di tipo biometrico. Quindi, l'autenticazione avanzata è più pratica e immediata. Inoltre, il livello di sicurezza è decisamente superiore, grazie alle funzioni di protezione incorporate nel dispositivo di autenticazione. Ad esempio, le smart card dispongono di un contatore dei tentativi che blocca la scheda quando si immette più volte un PIN errato. Questo sistema rende impossibili i cosiddetti "attacchi a forza bruta" anche con codici PIN relativamente semplici.

Per sottolineare il fatto che l'autenticazione avanzata consente di utilizzare password lunghe e complesse in modo pratico e immediato, il termine *password* è stato sostituito da *frase password*. Una frase password è semplicemente una password più lunga e complicata.

Security Platform Solution distingue questi due tipi di password come spiegato di seguito.

- **Password:** viene utilizzata in modalità Autenticazione password e corrisponde alla *password utente di base*.
- **Frase password:** viene utilizzata in modalità Autenticazione avanzata e corrisponde anch'essa alla password utente di base. In questo contesto specifico, tale password è chiamata *frase password utente di base*.

Installazione e gestione dell'autenticazione avanzata

I dispositivi di autenticazione vengono forniti mediante plug-in installabili separatamente. Il software Security Platform Solution rileva automaticamente i dispositivi di autenticazione installati.

La configurazione di questi dispositivi è diversa per ciascun utente, in quanto sistemi di autenticazione differenti possono essere utilizzati dai vari utenti di Security Platform. L'utilizzo dell'autenticazione avanzata può essere controllato utilizzando i relativi [criteri](#).

Come configurare l'autenticazione avanzata passo dopo passo

Come configurare l'autenticazione avanzata - Attività dell'amministratore	Componenti software richiesti
1. Installare il dispositivo di autenticazione.	L'installazione deve essere eseguita separatamente. Contattare il fornitore del plug-in del dispositivo di autenticazione in uso.
2. Abilitare l'uso dei dispositivi di autenticazione per tutti gli utenti.	Se il software Security Platform non è stato inizializzato: Inizializzazione guidata Se il software Security Platform è già stato inizializzato: Tool di configurazione - Avanzate - Configura...
Come configurare l'autenticazione avanzata - Attività dell'utente	Componenti software richiesti
3. Selezionare il dispositivo e il livello di autenticazione per l'utente attuale di Security Platform.	Se l'utente non è stato configurato: Inizializzazione utenti guidata Se l'utente è già stato configurato: Tool di configurazione - Impostazioni utente - Configura...

Soluzione Infineon Security Platform

Token, archivi e altri file di gestione di Security Platform

Soluzione Infineon Security Platform utilizza numerosi file (come token e archivi) per la gestione di attività quali il backup, il ripristino di emergenza o la reimpostazione della password. Alcuni di questi file sono utilizzati dagli amministratori e altri dagli utenti di Security Platform. Fare attenzione a non confondere queste tipologie di file.

La tabella seguente contiene alcune informazioni generali sui file di gestione di Security Platform.

File	Utilizzato da...	Scopo/Spiegazione
File Backup Password Proprietario	Amministratore	Utilizzato per l'autenticazione della Password Proprietario (anziché digitare la Password Proprietario). Questo file è compatibile con il File Backup Password Proprietario generata dall'applicazione Microsoft "Gestione Trusted Platform Module (TPM)".  Questo file non è necessario in modalità server poiché il Trusted Computing Management Server gestisce l'attività di preparazione e di fornitura della password.
Archivi utilizzati per il ripristino di emergenza e la reimpostazione della	Amministratore/Utente	Contengono le credenziali e le impostazioni di Security

password		<p>Platform, oltre ai file di backup di Personal Secure Drive. Questi archivi vengono creati durante il backup automatico o manuale. Sono richiesti per eseguire il ripristino dei dati in caso di danneggiamento del disco rigido, perdita di dati o malfunzionamento di Trusted Platform Module. I dati di reimpostazione della password, archiviati in un file, sono necessari per reimpostare le password utente di base.</p> <p> Questi archivi non sono necessari in modalità server, poiché Reset della Password, Backup e Ripristino della Security Platform sono gestiti dal Trusted Computing Management Server.</p>
Token di ripristino di emergenza	Amministratore	<p>Viene creato durante la configurazione delle funzionalità di Security Platform. (quando l'Inizializzazione Guidata di Security Platform è utilizzata). Il token è utilizzato per</p>

		<p>recuperare i dati quando si rende necessario eseguire un ripristino di emergenza (malfunzionamento di Trusted Platform Module).</p> <p> Questo file non è necessario in modalità server, poiché il Ripristino della Security Platform è gestito dal Trusted Computing Management Server.</p>
Token di reimpostazione della password	Amministratore	<p>Viene creato durante la configurazione delle funzionalità di Security Platform (quando l'Inizializzazione Guidata di Security Platform è utilizzata). Il file token è utilizzato per preparare la reimpostazione della password per un determinato utente.</p> <p> Questo file non è necessario in modalità server, poiché il Reset della Password è gestito dal Trusted Computing Management Server.</p>
Token Recupero di Emergenza/Reimpostazione Password	Amministratore	Creato durante l'Inizializzazione di Security Platform

		<p>(quando l'Inizializzazione Guidata Rapida di Security Platform è utilizzata).</p> <p>Unisce il Token Recupero di Emergenza e il Token Reimpostazione Password in un unico file.</p>
Archivio di migrazione	Utente	<p>Contiene le chiavi e i certificati utente che devono essere trasferiti a un'altra installazione di Security Platform. Questo archivio viene creato durante la fase di <i>esportazione</i> della procedura di migrazione. È richiesto per eseguire l'<i>importazione</i> dei dati migrati.</p> <p> Questo file non è necessario in modalità server, poiché la Migrazione è gestita dal Trusted Computing Management Server.</p>
Valore segreto per la reimpostazione della password	Utente	<p>Viene creato durante la configurazione delle impostazioni utente di Security Platform. Questa informazione è richiesta per</p>

		reimpostare la password utente di base.
File del codice di autorizzazione alla reimpostazione	Amministratore/Utente	<p>Contiene il codice di autorizzazione necessario per reimpostare la password di un utente di base. Questo file viene creato durante le procedure eseguite dall'amministratore per preparare la reimpostazione della password. È richiesto all'utente per poter reimpostare la propria password.</p> <p> In modalità server questo file è creato da Trusted Computing Management Server.</p>
File PKCS #12 (file di scambio delle informazioni personali)	Utente	Contiene la chiave privata e il certificato dell'utente. Questo file è necessario per importare un certificato.



Soluzione Infineon Security Platform

Funzionamento avanzato di Security Platform

[Backup e ripristino dei dati di Security Platform](#)

[Recupero Dati EFS e PSD mediante Agente Recupero Dati](#)

[Chiavi di Migrazione verso altri Sistemi](#)

[Reimpostazione della password utente di base](#)

[Difesa da Attacco Dizionario](#)

Technologies AG



Soluzione Infineon Security Platform

Backup e ripristino dei dati di Security Platform

Il backup di Security Platform comprende tutti i dati richiesti in caso di emergenza. Quando si verifica un grave errore dell'hardware, del supporto di archiviazione o di Trusted Platform Module, la procedura di ripristino di Security Platform consente di ristabilire l'accesso alle funzionalità del software.

Inoltre, è possibile eseguire il backup e il ripristino dei dati di Personal Secure Drive. I dati di altre applicazioni che utilizzano Soluzione Security Platform (ad esempio, i programmi di protezione della posta elettronica) non sono compresi nelle procedure di backup di Security Platform.



- In [modalità Server](#) il Backup e il Ripristino delle credenziali e delle impostazioni utente sono gestite da Trusted Computing Management Server, eccetto il Backup e il Ripristino dei file di immagine della Personal Secure Drive (PSD).
- Anche l'aggiornamento delle [credenziali e delle impostazioni](#) dell'utente gestito da Trusted Computing Management Server è basato su Backup e Ripristino.

Ambito del backup

Il backup di Security Platform comprende i seguenti dati:

Credenziali e impostazioni di Security Platform	
Contenuti del backup	Una copia delle credenziali e delle impostazioni utente memorizzate in Security Platform.
Finalità	Ripristinare le credenziali e le impostazioni utente nel caso di errori dell'hardware o del supporto di archiviazione. Senza questa operazione, non è possibile accedere alle funzionalità di Security Platform e i dati degli utenti andranno perduti.
Archivi	<ul style="list-style-type: none">• Archivio di backup generato automaticamente ("archivio di backup del sistema", ad esempio, file SPSystemBackup.xml nella cartella SPSystemBackup): in base alle impostazioni dell'amministratore di Security Platform. Questo archivio contiene le credenziali e le impostazioni di tutti gli utenti di Security Platform (per uno o più computer su cui è installato il software); include, inoltre, i dati di identificazione del computer e degli utenti, dati che verranno utilizzati durante la procedura di ripristino per mettere in corrispondenza ciascun computer con il proprio utente.• Archivio di backup generato manualmente (es. SPBackupArchive.xml) dall'utente di Security Platform. Questo archivio contiene le credenziali e le impostazioni un utente di Security Platform (per un computer su cui è installato il software). include, inoltre, i dati di identificazione del computer e dell'utente, dati che verranno utilizzati durante la procedura di ripristino per mettere in corrispondenza il computer con il proprio utente.
Ripristino di emergenza	
Contenuti del backup	Tutte le chiavi utente di base di Security Platform, crittografate specificatamente per il ripristino di emergenza.
Finalità	Crittografare nuovamente tutte le chiavi utente di base in caso di

	<p>errore di Trusted Platform Module. In questo caso dovrà essere impostata una nuova Security Platform e sarà creato un nuovo proprietario. Il ripristino di emergenza consente di crittografare nuovamente le chiavi utente di base dalla vecchia chiave del proprietario del software alla nuova.</p> <p>Senza questa operazione, non è possibile accedere alle funzionalità di Security Platform e i dati degli utenti andranno perduti.</p>
Archivi	<ul style="list-style-type: none"> • I Dati per il Recupero di Emergenza per tutti gli utenti sono compresi in File Compressi di Backup scritti automaticamente. Sono inclusi anche per l'utente interessato negli archivi di backup creati in modalità manuale, se il backup automatico è già stato configurato al momento dell'esecuzione del backup manuale. • Il Token per il Recupero di Emergenza (es. SPemRecToken.xml) o il Token combinato per il Recupero di Emergenza/Ripristino Password (es. SpToken_<PCName>.xml): Creato dall'Amministratore di Security Platform. È necessario per il ripristino dei dati per il Recupero di Emergenza.
<h3>Personal Secure Drive</h3>	
Contenuti del backup	<p>Una copia delle credenziali, delle impostazioni di configurazione e dei dati crittografati della PSD.</p>
Finalità	<p>Ripristinare i dati crittografati e le impostazioni di configurazione di PSD nel caso di errori dell'hardware o del supporto di archiviazione.</p> <p>Senza questa operazione, gli utenti non saranno più in grado di decrittografare i dati PSD.</p> <p>Nota:</p> <ul style="list-style-type: none"> • Diversamente dal backup di PSD, gli strumenti tradizionali per il backup del disco rigido producono file non crittografati. • Se le credenziali della PSD sono state perse e non è disponibile alcun backup delle credenziali ma il file di immagine della PSD o del backup è disponibile, questi dati possono essere recuperati attraverso Recupero Personal Secure Drive.

Archivi

- Le impostazioni di configurazione di PSD vengono salvate sia negli **archivi di backup generati automaticamente**, sia negli **archivi di backup generati manualmente**.
- **File di backup di PSD** (es. SpPSDBackup.fsb): È possibile creare una copia del file immagine di PSD durante il backup manuale di Security Platform.

Tipi di Backup

Tipo	Informazioni
Backup Sistem ("Backup Automatico")	<p>Comprende sempre credenziali e impostazioni del computer e di tutti gli utenti inizializzati nel momento in cui viene eseguito il backup del sistema (compresi i dati per il Recupero di Emergenza).</p> <p>Dettagli sull'esecuzione del Backup del Sistema</p>
Backup Manuale	<p>Comprende le credenziali e le impostazioni del computer e dell'utente corrente.</p> <p>Comprende i dati per il Recupero di Emergenza per l'utente corrente, se il Backup Automatico è già stato configurato nel momento in cui viene eseguito il backup manuale.</p> <p>A richiesta è possibile eseguire il backup del file di immagine della Personal Secure Drive (PSD) attualmente configurata per l'utente corrente.</p> <p>Dettagli sull'esecuzione del Backup Manuale</p>

Casistica di ripristino

Esistono vari casi in cui si rende necessario eseguire il ripristino dei dati, a seconda delle diverse condizioni di emergenza che potrebbero verificarsi:

Casistica	Ambito di ripristino
Disco rigido danneggiato o perdita di dati	Credenziali e impostazioni di Security Platform, Personal Secure Drive
Nuovo Trusted Platform Module	Ripristino di emergenza
Nuovo Security Platform da inizializzare	Ripristino di emergenza, credenziali e impostazioni di Security Platform, Personal Secure Drive

Come eseguire le procedure di backup e ripristino

Come configurare il backup automatico ("backup di sistema")	Componente Software da utilizzare
<p>Attività dell'amministratore: configurazione automatica del backup per tutti gli utenti (incluso le credenziali e le impostazioni di Security Platform, il ripristino di emergenza e le impostazioni di configurazione di PSD).</p>	<p>Se il software Security Platform non è stato inizializzato:</p> <p>Configurazione mediante Inizializzazione Guidata Rapida</p> <p>Qui il Backup del Sistema è configurato automaticamente con le impostazioni predefinite.</p> <p>Configurazione mediante Inizializzazione Guidata di Security Platform</p> <p>Seguire i passi indicati:</p> <ul style="list-style-type: none">• Avviare il tool di configurazione di Infineon Security Platform. Nella pagina di Benvenuto dell'Inizializzazione Guidata Rapida, selezionare Inizializzazione Avanzata• Selezionare Inizializzazione Security Platform e fare clic su Avanti.• Impostare la Password Proprietario e fare clic su Avanti.• Durante l'Inizializzazione Guidata, spunta la casella di spunta Backup Automatico (include il Ripristino di Emergenza) e clicca Successivo.• Ricerca una posizione sull'hard drive per salvare l'Archivio di Backup. Verrà creato un File Compresso di Backup composto da un file XML (es. SPSsystemBackup.xml) e da una cartella (es. SPSsystemBackup) nella posizione predefinita: <i>\\%ALLUSERSPROFILE%\Documenti\Security Platform.</i>

- Il backup programmato di default è stabilito per le ore 12:00 ogni giorno. Per cambiare l'orario, fare clic su **Programma...** , selezionare un'ora di inizio per creare un backup programmato, quindi fare clic su **Ok**, quindi su **Avanti**.
- Seleziona l'opzione **Crea un nuovo Token di Ripristino**.
- Ricerca una posizione di tua scelta per salvare il file del Token di Ripristino di Emergenza (nome di default del file: SPEmRecToken.xml).
- Imposta una nuova password del token e clicca **Successivo**.
- Conferma le impostazioni e clicca **Successivo**.
- Spunta la casella di spunta **Esegui un backup automatico adesso**. Clicca **Termina** nella pagina di Completamento.
- Le credenziali e le impostazioni di Security Platform vengono inserite in un backup per la prima volta ora. Backup regolari avranno luogo come programmato.

Se il software Security Platform è già stato inizializzato: [Tool di configurazione - Backup - Configura...](#)

Seguire i passi indicati:

- Lancia il Infineon Security Platform Settings Tool e seleziona **Backup**.
- Clicca su **Configura...** per lanciare l'Inizializzazione Guidata.
- Ricerca una posizione sull'hard drive per salvare l'Archivio di Backup. Verrà creato un File Compresso di Backup composto da un file XML (es. SPSystemBackup.xml) e da una cartella (es. SPSystemBackup) nella posizione predefinita:
`\\%ALLUSERSPROFILE%\Documenti\Security`

Platform.

- Il backup programmato di default è stabilito per le ore 12:00 ogni giorno. Per cambiare l'orario, fare clic su **Programma...** , selezionare un'ora di inizio per creare un backup programmato, quindi fare clic su **Ok**, quindi su **Avanti**.
- Conferma le impostazioni e clicca **Successivo**.
- Spunta la casella **Esegui un backup automatico ora** e clicca su **Termina** sulla pagina di Completamento.
- Le credenziali e le impostazioni di Security Platform vengono inserite in un backup per la prima volta ora. Backup regolari avranno luogo come programmato.



In [modalità Server](#) questo pulsante è disabilitato, poiché il backup automatico è gestito dal Trusted Computing Management Server, ovvero non è necessaria nessuna configurazione esplicita da parte dell'utente.

Come eseguire il ("backup manuale")

Componente Software da utilizzare

Compito Utente:
esecuzione del backup manuale per l'utente attuale.

Seguire i passi indicati:

- Lancia il Infineon Security Platform Settings Tool e seleziona **Backup**. [Tool di configurazione - Backup - Backup...](#)
- Clicca su **Backup...** per lanciare la Procedura Guidata di Backup.
- Clicca su **Ricerca...** e seleziona una posizione sull'hard drive per salvare l'Archivio di Backup (nome di default del file: SPBackupArchive.xml). Fare clic su **Avanti**.
- Configurazione le impostazioni di backup della Personal Secure Drive (vedere [Configurazione Impostazioni Backup Personal](#)

	<p>Secure Drive) e fare clic su Avanti.</p> <ul style="list-style-type: none"> • Conferma le impostazioni e clicca Successivo. • Clicca Termina nella pagina di Completamento. <p> Nella modalità Server, è possibile eseguire il backup solo dei propri Personal Secure Drive (PSD). In modalità Server, Trusted Computing Management Server esegue il backup delle credenziali e delle impostazioni utente. A parte le condizioni menzionate precedentemente, questo pulsante è disabilitato se il Personal Secure Drive (PSD) non è configurato.</p>
<p>Come eseguire il ripristino</p>	<p>Componente Software da utilizzare</p>
<p>Attività dell'amministratore: preparazione del ripristino dei dati per determinati utenti.</p> <p>Compito Utente: Eseguire il ripristino manualmente per l'utente attuale. Se il ripristino dei dati è già stato preparato, completare la procedura.</p> <p> Se è disponibile un archivio di backup generato manualmente e non occorre eseguire il ripristino di emergenza dei dati, non è necessaria alcuna preparazione del ripristino da parte dell'amministratore.</p>	<p>Tool di configurazione - Backup - Ripristina tudo...</p>

Come eseguire il ripristino ("Ripristino manuale")

Compito Utente:
Eseguire il ripristino manualmente per l'utente attuale.

Se i dati di Recupero di Emergenza sono compresi in un backup manuale e l'utente corrente è amministratore, questo backup può anche essere utilizzato per il ripristino del Recupero di Emergenza dell'utente corrente.

Componente Software da utilizzare

Seguire i passi indicati:

- Lancia il Infineon Security Platform Settings Tool e seleziona **Backup**. [Security Module - Backup - Ripristino...](#)
- Clicca su **Ripristina...** per lanciare la Procedura Guidata di Backup.
- Se si desidera ripristinare impostazioni e credenziali, selezionare la casella di controllo **Ripristino impostazioni e credenziali**. Fare clic su **Sfoggia...** e individuare il File Compresso di Backup (nome file predefinito: SPBackupArchive.xml).
- Fare clic su **Avanti**.
- Eseguire l'autenticazione e fare clic su **Successivo**.
- Conferma le impostazioni e clicca **Successivo**.
- Se si desidera ripristinare una o più Personal Secure Drive, configurare le impostazioni di ripristino della Personal Secure Drive (vedere [Configurazione Impostazioni Ripristino Personal Secure Drive](#)).
- Fare clic su **Avanti**.
- Conferma le impostazioni e clicca **Successivo**.
- È inoltre possibile selezionare la casella di controllo **Avvio Inizializzazione Utenti Guidata di Security Platform** se si desidera configurare altre funzionalità di Security Platform.
- Clicca **Termina** nella pagina di Completamento.
- Ora i tuoi certificati sono ripristinati. Puoi vedere i tuoi certificati su **Impostazioni Utente - Certificati Security Platform**.
- Clicca con il tasto destro del mouse sull'icona

TNA e carica il tuo PSD. Esegui l'autenticazione.



In [modalità Server](#), è possibile solo ripristinare la propria unità Personal Secure Drive (PSD). In modalità Server, Trusted Computing Management Server esegue il ripristino delle credenziali e delle impostazioni.

Criteri relativi al backup

- La configurazione del backup automatico può essere applicata mediante il criterio [*Applica configurazione di backup includendo il ripristino di emergenza*](#).
- Il percorso di destinazione dei file ottenuti mediante il backup automatico può essere determinato impostando il criterio [*Posizione archivio di backup*](#).
- È possibile attivare l'esecuzione immediata del backup di sistema, in caso di modifiche significative dei dati di Security Platform, utilizzando il criterio [*Attiva backup di sistema immediato*](#).



Infineon Security Platform Solution

Gestione della funzionalità di ripristino di emergenza

Il software Infineon Security Platform Solution è stato progettato per offrire un supporto completo non solo per i normali flussi di lavoro ma anche per le operazioni di ripristino del sistema, nel caso in cui si verificano errori gravi.

Uno dei problemi peggiori che può verificarsi è il malfunzionamento di Trusted Platform Module. Questa situazione provoca la perdita del Proprietario Infineon Security Platform che rappresenta la radice fisica per i segreti e la radice logica per tutte le chiavi Infineon Security Platform specifiche per l'Utente. Quando è necessario sostituire Trusted Platform Module, viene creato un nuovo Proprietario Infineon Security Platform poiché non c'è modo di trasferire una chiave esistente da un Trusted Platform Module ad un altro.

Per ovviare a questo potenziale inconveniente, un meccanismo di ripristino di emergenza è stato integrato nel software Infineon Security Platform Solution. Questo meccanismo consente la ri-crittografia delle Chiavi Utente di Base da un Proprietario Infineon Security Platform a un altro. A tale scopo, occorre configurare l'apposita funzione di backup (comprendente il ripristino di emergenza) durante l'installazione di Infineon Security Platform. Questa operazione viene eseguita dall'amministratore utilizzando l'[Inizializzazione Guidata Rapida di Security Platform](#) o l'[Inizializzazione guidata di Infineon Security Platform](#).

Il ripristino dei dati in caso di emergenza può essere eseguito mediante il [Backup guidato di Security Platform](#).



In [modalità server](#) il Backup e il Ripristino sono gestiti dal Trusted Computing Management Server, ad eccezione del Backup e del Ripristino delle file di immagini del Personal Secure Drive (PSD).

Token di ripristino di emergenza, password e archivi

I concetti alla base del ripristino di emergenza sono simili a quelli della [reimpostazione della password](#), per quel che riguarda l'utilizzo di token, password e archivi.

Il ripristino delle chiavi utente in caso di emergenza richiede alcune informazioni memorizzate in un archivio. I dati di questo archivio possono essere utilizzati soltanto in combinazione con il token di ripristino, protetto da una password dedicata.

L'archivio contiene le copie crittografate delle chiavi utente di base, allo scopo di consentirne il ripristino in caso di errore di Trusted Platform Module. Se la procedura di ripristino di emergenza non è stata configurata, gli utenti potrebbero non essere in grado di recuperare i dati crittografati in caso di malfunzionamento di Security Platform. Il ripristino di emergenza viene configurato una volta sola e i componenti del software Security Platform accedono automaticamente all'archivio corrispondente. Questo archivio deve essere accessibile a tutti gli utenti di Security Platform.

Per ulteriori informazioni sugli aspetti generali della gestione del ripristino di emergenza, consultare le [Domande frequenti](#).

[Come recuperare i dati del ripristino di emergenza passo dopo passo](#)



Inizializzazione forzata dell'utente quando non è disponibile un archivio di backup

Se la chiave utente di base non può essere caricata (ad esempio, perché la proprietà di Trusted Platform Module è stata cancellata e poi acquisita nuovamente), l'Inizializzazione utenti guidata di Security Platform non consente di procedere con la configurazione dell'utente.

La soluzione corretta per questi casi è il recupero dei dati del ripristino di emergenza.

Se per qualsiasi motivo non fosse disponibile un archivio di backup (ad esempio, il file è andato perduto o è danneggiato), non sarà più possibile recuperare la chiave utente di base. In questo caso, occorre procedere alla creazione di una nuova chiave avviando l'Inizializzazione utenti guidata di Security Platform mediante l'apposito [parametro della linea di comando](#): `SpUserWz.exe /forceinit`.

Nota:

- quando si crea una nuova chiave utente di base, si perdono tutti i dati precedentemente protetti.
- Il parametro della linea di comando: *SpUserWz.exe /forceinit* non è supportato in [modalità server](#).



Soluzione Infineon Security Platform

Come recuperare i dati del ripristino di emergenza passo dopo passo

I dati del ripristino di emergenza consentono di ristabilire le funzionalità di Infineon Security Platform in caso di malfunzionamento e successiva sostituzione di Trusted Platform Module. La procedura di ripristino è suddivisa in due parti.

Operazioni eseguite da un amministratore di Security Platform

- Ricreazione delle funzionalità di base di Infineon Security Platform (comprendente l'attivazione di Trusted Platform Module, l'inizializzazione di Security Platform e il recupero dei dati del ripristino di emergenza).



In [modalità server](#), il Trusted Platform Module deve essere attivato prima che l'amministratore effettui la connessione del sistema al Trust Domain. Non sono disponibili altre attività amministrative poiché questo genere di attività è gestito da Trusted Computing Management Server.

Operazioni eseguite da tutti gli utenti di Security Platform

- Ripristino delle chiavi utente di base per poter accedere nuovamente ai dati protetti oppure generazione di nuove chiavi con la conseguente perdita di tutti i dati protetti esistenti.



Condizioni preliminari

- **Archivio di backup comprendente i dati del ripristino di emergenza:** questo archivio viene creato in fase di configurazione della funzione di backup di Security Platform. Si raccomanda di configurare il backup e il ripristino di emergenza per poter conservare i dati degli utenti qualora si verificassero gravi errori di sistema. L'archivio di backup deve essere accessibile durante le procedure di ripristino. Questo file deve essere salvato in una posizione protetta, come una cartella di rete, e incluso nelle operazioni di backup eseguite normalmente. Se il archivio si trova su un disco rigido locale, si raccomanda di includerlo nel backup periodico del disco. Nella sezione [Domande frequenti](#) sono disponibili ulteriori suggerimenti per la corretta configurazione dei dati del ripristino di emergenza.

- **Token di ripristino di emergenza:** questo file protegge i dati del ripristino di emergenza da qualsiasi uso non autorizzato e richiede una password indipendente. Il token viene creato in fase di configurazione della funzione di backup di Security Platform. Dovrebbe essere conservato separatamente dal File Compresso di Backup su un supporto rimovibile in un luogo sicuro. Il token di ripristino di emergenza deve essere accessibile durante le procedure di ripristino.
- In [modalità server](#), il Backup e il Ripristino sono gestiti dal Trusted Computing Management Server, ad eccezione del Backup e del Ripristino delle file di immagini del Personal Secure Drive (PSD).

Operazioni dell'amministratore

Punto 1 - Preparazione di Trusted Platform Module	Come procedere
<p>Uno dei motivi per cui si rende necessario eseguire il ripristino dei dati è il malfunzionamento di Trusted Platform Module. In questo caso, occorre abilitare un nuovo chip nel BIOS di sistema.</p> <p>Se il malfunzionamento è dovuto ad altri sistemi hardware (ad esempio, un errore del disco rigido), è necessario configurare adeguatamente il sistema (ripristino del sistema operativo, dei profili utente e dei dati protetti) prima di ripristinare Infineon Security Platform.</p>	<p>Questa operazione viene eseguita da uno degli amministratori del sistema. Per informazioni dettagliate su come abilitare il chip, vedere</p>
Punto 2 - Inizializzazione di Security Platform e recupero dei dati del ripristino di emergenza	Come procedere
<p>Dopo aver abilitato Trusted Platform Module, è necessario inizializzare Security Platform e recuperare i dati del ripristino di emergenza. Il archivio di backup e il token di ripristino di emergenza devono essere entrambi accessibili per poter eseguire queste operazioni.</p>	<p>Il recupero dei dati del ripristino di emergenza può essere effettuato unicamente da un amministratore di Infineon Security Platform. Avviare l'Inizializzazione guidata di Infineon Security Platform e selezionare Ripristina Security Platform da un archivio di backup.</p>

Operazioni dell'utente

Ripristino dell'utente di Infineon Security Platform

Una volta completate le operazioni amministrative, è possibile eseguire il ripristino degli utenti di Infineon Security Platform. Il ripristino deve essere effettuato separatamente per ogni singolo utente.

Come procedere

Avviare l'[Inizializzazione utenti guidata di Security Platform](#). La procedura guidata rileva automaticamente lo stato del ripristino in corso. Inoltre, offre la possibilità di creare una nuova chiave utente di base o di ripristinare una chiave esistente da un archivio di backup. In genere, è preferibile ripristinare una chiave esistente, altrimenti i dati crittografati in precedenza non saranno più accessibili. Seguire le istruzioni visualizzate per completare correttamente la procedura.



Infineon Security Platform Solution

Aggiornare le Credenziali e le Impostazioni Utente (Modalita' Server)

Quando e' necessario un aggiornamento delle tue credenziali e impostazioni utente, sei informato con un messaggio. Questo viene visualizzato nella Barra dell'Area di Notifica mentre sei collegato a Windows. Puoi cliccare sul messaggio per eseguire l'aggiornamento. Se perdi o non presti attenzione al messaggio, puoi iniziare l'aggiornamento piu' attraverso la [Barra del Menu di Notificazione](#).

Un aggiornamento delle tue credenziali e delle tue impostazioni e' necessario nelle seguenti circostanze:

- Non hai ancora le credenziali e le impostazioni utente sulla piattaforma attuale (poiche' ti sei appena iscritto), ma il Trusted Computing Management Server ha gia' le credenziali e le impostazioni per il tuo utente (visto che potresti aver gia' usato un'altra piattaforma).
- Hai gia' le credenziali e le impostazioni utente sulla piattaforma corrente, ma le tue credenziali e impostazioni sono state cambiate da un'altra piattaforma.
- In passato avevi le credenziali e le impostazioni utente sulla piattaforma corrente, ma sono andate perse (ad esempio a causa di un hard disk rotto).
- Le vostre attuali credenziali utente e impostazioni non sono coerenti (ad esempio a causa di un errore in una modifica apportata precedentemente). In questo caso è necessario ricavare dal server le vostre ultime credenziali e impostazioni valide note.

In questo modo le tue credenziali e le tue impostazioni sono sincronizzate su piattaforme multiple e sono ripristinate su piattaforme rotte.



- Per cortesia assicurati di non aver caricato un Personal Secure Drive, prima di aggiornare la tue credenziali e le tue impostazioni.
- Nota che l'aggiornamento delle tue credenziali e impostazioni richiede l'[Autenticazione Utente](#).



©Infineon

Soluzione Infineon Security Platform

Recupero Dati EFS e PSD mediante Agente Recupero Dati

Un agente di recupero dati consente di accedere ai dati di EFS o PSD nei seguenti casi:

- Perdita delle credenziali di crittografia dei dati.
- Nessun backup delle credenziali è disponibile.
- Sono disponibili dati crittografati (file EFS, file di immagine PSD o di backup).
- È disponibile un agente recupero dati.

Informazioni dettagliate sul recupero EFS sono disponibili nella Microsoft TechNet.

Informazioni dettagliate sul Recupero PSD sono disponibili qui: [Recupero Personal Secure Drive](#).



©Infineon Technologies AG

Soluzione Infineon Security Platform

Migrazione delle chiavi verso altri computer

Una volta configurato un utente di sistema come utente di Infineon Security Platform, può presentarsi la necessità di definire un ambiente protetto specifico per quell'utente, non solo sul computer su cui è stata eseguita la configurazione, ma anche su altri computer a cui l'utente ha accesso. In questo senso, configurazioni diverse sui vari computer potrebbero causare problemi di compatibilità degli elementi di protezione; ad esempio, un messaggio di posta elettronica firmato su un determinato computer potrebbe non essere accettato dagli altri a causa delle diverse chiavi utilizzate per la firma.

Fondamenti della migrazione

Infineon Security Platform dà la possibilità di gestire questa situazione offrendo un percorso di migrazione per i valori segreti degli utenti. Il concetto alla base di questa tecnologia è la rigida separazione tra il ruolo amministrativo e quello operativo della migrazione. Questa separazione è necessaria per garantire l'identità dei valori segreti migrati, assicurando al tempo stesso che non possano essere trasferiti in nessun modo senza conoscere l'istanza amministrativa necessaria.

Dopo aver completato correttamente la migrazione di un utente, il computer di destinazione presenterà esattamente lo stesso ambiente protetto disponibile sul computer di origine. Dal punto di vista dell'utente di Infineon Security Platform, non esiste alcuna differenza tra i due sistemi sotto il profilo del comportamento operativo.

Ciononostante, i due computer continuano a funzionare come installazioni indipendenti di Infineon Security Platform. La migrazione delle chiavi utente non ha nessun impatto sulla struttura di protezione primaria di Infineon Security Platform. Inoltre, cosa ancor più importante, i valori segreti memorizzati in Trusted Platform Module non vengono in alcun modo influenzati dall'operazione.



In [modalità server](#), la migrazione delle credenziali e delle impostazioni dell'utente sono gestiti da Trusted Computing Management Server. In fase di accesso, l'utente ottiene gli aggiornamenti necessari delle credenziali e delle impostazioni dell'utente che sono cambiati. Ciò inoltre è denominata *roaming*. Aggiornamenti dal database server sovrascrive le credenziali e le impostazioni dell'utente locale.

In modalità [autonoma](#), le credenziali e le impostazioni specifiche dell'utente sul computer di origine e di destinazione vengono unite.

La migrazione viene eseguita utilizzando la [Migrazione guidata di Infineon Security Platform](#).



Migrazione verso un computer privo di chiavi e certificati utente:

La procedura di migrazione provvede ad installare nuove chiavi e certificati utente sul computer di destinazione.

È necessario configurare le apposite funzioni di Security Platform per poter utilizzare le nuove chiavi e i nuovi certificati.



Migrazione verso un computer sul quale sono già presenti chiavi e certificati utente (più chiavi utente di base):

Le chiavi e i certificati Security Platform, installati precedentemente sul computer di destinazione, vengono invalidati. In conseguenza di questa operazione, i dati crittografati potrebbero andare perduti. Decrittografare i dati prima di procedere alla migrazione o contattare l'amministratore del sistema per maggiori informazioni sulla procedura di ripristino.



Migrazione verso un computer sul quale sono già presenti chiavi e certificati utente (la stessa chiave utente di base):

Se il computer di destinazione utilizza la stessa chiave utente di base del computer di origine, la procedura di migrazione provvederà ad unire le chiavi e i certificati dei due sistemi. Al termine della migrazione, vengono attivate le chiavi e i certificati presenti nell'archivio di migrazione. Le chiavi e i certificati preesistenti vengono comunque mantenuti. In questo modo, si evita la perdita dei dati crittografati.

Ad esempio, se esistono dati crittografati con EFS o PSD sia sul computer di origine, sia su quello di destinazione, ma i due computer utilizzano certificati diversi, il certificato presente sul computer di origine verrà attivato su quello di destinazione. Il certificato utilizzato precedentemente sul computer di destinazione viene comunque mantenuto e può essere riattivato in qualsiasi momento.



La migrazione e Personal Secure Drive:

- Se un utente aveva configurato una Personal Secure Drive sul computer di destinazione su un supporto rimovibile (es. unità flash USB), questo supporto può inoltre essere utilizzato sul computer di destinazione.
- Se un utente aveva configurato una Personal Secure Drive sul computer di origine su un disco fisso, è importante eseguire il backup di tutti i file di immagine della Personal Secure Drive di cui eseguire la migrazione e salvare i file di immagine del backup del computer di origine in una posizione che possa essere accessibile da entrambi i computer. Per utilizzare una copia della Personal Secure Drive di origine sul computer di destinazione, il file di immagine del backup interessato del computer di origine deve essere ripristinato. Dopo la migrazione si avranno due Personal Secure Drive indipendenti sui computer di origine e di destinazione. Gli utenti potrebbero dover riconfigurare le Personal Secure Drive sul

computer di destinazione (vedere [Gestione Personal Secure Drive](#)). Per riconfigurare una Personal Secure Drive, selezionare *Desidero modificare le impostazioni della mia Personal Secure Drive* e seguire le istruzioni sul monitor.

- Si noti che le impostazioni e le credenziali della PSD esistenti sul computer di destinazione saranno sovrascritte, se le Chiavi Utente Base sui computer di origine e di destinazione sono differenti. In questo caso, si consiglia di salvare una copia non crittografata dei dati della PSD prima della migrazione. È possibile fare ciò cancellando la PSD con l'opzione di salvarne una copia non crittografata (vedere [Gestione Personal Secure Drive](#)).



Soluzione Infineon Security Platform

La migrazione passo dopo passo

La procedura di migrazione delle credenziali è suddivisa in due parti, una amministrativa e una riservata all'utente. La prima parte implica l'autorizzazione, la configurazione e la gestione della migrazione da parte dell'amministratore. Una volta completata questa fase, l'utente dovrà semplicemente esportare e importare le chiavi e i certificati dal sistema di origine a quello di destinazione.



In [modalità server](#), la migrazione di chiavi e certificati specifici per l'utente è gestita dal Trusted Computing Management Server, ovvero non devi eseguire i passi di migrazione (eccetto Utente Fase 3 e 4).

Operazioni dell'amministratore

Punto 1 - Esportazione dell'identità del computer di destinazione

Per eseguire la migrazione, occorre prima di tutto identificare un computer di destinazione, ovvero il sistema sul quale si vogliono trasferire le chiavi e i certificati utente. Per abilitare la migrazione, un amministratore del sistema di destinazione dovrà fornire (o meglio esportare) una chiave pubblica che identifichi il computer. Questa chiave verrà successivamente utilizzata per associare le chiavi e i certificati utente al computer di destinazione (nota: se il contenuto è protetto dalla chiave pubblica del sistema di destinazione, solo la chiave privata del computer protetto da Trusted Platform Module può accedere alle chiavi e ai certificati migrati). Questa operazione serve a creare un'origine attendibile per la migrazione (la cosiddetta "root of trust"), garantendo che soltanto i sistemi di destinazione prescelti possano accedere alle credenziali dell'utente.

Come procedere

L'amministratore Infineon Security Platform sul sistema di destinazione deve esportare il certificato del computer (chiave pubblica) in un file. Segui i passi indicati:

- Seleziona **Migrazione** nel Infineon Security Platform Settings Tool.
- Seleziona **Questa è la piattaforma di destinazione** e clicca **Salva....**
- Naviga fino alla posizione di memorizzazione del file di tua scelta a cui si può accedere da entrambi i computer. Il file viene salvato con il nome file di default **SpPubKeyArchive.xml**.

Mezzi di memorizzazione accettabili: Mezzi rimovibili o drive di rete mappati.

Prendere nota della posizione e del nome del file della chiave esportata pochè ti sarà richiesta per il passo

	successivo.
Punto 2 - Autorizzazione del proprietario del computer di origine	Come procedere
<p>La fase successiva della procedura di migrazione richiede che il proprietario del computer di origine autorizzi la migrazione delle chiavi e dei certificati utente verso un altro sistema. A tale scopo, il proprietario dovrà accedere alla chiave pubblica del computer di destinazione. Si tratta della stessa chiave precedentemente esportata da un amministratore di quel computer (vedere il punto 1). L'autorizzazione del computer di destinazione da parte del proprietario di Infineon Security Platform consente allo stack di protezione del software di garantire che le chiavi e i certificati utente possano essere associati unicamente al sistema di destinazione specificato.</p>	<p>Il proprietario di Infineon Security Platform sul computer fonte (computer su cui eseguire la migrazione) deve autorizzare l'esportazione delle chiavi e dei certificati utente per il computer designato per la destinazione. Segui i passi indicati:</p> <ul style="list-style-type: none">• Seleziona Migrazione nel Infineon Security Platform Settings Tool.• Seleziona Questa è la piattaforma fonte e clicca Autorizza....• Sulla schermata di Autorizza la Migrazione, clicca su Importa....• Naviga fino alla posizione del file chiave pubblico SpPubKeyArchive.xml e clicca su Apri.• Digitare la Password Proprietario del computer di origine o fornire un File di Backup della Password Proprietario e fare clic su OK.• Verifica che l'host name

	<p>del computer di destinazione insieme all'ID unico della Piattaforma sia elencato e poi clicca Chiudi.</p>
<p>Punto 1 e 2 combinazione - Esportazione e autorizzazione automatica</p>	<p>Come procedere</p>
<p>Esiste un modo alternativo per eseguire le due operazioni sopra descritte, ovvero l'esportazione e l'autorizzazione in modalità automatica. In questo modo, è possibile ignorare completamente il punto 1 ed effettuare una sola operazione molto simile a quella descritta al punto 2. Il proprietario di Infineon Security Platform sul sistema di origine dovrà autorizzare la migrazione delle chiavi e dei certificati utente verso il computer di destinazione previsto. La differenza risiede nel fatto che, anziché identificare manualmente il file contenente le credenziali del computer di destinazione, è possibile ricercare la piattaforma di destinazione utilizzando una comune finestra di dialogo per la ricerca delle risorse di rete. Una volta identificato il sistema, Infineon Security Platform tenta di contattare dinamicamente il computer di destinazione (utilizzando DCOM) e richiede le chiavi e i certificati della piattaforma. Se sul sistema di destinazione è installato il software Infineon Security Platform, la migrazione dei dati tra i due computer viene eseguita automaticamente.</p> <p>Condizioni preliminari</p> <ul style="list-style-type: none"> • Computer di origine: l'utente attuale (il proprietario di Infineon Security Platform) deve essere un membro del gruppo di 	<p>Il proprietario di Infineon Security Platform sul computer fonte (computer su cui eseguire la migrazione) deve autorizzare l'esportazione delle chiavi e dei certificati utente per il computer designato per la destinazione. Segui i passi indicati:</p> <ul style="list-style-type: none"> • Seleziona Migrazione nel Infineon Security Platform Settings Tool. • Seleziona Questa è la piattaforma fonte e clicca Autorizza.... • Sulla schermata di Autorizza la Migrazione, clicca su Cerca.... Questo aprirà una finestra di dialogo di ricerca di rete. • Naviga e trova il computer di destinazione e seleziona OK. • Questo inizierà il trasferimento automatico delle informazioni di migrazione dal computer

amministratori del computer di destinazione.

- Computer di destinazione: Infineon Security Platform deve essere installato e abilitato.
- Computer di destinazione: il criterio di sistema *Consenti agli amministratori di recuperare la chiave pubblica SRK in modalità remota* deve essere abilitato.
- Computer di destinazione: non devono esserci firewall che blocchino le richieste DCOM in entrata (ad esempio, i firewall integrati in Microsoft Windows XP o altri firewall).
- La rete deve essere configurata per consentire le richieste DCOM.
- Sia il sistema di origine, che quello di destinazione devono appartenere a domini trusting.

Nel caso in cui l'autorizzazione automatica non sia possibile, procedere manualmente come sopra indicato (Punto 1 e 2).

fonte al computer di destinazione.

Operazioni dell'utente



Se un utente aveva configurato delle Personal Secure Drive sul computer di origine, è importante eseguire il backup di tutti i file di immagine della Personal Secure Drive di cui eseguire la migrazione e salvare i file di immagine di backup (nome file predefinito: **SpPSDBackup.fsb**) del computer di origine in una posizione che permetta l'accesso da entrambi i computer. Per utilizzare una copia del file di immagine della PSD di origine sul computer di destinazione, devono essere resi disponibili i file di immagine di backup del computer di origine.

Punto 1 - Esportazione delle chiavi e dei certificati utente dal computer di origine

Una volta completate le operazioni amministrative, i singoli utenti di Infineon Security Platform potranno esportare in sicurezza le proprie chiavi e i propri certificati (protetti dalla chiave pubblica del sistema di destinazione e quindi leggibili unicamente da quella piattaforma).

Come procedere

Utenti di Infineon Security Platform sul computer fonte per esportare le loro chiavi e i loro certificati per migrazione. Seguire i passi indicati:

- Seleziona **Migrazione** nel Infineon Security Platform Settings Tool.
- Seleziona **Questa è la piattaforma fonte** e clicca su **Esporta....**
- Scegli il computer di destinazione dalla lista e clicca **Successivo**.
- Naviga fino alla posizione del file di archivio di tua scelta a cui si può accedere da entrambi i computer. Il file viene salvato con un nome di default come **SpMigrationArchive.xml**. Clicca su **Successivo**.
- Inserisci la Password

	<p>Utente di Base per il computer fonte e clicca Successivo.</p> <ul style="list-style-type: none">• Conferma le impostazioni e clicca Successivo.• Sulla schermata di Completamento verifica che l'esportazione di chiavi e certificati utente sia stata eseguita con successo e clicca Fine. <p>Prendere nota della posizione e del nome del file di archivio e del file di backup PSD poichè ti saranno richiesti nel passo successivo.</p>
Punto 2 - Importazione delle chiavi e dei certificati utente sul computer di destinazione	Come procedere
<p>A questo punto, gli utenti che dispongono di un proprio account nel sistema di destinazione dovranno importare le chiavi e i certificati.</p>	<p>Sul computer di destinazione, utente di Infineon Security Platform può importare le proprie chiavi e i propri certificati. Seguire i passi indicati:</p> <ul style="list-style-type: none">• Seleziona Migrazione nel Infineon Security Platform Settings Tool.• Seleziona Questa è la piattaforma di destinazione e clicca su Importa...• Naviga fino alla posizione del file di archivio SpMigrationArchive.xml e clicca Successivo.

- Inserisci la Password Utente di Base che era stata impostata sul computer fonte e clicca **Successivo**.
- Conferma le impostazioni e clicca **Successivo**.
- Se le caratteristiche della Security Platform erano state precedentemente configurate sulla piattaforma di destino, un messaggio di avviso apparirà. Leggere attentamente il messaggio di avviso e cliccare su **Sì**.
- Sulla schermata di Completamento, verifica che la migrazione delle chiavi e dei certificati utente sia stata eseguita con successo e clicca **Fine**.
- Sulla schermata finale della procedura guidata, avrai l'opportunità di andare automaticamente al passo successivo selezionando l'opzione **Inizia Inizializzazione Utenti Guidata Security Platform**.

 Prendere nota dei suggerimenti su [Migrazione e Personal Secure Drive](#).

Punto 3 - Configurazione delle applicazioni per utilizzare chiavi e certificati migrati

Come procedere:

Dopo aver completato la migrazione di chiavi e certificati, è importante associare queste nuove credenziali a ogni applicazione che si intende utilizzare sul computer di destinazione.

Siccome le credenziali possono essere utilizzate su applicazioni multiple, il vero metodo per importare chiavi e certificati migrati sarà unico per ogni provider di applicazione software individuale. Ad esempio, gli utenti possono configurare il sistema di Crittografia File per utilizzare i certificati migrati. Seguire i passi indicati:

- Vai a **Impostazioni Utente** Infineon Security Platform Settings Tool.
- Clicca **Configura....**
- Segui le istruzioni sullo schermo e clicca **Modifica...** nella pagina Caratteristiche Security Platform - Certificato Crittografia.
- Seleziona il certificato migrato, clicca su **OK** e procedi alla pagina di procedura guidata successiva.

Punto 4 – Riconfigurazione delle funzionalità utente - Personal Secure Drive

Come procedere:

Una volta completata la migrazione delle chiavi e dei certificati, l'utente deve riconfigurare le impostazioni della Personal Secure Drive sul computer di destinazione.

Se sono state configurate una o più Personal Secure Drive sul computer di origine, sarà necessario riconfigurare le Personal Secure Drive di cui si

è effettuata la migrazione sul computer di destinazione (vedi [Gestione Personal Secure Drive](#)). Per riconfigurare il Personal Secure Drive, selezionare l'opzione *Desidero modificare le impostazioni del mio Personal Secure Drive* e seguire le istruzioni riportate sullo schermo. Per utilizzare una copia della Personal Secure Drive di origine sul computer di destinazione, il file di immagine del backup interessato (nome file predefinito: **SpPSDBackup.fsb**) del computer di origine deve essere ripristinato. Dopo il ripristino si avranno due Personal Secure Drive indipendenti sui computer di origine e di destinazione.



Soluzione Infineon Security Platform

Reimpostazione della password utente di base

Soluzione Infineon Security Platform consente di reimpostare le password utente di base.

Questa funzione può essere utilizzata nel caso in cui un utente di Security Platform abbia dimenticato la password o quando si verificano dei problemi nel dispositivo di autenticazione. In questi casi, infatti, l'accesso dell'utente alle funzionalità di Security Platform viene bloccato e i dati riservati potrebbero andare perduti.



In [modalità server](#) Trusted Computing Management Server gestisce l'attività di creazione di un Token di Ripristino Password per tutti gli utenti, preparando e fornendo il Codice di Autorizzazione Ripristino Password per utenti specifici, non è pertanto necessario eseguire queste azioni. Di conseguenza tutti i pulsanti eccetto Ripristina e Attiva sono disattivati.

Token di reimpostazione della password, password e archivi

I concetti alla base della reimpostazione della password sono simili a quelli del [ripristino di emergenza](#), per quel che riguarda l'utilizzo di token, password e archivi.

La reimpostazione della password utente di base richiede alcune informazioni memorizzate in un archivio. I dati di questo archivio possono essere utilizzati soltanto in combinazione con il token di reimpostazione della password, protetto a sua volta da una password dedicata.

L'archivio contiene dati crittografati per ciascun utente, allo scopo di consentire la modifica della password utente di base senza conoscere quella attuale. Se la reimpostazione della password non è stata configurata, gli utenti potrebbero non essere in grado di reimpostare le proprie password. La reimpostazione viene configurata una volta sola e i componenti del software Security Platform accedono automaticamente all'archivio corrispondente. Questo file di archivio deve essere accessibile a tutti gli utenti di Security Platform.

Come abilitare la funzione di reimpostazione della password

La funzione di reimpostazione delle password utente di base può essere utilizzata esclusivamente se l'amministratore di Security Platform ha configurato tale funzione per tutti gli utenti.

Ciascun utente di Security Platform può reimpostare soltanto la propria password, purché abilitato all'operazione nel proprio account utente. L'abilitazione richiede l'immissione della password attuale oppure l'autenticazione avanzata. Quindi, se la password attuale è stata smarrita, non è possibile né abilitare, né eseguire la reimpostazione.

Come reimpostare la password di un utente

Per motivi di sicurezza, la reimpostazione della password implica l'esecuzione di due attività distinte: un'attività amministrativa e un'attività a carico dell'utente. Se il proprio account dispone sia dei privilegi di amministratore, sia dei diritti utente di Security Platform, è possibile reimpostare la password con un'unica operazione.

La reimpostazione della password passo dopo passo

Come abilitare la reimpostazione della password	Componenti software richiesti
<p>1. Attività dell'amministratore: configurazione dei dati necessari alla reimpostazione della password per tutti gli utenti.</p> <p> Questa operazione può essere imposta mediante il criterio Applica configurazione per la reimpostazione della password.</p>	<p>Se il software Security Platform non è stato inizializzato:</p> <p>Configurazione mediante Inizializzazione Guidata Rapida</p> <p>Qui il Ripristino Password è automaticamente configurato con le impostazioni predefinite.</p> <p>Configurazione mediante Inizializzazione Guidata di Security Platform</p> <p>Per configurare la Reimpostazione della Password segui i passi indicati:</p> <ul style="list-style-type: none">• Nella pagina di Benvenuto dell'Inizializzazione Guidata Rapida, selezionare Inizializzazione Avanzata• Durante l'Inizializzazione Guidata, spunta la casella di spunta Reimpostazione della Password e clicca Successivo.• Seleziona l'opzione Crea un nuovo token.• Ricerca una posizione di tua scelta per salvare il file del Token di Reimpostazione della Password (nome di default del file: SPPwdResetToken.xml). Mezzi di memorizzazione accettabili: Mezzi rimovibili o drive di rete mappati.• Imposta una nuova password del

token e clicca **Successivo**.

- Conferma le impostazioni e clicca **Successivo**.
- Nella pagina di Completamento, clicca **Termina**.

Se il software Security Platform è già stato inizializzato: [Tool di configurazione - Reimposta password - Configura...](#)

Per configurare la Reimpostazione della Password segui i passi indicati:

- Lancia il Infineon Security Platform Settings Tool e seleziona **Reimpostazione della Password**.
- Clicca **Configura...**
- Seleziona l'opzione **Crea un nuovo token**.
- Ricerca una posizione di tua scelta per salvare il file del Token di Reimpostazione della Password (nome di default del file: **SPPwdResetToken.xml**).
Mezzi di memorizzazione accettabili: Mezzi rimovibili o drive di rete mappati.
- Imposta una nuova password del token e clicca **Successivo**.
- Conferma le impostazioni e clicca **Successivo**.
- Nella pagina di Completamento, clicca **Termina**.

2. Attività dell'utente: abilitazione della funzionalità di reimpostazione per l'utente attuale.

Se l'utente non è stato configurato: [Inizializzazione utenti guidata](#)

Per abilitare la Reimpostazione della Password e creare un Personal Secret



Questa operazione può essere imposta mediante il criterio [Applica configurazione per la reimpostazione della password](#).

per l'utente, segui i passi indicati:

- Lancia il Infineon Security Platform Settings Tool. Nella pagina di Benvenuto dell'Inizializzazione Guidata Rapida, selezionare **Inizializzazione Avanzata**
- Durante l'Inizializzazione Utenti Guidata, spunta la casella di spunta **Abilita la reimpostazione della mia Password Utente di Base in caso di emergenza**.
- Ricerca una posizione sull'hard drive per salvare il file del Personal Secret (nome di default del file: **SPPwdResetSecret.xml**).
- Conferma le impostazioni e clicca **Successivo**.
- Le Security Platform Features possono essere configurate successivamente. Togli la spunta da tutte le opzioni e clicca **Successivo**.
- Nella pagina di Completamento, clicca **Termina**.

Se l'utente è già stato configurato: [Tool di configurazione - Reimposta password - Abilita...](#)

Per creare un nuovo Personal Secret per l'utente attuale, segui i passi indicati:

- Lancia il Infineon Security Platform Settings Tool e seleziona **Reimpostazione della Password**.

- Clicca **Abilita...** Appare un messaggio di informazione. Leggi il messaggio attentamente e clicca **OK**.
- Ricerca una posizione sull'hard drive per salvare il file del Personal Secret (nome di default del file: **SPPwdResetSecret.xml**). Clicca **Successivo**.
- Ricerca una posizione sull'hard drive per salvare il file del Personal Secret (nome di default del file: **SPPwdResetSecret.xml**).
- Quando ti viene chiesto **Vuoi sostituirlo**, clicca **Sì**.
- Esegui l'autenticazione e clicca **Successivo**.
- Conferma le impostazioni e clicca **Successivo**.
- Nella pagina di Completamento, clicca **Termina**.

Come reimpostare la password di un utente

3. Attività dell'amministratore: preparazione della reimpostazione della password per un determinato utente oppure definizione e reimpostazione della password, in un'unica operazione, per l'account dell'amministratore attuale.

Componenti software richiesti

[Tool di configurazione - Reimposta password - Prepara...](#) (avvia la Reimpostazione guidata password)

Per creare il Codice di Autorizzazione per la Reimpostazione della Password per un utente specifico, segui i passi indicati:

- Lancia il Infineon Security Platform Settings Tool e seleziona **Reimpostazione della**

Password.

- Clicca **Prepara...**
- Scegli un utente specifico dalla lista per il quale la password deve essere reimpostata e clicca **Successivo.**
- Naviga fino alla posizione del file del Token di Reimpostazione della Password (nome di default del file: **SPPwdResetToken.xml**), ed inserisci la password che protegge quel file. Clicca **Successivo.**
- Ricerca una posizione (ad esempio, un drive della rete mappata o un folder condiviso sull'hard drive) per salvare il Codice di Autorizzazione di Reimpostazione della Password (nome di default del file: **SPPwdResetCode.xml**), in modo che l'utente possa accedervi. Clicca **Successivo.**
- Nella pagina di Completamento, clicca **Termina.**

Per preparare e reimpostare la Password Utente di Base per l'amministratore attuale, segui i passi indicati:

- Lancia il Infineon Security Platform Settings Tool e seleziona **Reimpostazione della Password.**
- Clicca **Prepara...**
- Seleziona l'amministratore la cui password deve essere reimpostata, e clicca **Successivo.**

- Naviga fino alla posizione del file del Token di Reimpostazione della Password (nome di default del file: **SPPwdResetToken.xml**), ed inserisci la password che protegge quel file. Clicca **Successivo**.
- Naviga fino alla posizione del file del Personal Secret (nome di default del file: **SPPwdResetSecret.xml**) e clicca **Successivo**.
- Inserisci e conferma una nuova Password Utente di Base e clicca **Successivo**.
- Conferma le impostazioni e clicca **Successivo**.
- Nella pagina di Completamento, clicca **Termina**.

4. Attività dell'utente: reimpostazione della password per l'utente attuale (purché l'operazione sia già stata preparata per l'utente in questione).

[Tool di configurazione - Reimposta password - Reimposta...](#) (avvia la Reimpostazione guidata password)

Per reimpostare la Password Utente di Base per l'utente attuale, segui i passi indicati:

- Lancia il Infineon Security Platform Settings Tool e seleziona **Reimpostazione della Password**.
- Clicca **Reimposta...**
- Naviga fino alla posizione del file del Personal Secret (nome di default del file: **SPPwdResetSecret.xml**).
- Naviga fino alla posizione del file del Codice di Autorizzazione

di Reimpostazione della Password (nome di default del file: **SPPwdResetCode.xml**) e clicca **Successivo**.

- Inserisci e conferma una nuova Password Utente di Base e clicca **Successivo**.
- Conferma le impostazioni e clicca **Successivo**.
- Nella pagina di Completamento, clicca **Termina**.



Infineon Security Platform Solution

Protezione contro gli attacchi del dizionario



Note:

- Questa sezione riguarda esclusivamente i sistemi Security Platform dotati di Trusted Platform Module 1.2. I dettagli relativi al meccanismo di protezione di Security Platform contro gli attacchi del dizionario sono validi soltanto per i sistemi Security Platform che utilizzano Infineon Trusted Platform Module 1.2.
- La descrizione seguente è rivolta principalmente al proprietario di Security Platform.

Gli **attacchi del dizionario** uno dei metodi utilizzati per violare i sistemi di sicurezza e in particolare i sistemi basati sulle password; durante un attacco del dizionario, l'aggressore prova sistematicamente tutte le possibili password, iniziando dalle parole che hanno più probabilità di essere utilizzate, come nomi propri o nomi di luoghi. Il termine "dizionario" fa riferimento all'azione dell'aggressore, che passa in rassegna tutte le parole presenti nel dizionario nel tentativo di scoprire la password. Solitamente, gli attacchi del dizionario vengono eseguiti con appositi software e non manualmente.

Un eventuale attacco del dizionario di Security Platform Solution potrebbe individuare la [Password del proprietario](#), [quella di un utente password](#) oppure le chiavi protette da password. Gli attacchi del dizionario miranti a scoprire una password vengono chiamati anche **attacchi alle password**. Nella versione 1.2 standard di TCG, è stato introdotto un meccanismo di protezione contro questo tipo di attacchi. Security Platform Solution implementa tale meccanismo. Si noti che le misure di protezione vengono adottate non solo in presenza di attacchi reali, ma anche in caso di ripetuti inserimenti di password errate.

Come evitare gli attacchi del dizionario

Valutare attentamente i suggerimenti riportati di seguito al fine di evitare gli attacchi del dizionario:

- Attenersi alle prescrizioni generali di sicurezza raccomandate nei portali dedicati.
- Impostare una soglia di protezione relativamente bassa (vedere i criteri [di configurazione della soglia di protezione](#)).
- Utilizzare password complesse per evitare che vengano scoperte facilmente.

Cosa fare in caso di attacchi del dizionario

Valutare attentamente i suggerimenti riportati di seguito, nel caso in cui Security Platform rilevi un attacco del dizionario:

- In primo luogo, occorre disabilitare temporaneamente il sistema.
- Disconnettere il sistema dalla rete.
- Accedere al Visualizzatore eventi di Microsoft per ulteriori informazioni.
- Consultare i portali dedicati per informazioni aggiornate sui rischi più recenti per la sicurezza.
- Individuare ed eliminare l'applicazione o il servizio che hanno causato l'attacco. Se necessario, richiedere l'assistenza di uno specialista in materia di sicurezza.
- Adottare opportune misure di protezione per impedire ulteriori attacchi (ad esempio, installando patch di protezione, modificando le impostazioni del firewall e i criteri di protezione).

Una volta completate queste operazioni, è possibile riconnettere il sistema alla rete. Riavviare il sistema per abilitare nuovamente Security Platform.

[Misure di protezione contro gli attacchi del dizionario](#)

[Interfaccia utente per la protezione contro gli attacchi del dizionario](#)



©Infineon

Technologies AG

Soluzione Infineon Security Platform

Misure di protezione contro gli attacchi del dizionario



Note:

- Questa sezione riguarda esclusivamente i sistemi Security Platform dotati di Trusted Platform Module 1.2. I dettagli relativi al meccanismo di protezione di Security Platform contro gli attacchi del dizionario sono validi soltanto per i sistemi Security Platform che utilizzano Infineon Trusted Platform Module 1.2.
- La descrizione seguente è rivolta principalmente al proprietario di Security Platform.

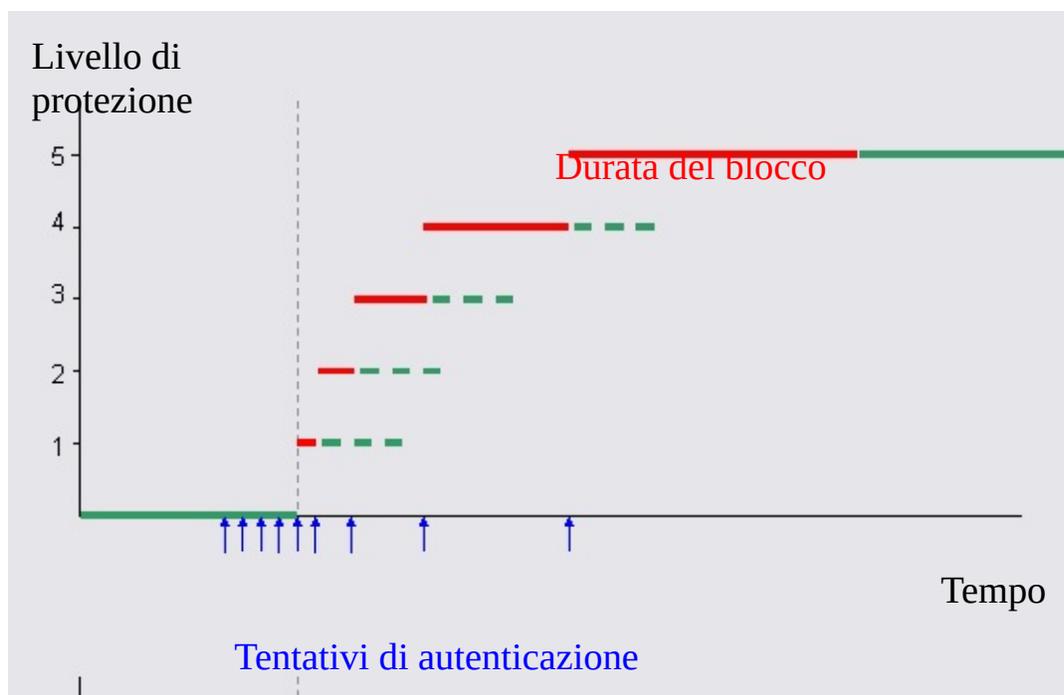
Security Platform Solution respinge eventuali attacchi del dizionario applicando le misure descritte di seguito:

- Se si verificano ripetuti tentativi di autenticazione non riusciti, Security Platform viene **temporaneamente disabilitato** fino al successivo riavvio del sistema. In questo modo, il proprietario di Security Platform potrà adottare ulteriori misure di protezione prima di abilitare nuovamente l'applicazione.
- Inoltre, l'applicazione viene **temporaneamente bloccata**: Ulteriori tentativi di autenticazione vengono così respinti per un determinato periodo di tempo. Ad ogni tentativo di autenticazione non riuscito, il **livello di protezione** viene incrementato raddoppiando la durata del blocco.
- Se non si verificano altri tentativi di autenticazione entro un determinato lasso di tempo, il livello di protezione viene nuovamente ridotto.
- Il proprietario di Security Platform può **reimpostare** il livello di protezione.

Le figure seguenti illustrano le misure di protezione.

Incremento del livello di protezione in caso di ripetuti tentativi di autenticazione non riusciti

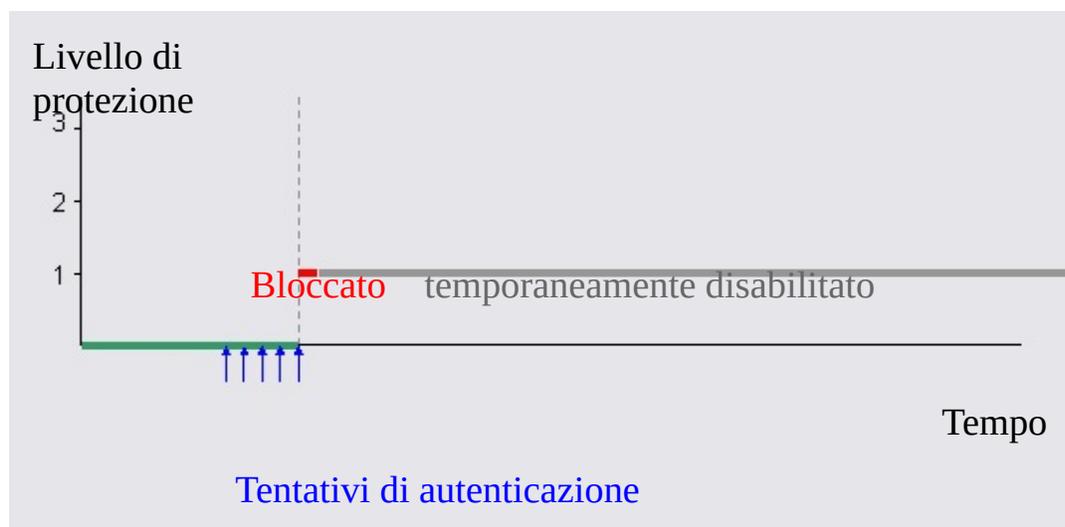
La figura mostra come i tentativi di autenticazione non riusciti causino un incremento del livello di protezione e il blocco dell'applicazione, purché Security Platform non sia stato temporaneamente disabilitato.



In questo esempio, la soglia di protezione corrisponde al quinto tentativo di autenticazione non riuscito. L'aggressore tenta più volte di completare l'autenticazione e quindi il livello di protezione viene innalzato non appena termina il blocco dell'applicazione.

Come evitare l'innalzamento dei livelli di protezione disabilitando Security Platform temporaneamente

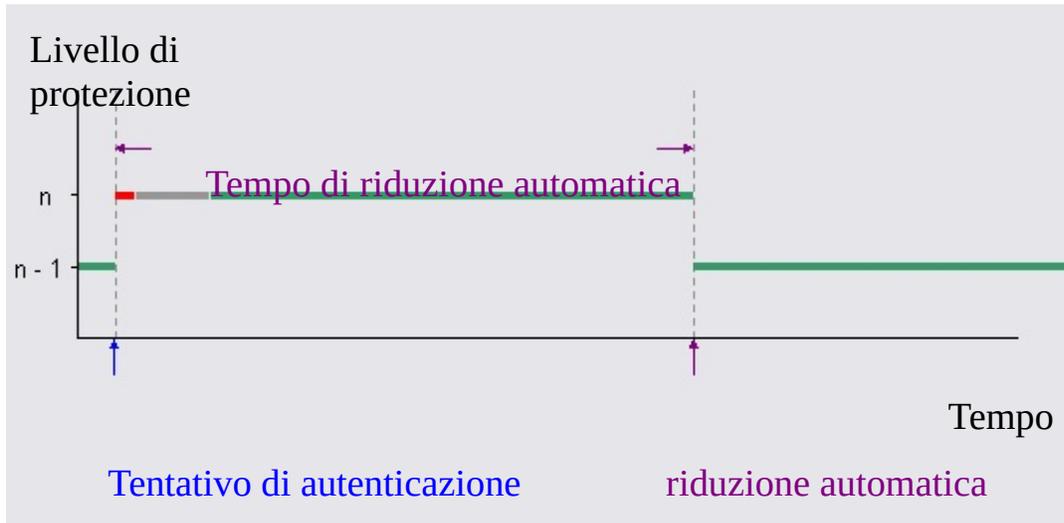
Per impedire ulteriori attacchi ed evitare il blocco prolungato dell'applicazione, Security Platform viene temporaneamente disabilitato quando si supera la soglia di protezione.



In questo esempio, Security Platform è protetto da ulteriori attacchi, anche se l'applicazione non è più bloccata. Security Platform verrà abilitato soltanto dopo aver riavviato il sistema.

Riduzione automatica del livello di protezione

La figura mostra come il livello di protezione venga ridotto automaticamente, dopo un certo lasso tempo, nel caso in cui non si verificano altri tentativi di autenticazione non riusciti.



In questo esempio, si nota un incremento del livello di protezione e il blocco dell'applicazione (**rosso**) causati da un tentativo di autenticazione non riuscito. Si presume che il sistema venga riavviato dopo qualche istante (**grigio**). Trascorso il tempo stabilito, il livello di protezione viene automaticamente ridotto. Si noti che il tempo di riduzione automatica sarà decisamente superiore alla durata del blocco se il livello di protezione impostato è basso.

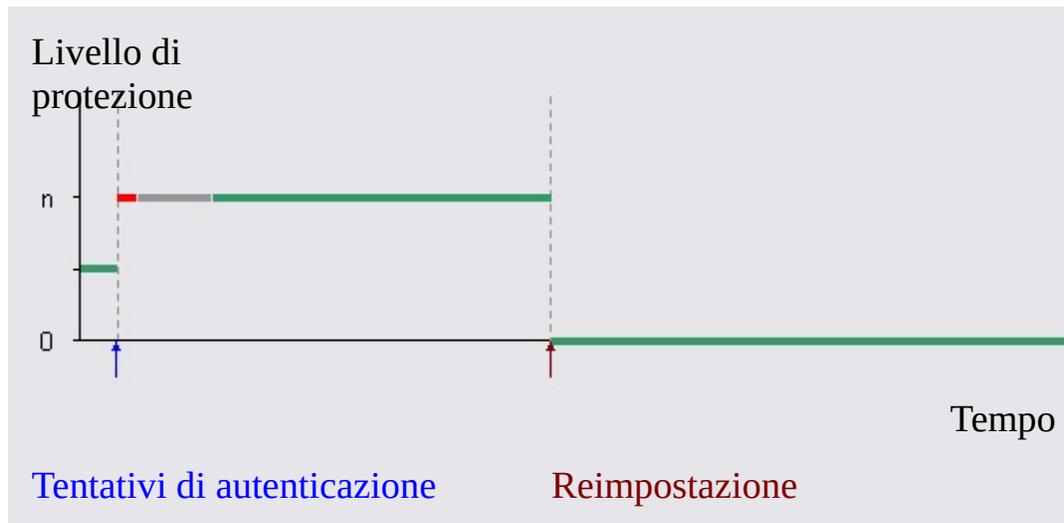


Note:

- Il tempo di riduzione automatica è indipendente dalla durata del blocco e dal riavvio del sistema.
- La riduzione automatica del livello di protezione non richiede il riavvio del sistema.
- Se il livello di protezione impostato è basso, il tempo di riduzione automatica sarà decisamente superiore alla durata del blocco.

Reimpostazione del livello di protezione

La figura mostra la reimpostazione del livello di protezione eseguita dal proprietario di Security Platform.



Come nella figura precedente, si nota un incremento del livello di protezione, l'attivazione del blocco (**rosso**) e la temporanea disattivazione del sistema fino al riavvio successivo (**grigio**). In questo esempio, si ipotizza che il proprietario di Security Platform abbia reimpostato il livello di protezione per evitare i tempi di attesa della riduzione automatica.

Parametri tipici di protezione contro gli attacchi del dizionario

La tabella seguente contiene alcuni dei parametri tipici di protezione per Infineon Trusted Platform Module. I valori elencati potrebbero variare in funzione del tipo di modulo in uso.

Tentativi consentiti per l'autenticazione della Chiave (es. utilizzata per l'autenticazione Utente in Security Platform)	5	Le misure di protezione contro gli attacchi del dizionario vengono attivate dopo 5 tentativi di autenticazione non riusciti rilevati nell'arco di 6 ore (vedere i criteri di configurazione della soglia di protezione e Configurazione Impostazioni Difesa da Attacchi a Dizionario).
Tentativi di autenticazione consentiti al proprietario di Security Platform	3	Le misure di protezione contro gli attacchi del dizionario vengono attivate dopo 3 tentativi di autenticazione non riusciti rilevati nell'arco di 6 ore (vedere i criteri di configurazione della soglia di protezione e Configurazione Impostazioni Difesa da Attacchi a Dizionario).
Tentativi consentiti per l'autenticazione dei Dati (es. utilizzati da Windows BitLocker in associazione con PIN)	10	Dopo 10 tentativi falliti saranno adottate misure di difesa da attacchi a dizionario entro 6 ore ((vedere i criteri di configurazione della soglia di protezione e Configurazione Impostazioni Difesa da Attacchi a Dizionario).
Durata minima del blocco	~10 secondi	La durata iniziale del blocco, attivato al superamento della soglia di protezione, è di 10 secondi.
Durata massima del blocco	~24 ore	La durata massima del blocco è di 24 ore. Tale limite viene applicato al superamento della soglia di protezione, quando sono stati

		rilevati almeno 15 tentativi di autenticazione non riusciti.
Tempo di riduzione automatica del livello di protezione	~6 ore	Il livello di protezione raggiunto viene automaticamente ridotto di una unità dopo circa 6 ore dall'attivazione del livello stesso. Tale riduzione viene applicata soltanto se non si verificano altri tentativi di autenticazione non riusciti entro 6 ore. In caso contrario, il livello di protezione verrà innalzato di una unità.

Queste impostazioni garantiscono un elevato livello di protezione in caso di attacchi reali del dizionario. Contemporaneamente, l'inserimento accidentale di una password errata viene gestito in modo semplice e flessibile.



La durata del blocco e i tempi di riduzione automatica del livello di protezione vengono calcolati soltanto sui sistemi in esecuzione.



©Infineon Technologies AG

Soluzione Infineon Security Platform

Interfaccia utente per la protezione contro gli attacchi del dizionario



Note:

- Questa sezione riguarda esclusivamente i sistemi Security Platform dotati di Trusted Platform Module 1.2. I dettagli relativi al meccanismo di protezione di Security Platform contro gli attacchi del dizionario sono validi soltanto per i sistemi Security Platform che utilizzano Infineon Trusted Platform Module 1.2.
- La descrizione seguente è rivolta principalmente al proprietario di Security Platform.

Il proprietario di Security Platform e l'amministratore del sistema sono responsabili delle impostazioni e delle misure di protezione contro gli attacchi del dizionario. Gli utenti di Security Platform vengono informati in caso di ripetuti errori di digitazione delle password o quando si verificano attacchi reali del dizionario.

La tabella seguente elenca gli elementi dell'interfaccia utente relativi agli attacchi del dizionario:

Configura la soglia di protezione contro gli attacchi del dizionario	Il proprietario di Security Platform o un amministratore autorizzato può impostare il numero di tentativi di autenticazione consentiti, raggiunto il quale vengono adottate le misure di protezione previste contro gli attacchi del dizionario. Ciò è possibile attraverso la configurazione delle Funzionalità di Security Platform , o mediante il criterio configurazione soglia attacco a dizionario .
Reimpostazione del livello di protezione	Modalità autonoma: Il Proprietario di Security Platform può azzerare til livello di difesa attraverso Tool di Configurazione - Avanzato - Azzerà.... . <i>SpTPMWz.exe</i> dell'Inizializzazione Guidata di Security Platform è successivamente avviato con il parametro linea di comando <i>-resetattack</i> .  Questa operazione richiede l'inserimento della password del proprietario. È possibile digitare la Password Proprietario o fornire un File di Backup della Password

Proprietario. Accertarsi di fornire la password corretta. In caso di ripetuti inserimenti di password del proprietario errate, Security Platform verrà temporaneamente bloccato. Durante il blocco dell'applicazione, non sarà possibile reimpostare il livello di protezione contro gli attacchi del dizionario.

Modalità server:

Trusted Computing Management Server offre un modo protetto e efficienti, controllate dal Server, reimpostare il livello di protezione contro gli attacchi del dizionario:

- Funzionalità reimpostazione del livello di protezione possono configurato e gestito senza presenza locale degli amministratori o conoscerne la Password del Proprietario.
- Reimpostazione del livello di protezione possono avviato per qualsiasi piattaforma Trust Domain in modalità remota da qualunque computer con connessione di rete al Trust Domain Server.



Se l'amministratore conosce la Password del Proprietario, il livello di protezione possono reconfigurato in loco avviando l'Inizializzazione guidata di Infineon Security Platform *SpTPMWz.exe* con parametri della riga di comando *-resetattack* o */resetattack*. Ciò è l'unico uso permesso della Inizializzazione guidata di Infineon Security Platform in modalità server.

Notifiche e avvisi

I **messaggi** relativi allo stato attuale delle misure di protezione vengono visualizzati soltanto nei seguenti casi:

- Autenticazione non riuscita (Security Platform proprietario e Security Platform utenti di)
- Superamento della soglia di protezione contro agli attacchi del dizionario
- Tentativi di autenticazione durante il blocco dell'applicazione

In caso di attacchi reali del dizionario (ovvero attacchi non dovuti ad errori accidentali durante un tentativo di

autenticazione), viene visualizzato un **messaggio di avviso o di errore.**



©Infineon Technologies AG

Soluzione Infineon Security Platform

Configurazione Impostazioni di Difesa da Attacchi a Dizionario

In questa pagina è possibile configurare il numero di tentativi di autenticazione consentiti per i diversi tipi di autenticazione prima che vengano adottate misure di difesa da attacchi a dizionario.



Note:

- Questo argomento riguarda unicamente Security Platform con un Trusted Platform Module 1.2. I dettagli del meccanismo di difesa da attacchi a dizionario di Security Platform sono validi solo per Security Platform con un Infineon Trusted Platform Module 1.2.
- Questo argomento si rivolge principalmente al Proprietario.



Disponibilità della pagina:

- Questa pagina di procedura guidata è disponibile solo se il [criterio Configurazione soglia attacchi a dizionario](#) non è configurato.

La seguente tabella fornisce dei suggerimenti sull'uso di questa pagina di procedura guidata.

Elemento Pagina Procedura Guidata	Spiegazione
<input type="radio"/> <i>Specificare contatori autenticazione</i>	Selezionare questa opzione se si desidera specificare il numero di tentativi consentiti per ciascun tipo di autenticazione singolarmente.
<input checked="" type="checkbox"/> <i>Solo contatori relativi a Security Platform</i>	<p>Selezionare questa opzione se si desidera configurare solo i tipi di autenticazione relativi alla Soluzione Security Platform.</p> <p>In questo caso verranno visualizzati solo i seguenti tipi di autenticazione:</p> <ul style="list-style-type: none">• Autenticazione proprietario• Autenticazione chiave (es. utilizzata per l'autenticazione Utente in Security Platform)• Autenticazione dati (es. utilizzata da Windows BitLocker in associazione a PIN)

	<p>Deselezionare questa opzione se si desidera anche configurare altri tipi di autenticazione non rilevanti per la soluzione Security Platform. Per maggiori informazioni su questi tipi di autenticazione fare riferimento alle specifiche fornite dal Trusted Computing Group (TCG) e dal vostro fornitore Trusted Platform Module.</p> <p>Si noti che vengono adottate misure di difesa da attacchi a dizionario quando il numero di tentativi consentivo per un determinato contatore viene superato, sia nel caso in cui il tipo di autenticazione interessato sia rilevante per la soluzione Security Platform sia nel caso contrario.</p>
<input checked="" type="radio"/> <i>Contatore globale autenticazione</i>	<p>Selezionare questa opzione se si desidera specificare un contatore globale di autenticazione per tutti i tipi di autenticazione. Qualsiasi autenticazione non riuscita aumenterà questo contatore, indipendentemente dal tipo di autenticazione.</p>
<input type="checkbox"/> <i>Tipi di Autenticazione</i>	<p>Questo elenco mostra tutti i tipi di autenticazione con I valori minimi, massimi e attualmente configurati per i numeri di tentativi di autenticazione consentiti. Si consiglia di modificare il numero di tentativi consentiti. Accertarsi di inserire solo numeri interi entro i valori minimo e massimo.</p>
<input checked="" type="checkbox"/> <i>Disattivazione temporanea piattaforma</i>	<p>Selezionare questa opzione se si desidera che le misure di difesa includano la disattivazione temporanea di Security Platform.</p>



Soluzione Infineon Security Platform

Reimpostazione del livello di protezione contro gli attacchi del dizionario



Note:

- Questa sezione riguarda esclusivamente i sistemi Security Platform dotati di Trusted Platform Module 1.2. I dettagli relativi al meccanismo di protezione di Security Platform contro gli attacchi del dizionario sono validi soltanto per i sistemi Security Platform che utilizzano Infineon Trusted Platform Module 1.2.
- La descrizione seguente è rivolta principalmente al proprietario di Security Platform.

All'avvio della procedura di reimpostazione, vengono visualizzate le informazioni di stato relative agli attacchi del dizionario. Successivamente, viene richiesta la password del proprietario di Security Platform.

Procedura di reimpostazione del livello di protezione

Operazione	Commento
1. Informazioni di stato relative agli attacchi del dizionario	<p>Questa pagina fornisce le seguenti informazioni dettagliate necessarie per decidere se il livello di difesa deve essere ripristinato o meno:</p> <p>Stato generale attacco a dizionario: Indica se il livello delle misure di difesa da attacchi a dizionario deve essere ripristinato o meno.</p> <p>Tempo blocco rimanente: Visualizza il tempo rimanente, se è in corso un blocco.</p> <p>Lista Tipi di Autenticazione: Visualizza informazioni di stato per diversi tipi di autenticazione, per esempio tipi di autenticazione per chiavi (es. utilizzati per l'autenticazione utente di Security Platform), proprietario e per l'accesso a dati protetti (es. utilizzati da Windows BitLocker in associazione con PIN).</p> <p>Le seguenti informazioni vengono visualizzate per ciascun tipo di autenticazione:</p> <ul style="list-style-type: none">• Tentativi Consentiti: Numero di tentativi di autenticazione a Trusted Platform Module consentiti prima che vengano adottate misure di difesa da attacchi a dizionario (vedere Interfaccia Utente Attacchi a Dizionario, sezione "Configurazione soglia attacco a dizionario").• Contatore Corrente: Numero attuale di tentativi effettivi falliti.• Prossimo Tempo Blocco: Indica il tempo di blocco dopo la successiva autenticazione fallita, se il contatore corrente ha già superato il numero di tentativi consentiti. Altrimenti indica il tempo di blocco quando la soglia sta per essere superata. <p>Il contatore corrente e il prossimo tempo di blocco dipendono dal numero di tentativi consentiti, dal numero totale di autenticazioni fallite nel passato e dal tempo trascorso</p>

dall'ultima autenticazione fallita (vedere [auto-riduzione livello di difesa](#)).

Aggiorna: Fare clic su questo pulsante o premere il tasto "F5" per aggiornare le informazioni sullo stato dell'attacco a dizionario.

Mostra tipi di autenticazione non critica: Per impostazione predefinita solo i tipi di autenticazione con contatori correnti superiori allo zero vengono visualizzati. Verificare questa opzione per visualizzare anche i tipi di autenticazione con contatore corrente a zero.

 Si noti che le informazioni di stato relative agli attacchi del dizionario vengono visualizzate soltanto se tali informazioni possono essere recuperate da Trusted Platform Module.

2. Password del proprietario di Security Platform

La password del proprietario è necessaria per reimpostare il livello di protezione. È possibile digitare la Password Proprietario o fornire un File di Backup della Password Proprietario.

 Accertarsi di inserire la password corretta. È possibile che vengano adottate le misure di protezione previste in caso di attacchi del dizionario. In tali condizioni, non sarà più possibile reimpostare il livello di protezione.



Infineon Security Platform Solution

Gli strumenti di Infineon Security Platform Solution



Ci sono differenze nel comportamento degli Strumenti di Security Platform Solution in [modalità server](#).

Il software Infineon Security Platform Solution comprende gli strumenti amministrativi indicati di seguito.

Strumenti di Security Platform Solution	Scopo
Tool di configurazione di Security Platform	<ul style="list-style-type: none">• Fornisce informazioni su Trusted Platform Module.• Consente, inoltre, di eseguire diverse attività amministrative. <p>Questo componente è designato come applet del pannello di controllo. Il Tool di configurazione costituisce un punto di accesso centrale per l'amministrazione di Infineon Security Platform.</p>
Inizializzazione Guidata Rapida Security Platform	<ul style="list-style-type: none">• Impostare rapidamente Infineon Security Platform e Utente (consigliato per la maggior parte degli utenti).
Inizializzazione guidata di Security Platform	<ul style="list-style-type: none">• Configura Infineon Security Platform (per utenti esperti).
Inizializzazione utenti guidata di Security Platform	<ul style="list-style-type: none">• Configura gli utenti di Infineon Security Platform (per utenti esperti).
Migrazione guidata di Security Platform	<ul style="list-style-type: none">• Consente di trasferire le chiavi e i certificati utente di Infineon Security Platform verso altri computer su cui è installato il software, garantendo la sicurezza e la riservatezza dei dati.
Backup guidato di Security Platform	<ul style="list-style-type: none">• Eseguire le operazioni di backup o ripristino dei dati correlati a Security Platform.

Reimpostazione guidata password di Security Platform	<ul style="list-style-type: none"> • Reimposta le password utente di base.
Importazione guidata PKCS #12 di Security Platform	<ul style="list-style-type: none"> • Importa i file Personal Information Exchange in Security Platform.
Visualizzatore certificati e Selezione certificati di Security Platform	<ul style="list-style-type: none"> • Consentono di gestire i certificati.
Icona di Notifica di Security Platform	<ul style="list-style-type: none"> • Consente di eseguire varie attività amministrative di Security Platform e di verificare lo stato del software.
Amministrazione dei criteri di Security Platform	<ul style="list-style-type: none"> • Consente di gestire i criteri di sistema e i criteri utente correlati a Infineon Security Platform.
Servizi integrativi di Security Platform	<ul style="list-style-type: none"> • Abilita alcune applicazioni standard per l'utilizzo delle funzionalità di Trusted Platform Module.
Servizi di Security Platform	<ul style="list-style-type: none"> • Forniscono lo stack del software conforme ai requisiti stabiliti dal Trusted Computing Group (TCG).



©Infineon

Infineon Security Platform Solution

Utilizzo delle procedure guidate di Security Platform

Security Platform Solution utilizza il Tool di configurazione come punto di accesso centrale per l'amministrazione di Infineon Security Platform. Tutte le attività di configurazione sono facilitate da apposite procedure guidate.

Pagine delle procedure guidate

Pagina di benvenuto

Questa è la pagina iniziale della procedura guidata. In questa pagina viene illustrato lo scopo della procedura guidata.

Tale pagina appare soltanto quando si utilizzano tutte le funzionalità della procedura guidata. Infatti, non viene visualizzata se si avvia la procedura dal Tool di configurazione per eseguire una determinata attività amministrativa.

Pagine successive

Nelle pagine successive delle varie procedure guidate, viene richiesto all'utente di immettere le informazioni necessarie all'esecuzione delle operazioni richieste.

Pagina di conferma

In questa pagina, vengono riassunte le informazioni specificate e le operazioni da eseguire.



Fino a questo momento, non è stata eseguita nessuna modifica. Le operazioni elencate verranno effettuate soltanto dopo aver selezionato il pulsante **Avanti**.

Pagina finale

Questa è la pagina finale della procedura guidata. È l'ultima pagina visualizzata, nella quale viene indicato il risultato finale della procedura (riuscita o meno) elencando tutte le operazioni effettuate.

Se la configurazione generale del software richiede l'avvio di un'altra procedura guidata, prima di poter utilizzare le funzionalità di Security Platform, è possibile scegliere di continuare automaticamente passando alla procedura guidata successiva.

Esempio: dopo aver inizializzato o ripristinato Security Platform (tramite l'Inizializzazione guidata della piattaforma), si desidera procedere con l'inizializzazione o il ripristino degli utenti (utilizzando l'Inizializzazione utenti guidata).

Al termine **dell'Inizializzazione guidata di Security Platform**, è possibile

scegliere se eseguire il [backup automatico](#) per aggiornare l'archivio del backup di sistema con le modifiche principali. Questa opzione è disponibile soltanto se non è stato configurato il criterio [Attiva backup di sistema immediato](#).

Indicazione dello stato di avanzamento delle procedure guidate

L'Indicazione Guidata Progresso nell'angolo superiore destro della pagina di procedura guidata visualizza le fasi necessarie della procedura guidata ed evidenzia la fase corrente. L'Indicazione Guidata Progresso è supportata da tutte le Procedure Guidate che dispongono di pagine di configurazione e fasi multiple. Vi informa sulle fasi da superare per eseguire una determinata attività:

- Ogni operazione è rappresentata da un piccolo rettangolo.
- Il rettangolo corrispondente all'operazione in corso viene evidenziato.
- Spostando il puntatore del mouse sui vari rettangoli è possibile visualizzare alcune informazioni su ciascuna operazione.

Comportamento delle procedure guidate in caso di errore

Quando si verifica un errore durante una procedura guidata, non viene apportata nessuna delle modifiche previste. In questi casi, viene visualizzato un messaggio di errore.

Condizioni preliminari per l'esecuzione delle procedure guidate

Condizione	Spiegazione
Diritti amministrativi e criteri di Windows	Inizializzazione guidata di Security Platform/Inizializzazione Guidata Rapida Security Platform (se la piattaforma non è ancora inizializzata): L'utente deve disporre dei diritti amministrativi Windows (in altre parole, l'utente attuale deve essere un membro del gruppo di amministratori). Se Trusted Platform Module è stato disabilitato nel sistema, l'utente deve essere autorizzato al riavvio del computer.
Criteri di Security Platform	L'accesso alle procedure guidate di Security Platform può essere limitato impostando i criteri Consenti iscrizione alla piattaforma e Consenti l'iscrizione dell'utente .
Stato dell'utente	Reimpostazione guidata password, Importazione guidata PKCS #12 L'utente attuale deve essere un utente configurato di Security Platform.
Stato di Security Platform e di Trusted Platform Module	Inizializzazione guidata di Security Platform Le possibili cause di errore sono indicate di seguito. <ul style="list-style-type: none">• È cambiato il proprietario di Infineon Security Platform dopo l'installazione del software.• La proprietà di Trusted Platform Module è stata acquisita ma Infineon Security Platform non è ancora installato. In queste condizioni, non è possibile eseguire la configurazione. Tutte le procedure guidate: È richiesta la connessione a Trusted Platform Module. Le possibili cause di errore sono indicate di seguito. <ul style="list-style-type: none">• Trusted Platform Module è stato disabilitato in modo permanente o temporaneo.• Trusted Platform Module non è presente.

	<ul style="list-style-type: none">• Problemi del driver. <p> Per informazioni dettagliate sullo stato di Infineon Security Platform, cliccare qui.</p>
Coerenza della configurazione standard	<p>Tutte le procedure guidate:</p> <p>La configurazione di Security Platform deve essere coerente con le altre impostazioni di sistema.</p> <p>Alcuni esempi delle possibili cause di errore sono indicati di seguito:</p> <ul style="list-style-type: none">• Impostazioni non valide per la configurazione dell'archivio di backup.• Non è possibile creare il token di ripristino di emergenza o di reimpostazione password.



Soluzione Infineon Security Platform

Finestre di dialogo Password utente di base e Autenticazione

Per poter gestire Security Platform e utilizzarne le funzionalità è necessario eseguire l'autenticazione utente in Security Platform. I contenuti della finestra di dialogo Autenticazione variano in funzione della modalità di autenticazione selezionata e dell'operazione che richiede l'autenticazione.

- [Informazioni generali](#)
- [Criteri e complessità delle password](#)
- [Finestre di dialogo per l'utilizzo delle funzionalità di Security Platform](#)
- [Finestre di dialogo per la gestione di Security Platform](#) - [Impostazione password utente di base](#)
 - [Modifica della password utente di base](#)
 - [Verifica della password utente di base](#)

Informazioni generali

La tabella seguente indica le varie password e finestre di dialogo per l'autenticazione che vengono visualizzate in diverse circostanze.

Tipo di operazione	Operazioni dell'utente	Soluzione Esempi in Security Platform
Impostazione della password utente di base	Modalità Autenticazione password <ul style="list-style-type: none">• Immettere e confermare la password. Modalità Autenticazione avanzata <ul style="list-style-type: none">• Inserire e confermare frase password.• Inserire il dispositivo di autenticazione e immettere il PIN (altre operazioni potrebbero essere necessarie, a seconda del dispositivo di autenticazione, ad esempio appoggiare un dito sul lettore di impronte digitali).	<ul style="list-style-type: none">• Inizializzazione utenti (Inizializzazione Guidata Rapida o Inizializzazione Utenti Guidata)• Reimpostazione password (Tool di configurazione - Reimpostazione password - Reimposta...)
Modifica password utente di base	Modalità Autenticazione password <ul style="list-style-type: none">• Immettere la vecchia password.• Immettere e confermare la nuova password. Modalità Autenticazione avanzata <ul style="list-style-type: none">• Inserire il dispositivo di autenticazione e	<ul style="list-style-type: none">• Modifica password (Tool di configurazione - Impostazioni utente - Cambia...)

	<p>immettere il PIN (altre operazioni potrebbero essere necessarie, a seconda del dispositivo di autenticazione, ad esempio appoggiare un dito sul lettore di impronte digitali).</p> <ul style="list-style-type: none"> • Immettere e confermare la nuova frase password. 	
<p>Verifica della password utente di base</p>	<p>Modalità Autenticazione password</p> <ul style="list-style-type: none"> • Immettere la password. <p>Modalità Autenticazione avanzata</p> <ul style="list-style-type: none"> • Inserire il dispositivo di autenticazione e immettere il PIN (altre operazioni potrebbero essere necessarie, a seconda del dispositivo di autenticazione, ad esempio appoggiare un dito sul lettore di impronte digitali). In alternativa, se si preferisce non utilizzare il dispositivo di autenticazione avanzata, è possibile immettere la frase password. 	<ul style="list-style-type: none"> • Autenticazione utente richiesta per utilizzare le funzionalità di Security Platform (come la crittografia di file e cartelle o la protezione della posta elettronica) • Abilitazione della reimpostazione password (Tool di configurazione - Reimpostazione password - Abilita...) • Esportazione dell'archivio di migrazione (Tool di configurazione - Migrazione - Esporta...) • Importazione dell'archivio di migrazione (Tool di configurazione - Migrazione - Importa...) • Ripristino delle credenziali utente (Tool di configurazione - Backup - Ripristina...)



Criteri e complessità delle password

Per informazioni riguardanti i criteri e i requisiti di complessità delle password, consultare [Gestione delle password](#).

Finestre di dialogo per l'utilizzo delle funzionalità di Security Platform

Le tabelle seguenti descrivono le finestre di dialogo necessarie per l'utilizzo delle funzionalità di Security Platform (come la crittografia di file e cartelle o la protezione della posta elettronica).

Autenticazione password	
<input type="password"/> Password utente di base	Immettere la password utente di base attuale.
<input checked="" type="checkbox"/> Memorizza la password per tutte le applicazioni	Selezionare questa casella di controllo per memorizzare la password ed evitare così di doverla digitare ad ogni richiesta di autenticazione visualizzata dalle varie applicazioni che utilizzano le funzionalità di Security Platform.
<input type="button" value="Dettagli..."/>	Cliccare su questo pulsante per visualizzare ulteriori informazioni sull'applicazione che richiede l'autenticazione a Security Platform.
Autenticazione avanzata con frase password	
<input type="password"/> Frase password utente di base	Immettere la frase password utente di base attuale.
<input type="checkbox"/> Autenticazione	Cambiare il metodo di autenticazione se si desidera utilizzare un dispositivo di autenticazione invece di immettere la frase password.
<input checked="" type="checkbox"/> Nascondi digitazione	Deselezionare questa casella di controllo se si desidera visualizzare la frase password digitata.
<input checked="" type="checkbox"/> Memorizza la frase password per tutte le	Selezionare questa casella di controllo per memorizzare la frase password ed evitare così di doverla digitare ad ogni richiesta di autenticazione visualizzata dalle varie

<i>applicazioni</i>	applicazioni che utilizzano le funzionalità di Security Platform.
<input type="checkbox"/> <i>Dettagli...</i>	Cliccare su questo pulsante per visualizzare ulteriori informazioni sull'applicazione che richiede l'autenticazione a Security Platform.
Autenticazione avanzata tramite smart card o token USB di protezione	
<input checked="" type="checkbox"/> <i>PIN</i>	Inserire la smart card o il token USB di protezione. Immettere il codice PIN.
<input type="checkbox"/> <i>Autenticazione</i>	Cambiare il metodo di autenticazione se si desidera immettere la frase password invece di utilizzare un dispositivo di autenticazione.
<input checked="" type="checkbox"/> <i>Memorizza il PIN per tutte le applicazioni</i>	Selezionare questa casella di controllo per memorizzare il codice PIN ed evitare così di doverlo digitare ad ogni richiesta di autenticazione visualizzata dalle varie applicazioni che utilizzano le funzionalità di Security Platform.
<input type="checkbox"/> <i>Dettagli...</i>	Cliccare su questo pulsante per visualizzare ulteriori informazioni sull'applicazione che richiede l'autenticazione a Security Platform.
Autenticazione avanzata tramite altri dispositivi di autenticazione	
<input type="checkbox"/> <i>Autenticazione utente</i>	Utilizzare il dispositivo di autenticazione avanzata per eseguire l'autenticazione utente (ad esempio, appoggiando un dito sul lettore di impronte digitali).
	 Per ulteriori informazioni, consultare la Guida in linea

	del plug-in di autenticazione avanzata.
<input type="checkbox"/> <i>Autenticazione</i>	Cambiare il metodo di autenticazione se si desidera immettere la frase password invece di utilizzare un dispositivo di autenticazione.
<input checked="" type="checkbox"/> <i>Memorizza per tutte le applicazioni</i>	Selezionare questa casella di controllo per memorizzare l'autenticazione ed evitare così di doverla eseguire nuovamente per le varie applicazioni che utilizzano le funzionalità di Security Platform.
<input type="checkbox"/> <i>Dettagli...</i>	Cliccare su questo pulsante per visualizzare ulteriori informazioni sull'applicazione che richiede l'autenticazione a Security Platform.



Finestre di dialogo per la gestione di Security Platform

Le tabelle seguenti descrivono le finestre di dialogo Password utente di base e Autenticazione che consentono la gestione di Security Platform.

Impostazione della password utente di base (Inizializzazione utenti, Reimpostazione password)

Autenticazione password	
<input type="password"/> Password	Immettere una password che soddisfi le impostazioni dei criteri password . Questa sarà la nuova password utente di base.
<input type="password"/> Conferma password	Immettere nuovamente la password per confermarla.
Autenticazione avanzata tramite smart card o token USB di protezione	
<input type="password"/> Frase password	Immettere una frase password che soddisfi le impostazioni dei criteri password . Questa sarà la nuova frase password utente di base.
<input type="password"/> Conferma frase password	Immettere nuovamente la frase password per confermarla.
<input type="password"/> PIN	Inserire la smart card o il token USB di protezione. Immettere il codice PIN.
Autenticazione avanzata tramite altri dispositivi di autenticazione	
<input type="password"/> Frase	Immettere una frase password che soddisfi le impostazioni

<i>password</i>	dei criteri password . Questa sarà la nuova frase password utente di base.
 <i>Conferma frase password</i>	Immettere nuovamente la frase password per confermarla.
 <i>Autenticazione utente</i>	Utilizzare il dispositivo di autenticazione avanzata per eseguire l'autenticazione utente (ad esempio, appoggiando un dito sul lettore di impronte digitali).  Per ulteriori informazioni, consultare la Guida in linea del plug-in di autenticazione avanzata.



Modifica password utente di base

Autenticazione password	
 <i>Vecchia password</i>	Immettere la password utente di base attuale.
 <i>Nuova password</i>	Immettere una password che soddisfi le impostazioni dei criteri password . Questa sarà la nuova password utente di base.
 <i>Conferma nuova password</i>	Immettere nuovamente la password per confermarla.
Autenticazione avanzata tramite smart card o token USB di protezione	
 <i>PIN</i>	Inserire la smart card o il token USB di protezione. Immettere il codice PIN.
 <i>Nuova frase password</i>	Immettere una frase password che soddisfi le impostazioni dei criteri password . Questa sarà la nuova frase password

	utente di base.
 Conferma nuova frase password	Immettere nuovamente la frase password per confermarla.
Autenticazione avanzata tramite altri dispositivi di autenticazione	
 Nuova frase password	Immettere una frase password che soddisfi le impostazioni dei criteri password . Questa sarà la nuova frase password utente di base.
 Conferma nuova frase password	Immettere nuovamente la frase password per confermarla.
 Autenticazione utente	Utilizzare il dispositivo di autenticazione avanzata per eseguire l'autenticazione utente (ad esempio, appoggiando un dito sul lettore di impronte digitali).  Per ulteriori informazioni, consultare la Guida in linea del plug-in di autenticazione avanzata.



Verifica della password utente di base (Abilitazione alla reimpostazione password, Esportazione/Importazione dell'archivio di migrazione, Ripristino delle credenziali utente)

Autenticazione password	
 Password	Immettere la password utente di base attuale.
Autenticazione avanzata	
 Dispositivo di	Specificare se si desidera utilizzare un dispositivo di autenticazione oppure immettere la frase password.

autenticazione ☉ Frase password	
Autenticazione avanzata con frase password	
☒☒☒ Frase password	Immettere la frase password utente di base attuale.
Autenticazione avanzata tramite smart card o token USB di protezione	
☒☒☒ PIN	Inserire la smart card o il token USB di protezione. Immettere il codice PIN.
Autenticazione avanzata tramite altri dispositivi di autenticazione	
☒ Autenticazione utente	Utilizzare il dispositivo di autenticazione avanzata per eseguire l'autenticazione utente (ad esempio, appoggiando un dito sul lettore di impronte digitali).  Per ulteriori informazioni, consultare la Guida in linea del plug-in di autenticazione avanzata.



Infineon Security Platform Solution

Gestione delle password

Password utilizzate in Security Platform Solution

Infineon Security Platform Solution utilizza più password diverse tra loro. Alcune di queste password sono riservate agli amministratori di Security Platform, mentre altre possono essere utilizzate da tutti gli utenti. Fare attenzione a non confondere le diverse password.



In [modalità server](#) le password amministrative e il Codice di Autorizzazione alla Reimpostazione non sono validi, poiché il Trusted Computing Management Server gestisce il compito di preparare e fornire queste password.

La tabella seguente contiene alcune informazioni generali sulle password di Security Platform e sul loro utilizzo.

Password	Utilizzata da...	Scopo/Spiegazione
Password del proprietario	Amministratore	È impostato durante l'inizializzazione di Security Platform ed è necessario per svolgere attività amministrative critiche per Security Platform. Può essere impostata manualmente o può essere creata una Password Proprietario casuale. Può essere salvato in un File di Backup Password Proprietario che può essere utilizzato per l'autenticazione con Password Proprietario (anziché digitare la Password Proprietario). Questo file è compatibile con il File di Backup Password Proprietario generato dall'applicazione Microsoft "Gestione Trusted Platform Module (TPM)".
Password del token di ripristino di emergenza	Amministratore	Protegge il token che consente di eseguire il ripristino di emergenza dei dati.

<p>Password del token di reimpostazione della password</p>	<p>Amministratore</p>	<p>Protegge il token di reimpostazione della password che consente di cambiare la password utente di base.</p>
<p>Password utente di base (nota anche come "password", in modalità Autenticazione avanzata oppure come "frase password utente di base")</p>	<p>Utente</p>	<p>Protegge la chiave utente di base che consente di accedere ai dati specifici di ciascun utente di Security Platform. Le funzionalità del software non possono essere utilizzate senza questa password.</p> <p>La password utente di base è richiesta anche per ripristinare e trasferire i dati dell'utente, nonché per configurare alcune impostazioni specifiche dell'utente stesso. Può essere reimpostata quando sia l'amministratore, sia l'utente hanno configurato questa funzione.</p> <p>In modalità Autenticazione avanzata, la password viene sostituita da una "frase password" protetta dal dispositivo di autenticazione.</p> <p> Questa è la password principale degli utenti di Security Platform. Per questioni di praticità, è comunemente chiamata "password".</p>
<p>Password PKCS #12</p>	<p>Utente</p>	<p>Protegge la chiave privata dell'utente archiviata in un file PKCS #12.</p>
<p>Codice di autorizzazione alla reimpostazione</p>	<p>Utente</p>	<p>Questa stringa di codice non è una password vera e propria anche se funziona allo stesso modo, per lo meno dal punto di vista dell'utente. Viene creata automaticamente quando si prepara la reimpostazione della password utente. È utilizzata per</p>

reimpostare la password utente di base.

Suggerimenti generali per la selezione delle password

- Utilizzare password diverse a fini diversi. In particolare, non riutilizzare la propria password di Windows. Riutilizzando la password di Windows per tutte le password collegate a Security Platform, il livello di protezione ottimizzato basato sull'hardware non sarà più efficace. Chi intende eseguire un attacco conoscendo la vostra Password di Windows potrebbe accedere ai vostri dati EFS e PSD, utilizzare le vostre credenziali di identificazione e autorizzazione e manomettere le impostazioni di Security Platform.
- Per migliorare la qualità delle password, si raccomanda l'uso di caratteri speciali. Occorre tener presente, tuttavia, che alcuni caratteri possono avere una posizione diversa sulla tastiera, in funzione delle impostazioni locali. Inoltre, alcuni caratteri possono addirittura non essere disponibili in base alla lingua di sistema. Inoltre, alcuni caratteri potrebbero non essere ammessi all'interno delle password, a seconda del sistema operativo e di altri componenti software.
- Evitare l'uso di password reperibili nei dizionari, anche se la password è formata da una combinazione di parole.
- L'aggiunta di cifre e l'uso di lettere maiuscole migliora la qualità delle password.
- La lunghezza minima e massima delle password resta normalmente invariata dopo la configurazione del sistema. Comunque, l'aspetto delle password può essere diverso nei vari sistemi, anche se le caratteristiche generali vengono mantenute in ogni installazione del software.
- Per evitare che la propria password venga letta da altri utenti, la funzione di copia non è supportata nei campi di inserimento delle password.

Complessità della password

La seguente tabella fornisce una panoramica dei requisiti di Complessità della Password:

Requisiti di Complessità dalla Password

Sono richiesti caratteri appartenenti ad almeno 3 delle seguenti categorie:

- Caratteri maiuscoli (da **A** a **Z**)
- Caratteri minuscoli (da **a** a **z**)
- Cifre in base 10 (da **0** a **9**)
- Caratteri non alfanumerici (es.: **!**, **\$**, **#**, **%**)

Criteri della Password del Proprietario e Complessità della Password

Ci sono requisiti speciali per la lunghezza e la complessità della Password del Proprietario. La tabella seguente contiene alcune informazioni generali sull'impostazione dei criteri predefiniti per le password:

Lunghezza minima predefinita	6 caratteri
Password complessa richiesta	No

Criteri e complessità delle password

Esistono requisiti particolari relativamente alla lunghezza e alla complessità delle password. La tabella seguente contiene alcune informazioni generali sull'impostazione dei criteri predefiniti per le password:

	Autenticazione della password - senza dispositivo di autenticazione	Autenticazione avanzata - un dispositivo di autenticazione protegge la frase password
Lunghezza minima predefinita	6 caratteri	20 caratteri
Password complessa richiesta	No	No

L'amministratore del sistema può modificare queste impostazioni. Ulteriori dettagli sui criteri delle password sono disponibili nella sezione dedicata ai [Criteri utente](#) di Infineon Security Platform.

 Se i diritti di accesso di cui si dispone non consentono di impostare o visualizzare i criteri delle password, contattare l'amministratore del sistema per conoscere i criteri effettivi della propria password.

 Queste opzioni nel campo password possono essere limitate in base alla politica del sistema [Abilita sicurezza campo password ristretta](#).



Infineon Security Platform Solution - Inizializzazione utenti guidata

Tool di configurazione di Infineon Security Platform

Il Tool di configurazione di Security Platform consente di ottenere varie informazioni sul modulo TPM installato nel sistema. Permette, inoltre, di eseguire diverse attività amministrative. Questo componente è designato come applet del pannello di controllo. Il Tool di configurazione costituisce un punto di accesso centrale per l'amministrazione di Infineon Security Platform.

La tabella seguente illustra le pagine del Tool di configurazione:

Pagina	Informazioni
Informazioni	<ul style="list-style-type: none">• Visualizza le impostazioni più significative di Infineon Security Platform
Impostazioni utente	<ul style="list-style-type: none">• Modifica password utente di base• Configurazione delle funzionalità di Security Platform specifiche per gli utenti• Gestione dei certificati di Security Platform• Disattivazione temporanea di Security Platform
Backup	<ul style="list-style-type: none">• Configurazione del backup automatico (attività dell'amministratore)• Backup manuale e ripristino• Creazione di una copia di backup dei dispositivi di autenticazione <p> In modalità server il backup e il ripristino sono gestiti dal Trusted Computing Management Server. Se il Personal Secure Drive (PSD) è stato configurato, allora un backup e ripristino manuale di questo drive possono essere fatti.</p>
Migrazione	<ul style="list-style-type: none">• Esportazione delle chiavi e dei certificati utente di Security Platform• Importazione delle chiavi e dei certificati utente di Security Platform <p> Questa pagina non è disponibile in modalità server, poiché la migrazione di chiavi e certificati specifici per l'utente è gestita dal Trusted Computing Management Server, ovvero non devi eseguire questo compito.</p>

[Reimpostazione password](#)

- Configurazione della funzione per tutti gli utenti (attività dell'amministratore)
- Abilitazione della funzione per l'utente attuale
- Preparazione della reimpostazione password per un determinato utente (attività dell'amministratore)
- Reimpostazione della password utente di base per l'utente attuale



In [modalità server](#) il Trusted Computing Management Server gestisce il compito di configurare, abilitare e preparare il codice di Autorizzazione al Reset della Password, ovvero l'amministratore o l'utente non devono eseguire questo compito. Di conseguenza tutte le opzioni tranne *Ripristina* e *Attiva* sono disabilitate.

[BitLocker](#)

- Usa la Crittografia unità BitLocker insieme al Trusted Platform Module per crittografare dati sul tuo disco.



- Questa pagina è disponibile solo se il sistema operativo supporta la crittografia unità BitLocker (es. le edizioni Enterprise e Ultimate di Windows 7 e Windows Vista) e l'utente corrente dispone dei diritti amministrativi.
- Questa pagina non è disponibile in [modalità server](#). Tuttavia, è possibile configurare BitLocker attraverso l'applet del pannello di controllo di Microsoft BitLocker.

[Avanzate](#)

- Modificare la Password Proprietario
- Configurazione delle funzionalità di Security Platform specifiche per la piattaforma
- Attivazione/disattivazione di Security Platform
- Configurazione dei criteri di Security Platform
- Azzerare il livello di difesa da attacchi a dizionario



- Questa pagina viene visualizzata unicamente se l'utente attuale dispone di diritti amministrativi appropriati.
- Questa pagina non è disponibile in [modalità](#)

[server](#), poiché il Trusted Computing Management Server gestisce il compito di configurare le funzionalità e i criteri di Security Platform.

Avvio dell'applicazione

- **Gestione di Security Platform**

Avvio del Tool di configurazione dall'[icona di notifica della barra delle applicazioni](#).



Nei sistemi operativi con Controllo account utente (ad es. Windows 7 e Windows Vista), il Tool di configurazione viene avviato senza privilegi elevati.

-  **Gestione di Security Platform**

Avvio del Tool di configurazione dall'[icona di notifica della barra delle applicazioni](#) con privilegi elevati.



Disponibile solo per gli utenti con diritti amministrativi nei sistemi operativi con Controllo account utente (ad es. Windows 7 e Windows Vista).



Infineon Security Platform Solution - Tool di configurazione

Informazioni su Infineon Security Platform

Questa pagina visualizza le impostazioni più significative di Infineon Security Platform.

Se il software è disabilitato, alcune informazioni non verranno visualizzate.

La tabella seguente descrive tutte le informazioni e le funzioni disponibili nella finestra di dialogo.

Elementi della pagina	Spiegazione
 <i>Security Platform Solution</i>	Versione del prodotto e modalità operativa della Security Platform Solution per l'utente attualmente collegato.
 <i>Stato di Security Platform</i>	Lo stato di chip, proprietario, utente e modalità operativa è descritto nella descrizione generale dello Stato di Security Platform .
 <i>Trusted Platform Module</i>	Produttore e versione dell'hardware e del firmware di Trusted Platform Module.
 <i>Test automatico</i>	Cliccare su questo pulsante per verificare il funzionamento di Trusted Platform Module. Vengono visualizzati i risultati del test.
 <i>Dettagli...</i>	Cliccare su questo pulsante per visualizzare informazioni dettagliate sulla configurazione di Infineon Security Platform.



Infineon Security Platform Solution - Tool di configurazione

Ulteriori dettagli

Questa finestra di dialogo contiene un elenco delle principali informazioni sul sistema. Tali informazioni comprendono:

- Versione prodotto
- [Modalità di funzionamento](#)
- [Stato Security Platform](#)
- Info componente
- Info Supporto Avanzato

È possibile salvare queste informazioni in un file:

Pulsante	Spiegazione
<input type="checkbox"/> <i>Salva...</i>	<p>Le informazioni di diagnostica possono essere salvate su file per poterle analizzare successivamente in modalità off-line. Selezionando questo comando, viene visualizzata una finestra di selezione, in cui è possibile scegliere l'unità, la cartella di destinazione e il nome da attribuire al file.</p> <p>Il formato del file di diagnostica di Security Platform è un normale formato di testo (estensione *.txt). In questo modo, il file può essere visualizzato con le più svariate applicazioni.</p>



©Infineon

Infineon Security Platform Solution - Inizializzazione utenti guidata

Stato Security Platform

Lo stato attuale dell'Infineon Security Platform è definito dallo stato attuale dei seguenti quattro componenti:

Stato chip (Stato Trusted Platform Module)

Fornisce informazioni sullo stato del Trusted Platform Module. I possibili stati sono indicati di seguito.

- **Abilitato** - Trusted Platform Module è accessibile ed è attualmente utilizzato dal software Infineon Security Platform.
- **Disabilitato** - Trusted Platform Module è stato bloccato e non può essere utilizzato. Questa condizione può essere ottenuta mediante una delle impostazioni del BIOS di sistema oppure attraverso un'impostazione del software Infineon Security Platform.

Soluzioni possibili: se Trusted Platform Module è disabilitato nel BIOS, consultare la documentazione del BIOS di sistema; altrimenti, [abilitare](#) Trusted Platform Module nel software Infineon Security Platform.

- **Temporaneamente disabilitato** - Trusted Platform Module è accessibile ma il suo utilizzo risulta bloccato fino a quando non viene riavviato il sistema. Le funzionalità di protezione che utilizzano il chip non sono disponibili.

Soluzione Possibile: [abilitare](#) Trusted Platform Module nel software Infineon Security Platform e riavviare il sistema.

Stato Proprietario

Fornisce informazioni sullo stato generale dell' Infineon Security Platform. I possibili stati sono indicati di seguito.

- **Non inizializzato** - il software Infineon Security Platform non è stato inizializzato e quindi la proprietà non è ancora acquisita oppure lo stato dell'inizializzazione non è coerente (ad esempio, a causa di un'interruzione dovuta a una perdita di corrente).
Soluzioni possibili: Inizializzazione Security Platform con l'[Inizializzazione Guidata Rapida di Security Platform](#) o con l'[Inizializzazione Guidata di Security Platform](#).
- **Inizializzato** - le principali operazioni di configurazione sono state completate, Trusted Platform Module è operativo e la proprietà del software è stata acquisita. Esiste un Proprietario Infineon Security Platform nell' Trusted Platform Module.
- **Modificato** - la proprietà di Infineon Security Platform è acquisita ma dopo questa operazione il Proprietario Infineon Security Platform è stato modificato. L'amministrazione di Security Platform lo indica come stato proprietario **Inizializzato (Modalità 1)**.
Soluzione Possibile: Avviare [l'Assistente di Inizializzazione della Security Platform](#) e seguire le istruzioni sullo schermo.
- **TPM inizializzato, Security Platform non inizializzata** - Nelle versioni precedenti del software Infineon Security Platform Solution il nome era "**Inizializzato altro SO**".
Caso 1: Nei sistemi operativi Windows 7 e Windows Vista, una circostanza possibile è che il Trusted Platform Module è stato inizializzato con l'applicazione Microsoft [Gestione Trusted Platform Module \(TPM\)](#), ovvero la Proprietà del Trusted Platform Module è stata presa, ma la Infineon Security Platform non è installata.
Caso 2: Questo può accadere anche in computer multi-piattaforma con diverse versioni di sistemi operativi installate, in cui la proprietà viene presa usando un sistema e poi viene avviato un sistema diverso.
In entrambi i casi, l'installazione della Infineon Security Platform rimane attiva. L'amministrazione di Security Platform lo indica come stato proprietario **Inizializzato (Modalità 2)**.
Soluzione Possibile: Avviare [l'Assistente di Inizializzazione della Security Platform](#) e seguire le istruzioni sullo schermo.

Stato Utente

Fornisce informazioni sullo stato dell'utente attualmente connesso. I possibili stati sono indicati di seguito.

- **Non inizializzato** - l'utente attualmente connesso non è stato configurato come utente di Infineon Security Platform oppure lo stato della configurazione utente non è coerente (ad esempio, a causa di un'interruzione dovuta a una perdita di corrente).
Soluzioni possibili: Inizializzazione dell'utente con l'[Inizializzazione Guidata Rapida di Security Platform](#) o con l'[Inizializzazione Utenti Guidata di Security Platform](#).
- **Inizializzato** - l'utente attualmente connesso è un utente valido di Infineon Security Platform; ciò significa che la configurazione dell'utente attuale è stata eseguita. La chiave utente di base è stata generata e memorizzata in un archivio di ripristino di emergenza, se presente.
- **Modificato** - l'utente di Infineon Security Platform è configurato ma la proprietà del software è stata successivamente modificata. Quindi, la chiave dell'utente attualmente connesso non può essere utilizzata in Infineon Security Platform. L'amministrazione di Security Platform lo indica come stato utente **Inizializzato (Modalità 3)**.
Soluzioni possibili:
Contattare l'amministratore per poter avviare [L'inizializzazione guidata di Security Platform](#) e selezionare l'opzione *Ripristina Security Platform da un archivio di backup*. In questo modo, è possibile preparare il ripristino delle credenziali utente da un archivio di backup creato in precedenza.
Successivamente, accedere al software utilizzando il proprio account utente e avviare [L'inizializzazione utenti guidata](#). (vedere [Come recuperare i dati del ripristino di emergenza passo dopo passo](#)).
Se non esiste nessun archivio di backup, sarà necessario eseguire una reinizializzazione forzata dell'utente. A tale scopo, avviare [L'inizializzazione utenti guidata](#) con il parametro della linea di comando - **forceinit**.



Il parametro della linea di comando **forceinit** non è supportato in [modalità server](#).

Stato sessione utente

Lo stato è disponibile solo in [modalità server](#).

Lo stato sessione utente controlla l'accesso di scrittura alle credenziali utente e alle impostazioni. In questo modo si garantisce che non vi siano modifiche incompatibili apportate da diverse piattaforme. Lo stato sessione si riferisce ad un determinato utente su una determinata piattaforma. È possibile modificare lo stato sessione attraverso il sottomenu *Credenziali Utente/Impostazioni* nel [menu di notifica della barra delle applicazioni](#). Sono utilizzati i seguenti stati:

- **Sola lettura:** Nessun accesso di scrittura corrente. L'accesso di scrittura è possibile cambiando lo stato in *Lettura/Scrittura Temporanea* o *Lettura/Scrittura Permanente*, poiché nessun'altra piattaforma si trova in uno dei due stati di *Lettura/Scrittura* possibili. Stato di default.
- **Lettura/Scrittura Temporanea:** Stato usato implicitamente dal Trusted Computing Management Server per l'accesso scritto. Impedisce le modifiche da altre piattaforme. Dopo l'accesso scritto lo stato *Sola lettura* sarà impostato di nuovo.
- **Lettura/Scrittura Permanente:** Stato attivato esplicitamente dall'utente mediante l'elemento del menu di notifica della barra delle applicazioni *Credenziali Utente/Impostazioni - Richiedi copia locale di lavoro*. Consente la modifica delle credenziali utente e delle impostazioni in modalità non in linea in una copia locale di lavoro. Impedisce le modifiche da altre piattaforme. Lo stato può essere modificato in *Sola lettura* solo mediante l'elemento del menu di notifica della barra delle applicazioni *Credenziali Utente/Impostazioni - Accetta modifiche locali* o *Credenziali Utente/Impostazioni - Elimina modifiche locali*.



Infineon Security Platform Solution - Tool di configurazione

Impostazioni utente di Infineon Security Platform

In questa pagina è possibile configurare le impostazioni di protezione per l'utente attualmente connesso a Infineon Security Platform.



Disponibilità della pagina:

- Questa pagina è disponibile soltanto se Security Platform è già stato inizializzato.
- Se Infineon Security Platform non è ancora configurato, un messaggio informa sulla situazione e l'[Inizializzazione Guidata Rapida](#) può essere avviata. In [modalità server](#) non verrà visualizzato alcun messaggio poiché Security Platform si inizializza automaticamente se il sistema del cliente è Infineon in un Trust Domain a gestione centralizzata.
- In un utente non ancora inizializzato, un messaggio informa sulla situazione e l'[Inizializzazione Guidata Rapida](#) può essere avviata. In [modalità server](#) un messaggio informa sulla situazione solo se l'utente corrente è un membro del Gruppo di Iscrizione dell'Utente e l'[Inizializzazione Guidata Rapida](#) può essere avviata.

Pulsanti:

- I pulsanti indicati di seguito sono disattivati se Infineon Security Platform è disabilitato o non ancora configurato, oppure se l'utente connesso non è stato inizializzato.
- L'abilitazione di alcune funzioni dipende dalle [impostazioni dei criteri utente](#).

La tabella seguente descrive tutte le funzioni relative alle impostazioni utente.

Pulsante	Spiegazione
<input type="checkbox"/> <i>Cambia...</i>	<p>Cliccare su questo pulsante per cambiare la password utente di base.</p> <p> L'archivio contenente i dati di ripristino di emergenza viene aggiornato automaticamente in modo da riportare le modifiche della password.</p>
<input type="checkbox"/> <i>Configura...</i>	Cliccare su questo pulsante per configurare le seguenti

	<p>funzionalità:</p> <ul style="list-style-type: none"> • Protezione della posta elettronica • Crittografia di file e cartelle con Encrypting File System (EFS) e Personal Secure Drive (PSD) • Autenticazione avanzata <p>A seconda dello stato di configurazione delle funzionalità dell'utente, saranno avviate l'Inizializzazione Guidata Rapida o l'Inizializzazione Utenti Guidata.</p>
<input type="checkbox"/> <i>Gestione...</i>	<p>Cliccare su questo pulsante per visualizzare, importare o eliminare i certificati protetti da Security Platform.</p> <p>Viene avviato il Visualizzatore certificati di Infineon Security Platform.</p>
<input type="checkbox"/> <i>Abilita/Disabilita...</i>	<p>In base allo stato attuale di Infineon Security Platform, è possibile eseguire una delle operazioni descritte di seguito. Disabilita: sospende il funzionamento di Infineon Security Platform fino a quando il sistema non viene riavviato. Le applicazioni progettate per utilizzare Security Platform non potranno più accedere ai dati protetti da Trusted Platform Module, come i dati crittografati con EFS, Personal Secure Drive e altri. L'accesso ai dati protetti viene ripristinato abilitando nuovamente Security Platform.</p> <p>Abilita: se si sceglie di abilitare Infineon Security Platform, viene chiesto di riavviare il sistema.</p> <p>Questo pulsante è disattivato se la funzione è stata bloccata nelle impostazioni dei criteri utente.</p> <p>Questa funzione non è disponibile per i sistemi Security Platform che utilizzano Trusted Platform Module 1.2.</p>



Soluzione Infineon Security Platform - Tool di configurazione

Backup di Infineon Security Platform

In questa pagina è possibile eseguire le operazioni di backup e ripristino delle credenziali e delle impostazioni di Security Platform e Personal Secure Drive. Se è abilitata l'[Autenticazione avanzata](#), è anche possibile creare i file di backup del dispositivo di autenticazione.



Pulsanti:

- I pulsanti per le attività di amministrazione sono disabilitati se l'utente non dispone dei diritti amministrativi richiesti.
- I pulsanti vengono disabilitati se le corrispondenti funzioni non sono disponibili nello stato attuale di Security Platform.

La tabella seguente descrive le funzioni di backup e ripristino.

Pulsante	Spiegazione
<input type="checkbox"/> <i>Configura...</i>	<p>Cliccare su questo pulsante per impostare il backup automatico di Security Platform. Viene avviata l'Inizializzazione guidata di Infineon Security Platform.</p> <p> <ul style="list-style-type: none">• Questa funzionalità è disponibile unicamente se l'account utente attuale dispone dei diritti amministrativi necessari.• Questo pulsante è disabilitato in modalità server, poiché il backup automatico è gestito dal Trusted Computing Management Server, ovvero nessuna configurazione esplicita è necessaria qui da parte dell'utente.</p>
<input type="checkbox"/> <i>Ripristina tutti...</i>	<p>Cliccare qui per ripristinare le impostazioni e le credenziali di Security Platform da un Archivio di backup del sistema. Può essere inoltre eseguito un Ripristino Recupero di Emergenza. È anche possibile eseguire il ripristino da un file compresso scritto manualmente se non è presente un file compresso di backup del sistema. In questo caso il Ripristino Recupero di Emergenza è possibile solo se il file compresso scritto manualmente comprende i dati corrispondenti. Se si dispone già di backup dei file di immagine, della propria</p>

Personal Secure Drive è anche possibile ripristinarli. In questo caso è possibile sia ripristinare un file di immagine per una PSD già configurata o impostare una nuova PSD per utilizzare il file di immagine ripristinato.

Viene avviato il [Backup guidato di Infineon Security Platform](#) relativamente alle operazioni di ripristino.



- Il pulsante è disattivato se Infineon Security Platform è disattivato o se l'utente non dispone dei diritti di amministratore.
- Questo pulsante è disabilitato in [modalità server](#), poiché il ripristino dal backup di sistema è gestito dal Trusted Computing Management Server, ovvero non è necessaria alcuna configurazione esplicita da parte dell'utente.

Backup...

Cliccare su questo pulsante per avviare il backup manuale delle impostazioni e delle credenziali di Security Platform. Se si sono impostate Personal Secure Drive è anche possibile effettuare il backup.

Viene avviato il [Backup guidato di Infineon Security Platform](#).



- Questo pulsante è disattivato se Infineon Security Platform è disattivato o non ancora installato.
- In [modalità server](#), è solo possibile eseguire il backup delle Personal Secure Drive. A parte le condizioni menzionate precedentemente, questo pulsante è disabilitato se il Personal Secure Drive (PSD) non è configurato.

Ripristina...

Cliccare su questo pulsante per avviare il ripristino manuale delle impostazioni e delle credenziali di Security Platform archiviate.

Se si dispone già di backup dei file di immagine della propria Personal Secure Drive è anche possibile ripristinarli. In questo caso è possibile sia ripristinare un file di immagine per una PSD già configurata o impostare una nuova PSD per utilizzare il file di immagine ripristinato.

Viene avviato il [Backup guidato di Infineon Security Platform](#)

relativamente alle operazioni di ripristino.



- Questo pulsante è disattivato se Infineon Security Platform è disattivato o non ancora installato.
- Nella modalità [autonoma](#), è possibile eseguire il Ripristino di emergenza se si dispone dei diritti di amministrazione.
- A parte le condizioni sopra menzionate, in [modalità server](#), questo pulsante è disabilitato se l'utente non è inizializzato e se il Personal Secure Drive (PSD) non è configurato.

Crea...

Cliccare su questo pulsante per creare il file di backup del dispositivo di autenticazione.



Questa funzionalità è disponibile unicamente se è abilitata l'[Autenticazione avanzata](#).



Infineon Security Platform Solution - Tool di configurazione

Migrazione di Infineon Security Platform

Questa operazione consente di copiare e trasferire le credenziali di protezione degli utenti da una piattaforma sorgente a una piattaforma di destinazione. In base alla configurazione attuale del sistema, l'utente di Infineon Security Platform può trasferire le proprie chiavi e i propri certificati da o verso l'installazione locale di Infineon Security Platform.

Questa funzionalità è presente nella Migrazione guidata di Infineon Security Platform.



Disponibilità della pagina:

- Questa pagina è disponibile soltanto se Security Platform è già stato inizializzato.
- Questa pagina non è disponibile in [modalità server](#), poiché la migrazione di credenziali di sicurezza specifiche dell'utente da una piattaforma fonte ad una piattaforma di destino è gestita dal Trusted Computing Management Server, ovvero l'amministratore o l'utente nel sistema cliente locale non deve eseguire questo compito.

[La migrazione passo dopo passo](#)

La tabella seguente illustra le funzioni disponibili per la migrazione.

Pulsante	Spiegazione
<input type="checkbox"/> <i>Ulteriori informazioni...</i>	Cliccare su questo pulsante per visualizzare la Guida contenente istruzioni dettagliate per eseguire la migrazione.
<input checked="" type="radio"/> <i>Questa è la piattaforma sorgente</i>	Selezionare questa opzione se si desidera esportare le credenziali a partire dalla piattaforma attuale. Le operazioni disponibili dalla piattaforma sorgente possono essere eseguite mediante i pulsanti Esporta... e Autorizza....
<input type="checkbox"/> <i>Esporta...</i>	Esporta le chiavi e i certificati utente verso la piattaforma di destinazione. Questa operazione viene eseguita dalla funzionalità di esportazione disponibile nella Migrazione guidata di Infineon Security Platform . La piattaforma di destinazione deve essere autorizzata dal relativo proprietario prima dell'esportazione. Il pulsante è disabilitato se si verifica una delle seguenti

	<p>situazioni:</p> <ul style="list-style-type: none"> • Infineon Security Platform è disabilitato. • Infineon Security Platform non è stato inizializzato. • L'utente di Infineon Security Platform non è stato configurato.
<input type="checkbox"/> <i>Autorizza...</i>	<p>Ogni migrazione delle chiavi e dei certificati utente da una piattaforma Infineon Security Platform a un'altra richiede l'autorizzazione della piattaforma sorgente da parte del proprietario di Infineon Security Platform. Selezionando questo pulsante viene visualizzata la finestra di autorizzazione.</p> <p> Il pulsante è disabilitato se si verifica una delle seguenti situazioni:</p> <ul style="list-style-type: none"> • Infineon Security Platform è disabilitato. • Infineon Security Platform non è stato inizializzato. • L'utente attuale non dispone dei diritti amministrativi richiesti.
<input checked="" type="radio"/> <i>Questa è la piattaforma di destinazione</i>	<p>Selezionare questa opzione se si desidera importare le credenziali nella piattaforma attuale. Le operazioni disponibili dalla piattaforma di destinazione possono essere eseguite mediante i pulsanti Importa... e Salva...</p>
<input type="checkbox"/> <i>Importa...</i>	<p>Importa le chiavi e i certificati utente dalla piattaforma sorgente. Questa operazione viene eseguita dalla funzionalità di importazione disponibile nella Migrazione guidata di Infineon Security Platform.</p> <p> Il pulsante è disabilitato se si verifica una delle seguenti situazioni:</p> <ul style="list-style-type: none"> • Infineon Security Platform è disabilitato. • Infineon Security Platform non è stato inizializzato.
<input type="checkbox"/> <i>Salva...</i>	<p>Le informazioni di migrazione possono essere salvate su file e</p>

quindi importate nella piattaforma di destinazione. Tali informazioni vengono salvate in formato XML. Questo è il primo passo per eseguire la migrazione di una chiave utente.



Il pulsante è disabilitato se si verifica una delle seguenti situazioni:

- È cambiato il proprietario di Infineon Security Platform (il proprietario è indicato alla pagina [Informazioni](#)).
- Infineon Security Platform non è inizializzato ma è presente un Proprietario di Infineon Security Platform.
- Le Chiavi Utente di Base dell'Amministratore che ha effettuato l'accesso in Infineon Security Platform non corrispondono al Proprietario di Infineon Security Platform.
- Infineon Security Platform è disabilitato.



Infineon Security Platform Solution - Tool di configurazione

Reimpostazione della password di Infineon Security Platform

Questa pagina consente di eseguire tutte le attività necessarie per configurare ed effettuare la reimpostazione delle password utente di base.



Disponibilità della pagina:

- In [modalità autonoma](#), questa pagina è disponibile soltanto se Security Platform è già stato inizializzato.

Pulsanti:

- I pulsanti per le attività di amministrazione sono disabilitati se l'utente non dispone dei diritti amministrativi richiesti.
- I pulsanti vengono disabilitati se le corrispondenti funzioni non sono disponibili nello stato attuale di Security Platform. Ad esempio, se la Reimpostazione della Password non è ancora stata configurata dall'amministratore, non può essere abilitata e la Reimpostazione della Password non può essere eseguita.
- In [modalità server](#) il Trusted Computing Management Server gestisce il compito di creare un Token per il Reset della Password per tutti gli utenti, abilitando al Reset della Password e preparando e fornendo il Codice di Autorizzazione al Reset della Password per utente specifico, ovvero l'amministratore o l'utente non deve eseguire questo compito. Di conseguenza tutti i pulsanti tranne *Reset* sono disabilitati.

La tabella seguente illustra le funzioni di reimpostazione delle password.

Pulsante	Spiegazione
<input type="checkbox"/> <i>Configura...</i>	Cliccare su questo pulsante per creare un token di reimpostazione della password per tutti gli utenti. L'operazione richiede diritti amministrativi appropriati.
<input type="checkbox"/> <i>Abilita...</i>	Cliccare su questo pulsante per abilitare la reimpostazione della password per l'utente attuale. Questa operazione è possibile unicamente se la reimpostazione è stata precedentemente configurata dall'amministratore.
<input type="checkbox"/> <i>Prepara...</i>	Questo pulsante consente di predisporre e definire il codice di

	autorizzazione per la reimpostazione della password di un dato utente. È anche possibile predisporre e reimpostare la password per il proprio account in un'unica operazione. Entrambe le opzioni richiedono diritti amministrativi appropriati.
<input type="checkbox"/> <i>Reimposta...</i>	Cliccare su questo pulsante per reimpostare la password utente di base per l'account attuale. L'operazione è possibile unicamente se la reimpostazione della password è stata correttamente predisposta per l'account in uso.



Infineon Security Platform Solution - Inizializzazione utenti guidata

BitLocker

Con questa pagina puoi usare la Crittografia unità BitLocker insieme al Trusted Platform Module per crittografare i dati nel tuo disco. La configurazione del BitLocker è eseguita con l'Applet del Pannello di Controllo del BitLocker Microsoft.



Disponibilità della pagina:

- Questa pagina è disponibile solo se il sistema operativo supporta la crittografia unità BitLocker (es. le edizioni Enterprise e Ultimate di Windows 7 e Windows Vista) e l'utente corrente dispone dei diritti amministrativi.
- Questa pagina non è disponibile in [modalità server](#).

La seguente tavola descrive le funzioni del BitLocker.

Pulsante	Informazioni
 <i>Stato Attuale...</i>	Stato attuale della Crittografia unità BitLocker. Stati possibili: <i>Configurato, Non Configurato, Riconfigurazione necessaria, Crittografato, Decrittografato.</i>
 <i>Configura...</i>	Clicca qui per avviare l'Applet del Pannello di Controllo del BitLocker Microsoft.  Questo pulsante è disabilitato se il Trusted Platform Module non è Inizializzato.



©Infineon

Technologies AG

Infineon Security Platform Solution - Inizializzazione utenti guidata

Impostazioni avanzate di Infineon Security Platform

In questa pagina è possibile configurare le impostazioni relative al proprietario di Security Platform e ai criteri di protezione.

Le impostazioni che possono essere modificate sono limitate al computer locale.

Le [impostazioni dei criteri](#) sono contenute nel file modello dei criteri di Infineon Security Platform.



Disponibilità della pagina:

- Questa pagina viene visualizzata unicamente se l'utente attuale dispone dei diritti amministrativi richiesti.
- Questa pagina non è disponibile in [modalità server](#).

Pulsanti:

- I pulsanti per la gestione dei criteri utente e dei criteri di sistema non sono disponibili nelle edizioni di Windows che non supportano Gestione Criteri di gruppo, ad es. le edizioni Home di Windows.
- I pulsanti vengono disabilitati se le corrispondenti funzioni non sono disponibili nello stato attuale di Security Platform.

La tabella seguente illustra le funzioni avanzate disponibili.

Pulsante	Informazioni
<input type="checkbox"/> <i>Modifica...</i>	<p>Cliccare su questo pulsante per cambiare la password del proprietario di Security Platform (vedi Modifica Password Proprietario).</p> <p> <ul style="list-style-type: none">• Questa funzione non è disponibile se Infineon Security Platform è disabilitato o non è stato inizializzato• In modalità server questa caratteristica non è disponibile, poiché la Security Platform è inizializzata automaticamente se il sistema del cliente è integrato in un Trust Domain con gestione centralizzata.</p>
<input type="checkbox"/> <i>Configura...</i>	<p>Cliccare su questo pulsante per configurare le seguenti funzionalità:</p>

- Backup automatico (comprende il ripristino di emergenza)
- Reimpostazione password
- Autenticazione avanzata
- Difesa da Attacchi a Dizionario

Viene avviata l'[Inizializzazione guidata di Infineon Security Platform](#).



- Questa funzione non è disponibile se Infineon Security Platform è disabilitato o non è stato inizializzato
- In [modalità server](#) questa caratteristica non è disponibile, poiché Reset della Password e Backup e Ripristino sono gestiti dal Trusted Computing Management Server.
- Si noti che la funzionalità *Difesa da Attacchi a Dizionario* è disponibile solo su Security Platform con Infineon Trusted Platform Module 1.2, se il criterio [configurazione soglia attacchi a dizionario](#) non è configurata.



Abilita/Disabilita...

Cliccare su questo pulsante per abilitare o disabilitare Security Platform.

In base allo stato attuale del software, è possibile eseguire l'una o l'altra operazione. In entrambi i casi, è richiesta la password del proprietario.

Disabilitare Infineon Security Platform: le applicazioni progettate per utilizzare Security Platform non potranno più accedere ai dati protetti da Trusted Platform Module, come i dati crittografati con EFS, Personal Secure Drive e altri. L'accesso ai dati protetti viene ripristinato soltanto quando Security Platform è nuovamente abilitato.



In un sistema che supporta la Crittografia unità BitLocker (ad esempio, Windows Vista Enterprise o Ultimate), se disabiliti la Security Platform, mentre il BitLocker è acceso, il sistema operativo ti chiederà di inserire la Password BitLocker al riavvio del sistema.

Abilitare Security Platform nel BIOS: in alcune condizioni particolari della piattaforma, occorre abilitare Security Platform nel BIOS. Ad esempio, se si riavvia il sistema per rendere effettiva l'abilitazione ma Security Platform non viene comunque abilitato al termine del riavvio, è necessario procedere all'abilitazione nel BIOS (vedi [Attivazione Trusted Platform Module](#)).



- Questa funzionalità non è disponibile se Infineon Security Platform non è attivo nel BIOS.
- Questa funzionalità non è disponibile se Infineon Security Platform non è ancora inizializzato.
- In [modalità server](#) questa caratteristica non è disponibile perché l'abilitazione/disabilitazione del Trusted Platform Module da parte del Proprietario non è possibile in questa modalità.

Reimposta...

Fare clic qui per [azzerare](#) il livello di difesa da attacchi a dizionario.
SpTPMWz.exe dell'Inizializzazione Guidata di Security Platform viene avviato con il parametro linea di comando *-resetattack*.



- Questo pulsante è disponibile solo su Security Platform con un Trusted Platform Module 1.2.
- In [modalità server](#) questo è l'unico utilizzo consentito dell'Inizializzazione Guidata di Security Platform.

Sistema...

Questo pulsante consente di gestire le impostazioni dei criteri di sistema.
Viene avviata l'utilità [Amministrazione dei criteri di sistema](#) di Infineon Security Platform.



- I criteri non sono disponibili nelle edizioni di Windows che non supportano Gestione Criteri di gruppo, ad es. le edizioni Home di

	<p>Windows.</p> <ul style="list-style-type: none">• In modalità server questa caratteristica non è disponibile, poiché un amministratore locale non deve configurare e gestire le impostazioni dei criteri. I criteri sono configurati in tutto il dominio da un amministratore di dominio attraverso il Trusted Computing Management Server.
<p><input type="checkbox"/> <i>Utente...</i></p>	<p>Questo pulsante consente di gestire le impostazioni dei criteri utente. Selezionando il pulsante, viene avviata l'utilità Amministrazione dei criteri utente di Infineon Security Platform.</p> <p> • I criteri non sono disponibili nelle edizioni Home di Windows.</p> <ul style="list-style-type: none">• In modalità server questa caratteristica non è disponibile, poiché un amministratore locale non deve configurare e gestire le impostazioni dei criteri. I criteri sono configurati in tutto il dominio da un amministratore di dominio attraverso il Trusted Computing Management Server.



Infineon Security Platform Solution - Inizializzazione utenti guidata

Modificare la Password Proprietario

Attraverso questo dialogo è possibile modificare la Password Proprietario.



Disponibilità del dialogo:

- Questo dialogo è disponibile solo nella pagina *Avanzato* di Tool di Configurazione.
- Questo dialogo non è disponibile in [modalità server](#) poiché le Password Proprietario sono gestite da Trusted Computing Management Server.

Prendere nota dei suggerimenti generali riguardanti la [gestione delle password](#).

La seguente tabella fornisce dei suggerimenti sull'uso di questo dialogo:

Elemento Dialogo	Spiegazione
<input type="password"/> <i>Vecchia Password</i>	Digitare qui la vecchia Password Proprietario. È possibile digitare la password o fornire un file di Backup della Password Proprietario. Per garantire che la Password Proprietario inserita manualmente soddisfi i principali requisiti di qualità, prendere in considerazione le regole base per la gestione delle password .
<input type="checkbox"/> <i>Da File...</i>	Fare clic qui per fornire un file di Backup della Password Proprietario se la Password Proprietario è stata salvata in un file di backup e non si desidera digitare la password.
<input type="password"/> <i>Nuova password</i>	Digitare qui la nuova Password Proprietario. È possibile digitare la password o generare una password casuale.
<input type="checkbox"/> <i>Casuale</i>	Fare clic qui per generare una Password Proprietario casuale anziché digitare una nuova password. In questo modo è possibile assicurarsi l'utilizzo di una password sicura che soddisfi i requisiti di lunghezza e complessità delle password .

	 Assicurarsi di rendere visibile, stampare o salvare la password casuale prima di chiudere il dialogo.
 <i>Conferma nuova password</i>	Inserire nuovamente la password per confermare (non è necessario se si è generata una nuova password casuale).
<input type="checkbox"/> <i>Su file...</i>	Fare clic qui per salvare la nuova Password Proprietario in un file di backup. Sarà possibile utilizzare questo file per l'autenticazione del Proprietario anziché digitare la password.
<input type="checkbox"/> <i>Stampa...</i>	Fare clic su questo pulsante per stampare la nuova Password Proprietario.  Accertarsi di conservare questa stampa in un luogo sicuro.
<input checked="" type="checkbox"/> <i>Nascondi password</i>	Eliminare la selezione da questa casella di controllo se si desidera visualizzare le password.

 Si noti che in base ai criteri di [Attivazione della protezione rigorosa del campo password](#) potrebbe non essere consentito tagliare, copiare, incollare e visualizzare le password non crittografate.



Infineon Security Platform Solution - Inizializzazione Guidata Rapida

Inizializzazione GUIDATA Rapida

L'Inizializzazione GUIDATA Rapida di Infineon Security Platform si rivolge alla maggior parte degli utenti che desiderino inizializzare rapidamente Security Platform e Utente con le impostazioni predefinite. Queste operazioni sono necessarie per attivare la funzionalità di Infineon Security Platform e per fornire una base per tutte le ulteriori attività su Infineon Security Platform.

Se si desidera eseguire l'inizializzazione di Security Platform e Utente utilizzando le impostazioni avanzate, si consiglia di utilizzare invece [Inizializzazione GUIDATA di Security Platform](#) e [Inizializzazione Utenti GUIDATA di Security Platform](#).



Disponibilità della procedura guidata:

- Questa procedura guidata richiede diritti di amministratore finché non viene eseguita l'inizializzazione di Security Platform.
- Se l'inizializzazione di Security Platform è già stata eseguita, la procedura guidata eseguirà unicamente le attività di configurazione specifiche dell'utente, che non richiedono diritti di amministratore.
- L'uso di questa procedura guidata può essere controllato con il [criterio Inizializzazione Rapida Controllo](#).
- Le fasi di inizializzazione della piattaforma di questa procedura guidata sono disponibili solo se il [criterio Permettere Iscrizione Piattaforma](#) è attivato con l'opzione *Permettere Gestione provider e procedura guidata*, o se questo criterio non è configurato (si applicano le stesse condizioni se si avvia questa procedura guidata dall'[Icona di Notifica della Barra delle Applicazioni](#)). Questo criterio diventa effettivo solo se Security Platform non è inizializzato prima.
- Le fasi di inizializzazione dell'utente di questa procedura guidata sono disponibili solo se il [criterio Permettere Iscrizione Utente](#) è attivato con l'opzione *Permettere Gestione provider e procedura guidata*, o se questo criterio non è configurato (si applicano le stesse condizioni se si avvia questa procedura guidata dall'[Icona di Notifica della Barra delle Applicazioni](#)). Questo criterio diventa effettivo solo se gli utenti non sono ancora inizializzati.
- Le fasi di inizializzazione piattaforma di questa procedura guidata non sono disponibili in [modalità server](#) poiché Security Platform si inizializza automaticamente se il sistema del cliente è integrato in un Trust Domain a gestione centralizzata.

Pagine e Fasi Procedura Guidata

Pagina/Fase	Commento
1. Benvenuto	Selezione inizializzazione rapida o avanzata.
2. Impostazioni	Configurazione Security Platform specifica dell'utente: Encrypting File System (EFS), Personal Secure Drive (PSD), Password Utente di Base (se l'Utente Security Platform non è ancora inizializzato).
3. Riepilogo	Conferma delle impostazioni e fasi necessarie procedura guidata.
4. Completamento	Panoramica stato completamento procedura guidata. Accesso al file protocollo e ai dati privati generati.
5. File Protocollo	Visualizzazione, stampa e salvataggio file protocollo.
6. Dati Privati	Visualizzazione dati privati generati.

Se Trusted Platform non è attualmente attivo, si consiglia di attivarla prima di impostare la propria piattaforma (vedi [Attivazione Trusted Platform Module](#)).

Se Trusted Platform dispone già di un Proprietario ma è ancora stata effettuata l'inizializzazione sul sistema operativo attuale, è necessaria l'autenticazione del Proprietario (vedi [Password Utente](#)).

Avvio dell'applicazione

Solo se Security Platform non è stato inizializzato:

Dall' [Icona di Notifica della Barra delle Applicazioni](#), fare clic sull'articolo menu [Inizializzazione Security Platform](#).

Se Security Platform è già inizializzato e l'utente corrente non è inizializzato o è inizializzato ma non sono state configurate le funzionalità EFS e PSD:

Dall' [Icona di Notifica della Barra delle Applicazioni](#), fare clic sull'articolo menu [Inizializzazione Utenti Security Platform](#).



©Infineon Technologies AG

Soluzione Infineon Security Platform - Inizializzazione Guidata Rapida

Benvenuto

Questa pagina di procedura guidata vi chiede se desiderate eseguire un'inizializzazione rapida o un'inizializzazione avanzata.

Inizializzazione Rapida

Inizializzazione rapida, consigliata per la maggior parte degli utenti, unisce l'inizializzazione della piattaforma e dell'utente con posizioni dei file di dati e impostazioni delle funzionalità predefinite. Le fasi specifiche della piattaforma vengono eseguite automaticamente senza alcun intervento dell'utente. Alcuni dati e file privati necessari a fini amministrativi e in caso di emergenza vengono generati automaticamente.

Salvataggio di dati e file privati generati automaticamente

Si consiglia di utilizzare un supporto rimovibile (es. unità flash USB) per salvare i [dati e file privati](#) generati automaticamente. Se non è disponibile alcun supporto rimovibile, i dati di output devono essere salvati sul disco rigido locale. Ciò richiede una protezione dati aggiuntiva. Di conseguenza, sarà necessario memorizzare o salvare i dati privati aggiuntivi che non sono necessari se si salvano i dati su un supporto rimovibile.

Inizializzazione Avanzata

L'inizializzazione avanzata, consigliata per gli utenti esperti, avvia l'[Inizializzazione Guidata di Security Platform](#) per eseguire le fasi di configurazione specifiche della piattaforma. A partire dal completamento della procedura guidata è possibile continuare con le fasi di configurazione specifiche dell'utente attraverso l'[Inizializzazione Utenti Guidata di Security Platform](#).

L'inizializzazione avanzata permette la configurazione avanzata dei dati privati, delle posizioni dei file di dati e delle funzionalità.

Scegliere questo tipo di inizializzazione se si desidera utilizzare l'[Autenticazione Avanzata](#) o [BitLocker](#), o se si vuole creare una [Personal Secure Drive \(PSD\)](#) su un supporto rimovibile (es. unità flash USB).



©Infineon Technologies AG

Infineon Security Platform Solution - Inizializzazione Guidata Rapida

Impostazioni

Attraverso questa pagina è possibile configurare le impostazioni specifiche dell'utente di Security Platform.



Disponibilità delle funzionalità:

- Questa pagina di procedura guidata è disponibile solo se il criterio *Permettere l'Iscrizione dell'Utente* è attivato con l'opzione *Permettere Gestione provider e procedura guidata*.
- La funzione EFS non è supportata nelle edizioni Home di Windows.
- La configurazione di EFS potrebbe essere bloccata dal criterio utente [Permettere configurazione EFS](#).
- La configurazione della PSD potrebbe essere bloccata dal criterio utente [Permettere configurazione PSD](#).
- Per riconfigurare queste funzionalità, fare clic su [Tool di Configurazione – Impostazioni utente - Configurare...](#)

La seguente tabella fornisce una spiegazione delle Funzionalità di Security Platform.

Funzionalità	Informazioni
<input checked="" type="checkbox"/> <i>Encrypting File System (EFS) basato sull'hardware</i>	<p>EFS fa parte della tecnologia di protezione del file system NTFS. Con EFS è possibile crittografare i propri file e cartelle. Security Platform Solution amplia la protezione di EFS proteggendo l'accesso alle chiavi di crittografia EFS con il Trusted Platform Module.</p> <p>Se si seleziona questa casella di controllo, l'Inizializzazione Guidata Rapida attiverà EFS, creerà una cartella crittografata <i>Documents\Dati Crittografati</i> o <i>Documenti\Dati Crittografati</i> (a seconda del sistema operativo) e creerà un collegamento dal desktop a questa cartella.</p> <p>Per ulteriori informazioni su EFS</p>
<input checked="" type="checkbox"/> <i>Personal Secure Drive (PSD)</i>	<p>PSD è un'unità crittografata presente nel computer. Appare come qualsiasi altra unità disco rigido. L'accesso ai file e alle cartelle della PSD avviene come per le altre unità. L'unica differenza è che il contenuto della PSD è completamente</p>

	<p>crittografato ed accessibile solo dopo aver caricato esplicitamente la PSD. Il caricamento della PSD richiede l'autenticazione utente. I dati della PSD sono salvati nel file di immagine PSD.</p> <p>Se si seleziona questa casella di controllo, l'Inizializzazione Guidata Rapida creerà una PSD e un collegamento dal desktop alla PSD. Il file di immagine della PSD sarà creato nella partizione del sistema, nella cartella <i>Security Platform</i> (a meno che il percorso non sia impostato mediante il criterio Posizione File per Personal Secure Drive).</p> <p>Per ulteriori informazioni su PSD</p>
<p> Password della chiave utente di base</p>	<p>Impostare la Password Utente di Base necessaria per l'utilizzo delle Funzionalità di Security Platform.</p>

Quando utilizzare EFS o PSD?

La seguente tabella paragona EFS e PSD. Fornisce inoltre dei suggerimenti sui casi in cui utilizzare le due funzionalità.

Criteri	EFS	PSD
<i>Tipo Crittografia</i>	Basata sui file e sulle cartelle: i file e le cartelle divisi vengono crittografati.	Basata sulla periferica: tutti i file contenuti nell'unità vengono crittografati.
<i>Sistemi Operativi Supportati</i>	Sistemi operativi supportati da Security Platform Solution, ad eccezione delle edizioni Home di Windows.	Tutti i sistemi operativi supportati da Security Platform Solution.
<i>Accesso e Gestione Dati</i>	Sempre visibili. Crittografia e decrittografia sono possibili solo dopo l'autenticazione dell'utente. Crittografia e decrittografia sono bloccate dopo il logout da EFS. Inoltre i diritti di accesso al file	Visibile e accessibile solo dopo il caricamento dell'unità (è necessaria l'autenticazione dell'utente). La PSD può essere scaricata esplicitamente. Inoltre possono essere impostati i

	system NTFS possono essere impostati se si desidera condividere dei file.	diritti di accesso al sistema NTFS.
<i>Recupero Dati</i>	Attraverso gli Agenti Dati EFS.	<ul style="list-style-type: none"> • Su sistemi operativi che supportano EFS: Attraverso gli Agenti Dati EFS. • Su sistemi operativi che non supportano EFS: Attraverso gli Agenti Recupero dati PSD.
<i>Condivisione Dati</i>	Possono essere condivisi tra numerosi utenti aggiungendo il certificato dell'altro utente.	Nessuna possibilità di condivisione dati, utente singolo.
<i>Posizione Dati</i>	Unità locali o cartelle web, file system NTFS.	Supporto rimovibile o disco rigido locale.
<i>Backup Dati</i>	Attraverso qualsiasi metodo o software per l'esecuzione del backup.	Attraverso Backup Security Platform Solution .
<i>Quando utilizzare EFS o PSD</i>	Se i dati da crittografare si trovano in cartelle speciali (es. <i>Documenti</i> o cartelle di dati specifiche dell'applicazione).	<ul style="list-style-type: none"> • Se il sistema operativo in uso è una edizione Home di Windows e pertanto non supporta EFS. • Se i dati da crittografare si trovano su un'unità rimovibile che si desidera utilizzare su diversi computer. In modalità server, Personal Secure Drive su un supporto rimovibile può essere trasferito liberamente. In modalità autonoma è necessario eseguire la migrazione delle credenziali e delle impostazioni o eseguire il

ripristino oppure aggiungere il backup del file di immagine.

- Se i dati da crittografare si trovano nel file system FAT32.



Infineon Security Platform Solution - Inizializzazione Guidata Rapida

Riepilogo

La pagina di riepilogo elenca le fasi che saranno eseguite.

Le fasi necessarie dipendono dalla piattaforma e dallo stato utente corrente. Ad esempio, su Security Platform già inizializzata, le fasi specifiche della piattaforma vengono ignorate e vengono eseguite solo le fasi specifiche dell'utente.



Per l'inizializzazione e la configurazione di Security Platform possono essere necessari alcuni minuti. In particolare la creazione di un'unità PSD di grandi dimensioni potrebbe impiegare un tempo prolungato.



©Infineon Technologies AG

Soluzione Infineon Security Platform - Inizializzazione Guidata Rapida

Completamento

La pagina di completamento mostra i risultati di tutte le fasi di inizializzazione e configurazione. È possibile trovare informazioni dettagliate nel file protocollo della procedura guidata. Fare clic su *Dettagli...* per accedere al file protocollo.



A seconda della piattaforma e dello stato dell'utente precedenti e della selezione della posizione in cui salvare l'output della procedura guidata, la procedura guidata potrebbe aver creato dei dati privati. Ciò è necessario a fini amministrativi e in caso di emergenza. In particolare se non è stato selezionato un supporto rimovibile (es. unità flash USB) per salvare l'output della procedura guidata è necessario stampare, salvare o memorizzare i dati privati in ogni caso prima di finalizzare la procedura guidata. A questo fine, fare clic su *Dettagli*.

Opzioni Avanzate

Se si desidera modificare le proprie impostazioni specifiche dell'utente o utilizzare le funzionalità aggiuntive, selezionare **Continuare con le opzioni avanzate**. In questo caso, l'[Inizializzazione Utenti Guidata](#) avviata una volta finalizzata la procedura guidata.



©Infineon

Technologies AG

Soluzione Infineon Security Platform - Inizializzazione Guidata Rapida

File Protocollo

Questo dialogo mostra il protocollo di tutte le fasi eseguite dalla procedura guidata.

Elementi delle finestre di dialogo	Spiegazione
<input type="checkbox"/> <i>Stampa...</i>	Fare clic qui per stampare il file protocollo. È possibile decidere se si desidera includere i dati privati generati necessari a fini amministrativi e in caso di emergenza nella stampa del protocollo.
<input type="checkbox"/> <i>Salva...</i>	Fare clic qui per salvare il file protocollo. È possibile decidere se si desidera includere i dati privati generati necessari a fini amministrativi e in caso di emergenza nel protocollo da salvare.  La versione del protocollo priva di dati privati è stata già salvata automaticamente (<i>SpProtocol_<PCName>_<UserName>.txt</i> fper utenti locali) o (<i>SpProtocol_<PCName>_<UserName>.<DomainName>.txt</i> per utenti dominio). Il percorso del file protocollo salvato automaticamente è mostrato in questo dialogo.
<input type="checkbox"/> <i>Visualizza</i>	Fare clic qui per visualizzare i dati privati generati.  La quantità e il tipo di dati privati dipende dalla piattaforma e dallo stato dell'utente precedenti e dalla selezione della posizione in cui salvare l'output della procedura guidata. Se la piattaforma era stata inizializzata prima dell'avvio della procedura guidata e si è selezionato un supporto rimovibile (es. unità flash USB) per salvare l'output della procedura guidata non sarà creato alcun dato privato.
	Al completamento della procedura guidata non ci sarà più possibilità di accedere ai dati privati generati. Assicurarsi di averli stampati, salvati o

archiviati con successo in qualsiasi forma prima di finalizzare la procedura guidata. Ciò è importante in particolare se non è stato selezionato un supporto rimovibile (es. unità flash USB) per salvare l'output della procedura guidata.



©Infineon

Technologies AG

Soluzione Infineon Security Platform - Inizializzazione Guidata Rapida

Dati Segreti

Questo dialogo visualizza i dati privati generati.



Se non è stato selezionato un supporto rimovibile (es. unità flash USB) per salvare l'output della procedura guidata necessario stampare, salvare o memorizzare tutti i dati privati generati. Essi saranno necessari per eseguire determinate attività amministrative critiche e in caso di emergenza.

La quantità e il tipo di dati privati dipende dalla piattaforma e dallo stato dell'utente precedenti e dalla selezione della posizione in cui salvarli.

La seguente tabella fornisce i dettagli sui dati privati generati e sui file corrispondenti. Le etichette **USB** e **HD** indicano se i dati o i file privati interessati sono creati e salvati e se si è selezionato un supporto rimovibile (es. unità flash USB) o un disco rigido (**HD**) per salvare l'output della procedura guidata.

Tipo	Finalità	Ambito	File corrispondente
Password Proprietario (USB, HD)	Necessaria per eseguire attività amministrative critiche per Security Platform.	Specifico della piattaforma. Creato automaticamente durante le fasi di inizializzazione specifiche della piattaforma se la piattaforma non è stata ancora inizializzata all'avvio della procedura guidata.	File di Backup Password Proprietario (USB) Nome file Predefinito: <i>SpOwner_<PC>.tpm</i> dove <i><PC></i> è il nome piattaforma. Creato e salvato solo se selezionato un supporto rimovibile (unità flash USB) per salvare l'output della procedura guidata. Non è necessario conoscere la Password Proprietario poiché è possibile utilizzare il File di Backup Password a partire dal supporto rimovibile (es. unità flash USB).
Password per Recupero di Emergenza/Token Reimpostazione Password (HD)	Protegge il Token combinato per Recupero di Emergenza /	Creato automaticamente durante le fasi di configurazione specifiche della	File combinato Recupero di Emergenza/Token Reimpostazione Password (USB, HD) Nome file predefinito: <i>SpToken_<PC>.xml</i>

	Reimpostazione Password necessari per eseguire un Recupero di Emergenza e la reimpostazione della Password Utente di Base.	piattaforma se non è stato selezionato un supporto rimovibile (es. unità flash USB) per salvare l'output della procedura guidata e la piattaforma non è inizializzata all'avvio della procedura guidata.	dove <PC> è il nome Questo token non necessita password dedicata se si utilizza un supporto rimovibile (es. USB).
Segreto Reimpostazione Password (USB, HD)	Segreto personale di un utente, necessario per reimpostare la sua Password Utente di Base.	Specifico dell'utente. Creato automaticamente durante le fasi di configurazione specifiche dell'utente se l'utente non è stata ancora inizializzato all'avvio della procedura guidata.	Segreto Reimpostazione (USB) Nome file predefinito: <i>SpPwdResetSecret_<PC></i> dove <PC> è il nome e <User> è il nome utente (locali) o una combinazione di nome utente e nome di dominio. Creato e salvato solo se è stato selezionato un supporto rimovibile (es. unità flash USB) per salvare l'output della procedura guidata. Se la procedura guidata non è necessaria conoscere la Password Utente di Base. È possibile utilizzare il File di Recupero di Emergenza per la Reimpostazione Password Utente di Base se si utilizza un supporto rimovibile (es. USB).

Suggerimenti generali sulla gestione dei dati privati: Vedi [Gestione Password](#).



Infineon Security Platform Solution - Inizializzazione guidata

Inizializzazione guidata di Infineon Security Platform

L'inizializzazione Guidata di Infineon Security Platform si rivolge agli utenti esperti che desiderino inizializzare Security Platform e configurare le Funzionalità di Security Platform (backup compreso Recupero di Emergenza, Reimpostazione Password, Autenticazione Avanzata, BitLocker). Queste operazioni sono necessarie per attivare la funzionalità di Infineon Security Platform e per fornire una base per tutte le ulteriori attività su Infineon Security Platform.

Se si desidera eseguire l'inizializzazione rapida di Security Platform e Utente utilizzando le impostazioni predefinite, si consiglia di utilizzare invece [Inizializzazione Guidata Rapida](#).

È anche possibile ripristinare un'installazione di Security Platform danneggiata, invece di iniziarne una nuova, selezionando *Ripristina Security Platform da un archivio di backup*.

Questa è la prima procedura guidata che deve essere eseguita per configurare correttamente Infineon Security Platform.



Disponibilità della procedura guidata:

- Questa procedura guidata è disponibile solo se l'utente attuale ha diritti amministrativi.
- Questa procedura guidata è disponibile solo se È abilitato il criterio *Consenti iscrizione piattaforma* con l'opzione *Consenti la gestione dell'interfaccia e del wizard* oppure tale criterio non è stato configurato (Le stesse condizioni sono applicate se la procedura guidata è avviata da [Icona TNA](#)). Questo criterio diventa effettivo solo se Security Platform non è inizializzato prima.
- Se Security Platform è stato inizializzato precedentemente, questo criterio non è attivo e è possibile utilizzare questa procedura guidata per configurare le funzionalità di Security Platform (le stesse condizioni sono applicate se la procedura guidata è avviata da [Icona TNA](#)).
- La procedura guidata non è disponibile in [modalità server](#), poiché la Security Platform è inizializzata automaticamente se il sistema cliente è integrato nel Trust Domain con gestione centralizzata.

Fasi Procedura Guidata

Operazione	Commento
1. Abilitazione di Trusted Platform Module	Solo se Trusted Platform Module non è attualmente abilitato.
2. Inizializzazione o ripristino	Solo se Security Platform non è stato inizializzato.
3. Configurazione della proprietà oppure Password del proprietario	Solo se Security Platform non è stato inizializzato. In base allo stato attuale di Security Platform, è possibile impostare o convalidare la password del proprietario.
4. Funzionalità	Backup comprendente il ripristino di emergenza, reimpostazione della password e autenticazione avanzata.
5. Backup	Solo se è stata selezionata la funzionalità <i>Backup</i> .
6. Ripristino di emergenza	Solo se è stata selezionata la funzionalità <i>Backup</i> .
7. Reimpostazione password	Solo se è stata selezionata la funzionalità <i>Reimpostazione password</i> .
8. BitLocker	<p>Solo se la caratteristica <i>BitLocker</i> è stata selezionata. Solo se lo stato del <i>BitLocker</i> è <i>Configurato</i>, <i>Riconfigurazione necessaria</i>, <i>Crittografato</i> o <i>Decrittografato</i>.</p> <p> • Questa funzionalità è disponibile solo se il sistema operativo supporta la crittografia unità BitLocker (ad es. le edizioni Enterprise o Ultimate di Windows 7 e Windows Vista).</p> <p>• Questa pagina non è disponibile in modalità server. Tuttavia, è possibile configurare BitLocker attraverso l'applet</p>

	del pannello di controllo di Microsoft BitLocker.
9. Autenticazione avanzata	Solo se Security Platform era già inizializzato all'avvio della procedura guidata. Solo se è stata selezionata la funzionalità <i>Autenticazione avanzata</i> .
10. Difesa da Attacchi a Dizionario	Disponibile solo su Security Platform con un Infineon Trusted Platform Module 1.2. Solo se la funzionalità <i>Difesa da Attacchi a Dizionario</i> è stata selezionata.

Avvio dell'applicazione

Solo se Security Platform non è stato inizializzato: [Dall'Icona di Notifica della Barra delle Applicazioni](#), fare clic sull'articolo menu **Inizializzazione Security Platform**. [Inizializzazione Guidata Rapida](#) si avvierà. Nella pagina di Benvenuto, selezionare **Inizializzazione Avanzata**. Inizializzazione Guidata Security Platform sarà avviata.

Se Security Platform è già stato inizializzato: avviare l'Inizializzazione guidata di Infineon Security Platform tramite il Tool di configurazione.

- Per configurare le funzionalità di Security Platform (backup comprendente il ripristino di emergenza, reimpostazione password e autenticazione avanzata): [Tool di configurazione - Avanzate - Configura...](#)
- Per configurare soltanto la funzionalità di reimpostazione della password: [Tool di configurazione - Reimpostazione password - Configura...](#)
- Per configurare soltanto la funzionalità di backup: [Tool di configurazione - Backup - Configura...](#)



Soluzione Infineon Security Platform - Inizializzazione guidata

Abilitato Trusted Platform Module

Il Trusted Platform Module deve essere abilitato per attivare la funzionalità principale. Solo successivamente la Security Platform può essere inizializzata e le successive operazioni di configurazione iniziale possono essere eseguite. La procedura per l'attivazione del Trusted Platform Module dipende dalla versione di Trusted Platform Module, dall'hardware Security Platform e dal BIOS.

Su **sistemi Trusted Platform Module 1.2 che supportano l'Interfaccia Presenza Fisica (PPI)** questa interfaccia è utilizzata per attivare Trusted Platform Module. A seconda dell'hardware e della BIOS questo può essere fatto senza l'interazione dell'utente, oppure può essere necessario eseguire alcuni passi aggiuntivi.

Su **tutti gli altri sistemi** bisognerà riavviare ed entrare nel sistema BIOS. Una descrizione su come abilitare il chip è disponibile qui:

Comunque la procedura guidata scopre automaticamente come abilitare il Trusted Platform Module sul tuo sistema e ti guida di conseguenza.

La tavola seguente mostra come abilitare il Trusted Platform Module su diversi tipi di Security Platform.

Tipo di Security Platform	Pulsante	Informazioni
Trusted Platform Module 1.2 PPI richiede il riavvio	<input type="checkbox"/> <i>Riavviare</i>	Il sistema è riavviato. Al riavvio seguire le istruzioni nella schermata di avvio per abilitare il Trusted Platform Module.
Trusted Platform Module 1.2	<input type="checkbox"/> <i>Chiudi</i>	Il sistema è spento e deve essere riavviato manualmente.

PPI richiede l'arresto	<i>sessione</i>	All'avvio del sistema seguire le istruzioni nella schermata di avvio per abilitare il Trusted Platform Module.
Trusted Platform Module 1.2 PPI non richiede l'avvio o l'arresto	<input type="checkbox"/> <i>Abilitato</i>	La <i>Physical Presence Interface</i> è utilizzata per attivare il Trusted Platform Module. Non è necessario riavviare o arrestare il sistema.  A seconda del sistema, potrebbero essere necessari alcuni passi ulteriori per abilitare il Trusted Platform Module. Per ulteriori informazioni controllare il manuale di sistema.
Tutti gli altri tipi (es. Trusted Platform Module 1.1 e/o PPI non supportata)	<input type="checkbox"/> <i>Riavviare</i>	Il sistema è riavviato e il Trusted Platform Module deve essere abilitato nella BIOS del Sistema.



Nota sul riavvio e sullo spegnimento del sistema:

Tutte le applicazioni aperte sono chiuse senza ulteriori indicazioni. Per evitare la perdita di dati, tutte le applicazioni devono essere chiuse prima che il sistema sia riavviato.



Infineon Security Platform Solution - Inizializzazione guidata

Inizializzazione o ripristino di Security Platform

In questa pagina della procedura guidata, viene chiesto se si desidera inizializzare o ripristinare Security Platform.



Questa pagina di procedura guidata non è disponibile in [modalità server](#), poiché la Security Platform è inizializzata automaticamente se il sistema cliente è integrato in un Trust Domain con gestione centralizzata, ovvero l'amministratore non deve eseguire questo compito.

Elementi della pagina	Spiegazione
⦿ <i>Inizializzazione della Security Platform</i>	Cliccare su questo pulsante per configurare una nuova installazione di Security Platform. In questo caso, verranno create nuove credenziali della piattaforma e degli utenti.
⦿ <i>Ripristino della Security Platform da un Archivio di Backup</i>	Cliccare su questo pulsante per ripristinare Security Platform in caso di errore, sostituzione o reimpostazione dell'hardware, del supporto di archiviazione o di Trusted Platform Module. L'operazione di ripristino consente di ristabilire l'accesso alle funzionalità di Security Platform.



Soluzione Infineon Security Platform - Inizializzazione guidata

Creazione del proprietario di Security Platform

Dopo aver abilitato Trusted Platform Module, è necessario impostare la proprietà della piattaforma. Questa operazione consente di associare il chip al computer in un'unica operazione. Durante questa operazione viene creato il Proprietario Infineon Security Platform che viene salvato nell' Trusted Platform Module assieme al segreto Proprietario Infineon Security Platform. Esso è protetto dalla [Password Proprietario](#) che deve essere definita qui. È possibile digitare la Password Proprietario o generare una Password Proprietario casuale. È possibile salvare la Password Proprietario in un file e utilizzare questo file di backup con la Password Proprietario o anche stamparla. Se si è optato per la generazione di una Password Proprietario casuale, è anche possibile renderla visibile per poterla memorizzare o annotare. Per amministrare Security Platform sono necessari la Password Proprietario o il file di backup con la Password Proprietario.



Questa pagina di procedura guidata non è disponibile in [modalità server](#), poiché la Security Platform è inizializzata automaticamente se il sistema cliente è integrato in un Trust Domain con gestione centralizzata, ovvero l'amministratore non deve eseguire questo compito.



L'acquisizione della proprietà durante l'Inizializzazione guidata di Security Platform crea una nuova chiave principale di archiviazione (SRK, Storage Root Key). Di norma, il proprietario di Security Platform viene impostato una volta sola per un determinato Trusted Platform Module. Poiché tutti i certificati a chiave pubblica sono vincolati alla chiave SRK di Trusted Platform Module, non sarà più possibile utilizzarli con la nuova chiave di archiviazione generata.

La tabella seguente fornisce alcuni suggerimenti per l'utilizzo della procedura guidata.

Elementi della pagina	Spiegazione
 Password	Impostare qui una Password Proprietario. È possibile digitare manualmente una Password Proprietario o generare una Password Proprietario casuale.  Per garantire che la Password Proprietario digitata

	<p>manualmente soddisfi i principali requisiti di qualità, dovrebbe essere presa in considerazione una serie di regole base per il trattamento della password.</p>
<input checked="" type="checkbox"/> <i>Conferma password</i>	<p>Inserire nuovamente la password per confermare (non è necessario se si è generata una password casuale).</p>
<input type="checkbox"/> <i>Casuale</i>	<p>Fare clic qui per generare una Password Proprietario casuale anziché digitare una nuova password. In questo modo è possibile essere certi di utilizzare una password sicura che soddisfi i requisiti di lunghezza e complessità.</p> <p> Accertarsi di rendere visibile, stampare o salvare la password casuale prima di continuare.</p>
<input type="checkbox"/> <i>In File...</i>	<p>Fare clic qui per salvare la nuova Password Proprietario in un file di backup. Sarà possibile utilizzare questo file per l'utenticazione del Proprietario anziché digitare la password.</p>
<input type="checkbox"/> <i>Stampa...</i>	<p>Fare clic su questo pulsante per stampare la Password Proprietario.</p> <p> Accertarsi di conservare la stampa in un luogo sicuro.</p>
<input checked="" type="checkbox"/> <i>Nascondere password</i>	<p>Eliminare la selezione di questa casella di controllo se si desidera visualizzare le password.</p>

 Si noti che a causa del criterio [Attivazione protezione rigorosa campo password](#) potrebbe non essere consentito tagliare, copiare, incollare e visualizzare le password.



Infineon Security Platform Solution - Inizializzazione guidata

Password del proprietario

La [Password Proprietario](#) è necessaria per eseguire attività amministrative critiche per Security Platform.

Questa pagina è visualizzata nell'[Inizializzazione Guidata di Security Platform](#) e nell'[Inizializzazione Guidata Rapida](#), se la Password Proprietario è già presente ma in assenza dell'inizializzazione di Security Platform.

Ciò si verifica nelle seguenti circostanze:

- Se la Password Proprietario è stata impostata attraverso l'applicazione [Microsoft Gestione Trusted Platform Module \(TPM\)](#).
- Quando l'inizializzazione di Security Platform è stata interrotta, ad esempio a causa di un calo di corrente o per altri motivi.
- Quando Security Platform è inizializzato ma il proprietario è stato definito su un altro sistema operativo.
- Quando Security Platform è stato inizializzato su un determinato sistema operativo e si tenta di inizializzare la piattaforma da un sistema operativo diverso accedendo al BIOS.

Per effettuare l'autenticazione, è possibile digitare la password o fornire un File di Backup della Password Proprietario.



Questa pagina non è disponibile in [modalità server](#), poiché la Security Platform è inizializzata automaticamente se il sistema cliente è integrato in un Trust Domain con gestione centralizzata, ovvero l'amministratore non deve eseguire questo compito.

In particolare, la password del proprietario viene richiesta nei seguenti casi:



Questa pagina di gestione non è disponibile nella [modalità server](#). Security Platform è inizializzata automaticamente se il client system è integrato in uno Trust Domain colla gestione centralizzata, i.e. l'amministratore non debba eseguire questa operazione.



Infineon Security Platform Solution - Inizializzazione guidata

Funzionalità di Security Platform

In questa pagina è possibile configurare le funzionalità di Security Platform, come ad esempio il backup, per tutti gli utenti.



Questa pagina di procedura guidata non è disponibile in [modalità server](#), poiché il Trusted Computing Management Server gestisce il compito di configurare le caratteristiche della Security Platform, ovvero *Backup*, *Reset della Password* ed *Autenticazione Avanzata*. La funzionalità *BitLocker* può essere configurata mediante l'applet del pannello di controllo Microsoft.

La tabella seguente illustra tutte le funzionalità di Security Platform.

Funzionalità	Informazioni
<input checked="" type="checkbox"/> <i>Backup automatico (comprende il ripristino di emergenza)</i>	<p>Selezionare questa funzionalità se si desidera configurare il backup automatico di Security Platform. Si consiglia di configurare sempre la funzionalità di <i>backup</i>. In caso contrario, qualora si verificassero gravi errori, potrebbero andare perduti tutti i dati degli utenti.</p> <p> Non è possibile deselezionare questa funzionalità se è abilitato il criterio Imponi la configurazione del backup includendo il ripristino di emergenza.</p>
<input checked="" type="checkbox"/> <i>Reimpostazione password</i>	<p>Selezionare questa funzionalità se si desidera creare un token di reimpostazione della password per tutti gli utenti. Si consiglia di configurare sempre la funzionalità di <i>Reimpostazione password</i>. In caso contrario, non sarà possibile reimpostare le password utente di base.</p> <p> Non è possibile deselezionare questa funzionalità se è abilitato il criterio Imponi la configurazione della reimpostazione password. Tale funzionalità può essere configurata soltanto una volta. La selezione è disabilitata se la <i>Reimpostazione password</i> è già stata configurata.</p>
<input checked="" type="checkbox"/> <i>BitLocker</i>	Controlla questa caratteristica se vuoi usare il Crittografia

	<p>unità BitLocker insieme al Trusted Platform Module per crittografare dati sul tuo disco.</p> <p> Questa funzionalità è disponibile solo se il sistema operativo supporta la crittografia unità BitLocker (ad es. le edizioni Enterprise o Ultimate di Windows 7 e Windows Vista).</p>
<p><input checked="" type="checkbox"/> <i>Autenticazione avanzata</i></p>	<p>Selezionare questa funzionalità se si desidera abilitare l'Autenticazione avanzata per tutti gli utenti oppure modificare la selezione dei dispositivi di autenticazione.</p> <p> Tale funzionalità è disponibile unicamente se è installato almeno un plug-in per l'Autenticazione avanzata. Questa funzionalità non è disponibile se Security Platform non era inizializzato prima dell'avvio della procedura guidata.</p>
<p><input checked="" type="checkbox"/> <i>Difesa da Attacchi a Dizionario</i></p>	<p>Verificare questa funzionalità, se si desidera configurare il numero di tentativi di autenticazione dovrebbero essere consentiti per i diversi tipi di autenticazione prima che siano adottate misure di difesa da attacchi a dizionario. Vedere Configurazione Impostazioni di Difesa da Attacchi a Dizionario.</p> <p> Si noti che questa funzionalità è disponibile solo su Security Platform con Infineon Trusted Platform Module 1.2, se il criterio Configurazione soglia attacchi a dizionario non è configurata. Questa funzionalità non è disponibile se Security Platform non era inizializzato prima dell'avvio della procedura guidata.</p>



Infineon Security Platform Solution - Inizializzazione guidata

Backup

Questa pagina consente di configurare il backup automatico di Security Platform. Vedere [Dati di Security Platform di Backup e Ripristino](#).



Questa pagina non è disponibile in [modalità server](#), poiché il Backup automatico è eseguito dal Trusted Computing Management Server, ovvero nessuna configurazione esplicita è necessaria da parte dell'utente.

La tabella seguente fornisce alcuni suggerimenti per l'utilizzo della procedura guidata.

Elementi della pagina	Spiegazione
<input type="text"/> <i>Percorso backup:</i> <input type="text"/> <i>Sfoglia...</i>	<p>Le credenziali e le impostazioni di Security Platform verranno salvate periodicamente in un archivio di backup.</p> <p>Immettere il percorso e il nome del file oppure ricercare il file desiderato. Verrà creato automaticamente un archivio di backup costituito da un file XML e da una cartella con lo stesso nome, ad esempio, file SPSystemBackup.xml nella cartella SPSystemBackup.</p> <p> Utilizzare l'estensione *.xml.</p>
<input type="checkbox"/> <i>Pianifica...</i>	<p>Consente di pianificare le operazioni di backup.</p> <p>Cliccare su questo pulsante per visualizzare e modificare la pianificazione esistente.</p> <p> Il backup automatico non viene eseguito se il PC è spento all'ora pianificata per l'esecuzione dell'operazione.</p> <p>L'account utente prescelto per il backup pianificato deve appartenere al gruppo "Amministratori" o "Backup Operators".</p>



Infineon Security Platform Solution - Inizializzazione guidata

Ripristino di emergenza

Questa pagina consente di configurare il ripristino di emergenza come parte delle procedure di backup automatico di Security Platform.



Disponibilità della pagina:

- questa pagina è disponibile unicamente se si è scelto di configurare il backup automatico di Security Platform.
- Questa pagina non è disponibile in [modalità server](#), poiché il Backup e il Ripristino automatico sono gestiti dal Trusted Computing Management Server, ovvero nessuna configurazione esplicita è necessaria da parte dell'utente.

Elementi della pagina



Si noti che il contenuto di questa pagina della procedura guidata può essere limitato dall'impostazione di alcuni [criteri di sistema](#).

La tabella seguente fornisce alcuni suggerimenti per l'utilizzo della procedura guidata.

Elementi della pagina	Spiegazione
☉ <i>Crea un nuovo token di ripristino</i>	Selezionare questa opzione se si desidera creare un nuovo token per il ripristino di emergenza. Il token verrà salvato nel percorso specificato. È necessario impostare la password di protezione del nuovo token.
☉ <i>Utilizza il token di ripristino esistente</i>	Selezionare questa opzione soltanto se sono soddisfatte le condizioni indicate di seguito. <ul style="list-style-type: none">• Si desidera ripristinare il sistema, in caso di necessità, utilizzando un token di ripristino di emergenza creato precedentemente.• Il token e la relativa password sono correntemente accessibili. È necessario verificare la password del token, ovvero immetterla una volta.
📄 <i>Percorso file</i> 🔍 <i>Sfoggia...</i>	Se le impostazioni attuali dei criteri di protezione consentono di specificare manualmente la posizione del file, è possibile modificarne il percorso e il nome. Immettere il percorso e il nome del file oppure ricercare il file desiderato. Il file è in formato XML.  Se è stata selezionata l'opzione <i>Crea nuovo token di ripristino</i> , occorre salvare il token di ripristino di emergenza in una posizione sicura, come un supporto rimovibile archiviato in un ambiente protetto. Non salvare il token di ripristino sul disco rigido. Infatti, in caso di errori di sistema o dell'unità, non sarà più possibile accedere al token, con la

	<p>conseguente perdita di dati. Archiviare il token di ripristino su un supporto di backup, come un'unità di memoria o un CD-ROM, per evitare che altri utenti possano accedervi.</p>
<p> <i>Password</i></p>	<p>Se è stata selezionata l'opzione <i>Crea nuovo token di ripristino</i>, occorre impostarne la password. Immettere quindi la password di protezione per il token di ripristino di emergenza. Consultare la sezione Suggerimenti generali in merito alla selezione delle password.</p> <p>Se è stata selezionata l'opzione <i>Utilizza il token di ripristino esistente</i>, occorre convalidarne la password. Immettere quindi la password del token esistente.</p> <p>Se è stata selezionata l'opzione <i>Utilizza l'archivio di ripristino esistente</i>, non è necessario specificare nessuna password.</p>
<p> <i>Conferma password</i></p>	<p>Se è stata selezionata l'opzione <i>Crea nuovo token di ripristino</i>, occorre confermarne la password specificata in precedenza. Immettere nuovamente la password per confermarla.</p>



Infineon Security Platform Solution - Inizializzazione guidata

Reimpostazione password

In questa pagina è possibile creare il token di reimpostazione della password per tutti gli utenti.



Disponibilità della pagina:

- questa pagina è disponibile soltanto se si è scelto di configurare la reimpostazione delle password.
- Questa pagina non è disponibile in [modalità server](#) poiché quest'attività è gestita da Trusted Computing Management Server.

Elementi della pagina

 Si noti che il contenuto di questa pagina della procedura guidata può essere limitato dall'impostazione di alcuni [criteri di sistema](#).

La tabella seguente fornisce alcuni suggerimenti per l'utilizzo della procedura guidata.

Elementi della pagina	Spiegazione
<input checked="" type="radio"/> <i>Crea un nuovo token</i>	Selezionare questa opzione se si desidera creare un nuovo token per la reimpostazione della password. Il token verrà salvato nel percorso specificato. È necessario impostare la password di protezione del nuovo token.
<input checked="" type="radio"/> <i>Utilizza un token esistente</i>	Selezionare questa opzione soltanto se sono soddisfatte le condizioni indicate di seguito. <ul style="list-style-type: none">• Si desidera reimpostare le password utilizzando un token creato in precedenza.• Il token e la relativa password sono correntemente accessibili. È necessario verificare la password del token, ovvero immetterla una volta.
<input type="text" value="Percorso file"/> <input type="button" value="Sfogli..."/>	Se le impostazioni attuali dei criteri di protezione consentono di specificare manualmente la posizione del file, è possibile modificarne il percorso e il nome. Immettere il percorso e il nome del file oppure ricercare il file desiderato. Il file è in formato XML.  Se è stata selezionata l'opzione <i>Crea nuovo token</i> , occorre salvare il token di reimpostazione della password in una posizione sicura, come un supporto rimovibile archiviato in un ambiente protetto. Non salvare il token sul disco rigido. Infatti, in caso di errori di sistema o dell'unità, non sarà più possibile accedere al token e quindi reimpostare le password utente di base. Archiviare il token su un supporto di backup,

	come un'unità di memoria o un CD-ROM, per evitare che altri utenti possano accedervi.
 <i>Password</i>	<p>Se è stata selezionata l'opzione <i>Crea nuovo token</i>, occorre impostarne la password. Immettere la password di protezione per il token di reimpostazione password. Consultare la sezione Suggerimenti generali in merito alla selezione delle password.</p> <p>Se è stata selezionata l'opzione <i>Utilizza un token esistente</i>, occorre convalidarne la password. Immettere quindi la password del token esistente.</p> <p>Se è stata selezionata l'opzione <i>Utilizza un archivio esistente</i>, non è necessario specificare nessuna password.</p>
 <i>Conferma password</i>	Se è stata selezionata l'opzione <i>Crea nuovo token</i> , occorre confermare la password specificata in precedenza. Immettere nuovamente la password per confermarla.



Infineon Security Platform Solution - Inizializzazione guidata

BitLocker

Con questa pagina puoi usare la Crittografia unità BitLocker insieme al Trusted Platform Module per crittografare i dati nel tuo disco.



Disponibilità della pagina:

- Questa pagina è disponibile solo se il sistema operativo supporta la crittografia unità BitLocker (ad es. le edizioni Enterprise o Ultimate di Windows 7 e Windows Vista).
- Questa pagina è disponibile solo se lo stato del BitLocker è *Configurato*, *Riconfigurazione necessaria*, *Crittografato* o *Decrittografato* e questa caratteristica è selezionata dall'utente.
- Questa pagina non è disponibile quando lo stato del BitLocker è "*Non Configurato*" poiché la prima configurazione del BitLocker richiede un riavvio del sistema. Invece l'Applet del Pannello di Controllo del BitLocker è avviato automaticamente dopo il completamento dell'Inizializzazione della Procedura Guidata.
- Questa pagina non è disponibile in [modalità server](#).

Elementi della pagina

La seguente tabella fornisce dei suggerimenti sul modo di utilizzo della pagina di procedura guidata.

Configura

Facendo click su questo pulsante si avvia l'Applet del Pannello di Controllo del BitLocker Microsoft.



©Infineon

Technologies AG

Infineon Security Platform Solution - Inizializzazione guidata

Autenticazione avanzata

In questa pagina è possibile abilitare l'Autenticazione avanzata per tutti gli utenti oppure modificare la selezione dei dispositivi di autenticazione.



Disponibilità della pagina:

- Questa pagina è disponibile soltanto in modalità [autonoma](#), se almeno uno plug-in di Autenticazione avanzata è installato.
- Questa pagina non è disponibile in modalità [server](#), poiché il Trusted Computing Management Server gestisce il compito di configurare l'Autenticazione Avanzata attraverso i criteri server, ovvero l'amministratore non deve eseguire questo compito.

La tabella seguente fornisce alcuni suggerimenti per l'utilizzo della procedura guidata.

Elementi della pagina	Spiegazione
<input type="checkbox"/> Elenco dei dispositivi di autenticazione	<p>Selezionare i dispositivi di autenticazione (uno o più) che si desidera abilitare per tutti gli utenti di Security Platform. Dopo aver abilitato i dispositivi, è possibile selezionare quello da utilizzare per l'autenticazione.</p> <p> • Per assicurarsi che gli utenti di Security Platform utilizzino realmente l'Autenticazione avanzata, abilitare il criterio utente Autenticazione avanzata obbligatoria.</p> <p>• In modalità autonoma, se il criterio Provider di autenticazione avanzata è impostato, soltanto i provider di autenticazione avanzata è indicato nel criterio sono disponibili per la configurazione. Ma se il criterio non è configurato, tutti i provider di autenticazione avanzata registrati saranno disponibili per la configurazione.</p>



Infineon Security Platform Solution - Inizializzazione utenti guidata

Inizializzazione utenti guidata di Infineon Security Platform

L'Inizializzazione Utenti Guidata di Infineon Security Platform si rivolge agli utenti esperti che desiderino inizializzare Utenti Security Platform e configurare le funzioni specifiche dell'utente (protezione e-mail, crittografia file e cartelle con EFS e PSD, Autenticazione Avanzata). Questa procedura guidata deve essere avviata per ciascun utente del computer che intenda utilizzare le Funzioni personalizzate di Infineon Security Platform (ovvero chi sarà Utente di Infineon Security Platform). Se si desidera eseguire l'inizializzazione rapida dell'Utente Security Platform utilizzando le impostazioni predefinite, si consiglia di utilizzare invece [Inizializzazione Guidata Rapida](#).



Disponibilità della procedura guidata:

- Questa procedura guidata è disponibile soltanto se è abilitato il criterio *Consenti l'iscrizione dell'utente* con l'opzione *Consenti la gestione dell'interfaccia e del wizard* oppure quando tale criterio non è stato configurato (stesse condizioni sono applicate se la procedura guidata è avviata da [Icona TNA](#)). Si noti che questo criterio è attivo solo per gli utenti ancora non inizializzati.
- Se l'utente è stato inizializzato precedentemente, questo criterio non è attivo e è possibile utilizzare questa procedura guidata per configurare le funzionalità specifiche (stesse condizioni sono applicate se la procedura guidata è avviata da [Icona TNA](#)).
- In [modalità server](#) questa procedura guidata è disponibile solo se l'utente attuale è membro del Gruppo Iscrizione Utenti.

Procedura guidata

La tabella seguente descrive la procedura guidata per gli utenti non ancora configurati. Se un utente è già stato configurato, sono richieste soltanto alcune operazioni specifiche della procedura guidata (come la configurazione delle funzionalità di Security Platform riservate agli utenti).

Operazione	Commenti
1. Dispositivo di autenticazione	<p>Solo se l'amministratore di Security Platform ha abilitato almeno un dispositivo di autenticazione. Solo per gli utenti non ancora configurati in Security Platform. Questa pagina è accessibile anche tramite le Funzionalità di Security Platform.</p> <p> Se è stata impostata l'Autenticazione avanzata e si utilizzano frasi password diverse per il dispositivo di autenticazione e per la piattaforma, verrà richiesto di sincronizzarle.</p>
2. Password utente di base	Solo per gli utenti non ancora configurati in Security Platform.
3. Reimpostazione della password utente di base	Disponibile solo se l'amministratore di Security Platform ha configurato la funzionalità di reimpostazione della password.
4. Funzionalità di Security Platform	Protezione della posta elettronica, crittografia di file e cartelle con EFS e PSD e autenticazione avanzata.
5. Richiesta certificato	Solo se è stata selezionata l'opzione <i>Protezione posta elettronica</i> o <i>Crittografia file e cartelle</i> (EFS o PSD).
6. Impostazioni per la protezione della posta elettronica	Solo se è stata selezionata la funzione <i>Protezione posta elettronica</i> .
7. Certificato di crittografia	Solo se è stata selezionata la funzione <i>Crittografia file e cartelle</i> (EFS o PSD).
8. Personal Secure	Solo se è stata selezionata la funzione <i>Crittografia di</i>

[Drive](#)

file e cartelle con Personal Secure Drive.

Avvio dell'applicazione

Se l'utente attuale non è ancora configurato: Dall'[Icona di Notifica della Barra delle Applicazioni](#), fare clic sull'articolo menu **Inizializzazione Utenti Security Platform**. [Inizializzazione Guidata Rapida](#) si avvierà. Nella pagina di Benvenuto, selezionare **Inizializzazione Avanzata**. Inizializzazione Utenti Guidata di Security Platform sarà avviata.

Se l'utente attuale è già stato configurato, avviare l'Inizializzazione utenti guidata tramite il Tool di configurazione.

- Per configurare le funzionalità specifiche di Security Platform per gli utenti (protezione della posta elettronica, crittografia di file e cartelle con EFS e PSD e autenticazione avanzata): [Tool di configurazione - Impostazioni utente - Configura...](#)

Fintantoché le funzionalità utente non sono configurate, si avvierà [l'Inizializzazione Guidata Rapida](#) anziché l'Inizializzazione Utenti Guidata. In questo caso, selezionare **Inizializzazione Avanzata** nella pagina di Benvenuto.

- Per abilitare la reimpostazione della password per l'utente attuale. [Tool di configurazione - Reimpostazione password - Abilita...](#)
- Per creare una copia di backup del dispositivo di autenticazione: [Tool di configurazione - Backup - Crea...](#)

Descrizione del parametro della riga di comando: la procedura guidata può essere avviata anche da Windows Explorer facendo doppio clic sul file *SpUserWz.exe*, nella directory di installazione di Security Platform Solution. È supportato il parametro della riga di comando indicato di seguito.

Parametro	Commenti
<i>-forceinit o /forceinit</i>	Forza la reinizializzazione dell'utente.  Con questa operazione, andranno perdute tutte le credenziali utente esistenti. Utilizzare il parametro della riga di comando unicamente se non è disponibile un archivio di backup.



Questo parametro di linea di comando non è supportato in [modalità server](#), poiché:

- L'utente non si troverà in una situazione in cui avrà bisogno di usare questo parametro.
- L'utente in un ambiente di Trust Domain non lo utilizza.



Infineon Security Platform Solution - Inizializzazione utenti guidata

Dispositivo di autenticazione

In questa pagina è possibile selezionare un dispositivo di autenticazione.



Disponibilità della pagina: questa pagina viene visualizzata unicamente se l'amministratore ha abilitato almeno uno dei dispositivi di autenticazione.

La tabella seguente fornisce alcuni suggerimenti per l'utilizzo della procedura guidata.

Elementi della pagina	Spiegazione
<input type="checkbox"/> Elenco dei dispositivi di autenticazione	<p>Selezionare il dispositivo di autenticazione che si desidera utilizzare.</p> <p>Se il criterio Autenticazione avanzata obbligatoria non è abilitato, è possibile specificare una <i>password</i>. Ciò significa che non si utilizza nessun dispositivo di autenticazione.</p> <p> È possibile selezionare un dispositivo di autenticazione diverso da quello attuale. Per farlo, è necessario modificare la <i>password</i>. Richiamare la procedura guidata per selezionare un altro dispositivo di autenticazione.</p>



Infineon Security Platform Solution -Inizializzazione utenti guidata

Sincronizza frase password utente di base

In questa pagina, è possibile specificare la modalità di sincronizzazione della frase password utente di base, nel caso in cui la frase utilizzata per il dispositivo di autenticazione non corrisponda a quella impostata per Security Platform.



Disponibilità della pagina: Questa pagina viene visualizzata soltanto se sono soddisfatte le condizioni indicate di seguito:

- È stata configurata l'Autenticazione avanzata.
- Il sistema ha rilevato frasi password diverse per il dispositivo di autenticazione e per Security Platform.

La tabella seguente fornisce alcuni suggerimenti per l'utilizzo della procedura guidata.

Elementi della pagina	Spiegazione
<input type="radio"/> <i>Usa frase password di Security Platform e aggiorna il dispositivo di autenticazione</i>	Selezionare questa opzione se si desidera aggiornare la configurazione del dispositivo di autenticazione impostando la frase password attualmente in uso per la piattaforma. Questa operazione è necessaria se la frase password è stata reimpostata senza aggiornare la configurazione del dispositivo di autenticazione.
<input type="radio"/> <i>Usa frase password del dispositivo di autenticazione e aggiorna Security Platform</i>	Selezionare questa opzione se si desidera aggiornare Security Platform impostando la frase password attualmente utilizzata dal dispositivo di autenticazione. È necessario selezionare questa opzione quando si utilizza lo stesso dispositivo di autenticazione per più installazioni di Security Platform e la frase password è stata modificata su un'installazione diversa da quella in uso.



Infineon Security Platform Solution - Inizializzazione utenti guidata

Reimpostazione della password utente di base

In questa pagina è possibile abilitare la reimpostazione della password utente di base (utile, ad esempio, quando si dimentica la password attuale).



Disponibilità della pagina: questa pagina viene visualizzata unicamente se l'amministratore ha configurato la reimpostazione delle password.

La tabella seguente fornisce alcuni suggerimenti per l'utilizzo della procedura guidata.

Elementi della pagina	Spiegazione
<input checked="" type="checkbox"/> <i>Abilita la reimpostazione della password utente di base in caso di necessità</i>	Selezionare questa casella di controllo per consentire che la password utente di base possa essere reimpostata in caso di necessità. Non è possibile deselezionare la casella di controllo se è abilitato il criterio Imponi l'abilitazione della reimpostazione password .
<input type="password"/> <i>Valore segreto personale</i> <input type="button" value="Sfoglia..."/>	Il valore segreto personale verrà scritto nel file specificato. Immettere il percorso e il nome del file oppure ricercare il file desiderato. Conservare il file in una posizione sicura. È indispensabile per reimpostare la password utente di base in caso di necessità.



Soluzione Infineon Security Platform - Inizializzazione utenti guidata

Conferma le tue impostazioni (fase 1)

L'amministratore del sistema può attivare una funzionalità specifica che consente di ripristinare le chiavi utente di base. In questo modo, verranno create voci aggiuntive nell'archivio di backup esistente.

Nota: la chiave utente di base viene sempre gestita in modo protetto, anche durante la procedura di ripristino.

Il sistema è pronto per generare la chiave utente di base. Nel caso in cui sia stata attivata la funzionalità di backup, verranno generati ulteriori dati di ripristino di emergenza, con le informazioni necessarie per ripristinare la chiave in tutta sicurezza.

Scegliere **Avanti** per generare la chiave utente di base.

Nota: non chiudere la sessione, né spegnere il computer o scollegare il cavo di alimentazione mentre l'operazione è in corso.

Technologies AG



Infineon Security Platform Solution -Inizializzazione utenti guidata

Funzionalità di Security Platform

In questa pagina è possibile configurare le funzionalità di Security Platform, come la crittografia di file e cartelle.



Disponibilità della pagina: questa pagina viene visualizzata unicamente se i criteri utente attuali consentono la configurazione di almeno una funzionalità.

Disponibilità delle funzionalità: dipende dalle [impostazioni dei criteri utente](#).

La tabella seguente illustra tutte le funzionalità di Security Platform.

Funzionalità	Informazioni
<input checked="" type="checkbox"/> <i>Posta elettronica protetta</i>	<p>Crittografia e/o firma dei messaggi di posta elettronica per evitare che persone non autorizzate possano leggere o modificare i propri messaggi. L'utilizzo di questa funzionalità garantisce che solo l'autore del messaggio e i destinatari selezionati possano decrittografare e leggere il testo inviato o convalidare l'identità del mittente.</p> <p>Se si sceglie di configurare questa funzione, è possibile richiedere un certificato di protezione della posta elettronica. (se l'indirizzo Web per la richiesta dei certificati è stato definito). La procedura guidata fornirà le informazioni necessarie per impostare la protezione della posta elettronica. La configurazione del client di posta elettronica non è compresa nella procedura guidata. Non è quindi possibile visualizzarne lo stato durante queste operazioni.</p>
<input checked="" type="checkbox"/> <i>Crittografia file e cartelle - Certificato di Crittografia</i>	<p>Selezionare questa funzionalità se si desidera visualizzare o modificare il proprio Certificato di Crittografia. Se si sceglie di configurare questa funzionalità è possibile selezionare un certificato. È inoltre possibile richiedere o creare un nuovo certificato.</p> <p> Il <i>Certificato di Crittografia</i> è visualizzato solo come funzionalità utente separata se EFS e PSD sono già configurati. La pagina del Certificato di Crittografia viene</p>

	visualizzata anche durante la prima configurazione di EFS o PSD.
<input checked="" type="checkbox"/> <i>Crittografia file e cartelle - Encrypting File System (EFS)</i>	<p>Il sistema operativo integra le funzionalità necessarie agli utenti per crittografare i contenuti di file e cartelle sul computer locale, utilizzando Microsoft Encrypting File System (EFS). In questo modo, l'accesso ai file contenuti nelle cartelle è consentito unicamente all'utente che ha creato i file stessi. Se si desidera consentire ad altri utenti di accedere alle cartelle EFS, occorre eseguire un'operazione amministrativa specifica per concedere i diritti di accesso e abilitare l'utilizzo dei file crittografati.</p> <p> la funzione EFS non è supportata nelle edizioni Home di Windows.</p>
<input checked="" type="checkbox"/> <i>Crittografia file e cartelle - Personal Secure Drive (PSD)</i>	<p>Personal Secure Drive consente di crittografare file e cartelle in modo simile a EFS. A differenza di EFS, PSD è supportato da tutti i sistemi operativi supportati da Security Platform Solution.</p> <p>PSD fornisce agli utenti autorizzati un'unità logica. Tale unità offre un sistema di crittografia e di protezione dell'accesso per tutti i suoi contenuti. La crittografia viene eseguita automaticamente. L'unità PSD non è accessibile, tramite l'identificatore UNC, per ottenere dati leggibili e può essere installata solo su un computer locale. Inoltre, l'unità PSD non consente l'accesso alla rete.</p> <p>Se si sceglie di configurare questa funzionalità è possibile gestire le proprie Personal Secure Drive.</p>
<input checked="" type="checkbox"/> <i>Autenticazione avanzata</i>	<p>Selezionare questa funzionalità per visualizzare o modificare le impostazioni di autenticazione. Se i criteri utente lo consentono, è possibile selezionare un dispositivo di autenticazione oppure l'Autenticazione password.</p> <p> Questa funzionalità è disponibile solo se l'amministratore ha abilitato almeno un dispositivo di autenticazione. Non è disponibile se l'account utente attuale non è stato configurato prima dell'avvio della procedura guidata.</p>

Riconfigurazione delle funzionalità: in alcuni casi particolari, può essere necessario riconfigurare una delle funzionalità del software. Vedere gli esempi descritti di seguito.

- Quando lo stato della *Crittografia file e cartelle - Certificato di Crittografia è Necessaria Riconfigurazione* è necessario risolvere prima questo aspetto. Se il certificato di crittografia non è valido o non è più disponibile, è possibile creare un nuovo certificato di crittografia o ripristinare le credenziali utente. Questo certificato è automaticamente reimpostato per EFS e/o PSD configurati.
- Se il certificato di crittografia non è disponibile e non si dispone del backup delle credenziali utente, è necessario creare un nuovo certificato di crittografia. Questo nuovo certificato verrà automaticamente reimpostato per l'EFS configurato. Ma questo certificato non può essere automaticamente reimpostato per la PSD configurata, di conseguenza è necessario cancellare la vecchia PSD e creare una nuova PSD con questo nuovo certificato di crittografia.
- Il certificato EFS o PSD non è valido o non è più disponibile. Questa condizione riguarda anche la funzione *Crittografia di file e cartelle con Encrypting File System (EFS)*, quando sono stati configurati sia Personal Secure Drive, che Encrypting File System e il certificato PSD è stato successivamente modificato.
- È stata eseguita un'operazione di ripristino ma l'unità PSD non è più accessibile (ad esempio, perché il file immagine PSD non è stato trovato).
- È stata configurata *Autenticazione avanzata* ma il dispositivo di autenticazione non è più disponibile oppure il tuo meccanismo di autenticazione e la tua Security Platform hanno Passphrase dell'Utente di Base diverse.



Infineon Security Platform Solution - Inizializzazione utenti guidata

Richiesta certificato

Le funzionalità di Infineon Security Platform specifiche per gli utenti richiedono l'utilizzo dei certificati. Tali certificati consentono agli utenti di comprovare la propria identità in forma elettronica. I certificati vengono generati esternamente e devono essere trasferiti in Infineon Security Platform tramite meccanismi predefiniti.



Disponibilità della pagina: questa pagina viene visualizzata unicamente se è stata selezionata almeno una delle funzionalità di protezione ed è abilitato il criterio di registrazione dei certificati ([URL di registrazione dei certificati durante la procedura guidata](#)). Contattare l'amministratore del sistema per ulteriori informazioni.

Elementi della pagina	Spiegazione
<input type="checkbox"/> <i>Richiedi certificato...</i>	<p>Mediante gli appositi criteri, l'amministratore di Infineon Security Platform ha imposto l'utilizzo di un certificato e ha definito il metodo di richiesta da seguire.</p> <p>Dopo aver selezionato il pulsante sopra indicato, viene visualizzata una pagina separata in cui è possibile registrare il certificato. Questa pagina è stata configurata dall'amministratore. Una volta completata la registrazione, continuare con le altre operazioni previste dalla procedura guidata.</p> <p> Tutte le applicazioni aperte vengono chiuse automaticamente senza preavviso. Per evitare la perdita di dati, è consigliabile chiudere tutte le applicazioni prima di riavviare il sistema.</p>

[Come registrare i certificati](#)



Infineon Security Platform Solution - Inizializzazione utenti guidata

Impostazioni per la protezione della posta elettronica

La funzionalità di protezione della posta elettronica consente di crittografare e/o firmare i messaggi di posta elettronica per impedire che vengano letti o modificati da persone non autorizzate. L'utilizzo di questa funzionalità garantisce che solo l'autore del messaggio e i destinatari selezionati possano decrittografare e leggere il testo inviato o convalidare l'identità del mittente.

La crittografia e la firma dei messaggi è supportata dalle applicazioni di posta elettronica più diffuse. Se si utilizza la funzione di protezione della posta elettronica, viene visualizzata una Guida per i client di posta elettronica supportati in cui è possibile trovare ulteriori informazioni.

Attualmente, sono supportati i seguenti client di posta elettronica:

- Microsoft Windows Mail/Outlook Express
- Microsoft Outlook 2003
- Microsoft Outlook XP
- Microsoft Outlook 2000
- Mozilla Thunderbird

È necessario configurare il client di posta elettronica per poter utilizzare il certificato digitale che viene protetto da Security Platform. Contattare l'amministratore del sistema per richiedere il certificato a un'Autorità di certificazione appropriata o a una delle autorità presenti in Internet.

Per ciascuno dei client di posta elettronica sopra indicati, è disponibile una Guida con informazioni dettagliate sulla configurazione. Per accedere alla Guida, utilizzare l'apposito pulsante.

Nota: se non si dispone di un certificato digitale per la protezione della posta elettronica, è necessario richiederlo prima di procedere con le operazioni di configurazione.

[Informazioni dettagliate](#)

Technologies AG



Infineon Security Platform Solution -Inizializzazione utenti guidata

Certificato di crittografia

Questa pagina vi permette di selezionare un certificato di crittografia da utilizzare per [EFS](#) e/o [PSD](#). Tale certificato è identificato tramite l'impronta digitale ed è sempre assegnato ad un Utente Infineon Security Platform in forma non ambigua.

Se non è attualmente registrato alcun certificato valido ma un altro certificato adatto è già disponibile, la procedura guidata offre automaticamente la possibilità di selezionare questo certificato. Se non è disponibile alcun certificato, la procedura guidata offre la possibilità di creare un nuovo certificato e di selezionarlo automaticamente.

Se non si desidera che la procedura guidata crei e/o selezioni automaticamente un certificato è anche possibile farlo manualmente.

La seguente tabella fornisce dei suggerimenti sul modo di utilizzo della pagina di procedura guidata.

Elemento Pagina Procedura Guidata	Informazioni
 <i>Certificato corrente</i>	È possibile trovare qui informazioni sul certificato di crittografia attualmente registrato (se è stato precedentemente selezionato un certificato).
 <i>Nuovo certificato</i>	È possibile trovare informazioni sul certificato di crittografia che sarà utilizzato in futuro (se un altro certificato diverso da quello corrente sarà utilizzato). Si può trattare di un certificato che verrà creato e/o selezionato automaticamente dalla procedura guidata o di un certificato creato e/o selezionato manualmente attraverso il pulsante <i>Modifica...</i>
 <i>Modifica...</i>	Fare clic su questo pulsante per creare e/o selezionare manualmente un certificato di crittografia. Verrà visualizzato il dialogo di Selezione Certificato .  Reimpostare dati crittografati esistenti: Si noti che il precedente certificato di crittografia è ancora necessario per decrittografare i dati crittografati

esistenti. Il processo di reimpostazioni necessario per utilizzare il nuovo certificato anche per i dati esistenti dipende dal sistema operativo in uso:

Su sistemi operativi che comprendono la procedura di reimpostazione guidata Encrypting File System Microsoft (ad es. Windows 7 e Windows Vista) è necessario eseguire la reimpostazione manuale.

Su tutti gli altri sistemi operativi, è necessario utilizzare lo strumento riga di comando "cipher.exe" o accedere ai file interessati per ottenerne la reimpostazione automatica.

Maggiori informazioni sono disponibili in Microsoft TechNet (cercare "procedura di reimpostazione assistita" o "cipher.exe").

 *Lunghezza chiave per nuovi certificati*

È possibile selezionare una lunghezza per la chiave dei nuovi certificati di crittografia, es. *1024 bit* o *2048 bit*.



Infineon Security Platform Solution - Inizializzazione Guidata Utente

Configurazione dell'Encrypting File System

Attraverso questa pagina di procedura guidata è possibile configurare un accesso facilitato ai vostri dati EFS crittografati. Si può inoltre tornare a Microsoft EFS senza protezione Security Platform.

La seguente tabella fornisce dei suggerimenti sul modo di utilizzo della pagina di procedura guidata.

Elemento Pagina Procedura Guidata	Spiegazione
<input checked="" type="checkbox"/> <i>EFS folder</i>	<p>Selezionare questa opzione per creare una cartella crittografata <i>Documents\Dati Crittografati</i> o <i>My Documents\Dati Crittografati</i> (a seconda del sistema operativo).</p> <p> Questa opzione non è sempre disponibile (ad es. se è già stata creata la cartella EFS oppure a causa delle impostazioni del file desktop.ini o a causa del file system FAT32).</p>
<input checked="" type="checkbox"/> <i>Collegamento dal desktop</i>	<p>Selezionare questa opzione se si desidera accedere alla <i>cartella EFS</i> attraverso un collegamento sul desktop.</p> <p> Se si elimina la selezione della casella di controllo una volta creato il <i>Collegamento dal desktop</i>, la procedura guidata eliminerà il collegamento esistente (purché non sia stato rinominato o spostato nel frattempo).</p>
<input type="checkbox"/> <i>Tornare...</i>	<p>Fare clic qui per tornare alla funzionalità EFS predefinita (Microsoft EFS) senza protezione Security Platform.</p> <p>Dopo essere tornati a Microsoft EFS, la crittografia dei file e delle cartelle funzionerà come segue:</p> <ul style="list-style-type: none">• Sarà possibile accedere a tutti i dati crittografati fintantoché il certificato EFS e la chiave saranno utilizzabili. Dopo essere ritornati a EFS, il primo

accesso ad un file crittografato con Security Platform Solution richiederà il certificato EFS, la chiave privata e l'[autenticazione utente](#). Una volta effettuato l'accesso al file sarà automaticamente re-crittografato con il nuovo certificato Microsoft EFS.

- I nuovi file saranno crittografati con Microsoft EFS compreso nel sistema operativo (senza protezione Security Platform).

Raccomandazione: [Decrittografare](#) i file EFS esistenti se non è possibile garantire che il certificato e la chiave privata EFS saranno utilizzati per tutto il tempo in cui si vorrà accedere ai file.



Questo pulsante è disponibile solo se è già stato precedentemente configurato EFS e si vuole eseguire nuovamente la configurazione.



©Infineon

Infineon Security Platform Solution

Personal Secure Drive

Attraverso le pagine di procedura guidata per Personal Secure Drive è possibile modificare le impostazioni di una Personal Secure Drive esistente, eliminare una Personal Secure Drive esistente o creare una nuova Personal Secure Drive. La configurazione della Personal Secure Drive fa parte dell'[Inizializzazione Utenti Guidata](#). Le relative pagine sono visualizzate se è stata selezionata funzionalità *Crittografia file e cartelle con Personal Secure Drive (PSD)*.

Fasi e Pagine Procedura Guidata

La seguente tabella illustra le fasi della procedura guidata e le pagine relative alla Personal Secure Drive.

Azione	Fasi/Pagine Procedura Guidata
Modificare le impostazioni di una PSD esistente	1. Gestione Personal Secure Drive 2. Modifica impostazioni Personal Secure Drive
Eliminare una PSD esistente	1. Gestione Personal Secure Drive 2. Eliminazione Personal Secure Drive
Creare una nuova PSD	1. Gestione Personal Secure Drive (solo se è presente almeno una PSD) 2. Specificazione di una lettera e di un'etichetta di unità per la Personal Secure Drive 3. Configurazione Personal Secure Drive



Infineon Security Platform Solution

Indicazione della lettera di unità e dell'etichetta di Personal Secure Drive

Attraverso questa pagina è possibile configurare la lettera e l'etichetta di unità della vostra Personal Secure Drive e le opzioni per il caricamento della PSD all'accesso e l'utilizzo di un collegamento sul desktop.

La seguente tabella fornisce dei suggerimenti sull'utilizzo della pagina di procedura guidata.

Elementi della pagina	Spiegazione
 Sarà eseguito il mapping della mia Personal Secure Drive nell'unità	Per specificare la lettera di unità da attribuire alla Personal Secure Drive, selezionare una lettera non utilizzata dall'elenco a discesa delle lettere disponibili (vedi Amministrazione Personal Secure Drive).
 Etichetta unità per la Personal Secure Drive	Per specificare l'etichetta dell'unità, inserire l'etichetta nel campo fornito. L'etichetta non dovrebbe superare la lunghezza di 32 caratteri. Ad esempio, si potrebbe utilizzare l'etichetta "La mia Secure Drive".
<input checked="" type="checkbox"/> Caricare Personal Secure Drive all'accesso	Selezionare questa opzione se si desidera caricare la propria PSD all'accesso.
<input checked="" type="checkbox"/> Creare collegamento sul desktop	Selezionare questa opzione se si desidera accedere alla PSD attraverso un collegamento sul desktop. Il nome del collegamento conterrà la lettera e l'etichetta di unità.



Infineon Security Platform Solution

Configurazione di Personal Secure Drive

Personal Secure Drive (PSD) funziona come una qualsiasi altra unità del sistema ma non è un'unità fisica vera e propria collegata al computer. Si tratta infatti di un file crittografato salvato su una delle unità locali del PC. Durante la configurazione di Personal Secure Drive, è necessario specificare le dimensioni del file e scegliere l'unità locale in cui salvarlo.

La seguente tabella fornisce dei suggerimenti su come utilizzare questa pagina di procedura guidata.

Elementi Dialogo	Spiegazione
<p> <i>Spazio di immagazzinamento</i></p>	<p>Per specificare le dimensioni dell'unità PSD, immettere il numero di megabyte (MB) di memoria da utilizzare nell'apposito campo oppure selezionare il valore desiderato utilizzando le frecce situate a destra del campo stesso.</p> <p>Anche le unità locali con supporti rimovibili (es. unità flash USB) sono supportate.</p> <p>La quantità di spazio sul disco necessaria è riservata su questa unità locale per uso esclusivo dalla Personal Secure Drive. Accertarsi che ci sia sufficiente spazio libero nell'unità locale per la vostra Personal Secure Drive.</p> <p> In modalità server, si consiglia di creare la PSD su un supporto rimovibile, se si desidera utilizzarla su più di una piattaforma (vedi Introduzione a Personal Secure Drive). In questo caso, utilizzare una lettera di unità disponibile in tutte le piattaforme.</p>
<p> <i>Selezionare l'unità in cui il file di immagine PSD dovrà essere salvato</i></p>	<p>Selezionare un'unità in cui il file di immagine PSD dovrà essere salvato.</p> <p> La selezione dell'unità è disattivata se il criterio Posizione File per Personal Secure Drive è impostato.</p>

Dimensione massima PSD

La dimensione di Personal Secure Drive non potrà più essere modificata successivamente, quindi si raccomanda di indicare un valore adatto alle proprie esigenze.

Si noti, inoltre, che non è possibile utilizzare tutto lo spazio dell'unità, poiché parzialmente occupato dal file system. Questo dipende dal sistema operativo e può avere un impatto significativo sulle unità minori. Anche il salvataggio di alcuni dati interni alla PSD riduce la dimensione massima della PSD.

Le dimensioni massime dell'unità PSD sono limitate, come indicato di seguito.

- Per i volumi FAT16, la dimensione massima dell'unità PSD è di 2 GB.
- Per i volumi FAT32, la dimensione massima dell'unità PSD è di 4 GB.
- Le dimensioni massime dell'unità PSD nella partizione di sistema possono essere ulteriormente limitate dal criterio [*Spazio minimo disponibile dopo la creazione di PSD.*](#)



Infineon Security Platform Solution

Riconfigurazione di Personal Secure Drive

Attraverso questa pagina è possibile modificare le impostazioni di una Personal Secure Drive esistente, eliminare una Personal Secure Drive esistente o creare una nuova Personal Secure Drive. Questa pagina viene visualizzata se è stata selezionata la funzionalità *Crittografia file e cartella con Personal Secure Drive (PSD)* e si dispone già di almeno una Personal Secure Drive. È necessario eseguire la procedura guidata diverse volte per eseguire azioni diverse o creare diverse Personal Secure Drive.

La seguente tabella fornisce dei suggerimenti su come utilizzare la pagina di procedura guidata.

Elementi della pagina	Spiegazione
<input type="checkbox"/> <i>Personal Secure Drive esistente(i)</i>	Questo elenco contiene tutte le Personal Secure Drive e il loro stato corrente. È possibile aggiornare l'elenco premendo il tasto "F5". Se si desidera modificare le impostazioni di una Personal Secure Drive esistente o eliminare una Personal Secure Drive, selezionare la relativa unità.
<input checked="" type="radio"/> <i>Modifica impostazioni PSD selezionata</i>	Selezionare questa opzione se si desidera modificare le impostazioni della Personal Secure Drive selezionata (es. lettera di unità, etichetta, opzioni per il caricamento della PSD all'accesso e utilizzo dei collegamenti dal desktop). La procedura guidata continuerà con la pagina Modifica impostazioni Personal Secure Drive .
<input checked="" type="radio"/> <i>Cancella PSD selezionata</i>	Selezionare questa opzione se si desidera eliminare la Personal Secure Drive selezionata. La procedura guidata continuerà con la pagina Eliminazione Personal Secure Drive .
<input checked="" type="radio"/> <i>Creare nuova PSD</i>	Selezionare questa opzione se si desidera creare una nuova Personal Secure Drive. La procedura guidata continuerà con le pagine di creazione di una nuova PSD .



TPM

©Infineon Technologies AG

Infineon Security Platform Solution

Modifica delle impostazioni di Personal Secure Drive

Attraverso questa pagina è possibile modificare la lettera e l'etichetta di unità della Personal Secure Drive, le opzioni di caricamento della PSD all'accesso e l'utilizzo di collegamenti dal desktop.

La seguente tabella fornisce dei suggerimenti sull'utilizzo della pagina di procedura guidata.

Elementi della pagina	Spiegazione
 Sarà eseguito il mapping della mia Personal Secure Drive nell'unità	Per modificare la lettera di unità per la Personal Secure Drive, selezionare una lettera non utilizzata dall'elenco a discesa delle lettere disponibili (vedi Amministrazione Personal Secure Drive).
 Etichetta di unità per la mia Personal Secure Drive	Per modificare l'etichetta di unità, inserire un'altra etichetta nell'apposito campo. L'etichetta non dovrebbe superare la lunghezza di 32 caratteri. Ad esempio, si potrebbe utilizzare l'etichetta "La mia Secure Drive".
<input checked="" type="checkbox"/> Caricare Personal Secure Drive all'accesso	Selezionare questa opzione se si desidera caricare la propria PSD all'accesso.
<input checked="" type="checkbox"/> Collegamento dal desktop	Selezionare questa opzione se si desidera accedere alla PSD attraverso un collegamento sul desktop. Il nome del collegamento conterrà la lettera e l'etichetta di unità.  Se si elimina la selezione della casella di controllo una volta creato il collegamento sul desktop, la procedura guidata eliminerà il collegamento esistente (purché non sia stato rinominato o spostato nel frattempo).

Infineon Security Platform Solution

Eliminazione di Personal Secure Drive

Se si sceglie di eliminare Personal Secure Drive (PSD), è possibile creare una copia decrittografata dell'intera unità prima di rimuoverla definitivamente.

Nota: selezionando **Avanti**, Personal Secure Drive verrà eliminato *definitivamente* e non sarà più possibile recuperarne i dati.

Per creare una copia non crittografata di Personal Secure Drive prima dell'eliminazione definitiva, cliccare sul pulsante di opzione *Salva una copia non crittografata dei contenuti di Personal Secure Drive prima di eliminarlo* e quindi specificare la posizione in cui salvare i file e le cartelle PSD in formato non crittografato.

Se si desidera eliminare definitivamente Personal Secure Drive senza crearne una copia, selezionare il pulsante di opzione *Elimina definitivamente Personal Secure Drive senza salvare una copia dei suoi contenuti*.



Technologies AG

Infineon Security Platform Solution - Migrazione guidata

Migrazione guidata di Infineon Security Platform

La Migrazione guidata di Infineon Security Platform viene utilizzata per trasferire in modo sicuro le chiavi e i certificati utente da un computer Infineon Security Platform a un altro.

Il computer di destinazione deve essere autorizzato dal proprietario di Infineon Security Platform prima di eseguire la migrazione. Tale autorizzazione fornisce gli strumenti amministrativi utili a controllare la distribuzione degli utenti di Infineon Security Platform, anche nelle reti di grandi dimensioni.

La procedura di migrazione deve essere eseguita da un utente di Infineon Security Platform e implica due operazioni: l'esportazione dalla piattaforma di origine e la successiva importazione sulla piattaforma di destinazione selezionata. In nessun caso è possibile effettuare la migrazione per un account utente diverso da quello attualmente connesso. Questo garantisce l'affidabilità della piattaforma dal punto di vista dell'utente di Infineon Security Platform.

La migrazione non è consentita se l'utente attualmente connesso non dispone di una chiave utente di base o se Infineon Security Platform è disabilitato (in modo permanente o temporaneo).



Disponibilità della procedura guidata:

- In modalità [autonoma](#), questa procedura guidata è disponibile soltanto se Security Platform è già stato inizializzato.
- Questa procedura guidata non è disponibile in [modalità server](#), poiché il Trusted Computing Management Server gestisce il compito di migrazione delle chiavi e dei certificati specifici degli utenti da un Infineon Security Platform all'altro in modo sicuro.

Procedura guidata

Operazione	Commenti
1. Importazione o esportazione	Consente di scegliere se importare o esportare le chiavi e i certificati utente da o verso un computer Security Platform.
2. Piattaforma di destinazione	Consente di specificare il computer di destinazione (solo se è selezionata l'opzione <i>Esporta</i>).
3. Percorso file di importazione oppure Percorso file di esportazione	Consente di specificare la posizione del file contenente i dati di migrazione.
4. Immissione della password o autenticazione	Consente di eseguire l'autenticazione per autorizzare le operazioni di migrazione.

Avvio dell'applicazione

Per avviare la Migrazione guidata dal Tool di configurazione: [Tool di configurazione - Migrazione - Esporta...](#) oppure [Tool di configurazione - Migrazione - Importa...](#)

Se si desidera esportare le chiavi e i certificati utente, selezionare *Questa è la piattaforma di origine.*

Se invece si vogliono importare le chiavi e i certificati utente, selezionare *Questa è la piattaforma di destinazione.*



©Infineon Technologies AG

Infineon Security Platform Solution - Migrazione guidata

Importazione o esportazione

Questa pagina consente di definire le operazioni di migrazione delle chiavi utente. È infatti possibile importare o esportare le chiavi e i certificati da o verso un altro computer Security Platform.



Questa pagina di procedura guidata non è disponibile in [modalità server](#), poiché la migrazione è gestita dal Trusted Computing Management Server.

Elementi della pagina	Spiegazione
⦿ <i>Importa</i>	Consente di importare i certificati e le chiavi utente di Infineon Security Platform da un file di migrazione al sistema Infineon Security Platform in uso. La posizione del file di migrazione deve essere nota.
⦿ <i>Esporta</i>	Consente di creare un file di migrazione contenente i certificati e le chiavi dell'utente di Infineon Security Platform attualmente connesso. Il sistema Infineon Security Platform di destinazione deve essere noto e autorizzato all'operazione dal proprietario della piattaforma.



©Infineon

Infineon Security Platform Solution - Migrazione guidata

Percorso del file da importare

È anche necessario specificare l'archivio di migrazione che contiene le chiavi e i certificati utente. Tale file è stato generato durante le operazioni di esportazione.



Questo pulsante non è disponibile in [modalità server](#), poiché Backup e Ripristino sono gestiti dal Trusted Computing Management Server.

Elementi della pagina	Spiegazione
<input type="text" value="Percorso backup"/> <input type="button" value="Sfogliare..."/>	<p>I dati di migrazione verranno letti da questo file. Immettere il percorso e il nome del file contenente i dati di migrazione oppure ricercare il file desiderato.</p> <p> Il file di migrazione è un file in formato XML.</p>



Infineon Security Platform Solution - Migrazione guidata

Percorso del file da esportare

Le chiavi e i certificati da trasferire vengono salvati in un archivio di migrazione. Questo file è necessario per completare la migrazione e può essere importato unicamente su un computer precedentemente autorizzato dal proprietario della piattaforma.



Questa pagina di procedura guidata non è disponibile in [modalità server](#), poiché la migrazione è gestita dal Trusted Computing Management Server.

Elementi della pagina	Spiegazione
<input type="text" value="Percorso backup"/> <input type="button" value="Sfogliare..."/>	I dati di migrazione verranno scritti nel file specificato. Immettere il percorso e il nome del file contenente i dati di migrazione oppure ricercare il file desiderato.
	Il file di migrazione è un file in formato XML.



Infineon Security Platform Solution - Migrazione guidata

Piattaforma di destinazione

Tutti i computer Infineon Security Platform che verranno utilizzati come piattaforma di destinazione per la migrazione dei dati devono essere autorizzati preventivamente dal proprietario del sistema Infineon Security Platform locale. Tale operazione deve essere eseguita su tutti i computer Infineon Security Platform della rete.



Questa pagina di procedura guidata non è disponibile in [modalità server](#), poiché la migrazione è gestita dal Trusted Computing Management Server.

Elementi della pagina	Spiegazione
<input type="checkbox"/> <i>Selezione del sistema Security Platform di destinazione</i>	<p>L'elenco di selezione comprende tutti i sistemi Infineon Security Platform che possono essere utilizzati come destinazioni valide per la migrazione dei certificati e delle chiavi utente dal sistema Infineon Security Platform in uso. Selezionare una delle voci in elenco come destinazione della migrazione.</p> <p> Se l'elenco non contiene nessuna piattaforma di destinazione, scegliere Annulla per arrestare la Migrazione guidata di Infineon Security Platform. In questo caso, il proprietario del sistema Infineon Security Platform locale dovrà autorizzare la migrazione per il computer in uso tramite il Tool di configurazione di Infineon Security Platform.</p>



©Infineon

Infineon Security Platform Solution - Backup Wizard

Backup guidato di Infineon Security Platform

Il Backup guidato di Infineon Security Platform viene utilizzato per eseguire le procedure di backup o per ripristinare i [dati collegati a Security Platform](#). Queste operazioni sono necessarie per proteggere i dati da perdite accidentali, nel caso in cui si verificano situazioni di emergenza.

Il file di backup contiene i dati identificativi del computer ("ID piattaforma") e dell'utente ("ID utente"). Durante la procedura di ripristino, queste informazioni vengono messe in corrispondenza con il nome del computer e dell'utente attuali.



Se la Chiave utente di base attuale è diversa rispetto alla Chiave utente di base da ripristinare, il processo di ripristino sovrascriverà le credenziali e le impostazioni installate nella posizione di destinazione. Si raccomanda quindi di ripristinare le credenziali utente in un account del computer di destinazione per il quale non è stata eseguita la procedura di inizializzazione utente di Security Platform.



In [modalità server](#) il Backup e il Ripristino sono gestiti dal Trusted Computing Management Server, cioè nessuna configurazione esplicita è necessaria. Se la Personal Secure Drive (PSD) è stata configurata, è possibile eseguire manualmente il backup e il ripristino dei file di immagine della Personal Secure Drive.



Questa icona scudo è visibile solo per gli utenti con diritti amministrativi in sistemi operativi con [Controllo account utente](#) (es. Windows 7 e Windows Vista).

Fasi Procedura Guidata

Scenario	Fasi Procedura Guidata	Informazioni
Backup Manuale	Configurazione impostazioni di backup	Fase necessaria.
	Configurazione impostazioni di backup PSD	Solo se le Personal Secure Drive sono incluse nel backup.
Ripristino	Configurazione impostazioni di ripristino	Non necessario per il solo ripristino di Personal Secure Drive.
	Confermare computer o selezionare computer	Solo se il computer non è elencato nei dati di backup. Non necessario per il solo ripristino di Personal Secure Drive.
	Selezione del token di ripristino di emergenza	Solo se si detengono diritti di amministratore e il backup comprende i dati per il Recupero di Emergenza e i dati di Recupero di Emergenza stessi saranno ripristinati. Non necessario per il solo ripristino di Personal Secure Drive.
	Confermare utente	Solo se vogliono ripristinare le credenziali e le impostazioni per l'account dell'utente corrente e l'utente nei dati di Backup è differente dall'utente attuale. Non necessario per il solo ripristino di Personal Secure

		Drive.
	Selezionare utente	Solo se si detengono diritti di amministratore e si sta per preparare il ripristino per altri utenti. Non necessario per il solo ripristino di Personal Secure Drive.
	Configurazione impostazioni di ripristino PSD	Solo se le Personal Secure Drive saranno ripristinate.

Si noti che non è necessario utilizzare una Procedura Guidata di Backup per eseguire il Backup del Sistema poiché è configurata un'attività di backup programmata mediante l'Inizializzazione Guidata di Security Platform o Inizializzazione Guidata Rapida esegue automaticamente il Backup del Sistema.

Avvio dell'applicazione

Backup manuale: Avviare il Backup guidato dal Tool di configurazione:

[Tool di configurazione - Backup - Backup...](#)

Ripristino manuale: Avviare il Backup guidato dal Tool di configurazione:

[Tool di configurazione - Backup - Ripristino...](#)

Recupero dei dati con ripristino di emergenza (attività

dell'amministratore): Avviare l'Inizializzazione guidata di Security Platform. Selezionare l'opzione [Ripristina Security Platform da un archivio di backup](#) nella pagina della procedura guidata *Inizializzazione o ripristino di Security Platform*.

Avvio della procedura guidata tramite le note o l'icona TNA: in base allo stato attuale di Security Platform, è possibile avviare il Backup guidato tramite la finestra delle note oppure [l'icona TNA](#) (ad esempio, quando l'amministratore di Security Platform ha predisposto il ripristino per l'utente attuale).



Infineon Security Platform Solution - Backup guidato

Backup o ripristino

Scegliere l'opzione appropriata per eseguire il backup o il ripristino dei dati.

Elementi della pagina	Spiegazione
☉ <i>Creare un manuale backup</i>	<p>Le operazioni seguenti consentono di creare una copia di backup delle proprie credenziali da un'installazione locale di Infineon Security Platform a un supporto protetto, preferibilmente un supporto rimovibile come un'unità di memoria, un disco rigido o un server. In questo modo, è possibile ripristinare le credenziali nel caso di perdita dei dati. La posizione da cui viene eseguito il backup deve essere nota.</p> <p> In modalità server, puoi solo fare un backup del tuo Personal Secure Drive (PSD).</p>
☉ <i>Ripristina del un manuale backup</i>	<p>Le operazioni seguenti consentono di ripristinare le proprie credenziali in Infineon Security Platform a partire da un file di backup creato in precedenza. È necessario indicare la posizione del file di backup per poter eseguire il ripristino.</p> <p> Nella modalità server, è possibile eseguire solo il backup di Personal Secure Drive (PSD).</p>
☉ <i>Ripristina del un sistema backup</i>	<p>Le seguenti operazioni ripristinano i dati credenziali per cui è stato eseguito il back-up su Infineon Security Platform. L'utente deve indicare la posizione del file di back-up per il processo di ripristino. L'utente può anche effettuare il ripristino manualmente da un archivio scritto, se non dispone di un archivio di back-up del sistema. È anche possibile eseguire un ripristino di emergenza.</p> <p> • Questo pulsante non è disponibile se l'utente non dispone dei diritti di</p>

amministratore.

- Queste pulsante non è disponibile in [modalità server](#), poiché Backup e Ripristino sono gestiti dal Trusted Computing Management Server.



Infineon Security Platform Solution - Backup Wizard

Configurazione Impostazioni Backup

Attraverso questa pagina è possibile specificare il File Compresso di Backup.



In [modalità server](#), questa pagina non è disponibile poiché il backup è trattato da Trusted Computing Management Server.

La seguente tabella fornisce dei suggerimenti sull'utilizzo della pagina di procedura guidata.

Elemento Pagina Procedura GUIDATA	Spiegazione
<input type="text" value="Posizione Backup"/> <input type="button" value="Sfogliare..."/>	Le credenziali e le impostazioni di Security Platform saranno salvate in un File Compresso di Backup. Digitare il percorso e il nome del file o cercarlo.  Il file di backup è un file in formato XML.



Soluzione Infineon Security Platform - Backup guidato

Configurazione delle impostazioni di backup di Personal Secure Drive

Attraverso questa pagina è possibile eseguire il backup dei file di immagine della Personal Secure Drive. Le impostazioni della PSD sono sempre comprese nel backup se è stata configurata una PSD mentre i file di immagine devono essere esplicitamente selezionati per essere inclusi nel backup.

La seguente tabella fornisce dei suggerimenti sull'utilizzo della pagina di procedura guidata.

Elementi della pagina	Spiegazione
<p><input type="text"/> <i>Destinazione predefinita backup Personal Secure Drive</i> <input type="button" value="Sfogliare..."/></p>	<p>Se si desidera eseguire il backup di uno o più file di immagine della Personal Secure Drive è necessario specificare il percorso di destinazione predefinito per i file di immagine di backup. Se si desidera effettuare il backup di diversi file di immagine in posizioni diverse, utilizzare il pulsante <i>Cambiare...</i> per stabilire il percorso per ciascuno.</p> <p>Se non si desidera eseguire il backup della Personal Secure Drive è possibile ignorare la selezione del percorso.</p>
<p><input type="checkbox"/> <i>Selezione delle Personal Secure Drive da includere nel backup</i></p>	<p>Questo elenco mostra tutte le Personal Secure Drive configurate sulla piattaforma. Selezionare le unità da includere nel backup. Accertarsi che sia specificato un valido file di immagine di backup per ciascuna unità selezionata e che ci sia spazio libero sufficiente nella cartella di destinazione.</p> <p>Se non si desidera eseguire il backup del file immagine della Personal Secure Drive accertarsi che non sia selezionata alcuna Personal Secure Drive.</p> <p>Menu di scelta rapida: Fare clic con il tasto destro sull'elenco per visualizzare un menu di scelta rapida</p>

	con tutte le azioni supportate.
<input type="checkbox"/> <i>Cambiare...</i>	<p>Fare clic su questo pulsante per modificare la posizione del backup e/o il nome file del file di immagine di backup.</p> <p>Verrà visualizzato un dialogo. Apportare le modifiche e chiudere nuovamente il dialogo.</p> <p> Non modificare l'estensione *.fsb del file di immagine di backup.</p>



Infineon Security Platform Solution - Backup guidato

Configurazione delle impostazioni di ripristino

In questa pagina è possibile specificare l'archivio di backup da cui eseguire il ripristino dei dati. Se si dispone dei diritti di amministratore, è anche possibile indicare i motivi dell'operazione di ripristino.



Disponibilità della pagina: Questa pagina non è disponibile in [modalità server](#), poiché il Backup e il Ripristino sono gestiti dal Trusted Computing Management Server, ovvero non è necessaria alcuna configurazione esplicita.

La tabella seguente fornisce alcuni suggerimenti per l'utilizzo della procedura guidata.

Elementi della pagina	Spiegazione
<ul style="list-style-type: none">⦿ <i>Disco rigido danneggiato o perdita di dati</i>⦿ <i>Nuovo Trusted Platform Module</i>⦿ <i>Nuovo Security Platform da inizializzare</i>	<p>In base allo stato attuale di Security Platform, viene selezionata una delle motivazioni indicate di seguito.</p> <ul style="list-style-type: none">• <i>Disco rigido danneggiato o perdita di dati</i> - Il software Security Platform ha un proprietario. Di solito, questa condizione si verifica quando i dati di alcuni utenti non sono più accessibili, sebbene Security Platform Solution sia inizializzato e pronto all'uso.• <i>Nuovo Trusted Platform Module</i> - Il software Security Platform non ha un proprietario ma sono presenti le impostazioni o le credenziali di una vecchia installazione del software. Questa condizione si verifica in genere quando il software Security Platform Solution era già stato installato in precedenza e quindi Trusted Platform Module era stato sostituito o reimpostato nel BIOS.• <i>Nuovo Security Platform da inizializzare:</i> Il software Security Platform non ha un proprietario. Non sono state trovate credenziali o impostazioni di

	<p>una vecchia installazione di Security Platform. Questa condizione si verifica in genere quando il ripristino viene eseguito da un PC sul quale il software Security Platform Solution non era mai stato installato.</p> <p>Si noti che questa selezione non può essere modificata.</p> <p> La motivazione del ripristino viene visualizzata unicamente per gli utenti che dispongono dei diritti di amministratore.</p>
<p> <i>Percorso e il nome dell'archivio di backup da ripristinare</i></p> <p><input type="checkbox"/> <i>Sfogliare...</i></p>	<p>Specificare l'archivio di backup da cui eseguire il ripristino. Immettere il percorso e il nome del file oppure ricercare il file desiderato.</p> <p> Il file di backup è un file in formato XML.</p>



Soluzione Infineon Security Platform - Backup guidato

Configurazione delle impostazioni di ripristino di Personal Secure Drive

Attraverso questa pagina è possibile eseguire il ripristino delle Personal Secure Drive. È possibile utilizzare il backup di un file di immagine PSD per una PSD già configurata o impostare una nuova PSD per utilizzare il file di immagine ripristinato.

La seguente tabella fornisce dei suggerimenti sull'utilizzo della pagine di procedura guidata.

Elemento Pagina Procedura Guidata	Spiegazione
<input type="text" value="abc"/> <i>Posizione predefinita backup Personal Secure Drive</i> <input type="button" value="Sfogliare..."/>	<p>Se si desidera ripristinare una o più Personal Secure Drive, specificare il percorso predefinito del file di immagine PSD da ripristinare. Questo percorso verrà considerato quale percorso di ripristino predefinito per tutti i file di immagine PSD. Se si desidera ripristinare diversi file di immagine da diverse posizioni, utilizzare il pulsante <i>Cambia...</i> per impostare ciascun percorso.</p> <p>Se non si desidera ripristinare una Personal Secure Drive è possibile ignorare la selezione del percorso.</p>
<input type="checkbox"/> <i>Selezionare le Personal Secure Drive da ripristinare</i>	<p>Questo elenco mostra tutte le Personal Secure Drive configurate nella piattaforma. Selezionare le unità da ripristinare e accertarsi che sia specificato un valido file di immagine di backup per ciascuna unità selezionata.</p> <p>Questo elenco potrebbe includere unità in stati differenti:</p> <ul style="list-style-type: none">• Personal Secure Drive completamente funzionali (sia le impostazioni che il file di immagine della PSD sono disponibili). Potreste dover procedere al ripristino di un'unità completamente funzionale, ad esempio, se si sono eliminati per errore alcuni file

dalla PSD e il backup del file immagine comprende tali file. In questo caso i dati attualmente presenti nella PSD saranno completamente sovrascritti.

- Personal Secure Drive prive di file di immagine (ad esempio se si sono appena ripristinate le impostazioni PSD da un File Compresso di Backup ma il file di immagine non è ancora stato ripristinato). In questo caso è necessario ripristinare il backup del file di immagine prima di poter accedere ai dati della PSD.
- Personal Secure Drive per le quali non sono disponibili chiavi applicabili. In questo caso è possibile ripristinare un backup del file di immagine che utilizza la chiave prevista. Valutate se eseguire prima il ripristino delle credenziali e delle impostazioni poiché successivamente potrebbe non essere necessario eseguire il ripristino del file di immagine.

Se non si desidera eseguire il ripristino di una Personal Secure Drive accertarsi che non sia selezionata alcuna Personal Secure Drive.

Menu di scelta rapida: Fare clic con il tasto destro sull'elenco per visualizzare il menu di scelta rapida con tutte le azioni supportate.

Aggiungi...

Fare clic su questo pulsante per aggiungere un'altra Personal Secure Drive all'elenco delle unità. In questo modo è possibile ripristinare una Personal Secure Drive a partire dal backup del file di immagine senza disporre del backup delle impostazioni corrispondenti. Verrà visualizzata una finestra di [dialogo](#) in cui è possibile configurare tutte le relative impostazioni della PSD.

Cambiare...

Fare clic su questo pulsante per impostare o modificare le impostazioni di ripristino della Personal

Secure Drive selezionata.

Ciò si rende necessario per esempio nei seguenti casi:

- Non è stato possibile trovare alcun backup del file di immagine nella posizione predefinita del backup della PSD.
- È stata trovata un backup del file di immagine nella posizione predefinita del backup della PSD, ma si desidera selezionare un altro backup del file di immagine valido.
- Lo stato locale della PSD selezionata richiede che la destinazione del file di immagine o la lettera unità siano modificate.

Verrà visualizzata una finestra di [dialogo](#) in cui è possibile configurare tutte le relative impostazioni della PSD.



Soluzione Infineon Security Platform - Procedura Guidata di Backup

Modificare Impostazioni di Ripristino/Aggiungere Personal Secure Drive

Mediante questa finestra di dialogo è possibile impostare o modificare le impostazioni di ripristino per una Personal Secure Drive o aggiungere un'altra Personal Secure Drive da ripristinare. A seconda dell'azione da eseguire verranno attivati solo i controlli necessari.

La seguente tabella fornisce dei suggerimenti sull'uso di questa finestra di dialogo:

Elemento Pagina Procedura Guidata	Spiegazione	Modificare	Aggiungere
<input type="checkbox"/> <i>Percorso file di immagine backup</i> <input type="checkbox"/> <i>Sforgia...</i>	Specificare il percorso del file di immagine del backup da ripristinare.	Deve essere impostato se non è stato trovato alcun file di immagine del backup adatto nella posizione predefinita del backup della PSD. Altrimenti il percorso può essere modificato.	Deve essere impostato
<input type="checkbox"/> <i>Unità di destinazione file di immagine</i>	Selezionare un'unità in cui ripristinare il file di immagine della PSD.	Deve essere impostato se non è possibile eseguire il ripristino del backup del file immagine nell'unità di destinazione	Deve essere impostata

		<p>salvata nelle impostazioni locali. Altrimenti l'unità di destinazione non può essere modificata.</p>	
<p> <i>Lettera Unità</i></p>	<p>Per specificare la lettera unità per la Personal Secure Drive, selezionare una lettera inutilizzata dall'elenco a discesa delle lettere disponibili (vedere Amministrazione Personal Secure Drive).</p>	<p>Deve essere impostato sse non è possibile utilizzare la lettera unità salvata nelle impostazioni locali. Altrimenti la lettera unità non può essere modificata.</p>	<p>Deve essere impostata</p>
<p> <i>Etichetta unità</i></p>	<p>Per specificare l'etichetta dell'unità, inserire l'etichetta nel campo fornito. L'etichetta non dovrebbe superare la lunghezza di 32 caratteri. Per esempio si potrebbe impostare l'etichetta "La mia Secure Drive".</p>	<p>Non può essere modificata</p>	<p>Deve essere impostata</p>
<p><input checked="" type="checkbox"/> <i>Caricamento all'accesso</i></p>	<p>Selezionare questa opzione se si desidera caricare la PSD all'accesso.</p>	<p>Non può essere modificato</p>	<p>Facoltativo</p>
<p><input checked="" type="checkbox"/> <i>Creare collegamento sul desktop</i></p>	<p>Selezionare questa opzione se si desidera accedere alla PSD attraverso un</p>	<p>Non può essere modificato</p>	<p>Facoltativo</p>

collegamento sul desktop.
Il nome di questo
collegamento conterrà la
lettera e l'etichetta unità.



©Infineon Technologies AG

Infineon Security Platform Solution - Backup guidato

Conferma computer

Questa pagina ti chiede di confermare se il computer nei dati di Backup specificati deve essere recuperato nel tuo computer.



Disponibilità della pagina:

- questa pagina è visualizzata solo se i dati di Backup specificati contengono dati per un altro computer rispetto al tuo.
- Questa pagina non è disponibile in [modalità server](#), poiché il Backup e il Ripristino sono gestiti dal Trusted Computing Management Server.

La tabella seguente fornisce alcuni suggerimenti per l'utilizzo della procedura guidata.

Elementi della pagina	Spiegazione
 <i>Computer in uso: Nome computer / ID piattaforma</i>	Vengono visualizzati il nome del computer in uso e l'ID della piattaforma.  Il nome del computer potrebbe essere stato modificato successivamente al backup. Per questo motivo, viene indicato anche l'identificativo della piattaforma.
 <i>Computer nei dati di Backup: Nome computer / ID piattaforma</i>	Vengono visualizzati il nome del computer e l'ID della piattaforma per il sistema da cui è stato eseguito il backup.



©Infineon

Infineon Security Platform Solution - Backup guidato

Selezione computer

In questa pagina è possibile selezionare il computer che si desidera ripristinare.



Disponibilità della pagina:

- questa pagina è visualizzata solo se i dati di Backup specificati contengono dati per diversi computer ma non per il tuo computer.
- Questa pagina non è disponibile in [modalità server](#), poiché backup e ripristino sono gestiti dal Trusted Computing Management Server.

La tabella seguente fornisce alcuni suggerimenti per l'utilizzo della procedura guidata.

Elementi della pagina	Spiegazione
<i>Computer in uso: Nome computer/ID piattaforma</i>	Vengono visualizzati il nome del computer in uso e l'ID della piattaforma. Il nome del computer potrebbe essere stato modificato successivamente al backup. Per questo motivo, viene indicato anche l'identificativo della piattaforma.
<i>Computer nei dati di Backup: Nome computer/ID piattaforma</i>	Vengono visualizzati il nome del computer e l'ID della piattaforma per i sistemi da cui è stato eseguito il backup. Selezionare il computer da ripristinare.



Infineon Security Platform Solution - Backup guidato

Selezione del token di ripristino di emergenza

Se la procedura di ripristino comprende anche il ripristino di emergenza, occorre specificare il token corrispondente. In questa pagina è possibile selezionare il token di ripristino di emergenza.

Il file contenente i dati del ripristino di emergenza può essere utilizzato soltanto in combinazione con il token di ripristino, protetto da una password dedicata. Il file token viene generato durante la configurazione del ripristino di emergenza; tale configurazione è eseguita dall'amministratore di Security Platform per tutti gli utenti.



Disponibilità della pagina:

- Questa pagina è visualizzata solo se l'Amministratore della Security Platform ripristina le credenziali e le impostazioni della piattaforma da un Archivio di Backup creato automaticamente.
- Questa pagina è visualizzata solo se un Recupero di Emergenza è necessario (cioè il motivo di ripristino è un *Nuovo Trusted Platform Module* o una *Nuova Security Platform che devono essere inizializzati*).
- Questa pagina non è disponibile in [modalità server](#), poiché il Backup e il Ripristino sono gestiti dal Trusted Computing Management Server.

La tabella seguente fornisce alcuni suggerimenti per l'utilizzo della procedura guidata.

Elementi della pagina	Spiegazione
<input type="text"/> <i>Percorso del token di ripristino di emergenza</i> <input type="button" value="Sfogliare..."/>	Immettere il percorso e il nome del file oppure ricercare il file desiderato. Il file è in formato XML.
<input type="password"/> <i>Password</i>	Immettere la password di protezione del token di ripristino di emergenza.



Infineon Security Platform Solution - Backup guidato

Conferma utente

Questa pagina ti chiede di confermare che l'utente nei dati di Backup specificati deve essere recuperato per l'account dell'utente attuale.



Disponibilità della pagina:

- questa pagina è visualizzata per un utente senza diritti amministrativi se i dati di Backup specificati contengono dati per un altro utente rispetto all'account dell'utente attuale.
- Questa pagina non è disponibile in [modalità server](#), poiché backup e ripristino sono gestiti dal Trusted Computing Management Server.

La tabella seguente fornisce alcuni suggerimenti per l'utilizzo della procedura guidata.

Elementi della pagina	Spiegazione
 <i>Account utente: Nome utente/ID utente</i>	Vengono visualizzati il nome e l'ID dell'account utente attuale.  Il nome dell'utente potrebbe essere stato modificato successivamente al backup. Per questo motivo, viene indicato anche l'identificativo dell'utente.
 <i>Utente nei dati di Backup: Nome utente/ID utente</i>	Vengono visualizzati il nome e l'ID dell'utente che ha eseguito il backup.



©Infineon

Infineon Security Platform Solution - Backup guidato

Selezione utenti

Questa pagina ti chiede di selezionare gli utenti dai dati di Backup da recuperare.



Disponibilità della pagina:

- questa pagina è visualizzata ad un amministratore se gli utenti nei dati di Backup specificati non possono essere evidenziati automaticamente agli utenti nel tuo computer.
- Questa pagina non è disponibile in [modalità server](#), poiché il Backup e il Ripristino sono gestiti dal Trusted Computing Management Server.

La tabella seguente fornisce alcuni suggerimenti per l'utilizzo della procedura guidata.

Elementi della pagina	Spiegazione
 <i>Nome utente attuale</i>  <i>Utente dai dati di Backup</i>	Viene visualizzato l'account utente attivo. Se si desidera ripristinare questo account, cliccare sulla freccia a destra nella casella di testo e selezionare un utente dall'elenco.
 <i>Nome utente</i>  <i>Utente dai dati di Backup</i>	Vengono visualizzati gli account validi degli utenti che si sono connessi almeno una volta a questo computer. Per aggiungere altri utenti non presenti in elenco, fare doppio clic su "<AGGIUNGI UTENTE>". Per predisporre il ripristino di altri utenti, cliccare sulla freccia a destra nella casella di testo per ciascun utente e quindi selezionare un utente dall'elenco.  Alla successiva connessione di questi utenti, verrà visualizzata una nota in cui si richiede di completare la procedura di ripristino. Inoltre, per tali utenti, sarà disponibile una voce del menu TNA che consente di completare il ripristino.



Soluzione Infineon Security Platform - Reimpostazione guidata password

Reimpostazione guidata password di Infineon Security Platform

La Reimpostazione guidata password di Infineon Security Platform consente di reimpostare le password utente di base. Questa operazione prevede sia attività eseguite dall'amministratore, sia attività a carico dell'utente. Mediante la Reimpostazione guidata password è possibile eseguire sia le procedure amministrative, sia le procedure destinate agli utenti.



Disponibilità della procedura guidata:

- In modalità [autonoma](#), questa procedura guidata è disponibile soltanto se Security Platform è già stato inizializzato.
- In [modalità server](#), non sono disponibili attività amministrative in questa procedura guidata poiché questo genere di attività è gestito da Trusted Computing Management Server.



Questa icona scudo è visibile solo per gli utenti con diritti amministrativi in sistemi operativi con [Controllo account utente](#) (es. Windows 7 e Windows Vista).

Fasi Procedura Guidata

Operazioni dell'amministratore: le pagine della procedura guidata relative alla preparazione della reimpostazione password per un determinato utente sono destinate agli amministratori di Security Platform o al personale del supporto tecnico. È necessario immettere la password di protezione del token di ripristino. Se la password utente di base dell'amministratore attuale deve essere reimpostata, la procedura guidata prosegue automaticamente con le attività riservate agli utenti.

Operazioni dell'utente: le pagine della procedura guidata che consentono di reimpostare la password dell'utente attuale presuppongono che tale operazione sia già stata predisposta dagli amministratori per quel determinato utente.

Operazione	Commento
1. Selezione del token di reimpostazione password	Attività dell'amministratore
2. Selezione dell'utente di cui reimpostare la password	Attività dell'amministratore
3. Visualizzazione e salvataggio del codice di autorizzazione alla reimpostazione	Attività dell'amministratore (disponibile soltanto se l'utente selezionato è diverso dall'utente attuale)
4. Indicazione dei valori segreti per la reimpostazione della password utente di base	Attività dell'utente
5. Impostazione della nuova password utente di base	Attività dell'utente  Se è stata impostata l'Autenticazione avanzata ma il dispositivo di autenticazione non è in funzione oppure non è disponibile, è possibile utilizzare la nuova frase password utente di base senza

aggiornare la configurazione del dispositivo.

Avvio dell'applicazione

Avviare la Reimpostazione guidata password di Infineon Security Platform tramite il Tool di configurazione: [Tool di configurazione - Reimpostazione password.](#)



©Infineon Technologies AG

Infineon Security Platform Solution - Reimpostazione guidata password

Preparazione o esecuzione della reimpostazione password

In questa pagina della procedura guidata viene chiesto di scegliere se eseguire le operazioni amministrative per la reimpostazione della password, oppure le operazioni destinate agli utenti.

Elementi della pagina	Spiegazione
<p>☉ <i>Prepara il codice di autorizzazione alla reimpostazione della password per un determinato utente. Prepara ed esegue la reimpostazione della password in un'unica operazione per l'account dell'amministratore attuale.</i></p>	<p>Operazioni eseguite dall'amministratore per la reimpostazione della password. Se la password utente di base dell'amministratore attuale deve essere reimpostata, la procedura guidata prosegue automaticamente con le attività riservate agli utenti.</p> <p> Questo elemento della pagina della procedura guidata non è disponibile in modalità server poiché quest'attività è gestita da Trusted Computing Management Server.</p>
<p>☉ <i>Reimposta password attuale (l'operazione è già stata predisposta per l'account utente attivo)</i></p>	<p>Operazioni dell'utente per la reimpostazione della password.</p>

 Questa pagina non viene visualizzata se la procedura guidata è stata avviata dal Tool di configurazione di Security Platform.



Infineon Security Platform Solution - Reimpostazione guidata password

Selezione dell'utente di cui reimpostare la password

Questa pagina della procedura guidata consente di selezionare l'utente di cui si desidera reimpostare la password.



Disponibilità della pagina: Questa pagina non è disponibile in [modalità server](#) poiché quest'attività è gestita da Trusted Computing Management Server.

Elementi della pagina	Spiegazione
Utenti	L'elenco contiene tutti gli utenti di Security Platform per i quali è stata abilitata la funzionalità di reimpostazione della password utente di base (vedi Inizializzazione GUIDATA Rapida o Inizializzazione Utenti GUIDATA). Selezionare l'utente di cui reimpostare la password.



Questa pagina appartiene alle procedure amministrative richieste per la reimpostazione della password.



Infineon Security Platform Solution - Reimpostazione guidata password

Selezione del token di reimpostazione della password

In questa pagina della procedura guidata viene chiesto di specificare il token di reimpostazione della password.



Disponibilità della pagina: Questa pagina non è disponibile in [modalità server](#) poiché quest'attività è gestita da Trusted Computing Management Server.

Elementi della pagina	Spiegazione
 <i>Percorso del token di reimpostazione</i>	Immettere il percorso e il nome del file token per la reimpostazione della password. Il token è stato creato durante la configurazione dei dati di reimpostazione eseguita dall'amministratore per tutti gli utenti (vedere Inizializzazione guidata).
 <i>Sfoglia...</i>	Cliccare su questo pulsante per selezionare il token di reimpostazione della password.
 <i>Password</i>	Immettere la password di protezione del token. Tale password è stata specificata durante la configurazione dei dati di reimpostazione password eseguita dall'amministratore per tutti gli utenti. Nota: il token di reimpostazione della password è necessario per reimpostare le password utente di base. Il file token è protetto da un'altra password specifica.



Questa pagina appartiene alle procedure amministrative richieste per la reimpostazione della password.



©Infineon Technologies AG

Infineon Security Platform Solution - Reimpostazione guidata password

Visualizzazione e salvataggio del codice di autorizzazione alla reimpostazione

Questa pagina della procedura guidata visualizza il codice di autorizzazione alla reimpostazione. Tale codice autorizza l'utente a reimpostare la password utente di base.



Disponibilità della pagina: Questa pagina non è disponibile in [modalità server](#) poiché quest'attività è gestita da Trusted Computing Management Server.

Elementi della pagina	Spiegazione
<i>Codice di autorizzazione alla reimpostazione</i>	Questa stringa di codice deve essere trasferita all'utente che dovrà reimpostare la propria password. Il codice è necessario per reimpostare la password utente di base.
<input type="checkbox"/> <i>Salva su file...</i>	Questo pulsante consente di salvare su file il codice di autorizzazione alla reimpostazione. Il file può essere inviato all'utente che dovrà leggerne il contenuto. Se l'utente non è connesso (ed è quindi impossibile inviargli il file), occorre comunicargli (ad esempio, al telefono) il codice e il valore checksum come appaiono sullo schermo. In questo caso, l'utente dovrà immettere il codice di autorizzazione manualmente.
<i>Checksum</i>	Questo valore aiuta l'utente durante l'immissione manuale del codice di autorizzazione alla reimpostazione. Il valore checksum della stringa immessa è visibile all'utente. Se tale valore corrisponde a quello trasferito con il codice di autorizzazione, significa che la stringa di codice immessa è corretta.



Questa pagina appartiene alle procedure amministrative richieste per la reimpostazione della password. Il codice di autorizzazione alla reimpostazione deve essere trasferito all'utente che dovrà reimpostare la propria password. Se

occorre reimpostare la password utente di base del proprio account, questa pagina non verrà visualizzata. In questo caso, la procedura guidata prosegue automaticamente con le operazioni destinate agli utenti, consentendo di reimpostare subito la propria chiave utente di base.



©Infineon Technologies AG

Soluzione Infineon Security Platform - Reimpostazione guidata password

Indicazione dei valori segreti per la reimpostazione della password utente di base

In questa pagina della procedura guidata viene chiesto di indicare i valori segreti per la reimpostazione della password utente di base, ovvero il proprio "Valore segreto personale" e il "Codice di autorizzazione alla reimpostazione".

Elementi della pagina	Spiegazione
<input type="text"/> <i>Valore segreto personale</i>	Questo valore viene creato durante l'abilitazione della funzionalità di reimpostazione per la password utente di base (vedere Inizializzazione Guidata Rapida o Inizializzazione utenti guidata). È possibile digitare manualmente il Segreto Personale o fornire il file del Segreto Personale.
<input type="checkbox"/> <i>Ricavare da file...</i>	Se si è salvato il Segreto Personale in un file, fare clic su questo pulsante per fornire il file Segreto Personale.
<input checked="" type="checkbox"/> <i>Nascondi segreto</i>	Annullare la selezione di questa casella se si desidera eliminare la crittografia del segreto rendendolo visibile.  L'opzione all'interno del campo Segreto Personale potrebbe essere limitata a seconda dei criteri di sistema Attiva protezione rigorosa campo password .
	Nota: le voci indicate di seguito non compaiono nella pagina se la reimpostazione password è stata predisposta per il proprio account utente. In questo caso, non è necessario indicare il codice di autorizzazione alla reimpostazione.
<input type="text"/> <i>Codice di autorizzazione alla reimpostazione</i>	Questa stringa di codice viene inviata all'utente dall'amministratore di Security Platform o dal personale del supporto tecnico. È possibile leggere il codice dal file ricevuto oppure immetterlo direttamente.
<input type="checkbox"/> <i>Recupera da file...</i>	Cliccare su questo pulsante se il codice di autorizzazione alla reimpostazione è stato fornito su file. In caso contrario, immettere la stringa di codice manualmente.

 <i>Prendi dal Server</i>	<p>Questo elemento di procedura guidata è disponibile solo in modalità server. Cliccare su questo pulsante per recuperare il Codice di Autorizzazione al Reset dal server.</p> <p> Il sistema cliente deve essere integrato in un Trust Domain con gestione centralizzata.</p>
 <i>Checksum</i>	<p>Questo valore facilita l'immissione manuale del codice di autorizzazione alla reimpostazione. Se il valore visualizzato corrisponde a quello ricevuto con il codice di autorizzazione, significa che la stringa di codice immessa è corretta.</p>

 Questa pagina appartiene alle procedure di reimpostazione della password riservate agli utenti. Se occorre reimpostare la password utente di base del proprio account, questa pagina verrà visualizzata soltanto dopo aver completato le operazioni amministrative richieste.

Infineon Security Platform Solution - Importazione guidata di PKCS #12

Importazione guidata PKCS #12 di Infineon Security Platform

L'Importazione guidata PKCS #12 di Infineon Security Platform viene utilizzata per importare i file Personal Information Exchange nei sistemi Security Platform.

I file Personal Information Exchange (PKCS #12) hanno estensione ".pfx" o ".p12". I file PKCS #12 generati contengono i certificati e le chiavi private dell'utente. Inoltre, possono contenere anche una catena di certificati, ovvero tutti i certificati rilasciati da un'Autorità di certificazione (CA) necessari per convalidare il proprio certificato. Per garantire la massima sicurezza, le chiavi private presenti nei file PKCS #12 sono protette da un'apposita password.

Differenze rispetto all'Importazione guidata certificati di Microsoft

PC privo di Security Platform: i file PKCS #12 vengono importati utilizzando l'*Importazione guidata certificati di Microsoft*. Le chiavi private sono protette dal software.

PC con Security Platform: i file PKCS #12 vengono importati utilizzando l'*Importazione guidata PKCS #12 di Security Platform*. Le chiavi private sono protette da Trusted Platform Module. In questo modo, viene migliorato il livello di protezione delle chiavi private.

Procedura guidata

Operazione	Commenti
1. Importazione del file PKCS #12	Selezione del file da importare.
2. Opzioni	Opzioni di importazione di PKCS #12.

Avvio dell'applicazione

Per avviare l'Importazione guidata PKCS #12 di Infineon Security Platform, scegliere **Importa...** nel Visualizzatore certificati di Security Platform. Il Visualizzatore certificati può essere avviato tramite il Tool di configurazione ([Tool di configurazione - Impostazioni utente - Gestione...](#)).



Technologies AG

Infineon Security Platform Solution - Importazione guidata di PKCS #12

Importazione del file PKCS #12

In questa pagina della procedura guidata viene chiesto di specificare il file PKCS #12 che si desidera importare.

Elementi della pagina	Spiegazione
 <i>Nome file</i>	Immettere oppure copiare e incollare il percorso completo del file, ad esempio D:\certificati\ilmiofilePKCS12.pfx oppure D:\certificati\ilmiofilePKCS12.p12.
 <i>Sfoglia</i>	Cliccare su questo pulsante per ricercare il file PKCS #12 desiderato invece di immetterne il percorso manualmente o copiarlo/incollarlo.
 <i>Immettere la password di protezione del file</i>	Per garantire la massima sicurezza, le chiavi private presenti nei file PKCS #12 sono protette da un'apposita password. Immettere la password nella casella corrispondente.



Infineon Security Platform Solution - Importazione guidata di PKCS #12

Opzioni

In questa pagina della procedura guidata viene chiesto di impostare le opzioni di importazione del file PKCS #12.

Elementi della pagina	Spiegazione
<input type="checkbox"/> <i>Archivio certificati</i>	Il file PKCS #12 verrà salvato in un determinato archivio certificati, ad esempio <i>Personale</i> . In questa casella, viene visualizzato il nome dell'archivio certificati.
<input type="checkbox"/> <i>Sfoggia...</i>	Cliccare su questo pulsante se si desidera utilizzare un archivio certificati diverso.  È possibile importare un certificato in un archivio qualsiasi. Nella maggior parte dei casi, i certificati vengono importati negli archivi <i>Personale</i> o <i>Autorità di certificazione fonti attendibili</i> , a seconda che si tratti di un certificato appartenente all'utente o a una CA principale. Suggerimenti: se si desidera importare un certificato utente, selezionare l'archivio certificati <i>Personale</i> .
<input checked="" type="checkbox"/> <i>Includi l'intera catena di certificati, se disponibile nel file PKCS #12</i>	I file PKCS #12 possono contenere, oltre al proprio certificato, anche una catena completa di certificati. Una catena di certificati comprende tutti i certificati rilasciati da un'Autorità di certificazione (CA) necessari per convalidare il proprio certificato. Selezionare questa casella di controllo per importare l'intera catena di certificati (purché disponibile nel file PKCS #12 selezionato).  Se si sceglie di importare l'intera catena di certificati, tutti i certificati CA verranno automaticamente memorizzati negli archivi certificati corrispondenti. Esempio

	<p>Si è scelto di importare un file PKCS #12 contenente il proprio certificato utente, la chiave privata, un certificato di una CA intermedia e un altro certificato di una CA principale attendibile.</p> <p>È stato selezionato l'archivio certificati <i>Personale</i>.</p> <ul style="list-style-type: none">→ Il proprio certificato verrà salvato nell'archivio <i>Personale</i>.→ Il certificato della CA intermedia verrà salvato nell'archivio <i>Autorità di certificazione intermedie</i>.→ Il certificato della CA principale verrà salvato nell'archivio <i>Autorità di certificazione fonti attendibili</i>.
<input checked="" type="checkbox"/> <i>Abilita la protezione avanzata chiave privata</i>	<p>Selezionare questa casella di controllo se si vuole garantire che la chiave privata non venga utilizzata da altri utenti.</p> <p>Attivando la <i>protezione avanzata chiave privata</i>, verrà richiesta una password ogni volta che si utilizza la chiave.</p>



Infineon Security Platform Solution - Icona TNA

Icona TNA di Security Platform

L'icona TNA costituisce il punto d'accesso alle attività amministrative di Security Platform, in base allo stato del software. Grazie a questa icona, è possibile accedere a un menu dedicato, denominato menu TNA. Inoltre, una serie di note e le descrizioni dei comandi forniscono informazioni utili circa lo stato del software.

Icona TNA

Questa icona si trova nell'area di notifica della barra delle applicazioni (Taskbar Notification Area, TNA) e consente di accedere a diverse attività amministrative di Security Platform, in funzione dello stato del software.

L'aspetto dell'icona indica chiaramente lo stato attuale di Security Platform:

 Security Platform è pronto all'uso.

 Security Platform è inizializzato ma è stato disabilitato in modo permanente o temporaneo. È consentita l'abilitazione di Security Platform da parte dell'utente attuale.

 Security Platform non è stato inizializzato per l'utente attuale.

 Security Platform è stato disabilitato in modo permanente o temporaneo, oppure il test automatico non è riuscito. L'utente attuale non può modificare lo stato di Security Platform.

 Security Platform non è stato inizializzato.

Menu TNA

Questo menu viene visualizzato facendo clic sull'icona TNA.

Il menu consente di eseguire diverse attività amministrative in base allo stato del software:

- Inizializzazione di Security Platform
- Inizializzazione utenti di Security Platform
- Amministrazione di Security Platform
- Visualizzazione della Guida Online per eseguire varie attività

	 Non tutti gli elementi del menù sono disponibili in modalità server .
Balloons	<p>Le balloons forniscono informazioni circa i cambiamenti di stato di Security Platform e suggeriscono le attività da eseguire in base ai diversi stati del software.</p> <p> In modalità server, i compiti che non richiedono l'interazione dell'utente sono gestiti dal Trusted Computing Management Server. Aree commenti relative a questi compiti non sono disponibili.</p>
Descrizioni dei comandi	Spostando il mouse sull'icona TNA, vengono visualizzate alcune brevi informazioni di stato sotto forma di descrizione comandi.



Infineon Security Platform Solution - Icona TNA

Elementi del Menu Icona di Notifica

In funzione dello stato attuale di Infineon Security Platform e dell'utente attualmente connesso, il menu Icona di Notifica può presentare elementi diversi.

Grazie a questo menu, è possibile utilizzare tutti gli strumenti di Infineon Security Platform, purché l'utente disponga delle autorizzazioni necessarie. Se l'utente attualmente connesso non è autorizzato all'uso di un determinato comando, la voce corrispondente non apparirà nel menu.



Questa icona scudo è visibile solo per gli utenti con diritti amministrativi in sistemi operativi con [Controllo account utente](#) (es. Windows 7 e Windows Vista).

La tabella seguente elenca tutti gli elementi di menu.

Elementi di menu	Informazioni
<i>Gestione di Security Platform</i>	Avvia il Tool di configurazione di Infineon Security Platform .  Nei sistemi operativi con Controllo account utente, il Tool di configurazione viene avviato senza privilegi elevati.
<i>Inizializzazione di Security Platform</i>	Avvia l' Inizializzazione utenti guidata di Infineon Security Platform . Il comando è disponibile se non è ancora stata eseguita la configurazione di Infineon Security Platform. Questa voce apparirà in grigio (disattivata) se il criterio <i>Consenti iscrizione alla piattaforma</i> è disabilitato (Questo criterio è attivo se Security Platform non è stato inizializzata precedentemente).  Questo oggetto del menù non è disponibile in modalità server , poiché la Security Platform viene inizializzata automaticamente se il sistema cliente è integrato in un Trust Domain con gestione

	Centralizzata.
<p><i>Inizializzazione utenti di Security Platform</i></p>	<p>Avvia l'Inizializzazione utenti guidata di Infineon Security Platform.</p> <p>Il comando è disponibile se non è ancora stata eseguita la configurazione degli utenti di Infineon Security Platform. Questa voce apparirà in grigio se Security Platform è non inizializzato e il criterio <i>Consenti l'iscrizione dell'utente</i> è disabilitato (questo criterio è attivo solo per gli utenti ancora non inizializzati).</p> <p> Questo elemento del menu non è disponibile in modalità server se l'utente attuale non è un membro del Gruppo di Iscrizione Utenti.</p>
<p><i>Abilita backup delle funzionalità di Security Platform</i></p>	<p>Consente di includere le chiavi e le credenziali utente nelle operazioni di backup automatico. Verrà richiesto di eseguire l'autenticazione in Security Platform. Questa voce è disponibile quando l'amministratore di Security Platform ha già configurato il backup ma l'utente attuale non ha ancora abilitato la funzione.</p> <p> Questo oggetto del menù non è disponibile in modalità server, poiché il Backup e il Ripristino sono gestiti dal Trusted Computing Management Server.</p>
<p><i>Abilita reimpostazione password</i></p>	<p>Abilita la funzionalità di reimpostazione della password per l'account utente attuale. Questa voce è disponibile quando l'amministratore di Security Platform ha già configurato la reimpostazione password ma l'utente attuale non ha ancora abilitato la funzione.</p>

<p><i>Personal Secure Drive - Caricamento</i></p> <p>o</p> <p><i>Personal Secure Drive - <LetteraUnità:EtichettaUnità> - Caricamento</i></p>	<p>Caricare Personal Secure Drive. Se si è eseguita l'installazione di più di una PSD, nel menu verranno riportate tutte le unità (<LetteraUnità:EtichettaUnità>). Questo articolo menu è disponibile se si è configurata almeno una PSD (attualmente non caricata).</p>
<p><i>Personal Secure Drive - Scaricamento</i></p> <p>o</p> <p><i>Personal Secure Drive - <LetteraUnità:EtichettaUnità> - Scaricamento</i></p>	<p>Scaricare Personal Secure Drive. Se si è eseguita l'installazione di più di una PSD, nel menu verranno riportate tutte le unità (<LetteraUnità:EtichettaUnità>). Questo articolo menu è disponibile se si è configurata almeno una PSD (attualmente caricata).</p>
<p><i>Personal Secure Drive - Caricamento all'Accesso</i></p> <p>o</p> <p><i>Personal Secure Drive - <LetteraUnità:EtichettaUnità> - Caricamento all'Accesso</i></p>	<p>Specificare se si desidera caricare la PSD automaticamente dopo aver eseguito l'accesso in Windows. Se si è eseguita l'installazione di più di una PSD, nel menu verranno riportate tutte le unità (<LetteraUnità:EtichettaUnità>). Se viene visualizzato un segno di spunta qui, la PSD sarà caricata. Fare clic qui per aggiungere/rimuovere il segno di spunta. Questo articolo menu è disponibile se si è configurata almeno una PSD.</p>
<p><i>Personal Secure Drive - Creare/Gestione</i></p>	<p>Creare, modificare o cancellare una Personal Secure Drive mediante Inizializzazione Utenti Guidata.</p>
<p><i>Personal Secure Drive - Scaricare tutto</i></p>	<p>Scaricare tutte le Personal Secure Drive attualmente caricate.</p>
<p><i>Disconnessione da Encrypting File System</i></p>	<p>Consente di disconnettersi da Encrypting File System. Sarà quindi necessario eseguire di nuovo l'autenticazione per accedere ai dati protetti EFS. Questa voce è disponibile soltanto se è stata</p>

	<p>eseguita almeno un'autenticazione per accedere ai dati protetti da EFS.</p>
<p><i>Modifica password utente di base</i></p>	<p>Cliccare su questo pulsante per cambiare la password utente di base.</p> <p>Questa voce di menu è disponibile soltanto quando la password utente di base è scaduta. La scadenza della password può essere impostata mediante l'apposito criterio utente <u>Durata massima della password utente di base</u>.</p>
<p><i>Sincronizza frase password utente di base</i></p>	<p>Cliccare qui se si desidera utilizzare la stessa frase password, sia sul dispositivo di autenticazione, sia su Security Platform. Questa voce di menu è disponibile soltanto quando si utilizzano frasi password diverse per il dispositivo di autenticazione e per Security Platform. Possibili cause:</p> <ul style="list-style-type: none">• La frase password utente di base è stata <u>reimpostata</u> senza aggiornare la configurazione del dispositivo di autenticazione.• Si utilizza lo stesso dispositivo di autenticazione per più installazioni di Security Platform e la frase password è stata modificata su un'installazione diversa da quella in uso.
<p><i>Riconfigurazione delle funzionalità utente</i></p>	<p>Cliccare su questo pulsante per riconfigurare le funzionalità di Security Platform. Questa voce è disponibile soltanto quando PSD o EFS richiede riconfigurazione. Possibili cause:</p> <ul style="list-style-type: none">• Il certificato EFS o PSD non è valido o non è più disponibile. Questa condizione riguarda anche la funzione <i>Crittografia di file e cartelle con Encrypting File System (EFS)</i>, quando sono stati configurati sia Personal

	<p><i>Secure Drive, che Encrypting File System e il certificato PSD è stato successivamente modificato.</i></p> <ul style="list-style-type: none">• È stato eseguito un ripristino e la vostra PSD non può più essere caricata (es. perché la lettera di unità non è in uso).
<p><i>Disabilita Security Platform temporaneamente fino al riavvio successivo</i></p>	<p>Cliccare su questo comando per interrompere il funzionamento di Infineon Security Platform fino al successivo riavvio del sistema. Le applicazioni che utilizzano Security Platform non potranno più accedere ai dati protetti da Trusted Platform Module, come i dati di EFS, Personal Secure Drive e altri. L'accesso ai dati protetti viene ripristinato soltanto quando Security Platform è nuovamente abilitato. Il comando è disponibile soltanto se Infineon Security Platform è stato inizializzato e abilitato. Si noti che tale funzione non è disponibile per i sistemi Security Platform che utilizzano Trusted Platform Module 1.2.</p>
<p><i>Attivazione di Security Platform</i></p>	<p>Il comando è disponibile per gli amministratori se Security Platform è stato inizializzato in modalità autonoma, se Security Platform è stato disabilitato dal proprietario. È richiesta la password del proprietario. Il comando è inoltre disponibile per gli utenti se Security Platform è stato inizializzato con una versione di Trusted Platform Module inferiore a 1.2, se Security Platform è stato temporaneamente disabilitato dall'utente. In questo caso, è necessario che l'utente riavvii il sistema.</p> <p> Questo oggetto del menù non è</p>

	<p>disponibile in modalità server, poiché la Security Platform viene inizializzata automaticamente se il sistema cliente è integrato in un Trust Domain con gestione Centralizzata.</p>
<p><i>Ripristina Security Platform</i></p>	<p>Ripristina le credenziali e le impostazioni di Security Platform da un archivio di backup. Il comando è disponibile soltanto per gli amministratori del sistema, nei casi in cui Security Platform non sia stato inizializzato, l'inizializzazione sia stata eseguita con un altro sistema operativo o sia cambiato il proprietario della piattaforma.</p> <p> Questo oggetto del menù non è disponibile in modalità server, poiché il Backup e il Ripristino sono gestiti dal Trusted Computing Management Server.</p>
<p><i>Ripristina funzionalità di Security Platform</i></p>	<p>Ripristina le credenziali e le impostazioni utente da un archivio di backup. Il comando è disponibile soltanto se non è possibile caricare la chiave utente di base, ovvero non è possibile utilizzare le funzionalità di Security Platform.</p> <p> Questo oggetto del menù non è disponibile in modalità server, poiché il Backup e il Ripristino sono gestiti dal Trusted Computing Management Server.</p>
<p><i>Credenziali / Impostazioni Utente - Richiedere Copia Lavoro Locale</i></p>	<p>Ottenere una copia lavoro locale delle tue credenziali e delle tue impostazioni utente dal Trusted Computing Management Server. Blocca i cambiamenti da altri computer fino a che non hai accettato o scartato i tuoi cambiamenti locali (lo stato della sessione utente in modalità server è impostato su</p>

"Lettura/Scrittura permanente").

 Questo oggetto del menù è disponibile solo in [modalità server](#).

Esegui questa azione prima di portare offline la tua piattaforma se vuoi cambiare le tue credenziali o le tue impostazioni utente senza avere una connessione di rete al Trusted Computing Management Server. Un tipico esempio è il cambiamento o il reset della tua Password Utente di Base su un notebook offline.

Precondizioni:

- L'utente attuale è stato inizializzato in modalità utente.
- La tua Piattaforma è connessa al Trusted Computing Management Server.
- Non c'è alcuna copia locale di lavoro attiva sulla stessa piattaforma (lo stato della sessione utente sulla stessa piattaforma non è impostato su "Lettura/Scrittura permanente").

Se è presente un accesso di scrittura corrente alle vostre credenziali utente o se le vostre credenziali utente non sono aggiornate, sarete informati che al momento non è possibile richiedere alcuna copia locale di lavoro. Nel primo caso, attendete qualche istante e tentate nuovamente. Nel secondo caso, l'area commenti vi inviterà ad aggiornare le vostre credenziali utente.

Dettagli sullo [stato della sessione utente](#).

*Credenziali / Impostazioni
Utente - Accettare
Cambiamenti Locali*

Rilasciare i cambiamenti delle credenziali o delle impostazioni utente al Trusted Computing Management Server. Permettere i

cambiamenti da un'altra piattaforma.

 Questo oggetto del menù è disponibile solo in [modalità server](#).

Eeguire questa azione quando la tua piattaforma è online di nuovo, dopo aver cambiato le tue credenziali o le tue impostazioni localmente.

Precondizioni:

- L'utente attuale è stato inizializzato in modalità utente.
- La tua Piattaforma è connessa al Trusted Computing Management Server.
- C'è una copia lavoro locale attiva (lo stato della sessione utente su questa piattaforma è "Lettura/Scrittura permanente").

Credenziali / Impostazioni Utente - Abbandonare i Cambiamenti Locali

Abbandonare i cambiamenti delle tue credenziali o impostazioni utente. Permettere i cambiamenti da un'altra piattaforma.

 Questo oggetto del menù è disponibile solo in [modalità server](#).

Esegui questa azione quando la tua piattaforma è online di nuovo, e non hai cambiato le credenziali o le impostazioni, o se vuoi eliminare i tuoi cambiamenti.

Precondizioni:

- L'utente attuale è stato inizializzato in modalità utente.
- La tua Piattaforma è connessa al Trusted Computing Management Server.
- C'è una copia lavoro locale attiva (lo stato della sessione utente su questa

	<p>piattaforma è "Lettura/Scrittura permanente").</p>
<p><i>Aggiornare le Credenziali e le Impostazioni Utente</i></p>	<p>Eeguire questo compito per aggiornare le tue credenziali e le tue impostazioni utente sulla piattaforma attuale.</p> <p> Questo oggetto del menù è disponibile solo in modalità server.</p> <p>Precondizioni:</p> <ul style="list-style-type: none"> • L'utente attuale è stato inizializzato in modalità utente. • La tua Piattaforma è connessa al Trusted Computing Management Server. <p>Informazioni sugli aggiornamenti sulle credenziali e sulle impostazioni utente</p>
<p><i>Aggiornare</i></p>	<p>Aggiornare l'Icona di Notifica della Barra delle Applicazioni e il Menu di Notifica della Barra delle Applicazioni.</p>
<p><i>Cancellazione Cache Autenticazione</i></p>	<p>Invertire l'effetto di <i>Ricorda password per tutte le applicazioni</i>, come impostato nel dialogo di autenticazione della Password Utente di Base. Si verrà in seguito invitati ad effettuare una nuova autenticazione quando necessario.</p> <p> Questo articolo menu è disponibile solo se <i>Ricorda password per tutte le applicazioni</i> è stato in precedenza selezionato nel dialogo di autenticazione della Password Utenti di Base.</p>
<p><i>Attivazione Infineon TPM Strong Cryptographic Provider</i></p>	<p>Per attivare Infineon TPM Strong Cryptographic Provider è necessario generare una chiave. Fare clic qui per autorizzare la generazione della chiave.</p>

<i>Guida</i>	Visualizza la Guida Online di Infineon Security Platform.
Guida sensibile al contesto per vari elementi di menu	In base al contesto, viene visualizzata la Guida rapida con informazioni relative allo stato attuale della piattaforma e alle operazioni richieste.



©Infineon Technologies AG

Infineon Security Platform Solution - Icona TNA

Come disabilitare Trusted Platform Module

Trusted Platform Module può essere disabilitato in due modi diversi.

- **Disabilitazione temporanea**

Il chip di protezione viene disabilitato fino al successivo riavvio del sistema. L'eventuale accesso di altri utenti non influenza lo stato attuale del chip.

- **Disabilitazione permanente**

Questa operazione esclude "fisicamente" il chip di protezione. Se Infineon Security Platform è già stato configurato, è possibile eseguire l'operazione tramite il [Tool di configurazione di Infineon Security Platform](#).

Per abilitare nuovamente Infineon Security Platform, utilizzare lo stesso Tool di configurazione. Nel caso in cui Infineon Security Platform non sia stato configurato, è necessario abilitare il chip dal BIOS di sistema.



©Infineon

Technologies AG

Infineon Security Platform Solution - Icona TNA

Come disabilitare Infineon Security Platform temporaneamente

Un particolare meccanismo consente di disattivare Infineon Security Platform fino a quando il sistema non viene riavviato. Questa disattivazione temporanea resta valida anche quando gli utenti di Infineon Security Platform si connettono o disconnettono dalla piattaforma.

Tutte le funzionalità di Infineon Security Platform e di Trusted Platform Module vengono bloccate per impedirne l'utilizzo.



©Infineon

Technologies AG

Infineon Security Platform Solution - Icona TNA

Come abilitare Infineon Security Platform

Per attivare la Security Platform, passare a **Avanzate** in Tool di configurazione e fare clic su **Abilita...** (vedere [Impostazioni avanzate](#)). Si noti che soltanto il [proprietario di Security Platform](#) può eseguire questa azione in quanto sono richiesti i diritti amministrativi e la password del proprietario.

Dopo aver abilitato Security Platform, eseguire la configurazione iniziale di Security Platform e utenti attraverso l'[Inizializzazione Rapida Guidata](#) (consigliata per la maggior parte degli utenti), o mediante l'[Inizializzazione Guidata](#) e [Inizializzazione Utenti Guidata](#) (consigliata per gli utenti esperti).



©Infineon

Technologies AG

Soluzione Infineon Security Platform - Amministrazione dei criteri

Amministrazione dei criteri di Infineon Security Platform

L'Editor Criteri Gruppo Locale consente di amministrare le impostazioni di protezione relative a Infineon Security Platform:

Criteri di sistema:	impostazioni di protezione del computer.
Criteri utente:	impostazioni di protezione per gli utenti del computer.



In [modalità server](#), i criteri sono configurati in tutto il dominio da un amministratore di dominio attraverso Trusted Computing Management Server.

Condizioni preliminari e restrizioni



- I criteri utente e di sistema possono essere modificati unicamente dagli amministratori.
- L'Editor Criteri di gruppo locali non è disponibile nelle edizioni Home di Windows.

Come registrare i Criteri di Security Platform

Nei sistemi operativi che supportano il formato dei criteri ADMX (es. Windows 7 e Windows Vista), i Criteri di Security Platform vengono registrati automaticamente (file modello amministrativo **IfxSpPol.admx**).

Su sistemi operativi diversi, è necessario eseguire le seguenti fasi per registrare manualmente i Criteri di Security Platform (file modello amministrativo **IfxSpPol.adm**), prima di accedere ai criteri da [Tool di Configurazione](#):

1. Avviare Editor Criteri Gruppo Locale (gpedit.msc)
2. Fare clic con il tasto destro su **Modelli Amministrativi di Configurazione Computer** o **Configurazione Utente**.
3. Nel menu di scelta rapida, fare clic su **Aggiungi/Rimuovi modelli...** .
Viene visualizzata la finestra di dialogo "Aggiungi/Rimuovi Modelli".
4. Fare clic su **Aggiungi**.
Viene visualizzata la finestra di dialogo di ricerca "Modelli Criteri".
5. Selezionare il modello **IfxSpPol.adm**, e fare clic su **Apri** per aggiungere il modello "Security Platform".
6. Fare clic su **Chiudi** per registrare il nuovo modello amministrativo.

Come modificare i Criteri Sistema e i Criteri Utente

1. Avviare [Tool di Configurazione](#) da [Icona di Notifica della Barra delle Applicazioni](#).
Su sistemi operativi dotati di Controllo account utente (es. Windows 7 e Windows Vista), fare clic su  **Gestire Security Platform**.
Su sistemi operativi diversi, fare clic su **Gestire Security Platform**.
2. Per modificare i Criteri Sistema, fare clic su **Sistema...** nella scheda **Avanzate**.
Per modificare i Criteri Utente, fare clic su **Utente...** nella scheda **Avanzate**.

L'Editor Criteri Gruppo Locale è avviato. Visualizza i Criteri Sistema o i Criteri Utente di Infineon Security Platform.

Ulteriori informazioni

Per informazioni dettagliate sui criteri di sistema e i criteri utente, consultare la sezione Introduzione ai criteri di gruppo Microsoft e il sito Microsoft TechNet. Per consultare la Guida in linea Microsoft, ridurre a icona tutte le finestre attualmente aperte in modo da visualizzare il desktop di Windows. Premere F1 ed eseguire la ricerca desiderata utilizzando una parola chiave appropriata.



©Infineon Technologies AG

Soluzione Infineon Security Platform - Amministrazione dei criteri

Criteri di sistema di Infineon Security Platform

Il software Soluzione Infineon Security Platform supporta le impostazioni dei criteri di sistema indicate di seguito.



In [modalità server](#), i criteri di sistema sono configurati in tutto il dominio da un amministratore di dominio attraverso Trusted Computing Management Server. Tenere presente che le impostazioni valide solo per la modalità server vengono descritte nel file modello amministrativo fornito da Trusted Computing Management Server.



Valore predefinito: se non si imposta esplicitamente un determinato criterio (lo stato indicato nell'editor locale Criteri di gruppo è **Non configurato**), viene applicato automaticamente un valore predefinito.

Impostazioni di tutte le versioni

Impostazioni validi per la versione modalità autonoma e anche per la versione modalità server.

Criteria	Informazioni	Valore predefinito
<i>Preparare registrazione TPM</i>	<p>Abilitato: Su le piattaforme non inizializzati in cui Trusted Platform Module è stato disabilitato e la Physical Presence Interface (PPI) è stato supportato, Trusted Platform Module verrà preparato automaticamente per essere abilitato. Il software offre istruzioni agli utenti per completare l'abilitazione.</p> <p>Disabilitato: Trusted Platform Module non è preparato per l'abilitazione automaticamente.</p>	Disabilitato
<i>Consenti agli amministratori di utilizzare le chiavi della piattaforma in modalità remota</i>	<p>Abilitato: gli amministratori possono utilizzare le chiavi della piattaforma non solo a livello locale ma anche in remoto.</p> <p>Disabilitato: Non è consentito l'utilizzo delle chiavi della piattaforma in modalità remota. Per motivi di riservatezza, l'accesso a queste chiavi è sottoposto a restrizioni, come stabilito dal Trusted Computing Group (TCG). In questo modo, tutte le chiavi che potrebbero consentire l'identificazione di Security Platform risulteranno nascoste all'accesso remoto. Il</p>	Disabilitato

criterio richiede che tutti i computer interessati appartengano a domini trusted ed è quindi rilevante soltanto per i sistemi operativi che supportano l'appartenenza al dominio.



Si noti che questo criterio non influenza la gestione e il funzionamento di Security Platform.

Consenti la lettura della memoria NV non protetta di TPM

Consente di stabilire quali utenti possono leggere la memoria non volatile (NV) e non protetta di Trusted Platform Module 1.2. Tale memoria può contenere dati riservati.

Abilitato: Specificare se la lettura dei dati archiviati nella memoria NV debba essere consentita solo agli amministratori locali, anche agli amministratori remoti oppure solo agli utenti locali o a tutti gli utenti.

Disabilitato: Nessun utente può leggere i dati presenti nella memoria NV.



Questo criterio è rilevante esclusivamente per i sistemi Security Platform che utilizzano Trusted Platform Module 1.2.

Si noti che l'amministrazione e la funzionalità di Security Platform non sono influenzate da questa impostazione.

Abilitato/Amministratori locali

Configura la soglia di protezione contro gli attacchi del dizionario

Determina il numero di tentativi di autenticazione consentiti in Trusted Platform Module, prima che vengano adottate misure di difesa da attacchi a dizionario.

Abilitato: Specifica quanti tentativi di autenticazione dovrebbero essere consentiti per le chiavi (utilizzate per l'autenticazione Utente di Security Platform), per il proprietario e per l'accesso a dati protetti (utilizzati da Windows BitLocker in associazione a PIN) prima che siano adottate misure di difesa da attacchi a dizionario.

Disabilitato: Non è possibile configurare nessuna soglia di protezione. Vengono attivati i valori predefiniti.



Questo criterio è applicabile unicamente ai sistemi Security Platform dotati di Infineon Trusted Platform Module 1.2. E deve essere impostato prima di inizializzare il Security Platform. Eventuali modifiche apportate in seguito avranno effetto soltanto alla successiva [reimpostazione del livello di protezione](#).

Se questo criterio non è configurato, le stesse impostazioni possono essere impostate singolarmente per ciascuna piattaforma in modalità autonoma mediante

Abilitato

Proprietario: 3 tentativi

Chiave: 5 tentativi

Dati: 10 tentativi

	<p>l'inizializzazione guidata (vedere Configurazione impostazioni di difesa da attacchi a dizionario).</p> <p>In questo caso non è necessario alcun ripristino del livello di difesa perché le impostazioni abbiano effetto.</p> <p>Il numero di tentativi di autenticazione consentiti è identico per tutti gli utenti di Security Platform. Si consiglia di valutare questo aspetto nel caso in cui esistano più utenti paralleli nel sistema (ad esempio, mediante la funzione Cambio rapido utente).</p> <p>Ulteriori informazioni sugli attacchi del dizionario</p>	
<p><i>Attivazione di sicurezza del campo password ristretta</i></p>	<p>Abilitato: La funzione di taglia, copia, incolla e visualizzazione della password non è disponibile nei campi della password.</p> <p>Disabilitato: La funzione di incolla è disponibile nei campi della password. Inoltre la funzione di taglia e copia è disponibile quando la password è visibile in formato testo.</p>	<p>Disabilitato</p>
<p><i>Eliminazione delle chiavi durante gli stati di risparmio energia.</i></p>	<p>Abilitato: Le chiavi di Security Platform sono eliminate prima che venga attivato lo stato di risparmio energia di tipo standby (S3) o sospensione (S4). Il livello di sicurezza durante lo stato di risparmio energia è elevato.</p>	<p>Abilitato</p>

	<p>Quando si disattiva lo stato di risparmio energia, l'utente deve effettuare una nuova autenticazione per le funzioni di Security Platform.</p> <p>Disabilitato: le chiavi di Security Platform non sono eliminate.</p>	
<p><i>Provider di Autenticazione Avanzata</i></p>	<p>Abilitato: Inserire un class ID (CLSID) di Provider Autenticazione Avanzata, o CLSID multiple separate da punto e virgola. Solo i provider specificati qui verranno accettati per utilizzare l'Autenticazione Avanzata sui sistemi clienti che non sono ancora predisposti. Se non conosce un class ID di Provider Autenticazione Avanzata, contatta il produttore di provider di Autenticazione Avanzata. Esempio di Class ID: {76D8D888-B5AC-49FC-9408-8A45D37F3AC6}.</p> <p>Disabilitato: nessun provider di Autenticazione Avanzata può essere specificato. L'Autenticazione Avanzata non può essere utilizzata su sistemi clienti che non sono ancora predisposti.</p>	<p>In modalità server, si comporta come se fosse disabilitato.</p> <p>In modalità stand-alone, stesso comportamento come nella ex versioni del prodotto, vale a dire fornitori di installato può essere utilizzato.</p>
<p><i>Consenti agli</i></p>	<p>Abilitato: Non è necessaria la</p>	<p>Disabilitato</p>

amministratori di diventare proprietari in modalità remota

presenza in loco di un amministratore per acquisire la proprietà del software sul computer. Questa funzionalità può essere molto utile per le reti di grandi dimensioni, in cui occorre eseguire la configurazione di più client.

Disabilitato: non è consentito acquisire la proprietà in modalità remota.



Il criterio richiede che tutti i computer interessati appartengano a domini trusted, ed è quindi rilevante soltanto per i sistemi operativi che supportano l'appartenenza al dominio.

Consenti agli amministratori di diventare proprietari in modalità remota

Consente di stabilire quali utenti possono leggere la chiave pubblica Storage Root Key (SRK) di Trusted Platform Module. La chiave pubblica SRK richiede particolare protezione, in quanto Security Platform può essere identificato attraverso tale chiave.

Abilitato: Gli amministratori possono recuperare la chiave pubblica SRK non solo a livello locale ma anche in remoto.

Disabilitato: non è consentito recuperare la chiave pubblica SRK in modalità remota.



La funzione di migrazione

Disabilitato

[Esportazione e autenticazione automatica](#) necessita l'abilitazione di questo criterio sul computer di destinazione. Il criterio richiede che tutti i computer interessati appartengano a domini trusted. Questo criterio è rilevante soltanto per i sistemi operativi che supportano l'appartenenza al dominio.

Impostazioni della versione modalità autonoma

Impostazioni validi solo per la versione modalità autonoma.

Criteri	Informazioni
<i>Password del Proprietario - Lunghezza minima della password</i>	<p>Abilitato: Inserire la lunghezza minima della Password proprietario, ad es. 6. La lunghezza minima della password è valida per le Password proprietario che sono impostate o modificate di conseguenza.</p> <p>Disabilitato: La lunghezza minima della password è di 6 caratteri.</p> <p> Questa impostazione si applica solo per le Password del Proprietario attivate su una Security Platform in modalità autonoma. La lunghezza minima della password per le Password del Proprietario definite tramite il Trusted Computing Management Server è stabilita dalla politica del Trusted Computing Management Server con lo stesso nome.</p> <p>Ulteriori informazioni sulla gestione delle password</p>
<i>Password del Proprietario - Le password devono essere conformi ai requisiti di complessità</i>	<p>Abilitato: I requisiti di complessità della password sono applicati per le Password di Proprietario che sono impostate o modificate di conseguenza.</p> <p>Disabilitato: non viene applicato nessun requisito di complessità.</p> <p> Questa impostazione si applica solo per le Password del Proprietario attivate su una Security Platform in modalità autonoma. I requisiti di complessità per le Password del Proprietario stabiliti tramite il Trusted Computing Management Server sono stabiliti dalla politica del Trusted Computing Management Server con lo stesso nome. Ulteriori informazioni sui requisiti di complessità delle password</p>
<i>Consenti iscrizione alla piattaforma</i>	<p>Abilitato/Consenti la gestione dell'interfaccia e del wizard: l'amministratore è autorizzato all'uso dell'Inizializzazione guidata di Security Platform e dell'interfaccia del management provider per l'inizializzazione del software.</p>

	<p>Abilitato/Consenti soltanto la Management Provider dell' interfaccia: l'amministratore può accedere all'interfaccia del management provider ma non può eseguire l'Inizializzazione guidata di Security Platform.</p> <p>Disabilitato: l'amministratore di Security Platform non è autorizzato ad eseguire nessuna delle funzioni del software.</p>
<p><i>Imponi la configurazione del backup includendo il ripristino di emergenza</i></p>	<p>Abilitato: la configurazione del backup automatico (comprendente il ripristino di emergenza) è obbligatoria per l'inizializzazione di Security Platform. Tale obbligo viene meno se Security Platform è già stato inizializzato senza configurare il backup automatico.</p> <p>Disabilitato: la configurazione del backup automatico non è obbligatoria. Le operazioni di backup possono essere configurate anche dopo l'inizializzazione di Security Platform selezionando Tool di configurazione - Backup - Configura....</p>
<p><i>Percorso dell'archivio di backup</i></p>	<p>Abilitato: Inserire un percorso includendo il nome del file, ad esempio \\BackupServer\SecurityPlatformShare\SPSystemBackup.xml. Il percorso specificato verrà imposto durante la configurazione della funzionalità di backup. Verrà creato automaticamente un archivio di backup costituito da un file XML e da una cartella con lo stesso nome, ad esempio, file SPSysSystemBackup.xml nella cartella SPSysSystemBackup. Se questa funzionalità è già stata impostata, il percorso di backup esistente verrà mantenuto fino a quando la funzione non viene riconfigurata.</p> <p> Assicurarsi di immettere un percorso valido che sia accessibile a tutti i PC di Security Platform. In caso contrario, la configurazione del backup non verrà completata.</p> <p>Disabilitato: consente di specificare il percorso di destinazione desiderato durante la configurazione del backup.</p>
<p><i>Attiva backup di sistema</i></p>	<p>Abilitato: L'archivio di backup del sistema viene aggiornato immediatamente in caso di modifiche significative dei dati di</p>

<p><i>immediato</i></p>	<p>Security Platform.</p> <p> Precondizioni: È necessario configurare il backup automatico. Inoltre, occorre consentire l'accesso in scrittura all'archivio di backup del sistema.</p> <p>Disabilitato: L'archivio di backup del sistema non viene aggiornato immediatamente in caso di modifiche significative dei dati di Security Platform. Se è stato configurato il backup automatico ed è consentito l'accesso in scrittura all'archivio di backup, l'aggiornamento verrà eseguito al prossimo backup di sistema pianificato.</p>
<p><i>Utilizza la chiave pubblica del token di ripristino di emergenza presente in archivio</i></p>	<p>Abilitato: Inserire un percorso includendo il nome del file della chiave pubblica, ad esempio \\NomeServer\NomeCartella\NomeFile.xml. Il percorso specificato verrà imposto durante la configurazione del ripristino di emergenza. Se il ripristino di emergenza è già stato configurato su un PC Security Platform, l'impostazione non avrà alcun effetto sul computer in uso.</p> <p> Assicurarsi di immettere un percorso valido che sia accessibile a tutti i PC di Security Platform. In caso contrario, la configurazione del ripristino di emergenza non verrà completata.</p> <p>Disabilitato: il Token di ripristino di emergenza può essere creato o selezionato quando è configurato il ripristino di emergenza.</p> <p>Ulteriori informazioni sulla configurazione del ripristino di emergenza Come creare un file di archivio della chiave pubblica da un file token</p>
<p><i>Imponi la configurazione della reimpostazione password</i></p>	<p>Abilitato: la configurazione della reimpostazione password è obbligatoria per l'inizializzazione di Security Platform. Tale obbligo viene meno se il software è già stato inizializzato senza configurare la reimpostazione password.</p> <p>Disabilitato: la configurazione della reimpostazione</p>

password non è obbligatoria. Tale operazione può essere eseguita anche dopo l'inizializzazione di Security Platform selezionando [Tool di configurazione - Reimpostazione password - Configura...](#).

Utilizza la chiave pubblica del token di reimpostazione password presente in archivio

Abilitato: Inserire un percorso includendo il nome del file della chiave pubblica, ad esempio

\\NomeServer\NomeCartella\NomeFile.xml.

Il percorso specificato verrà imposto durante la configurazione della reimpostazione password.

Se la funzione è già stata configurata su un PC Security Platform, l'impostazione non avrà alcun effetto sul computer in uso.



Assicurarsi di immettere un percorso valido che sia accessibile a tutti i PC di Security Platform. In caso contrario, la configurazione della reimpostazione password non verrà completata.

Disabilitato: il Token di reimpostazione password può essere creato o selezionato quando è configurata la reimpostazione della password.

[Ulteriori informazioni sulla configurazione della reimpostazione password](#)

[Come creare un file di archivio della chiave pubblica da un file token](#)

Impostazioni delle versioni precedenti del prodotto

Impostazioni validi solo per le versioni precedenti del prodotto.

Criteri	Informazioni	Valore predefinito
<i>Percorso dell'archivio di ripristino di emergenza</i>	<p>Questo criterio è rilevante unicamente per le versioni precedenti del software Soluzione Security Platform.</p> <p>In tali versioni, il percorso dell'archivio di ripristino di emergenza poteva essere impostato direttamente durante l'inizializzazione di Security Platform. Questo criterio consentiva di imporre l'utilizzo del percorso indicato.</p> <p>Nella versione attuale del software, il percorso del file viene impostato automaticamente.</p>	---
<i>URL per la registrazione dei certificati durante la procedura guidata</i>	Consultare la sezione Criteri utente .	Disabilitato



Soluzione Infineon Security Platform - Amministrazione dei criteri

Criteri utente di Infineon Security Platform

Il software Infineon Security Platform Solution supporta le impostazioni dei criteri utente indicate di seguito.



In [modalità server](#), i criteri utente sono configurati in tutto il dominio da un amministratore di dominio attraverso Trusted Computing Management Server. Tenere presente che le impostazioni valide solo per la modalità server vengono descritte nel file modello amministrativo fornito da Trusted Computing Management Server.



Valore predefinito: se non si imposta esplicitamente un determinato criterio (lo stato indicato nell'editor locale Criteri di gruppo è **Non configurato**), viene applicato automaticamente un valore predefinito.

Impostazioni di tutte le versioni

Impostazioni validi per la versione modalità autonoma e anche per la versione modalità server.

Criteri	Informazioni	Valore predefinito
<i>Password utente di base - Lunghezza minima della password</i>	Abilitato: immettere la lunghezza minima della password utente di base, ad esempio 6. La lunghezza minima specificata è valida per le password che verranno impostate o modificate successivamente. Disabilitato: La lunghezza minima della password è di 6 caratteri. Ulteriori informazioni sulla gestione delle password	Abilitato caratteri
<i>Password utente di base - Le password devono essere conformi ai requisiti di complessità</i>	Abilitato: vengono applicati i criteri di complessità per le password utente di base che saranno impostate o modificate successivamente. Disabilitato: non viene applicato nessun requisito di complessità. Ulteriori informazioni sui requisiti di complessità delle password	Disabilitato
<i>Password utente di base - Durata massima della password</i>	Determina il periodo di validità (in giorni) della password utente di base prima che il sistema ne richieda la modifica. Abilitato: <ul style="list-style-type: none">• <i>Durata massima della password utente di base:</i> Immettere la durata massima della password utente di base, ad esempio 42 giorni.• <i>Avviso di scadenza password utente di base:</i> specificare quando si desidera visualizzare l'avviso, ad esempio 7 giorni prima della scadenza della password.	Disabilitato

	<p>Disabilitato: la password utente di base non ha una durata massima, quindi non scade.</p>	
<p><i>Frase password utente di base - Lunghezza minima della frase password</i></p>	<p>Abilitato: immettere la lunghezza minima della frase password utente di base, ad esempio 20. La lunghezza minima specificata è valida per le frasi password che verranno impostate o modificate successivamente.</p> <p>Disabilitato: la lunghezza minima della frase password è di 20 caratteri.</p> <p> Questo criterio è rilevante unicamente se si utilizza l'Autenticazione avanzata.</p> <p>Ulteriori informazioni sull'Autenticazione avanzata</p>	<p>Abilitato caratteri</p>
<p><i>Frase Password utente di base - La frase password deve essere conforme ai requisiti di complessità</i></p>	<p>Abilitato: vengono applicati i criteri di complessità per le frasi password utente di base che saranno impostate o modificate successivamente.</p> <p>Disabilitato: non viene applicato nessun requisito di complessità.</p> <p> Questo criterio è rilevante unicamente se si utilizza l'Autenticazione avanzata.</p> <p>Ulteriori informazioni sui requisiti di complessità delle password</p> <p>Ulteriori informazioni sull'Autenticazione avanzata</p>	<p>Disabilitato</p>
<p><i>Inizializzazione Rapida Controllo</i></p>	<p>Attivato/Consenti: l'Inizializzazione Guidata Rapida o l'Inizializzazione Guidata di Security Platform e l'Inizializzazione Utenti Guidata possono essere utilizzate per l'inizializzazione di piattaforme e utenti.</p> <p>Attivato/Applica: l'Inizializzazione Guidata Rapida deve essere utilizzata per l'inizializzazione di piattaforme e/o utenti. Anche</p>	<p>Attivato</p>

	<p>le funzionalità disponibili (EFS, PSD) devono essere inizialmente configurate mediante l'Inizializzazione Guidata Rapida.</p> <p>Disabilitato: l'Inizializzazione Guidata Rapida non può essere utilizzata per l'inizializzazione di piattaforme e utenti. Dovranno invece essere utilizzate l'Inizializzazione Guidata di Security Platform e l'Inizializzazione Utenti Guidata.</p>	
<p><i>Consenti agli utenti di disabilitare temporaneamente le funzionalità di Security Platform</i></p>	<p>Abilitato: gli utenti di Infineon Security Platform possono disattivare le funzionalità di Security Platform fino al successivo riavvio del computer.</p> <p>Disabilitato: la possibilità di disattivare temporaneamente Infineon Security Platform non è disponibile nell'interfaccia utente del software.</p> <p> Questo criterio è applicabile unicamente ai sistemi Security Platform dotati di Infineon Trusted Platform Module 1,1. Quando un altro utente accede al sistema, le funzionalità di Security Platform precedentemente disattivate restano tali fino a quando il computer non viene riavviato.</p>	<p>Abilitato</p>
<p><i>Consenti la configurazione della protezione per la posta elettronica</i></p>	<p>Abilitato: gli utenti possono configurare la funzionalità di Security Platform <i>Protezione della posta elettronica</i>.</p> <p>Disabilitato: non è consentito configurare la funzionalità, ma è possibile utilizzare una configurazione precedente.</p>	<p>Abilitato</p>
<p><i>Consenti la configurazione di EFS</i></p>	<p>Abilitato: gli utenti possono configurare la funzionalità di Security Platform <i>Crittografia di file e crittografia cartelle con Encrypting File System (EFS)</i>.</p> <p>Disabilitato: non è consentito configurare la funzionalità, ma è possibile utilizzare una</p>	<p>Abilitato</p>

	<p>configurazione precedente.</p> <p> la funzione EFS non è supportata dalle edizioni Home di Windows.</p>	
<p><i>Consenti la configurazione di PSD</i></p>	<p>Abilitato: gli utenti possono configurare la funzionalità di Security Platform <i>Crittografia di file e cartelle con Personal Secure Drive (PSD)</i>.</p> <p>Disabilitato: non è consentito configurare la funzionalità, ma è possibile utilizzare una configurazione precedente.</p>	<p>Abilitato</p>
<p><i>Autenticazione avanzata obbligatoria</i></p>	<p>Abilitato: l'abilitazione della funzione di reimpostazione della password è obbligatoria per l'inizializzazione utenti.</p> <p>Tale obbligo viene meno se un utente di Security Platform è già stato configurato senza abilitare la reimpostazione password.</p> <p>Disabilitato: l'abilitazione della reimpostazione password non è obbligatoria. La funzione può essere abilitata anche successivamente all'inizializzazione utenti selezionando Tool di configurazione - Reimpostazione password - Abilita....</p>	<p>Disabilitato</p>
<p><i>Imponi l'abilitazione della reimpostazione password</i></p>	<p>Abilitato: gli utenti di Security Platform dovranno utilizzare l'Autenticazione avanzata (specificando la frase password richiesta).</p> <p>Disabilitato: gli utenti potranno scegliere se utilizzare l'Autenticazione avanzata (specificando la frase password) oppure l'Autenticazione password (con la password utente di base).</p> <p> Questo criterio è rilevante unicamente se è stato abilitato almeno un dispositivo di autenticazione per tutti gli utenti. L'utilizzo dell'Autenticazione avanzata non è obbligatorio se un utente di Security Platform è già stato</p>	<p>Disabilitato</p>

	<p>configurato senza selezionare un dispositivo di autenticazione avanzata.</p> <p>Ulteriori informazioni sull'Autenticazione avanzata</p>	
<p><i>Abilita memorizzazione della password utente di base</i></p>	<p>Abilitato: la password utente di base viene memorizzata nella cache del software Infineon Security Platform, evitando così di doverla immettere più volte durante ciascuna sessione di accesso. In questo modo, vengono ridotte le richieste di password visualizzate.</p> <p>Disabilitato: La finestra di dialogo relativa alla password utente di base non consente la memorizzazione nella cache della password utente di base stessa.</p>	<p>Abilitato</p>
<p><i>URL per la registrazione dei certificati durante la procedura guidata</i></p>	<p>Abilitato: consente di specificare l'indirizzo Web che verrà utilizzato per richiedere i certificati, mediante un browser Web, durante l'Inizializzazione utenti guidata di Infineon Security Platform.</p> <p>La pagina per la richiesta dei certificati è disponibile unicamente durante l'Inizializzazione utenti guidata, a condizione che questo criterio sia abilitato e che sia stata selezionata almeno una delle funzionalità di Security Platform da configurare.</p> <p>Disabilitato: la pagina di richiesta dei certificati non è disponibile nell'Inizializzazione utenti guidata di Infineon Security Platform.</p> <p>Nota:</p> <ul style="list-style-type: none"> • Questa impostazione è supportata come criterio di sistema per garantire la compatibilità con le versioni precedenti del software Security Platform Solution. • Suggerimenti: utilizzare l'impostazione come criterio utente. 	<p>Disabilitato</p>

	<ul style="list-style-type: none"> • Sebbene l'impostazione sia indipendente dall'utilizzo dei certificati, esiste anche un criterio utente specifico per i certificati EFS (<i>Registrazione e tipo di certificato EFS</i>). 	
<p><i>Registrazione e tipo di certificato EFS</i></p>	<p>Abilitato: consente di limitare le tipologie dei certificati EFS disponibili. È anche possibile abilitare la registrazione di certificati EFS esterni, specificando l'indirizzo Web dell'Autorità di certificazione.</p> <p>1. Tipo di certificato EFS: specificare se si desidera consentire l'uso di tutti i tipi di certificati (certificati di dominio, esterni e autofirmati) o soltanto di alcuni. Tale restrizione viene applicata in fase di registrazione o selezione dei certificati da parte degli utenti.</p> <ul style="list-style-type: none"> • Certificato di dominio: un certificato registrato tramite un'Autorità di certificazione interna al dominio. • Certificato esterno: un certificato registrato tramite un'Autorità di certificazione esterna accessibile sul Web. • Certificato autofirmato: un certificato creato sul proprio PC. <p>2. URL di richiesta dei certificati: immettere l'indirizzo web dell'Autorità di certificazione per la registrazione dei certificati EFS, ad esempio https://www.companyname.com/foldername. L'indirizzo specificato verrà utilizzato per richiedere un certificato EFS a un'Autorità di certificazione esterna (CA).</p> <ul style="list-style-type: none"> • L'indicazione dell'URL di richiesta del certificato è opzionale. • Se non si specifica nessun indirizzo Web, non sarà possibile richiedere certificati 	<p>Disabilitato</p>

	<p>EFS esterni.</p> <ul style="list-style-type: none"> • Se si desidera abilitare l'uso di certificati EFS esterni, immettere un indirizzo valido che sia accessibile a tutti i PC di Security Platform. In caso contrario, la registrazione dei certificati EFS non verrà completata. <p>Disabilitato: non vengono applicate restrizioni relativamente al tipo di certificati EFS. Non occorre impostare l'indirizzo Web da cui recuperare i certificati, poiché non è possibile richiedere certificati EFS esterni.</p> <p>Nota:</p> <ul style="list-style-type: none"> • I certificati EFS vengono utilizzati non solo per Encrypting File System, ma anche per Personal Secure Drive. • Sebbene questo criterio sia valido soltanto per i certificati EFS (da utilizzarsi per EFS o PSD), esiste anche un criterio utente indipendente dall'uso dei certificati (<i>URL per la registrazione dei certificati durante la procedura guidata</i>). <p>Come registrare e selezionare un certificato EFS</p>	
<p><i>Mostra avviso di scadenza dei certificati EFS</i></p>	<p>Abilitato: consente di visualizzare una nota che avvisa gli utenti di Security Platform dell'imminente scadenza del certificato EFS. Specificare quando visualizzare la notifica, ad esempio 14 giorni prima della scadenza del certificato.</p> <p>Disabilitato: la scadenza del certificato non viene notificata.</p>	<p>La notifi visualizz giorni pr scadenza certificat</p>
<p><i>Periodo di validità dei certificati auto-</i></p>	<p>Abilitato: Specificare per quanto tempo i certificati EFS auto-dichiarati saranno validi.</p> <p>Disabilitato: il periodo di validità è di 10 anni.</p>	<p>Abilitato periodo c di 10 anr</p>

<i>dichiarati EFS</i>		
<i>Percorso file per Personal Secure Drive</i>	<p>Abilitato/Unità PSD predefinita: imposta l'unità in cui verranno creati i file immagine di Personal Secure Drive. Immettere una lettera di unità valida nel campo di modifica, inclusi i due punti, ma senza nessun altro percorso (ad esempio C:). Se l'unità indicata non è valida, non sarà possibile creare il file immagine di Personal Secure Drive.</p> <p>Disabilitato: consente di selezionare l'unità di destinazione in cui creare i file immagine di Personal Secure Drive.</p>	Disabilitato
<i>Spazio minimo disponibile dopo la creazione di PSD</i>	<p>Abilitato: se PSD viene salvato nell'unità di sistema (dove è installato il sistema operativo in uso), occorre lasciare una determinata quantità di spazio disponibile dopo la configurazione di PSD. Specificare quanto spazio deve restare libero nell'unità di sistema dopo la configurazione di PSD.</p> <p>Disabilitato: non viene applicata alcuna restrizione relativamente allo spazio disponibile nella partizione di sistema dopo la creazione di PSD.</p> <p><u>Esempio:</u> il criterio è abilitato e impostato a 5000 MB. Le dimensioni minime del drive PSD sono di 20 MB per Windows 7 e Windows Vista e 10 MB per tutti gli altri sistemi operativi.</p> <ul style="list-style-type: none"> • Supponendo, per esempio, che lo spazio disponibile prima della creazione di PSD fosse 5050 MB, la dimensione massima di PSD sarà 50 MB. • Se fossero disponibili soltanto 5000 MB, non sarebbe possibile salvare PSD nell'unità di sistema. 	Il criterio abilitato impostato a 5000 MB.
<i>Consenti agli</i>	Abilitato: gli utenti sono autorizzati ad importare	Abilitato

<p><i>utenti di importare le chiavi</i></p>	<p>le proprie chiavi private in Security Platform. Tali chiavi possono essere importate, unitamente ai certificati, utilizzando le utilità Visualizzatore certificati e Selezione certificati.</p> <p>Disabilitato: non è consentito importare chiavi private in Security Platform.</p>	
<p><i>Applica la protezione avanzata chiave privata per le chiavi di firma MS-CAPI</i></p>	<p>Abilitato: tutte le chiavi utilizzate esclusivamente per operazioni di firma nell'interfaccia MS-CAPI vengono protette mediante la protezione avanzata chiave privata. La chiave verrà protetta da una password che dovrà essere specificata ogni volta che si utilizza la chiave per operazioni di firma.</p> <p>Disabilitato: le chiavi di firma non vengono protette in modo particolare.</p> <p> La password può essere memorizzata nella cache del software per evitare di ripeterne l'immissione. Questa password non è correlata alla chiave utente di base e quindi non è influenzata dal meccanismo di memorizzazione utilizzato per la password utente di base.</p>	<p>Disabilitato</p>
<p><i>Creazione della Chiave Utente di Base non migrabile</i></p>	<p>Attivato/Su richiesta: Si suggerisce agli utenti di creare la propria Chiave Utente di Base non migrabile quando stanno per utilizzare Infineon TPM Strong Cryptographic Provider per la prima volta. Si noti che Strong Cryptographic Provider necessita di una Chiave Utente di Base non migrabile.</p> <p>Attivato/Automatico: Per i nuovi utenti, la Chiave Utente di Base non migrabile viene creata automaticamente durante l'inizializzazione dell'utente. Per utenti già inizializzati, la Chiave Utente di Base non migrabile viene creata su richiesta.</p>	<p>Attivato richiesto</p>

Disabilitato: Non viene creata alcuna Chiave Utente di Base non migrabile: Infineon TPM Strong Cryptographic Provider non può essere utilizzato.

Impostazioni della versione modalità autonoma

Impostazioni validi solo per la versione modalità autonoma.

Criteri	Informazioni	Valore predefinito
<i>Frequenza degli avvisi relativi al backup</i>	<p>Abilitato: visualizza un messaggio di avviso nel caso in cui il backup delle credenziali e delle chiavi utente non sia stato completato correttamente (ad esempio, perché il percorso di backup non è accessibile). Specificare la frequenza di visualizzazione della notifica, ad esempio ogni due giorni 2 dopo il verificarsi dell'errore, fino al prossimo backup completato correttamente.</p> <p>Disabilitato: gli errori di backup non vengono notificati.</p>	Notifica quotidiana.
<i>Consenti l'iscrizione dell'utente</i>	<p>Abilitato/Consenti la gestione dell'interfaccia e del wizard: Gli utenti possono essere inizializzati attraverso l'interfaccia di Management Provider, Inizializzazione Guidata Rapida o Inizializzazione Guidata Utente.</p> <p>Abilitato/Consenti soltanto la Management Provider dell' interfaccia: Gli utenti possono solo essere inizializzati attraverso l'interfaccia di Management Provider.</p> <p>Disabilitato: l'utente non è autorizzato ad eseguire nessuna delle funzioni di Security Platform.</p>	Abilitato/Consenti la gestione di Management Provider e del wizard



Soluzione Infineon Security Platform

Servizi integrativi di Security Platform

I servizi integrativi di Security Platform abilitano alcune applicazioni standard all'utilizzo delle funzionalità di Trusted Platform Module. Ciò è possibile per applicazioni che supportino Microsoft Crypto-API, Microsoft Cryptography Next Generation (CNG) API, o PKCS #11 Crypto-API.

La tabella seguente elenca tutti i componenti dei servizi integrativi.

Nome provider	Spiegazione	Crypto-API	Applicazioni e servizi supportati (esempi)
Infineon TPM Cryptographic Provider (CSP utente, senza supporto AES)	Utilizzato per i certificati utente. È richiesta l' autenticazione utente per poter utilizzare la chiave privata del certificato.	Crypto-API Microsoft	<ul style="list-style-type: none">• Crittografia di file e cartelle con EFS e PSD• Protezione della posta elettronica (S/MIME) con Outlook e Windows Mail/Outlook Express• Autenticazione client SSL/TLS con Internet Explorer• Registrazione dei certificati mediante lo snap-in Certificati di Microsoft e Autorità di certificazione pubbliche (CA) che supportano Internet Explorer.• Macro firmate in Microsoft Office
Infineon TPM RSA and AES Cryptographic Provider (CSP utente con supporto AES. Non disponibile in Windows 2000)	Questa chiave può essere trasferita a un altro Trusted Platform Module.		

			<ul style="list-style-type: none"> • Checkpoint per reti private virtuali (VPN) che utilizzano le Crypto-API Microsoft • Autenticazione delle applicazioni client che utilizzano le Crypto-API Microsoft • Firma digitale Adobe e crittografia dei file Adobe • Autenticazione utente con EAP-TLS
<p>Infineon TPM PKCS #11 Provider (noto anche come "Token TPM Cryptoki")</p>		<p>Crypto-API PKCS #11</p>	<ul style="list-style-type: none"> • Protezione della posta elettronica (S/MIME) con Mozilla Thunderbird • Autenticazione client SSL/TLS con Mozilla Firefox • Registrazione dei certificati tramite Autorità di certificazione pubbliche (CA) che supportano Mozilla Firefox • Registrazione dei certificati tramite CA basate sul

			<p>server di certificazione Sun</p> <ul style="list-style-type: none"> • Protezione dell'accesso al Web e dell'accesso remoto con RSA SecurID • Autenticazione delle applicazioni client che utilizzano l'interfaccia PKCS #11
<p>Infineon TPM Strong Cryptographic Provider (Senza supporto AES)</p>	<p>Utilizzato per Certificati Utente. L' Autenticazione Utente è necessaria per ciascun utilizzo della chiave privata del certificato. La chiave privata del Certificato Utente non può eseguire la migrazione, è limitata a Trusted Platform Module.</p>	<p>Crypto-API Microsoft</p>	<ul style="list-style-type: none"> • Specificamente pensato per l'autenticazione utente in un VPN.
<p>Infineon TPM Platform Cryptographic Provider (Piattaforma CSP)</p>	<p>Utilizzato per i certificati del computer. Non è necessaria un'autorizzazione specifica per l'utilizzo della chiave privata del certificato, in quanto tale chiave è protetta da Trusted Platform Module.</p>	<p>Microsoft Crypto-API</p>	<ul style="list-style-type: none"> • Autenticazione EAP-TLS IEEE 802.11 tra client WLAN e server RADIUS (durante la fase di handshake TLS), in un'organizzazione amministrata, sul

	<p>La chiave privata del certificato del computer non può essere trasferita, essendo vincolata a Trusted Platform Module. Per utilizzare la piattaforma CSP è necessario disporre dei privilegi di amministratore o essere un membro del gruppo di amministratori.</p>		<p>lato del client WLAN</p> <ul style="list-style-type: none"> • Autenticazione EAP-TLS IEEE 802.1X, in reti LAN cablate, tra client e server RADIUS (durante la fase di handshake TLS), in un'organizzazione amministrata, sul lato del client • Autenticazione del computer IPsec sul lato del client VPN
<p>Infineon TPM Key Storage Provider (KSP)</p>	<p>Provider di Strumenti di Archiviazione Chiavi Limitato. Fornisce l'accesso unicamente ad altri Provider del Servizio di Crittografia TPM Infineon. Supporta unicamente le operazioni di firma e crittografia ma non la creazione di coppia di chiavi TPM RSA.</p>	<p>Microsoft Cryptography Next Generation (CNG) API</p>	<ul style="list-style-type: none"> • Microsoft .NET 3.0 • Per ulteriori esempi, vedi altri Provider del Servizio di Crittografia.

Per ulteriori informazioni sulle altre applicazioni supportate, contattare il supporto tecnico clienti.



Infineon Security Platform Solution

Servizi di Security Platform

I servizi di Security Platform costituiscono lo stack del software conforme ai requisiti stabiliti dal Trusted Computing Group (TCG).

Lo stack TCG (TSS) è composto dai seguenti moduli:

- TSS (Stack software TCG) Service Provider
- Servizio di base TSS
- Libreria del driver TSS

Lo stack TCG è parte integrante della piattaforma conforme alle specifiche TCG e fornisce funzioni che possono essere utilizzate da applicazioni e sistemi operativi avanzati.



Suggerimenti

Rivolgersi al supporto tecnico clienti per conoscere la disponibilità di aggiornamenti per il firmware di Trusted Platform Module.



Soluzione Infineon Security Platform

Server Integration Services

Il componente *Server Integration Services* comunica con il Trusted Computing Management Server, ed abilita l'integrazione della Security Platform con il Trusted Computing Management Server (vedere [modalità server](#)).

È un componente interno senza alcuna interfaccia utente grafica. Il *Client Side Control Agent* è un componente di base del *Server Integration Services*.

Nome del Componente	Spiegazione
<i>Client Side Control Agent</i>	Sincronizza lo status della piattaforma e le credenziali dell'utente con il Trusted Computing Management Server (vedere stato sessione utente).

Se il *Server Integration Services* non è incluso nella vostra versione dell'*Infineon TPM Professional Package Software*, contattate il vostro venditore per richiederlo.

Per sapere come installare il *Server Integration Services*, fare riferimento a *ReadmeServerIntegrationServices.txt*. Per identificare la versione installata, controllare la versione di *Client Side Control Agent* elencata in *Ulteriori Dettagli* di [Strumenti di Impostazione](#).



Infineon Security Platform Solution

Come utilizzare le funzionalità di Security Platform nelle applicazioni

Infineon Security Platform Solution supporta le [chiavi pubbliche fornite da Windows 2000/Windows XP](#) e le [funzionalità PKI basate sullo standard PKCS #11](#). Tale supporto include l'intera sequenza di operazioni richieste, tra cui la [registrazione](#) dei [certificati digitali](#), la configurazione delle applicazioni che utilizzano i certificati e la gestione delle funzioni specifiche per gli utenti di Infineon Security Platform.

Le applicazioni/funzioni che utilizzano i certificati digitali sono indicate di seguito.

- [Personal Secure Drive \(PSD\)](#)
- [Encrypting File System \(EFS\)](#)
- [Protezione della posta elettronica](#)
- [Macro firmate in Microsoft Word](#)
- [Protezione delle connessioni di rete](#)



©Infineon

Technologies AG

Soluzione Infineon Security Platform

Certificati e infrastruttura a chiave pubblica (PKI)

Per utilizzare le funzionalità di Security Platform nelle proprie applicazioni, è necessario richiedere uno o più certificati. Se nel dominio non si utilizzano certificati autofirmati, né certificati ottenuti da un'Autorità di certificazione (CA), è indispensabile accedere ad un'infrastruttura a chiave pubblica (PKI).

I certificati vengono gestiti mediante le utilità [Visualizzatore certificati e Selezione certificati di Security Platform](#).



Gli argomenti seguenti sono destinati in modo particolare agli amministratori, in quanto forniscono alcune informazioni di base riguardanti i certificati e le PKI.

[Certificati digitali](#)

[Infrastruttura a chiave pubblica nei sistemi operativi Windows](#)

[L'infrastruttura a chiave pubblica in PKCS #11](#)



©Infineon

Technologies AG

Infineon Security Platform Solution

Certificati digitali

I certificati digitali sono credenziali elettroniche che confermano l'identità di un individuo o di una società. Un certificato digitale associa sostanzialmente l'identità del proprietario a una coppia di chiavi elettroniche che possono essere utilizzate per firmare informazioni digitali.

Un certificato digitale deve contenere le seguenti informazioni:

- chiave pubblica del proprietario
- nome del proprietario
- data di scadenza del certificato digitale
- numero di serie del certificato digitale
- nome dell'authority di certificazione che ha rilasciato il certificato
- certificato digitale dell'authority che ha rilasciato il certificato

Oltre a queste informazioni, un certificato digitale può contenerne altre fornite da ciascun utente, come ad esempio:

- indirizzo postale
- indirizzo e-mail (per alcune applicazioni questo campo è obbligatorio)
- informazioni base per la registrazione (paese, età, sesso, ecc.)

In genere i certificati digitali vengono rilasciati e gestiti da un ente riconosciuto, denominato authority di certificazione. L'[ottenimento di un certificato](#) è un processo uguale per gran parte delle authority di certificazione. Molte authority raccolgono un numero di certificati digitali sempre crescente e rilasciano certificati che possono essere utilizzati per scopi che vanno dalla protezione delle e-mail a quella delle comunicazioni su Internet o intranet.



©Infineon

Technologies AG

Infineon Security Platform Solution

Come ottenere un certificato digitale da un'Autorità di certificazione pubblica (CA)

Per poter utilizzare la tecnologia a chiavi pubbliche offerta da Microsoft, è necessario richiedere un **ID digitale**. A causa della crescente domanda di ID digitali, numerose Autorità private di certificazione (CA), come VeriSign e Thawte, offrono certificati digitali utilizzabili per vari scopi, come la protezione della posta elettronica o la firma delle macro.

Questi enti privati possono rilasciare diversi tipi di certificati, tra cui:

- Certificati personali, per la firma digitale della posta elettronica e lo scambio protetto di informazioni all'interno di un network pubblico.
- Certificati di autenticazione per client e server, utilizzati per la trasmissione protetta di informazioni tra più client e server.
- Certificati per editori di software, utilizzati dalle società di informatica per la firma digitale dei propri software.

Le Autorità di certificazione (CA) possono rilasciare anche altri tipi di certificati. Ogni CA ha redatto una Dichiarazione delle procedure di certificazione (CPS) che costituisce la base della propria attività. È buona norma visitare il sito Web di più Autorità di certificazione e leggerne la dichiarazione CPS prima di scegliere quella a cui richiedere il proprio certificato.

Al momento di scegliere un'Autorità di certificazione, si consiglia di valutare i seguenti aspetti:

- L'Autorità di certificazione deve essere un ente affidabile che utilizza pratiche di certificazione adatte alle proprie esigenze e opera efficientemente nel proprio paese.
- L'Autorità di certificazione deve essere ben conosciuta, poiché questo indica che più persone l'hanno ritenuta attendibile e degna di fiducia. Se si sceglie un'Autorità di dubbia reputazione, alcuni utenti potrebbero rifiutare il certificato.
- L'Autorità di certificazione deve richiedere informazioni dettagliate all'utente per verificarne le credenziali.
- L'Autorità di certificazione deve disporre di un sistema di ricevimento online delle richieste di certificato, ad esempio richieste generate mediante un server di gestione delle chiavi. Questo sistema consente significativi risparmi in termini di tempo e rende più rapide le procedure di richiesta, ricevimento e installazione dei certificati.

- Il costo dei servizi di certificazione deve essere adatto alle proprie esigenze.

Dopo aver scelto l'Autorità di certificazione, occorre presentare alla stessa la propria richiesta di certificato. Molte CA supportano procedure di registrazione on-line.



Selezionare il [provider del servizio di crittografia](#), da utilizzare per il certificato, tra quelli forniti da Security Platform Solution.

Una volta evasa la richiesta, verranno inviate istruzioni su come installare e utilizzare il certificato.



©Infineon

Technologies AG

Soluzione Infineon Security Platform

Infrastruttura a chiave pubblica (PKI) nei sistemi operativi Windows

Il sistema operativo Microsoft Windows 2000 ha integrato nella piattaforma Windows un'infrastruttura a chiave pubblica (PKI) completa. Tale infrastruttura migliora i servizi di crittografia a chiave pubblica basati su Windows, che sono stati introdotti in questi anni, fornendo un insieme integrato di servizi e di strumenti amministrativi per la creazione, lo sviluppo e la gestione delle applicazioni basate sulle chiavi pubbliche.

Ciò significa che gli sviluppatori di applicazioni potranno avvantaggiarsi di meccanismi di protezione basati su valori segreti condivisi o sulle chiavi pubbliche, in base alle loro esigenze. Inoltre, le aziende saranno in grado di amministrare diversi ambienti e applicazioni utilizzando strumenti e criteri che siano coerenti tra loro in tutto l'organizzazione aziendale.

L'infrastruttura a chiave pubblica (PKI) non sostituisce i meccanismi di verifica dell'attendibilità e delle autorizzazioni esistenti nel dominio Windows, meccanismi basati sul controller di dominio (DC) e sul Centro distribuzione chiave Kerberos (KDC). In realtà, l'infrastruttura PKI funziona in congiunzione con tali servizi e offre caratteristiche avanzate che rendono le applicazioni prontamente scalabili per rispondere alle esigenze delle reti Extranet o Internet. Un'infrastruttura a chiave pubblica soddisfa quindi il bisogno di procedure di identificazione e autenticazione scalabili e distribuite, garantendo integrità e riservatezza dei dati e fornendo un framework di servizi, tecnologie, protocolli e regole che consentono di sviluppare e gestire un sistema di protezione delle informazioni solido e scalabile. Il supporto per la creazione, lo sviluppo e la gestione delle applicazioni basate sulle chiavi pubbliche viene fornito in modo analogo sia alle postazioni, sia ai server che utilizzano Windows 2000 o Windows NT4.

I componenti di base di un'infrastruttura a chiave pubblica comprendono i certificati digitali, gli elenchi di revoca dei certificati e le autorità di certificazione. Gli amministratori della società dovranno verificare che sia installata un'infrastruttura PKI prima di utilizzare nelle proprie reti i sistemi di crittografia a chiave pubblica.

Ulteriori informazioni sull'infrastruttura a chiave pubblica Microsoft (PKI) e sui Servizi certificati sono disponibili sul sito Microsoft TechNet.

La configurazione di un'infrastruttura PKI all'interno di un'organizzazione

richiede le seguenti operazioni:

- Configurazione di Active Directory
- Come installare un'Autorità di certificazione
- Modifica del modello di certificato utente
- Come registrare i certificati

Il presente documento contiene alcune informazioni generali sulle operazioni sopra citate e i collegamenti utili ad approfondire gli argomenti correlati.



©Infineon

Technologies AG

Infineon Security Platform Solution

Come configurare Active Directory

Active Directory è il servizio directory utilizzato da Microsoft Windows 2000 che costituisce la base delle reti distribuite. Active Directory facilita la memorizzazione protetta, strutturata e ordinata gerarchicamente delle informazioni relative ad alcuni elementi delle reti aziendali, come utenti, computer, servizi e altro ancora.

Active Directory deve essere installato nei domini in cui si intende configurare un'infrastruttura a chiave pubblica, poiché tutte le informazioni riguardanti la posizione e i criteri delle CA, oltre ai certificati e agli elenchi di revoca, vengono archiviate in Active Directory.

Dopo aver installato Active Directory in un dominio, occorre aggiungere gli utenti desiderati. Utilizzando lo snap-in "Utenti e computer di Active Directory" è possibile inserire, spostare, eliminare o modificare le proprietà di alcuni elementi, come utenti, contatti, gruppi, ecc.

Ulteriori informazioni su Active Directory sono disponibili sul sito Microsoft TechNet.

Il passaggio successivo per la configurazione di un'infrastruttura a chiave pubblica è l'installazione di un'Autorità di certificazione.

Technologies AG



Infineon Security Platform Solution

Come installare un'Autorità di certificazione

Un'Autorità di certificazione (CA) è un servizio che rilascia i certificati necessari per eseguire un'infrastruttura a chiave pubblica (PKI). In genere, tali certificati vengono rilasciati ai richiedenti in base a una serie di criteri prestabiliti.

L'Autorità di certificazione garantisce la validità dell'associazione tra la chiave pubblica di un soggetto e l'identità di tale soggetto archiviata nel certificato.

L'Autorità di certificazione può essere un ente privato esterno o un organismo gestito internamente a un'azienda (dal momento che la presenza di un'Autorità di certificazione è un importante indicatore di affidabilità, molte società hanno scelto di averne una al loro interno).

L'infrastruttura a chiave pubblica di Windows 2000 presuppone un modello di CA di tipo gerarchico, caratterizzato da scalabilità, facilità di gestione e supporto dei certificati rilasciati da altre CA private.

Windows 2000 supporta due tipi di servizi CA: globali (enterprise) o autonomi (standalone). La differenza principale tra questi due servizi CA risiede nel modo in cui vengono emessi i certificati. Una CA autonoma rilascia i certificati senza l'autenticazione del richiedente, con la semplice approvazione della richiesta da parte del proprio amministratore in base ad alcune informazioni supplementari.

Una CA globale invece richiede l'esistenza di un dominio Windows 2000 e autentica il richiedente in base alle informazioni utilizzate per l'accesso al dominio. Inoltre, una CA globale utilizza modelli di certificato per distinguere tra le diverse tipologie di certificati, in funzione dell'utilizzo previsto. Gli utenti possono ottenere vari tipi di certificati, in base ai diritti di accesso al dominio di cui dispongono e delle finalità d'uso dei certificati stessi.

È necessario installare una CA globale quando si desidera rilasciare i certificati soltanto agli utenti o ai computer di un'organizzazione che appartenga a un dominio Windows 2000. Se invece si vogliono emettere certificati per utenti o computer al di fuori di un dominio Windows 2000, occorre installare una CA autonoma.

Nota: le CA globali dispongono di un modulo di criteri particolare che determina il modo in cui i certificati verranno elaborati ed emessi. Le informazioni sui criteri utilizzati da questi moduli sono memorizzate in un oggetto CA di Active Directory. Pertanto, prima di installare una CA globale, è indispensabile disporre di una versione pienamente funzionante di Active Directory e del server DNS.

Consultare il sito Microsoft TechNet per ulteriori istruzioni su come installare una CA nel proprio dominio.

Il passaggio successivo, necessario per installare un'infrastruttura a chiave pubblica (PKI), implica la modifica del modello di certificato utente, allo scopo di abilitare l'uso dei [provider del servizio di crittografia](#) forniti da Security Platform Solution.



©Infineon

Technologies AG

Infineon Security Platform Solution

Modifica del modello di certificato utente

Utilizzando la Richiesta guidata certificato, è possibile selezionare, per un modello di certificato, soltanto uno dei provider del servizio di crittografia (CSP) memorizzati in Active Directory. Per abilitare l'uso dei [provider del servizio di crittografia](#) forniti da Security Platform Solution e richiedere quindi un certificato utente, occorre modificare il modello di certificato corrispondente.

Come modificare il modello di certificato utente archiviato in Active Directory

1. **Installazione di ADSI Edit**

Il modello di certificato utente può essere modificato utilizzando l'editor Active Directory Services Interface (ADSI). L'editor è uno degli snap-in di Microsoft Management Console ed è parte degli Strumenti di supporto situati nella cartella Support\Tools del CD-ROM del sistema operativo Windows 2000 Server. Per installare tali strumenti, fare doppio clic sull'icona Setup nella cartella. Per ulteriori informazioni sull'installazione e sull'utilizzo degli Strumenti di supporto di Windows 2000 e della relativa Guida in linea, consultare il file Readme.doc presente nella cartella Support\Tools del CD-ROM di Windows 2000. Per informazioni dettagliate sull'utilizzo di ADSI Edit, leggere la Guida in linea di Microsoft Windows 2000 Resource Kit Tools.

2. **Avvio di ADSI Edit**

Adsiedit.msc (lo snap-in di MMC per ADSI Edit) tenta automaticamente di caricare il dominio a cui si è connessi in quel momento. Se il computer è installato in un gruppo di lavoro o non è connesso al dominio, viene visualizzato più volte il messaggio di errore "Il dominio specificato non esiste". Per ovviare a questo problema, aprire mmc.exe, inserire manualmente lo snap-in di ADSI Edit, creare le eventuali connessioni necessarie per le varie credenziali e quindi salvare il file della console. In questo modo, viene creata una console predefinita che interagisce con ADSI Edit.

3. **Selezione del modello di certificato utente**

Per estendere un modello di certificato è necessario modificare i seguenti nodi in Adsiedit.msc:

CN=<nome del modello>, CN=Modelli certificati, CN=Servizi Chiavi pubbliche, CN=Servizi, CN=Configurazione, DC=<nome del dominio>

4. **Modifica del modello di certificato utente**

Cliccare con il pulsante destro del mouse su **CN=Utente** e quindi scegliere

Proprietà nel menu visualizzato.

Scegliere la proprietà da visualizzare: *pKIDefaultCSPs*.

Modifica attributo:

Inserire il testo seguente: *<n>,Infineon TPM Cryptographic Provider* (dove *<n>* indica il numero successivo nell'elenco **Valori**).

Esempio: l'elenco **Valore** contiene due voci:

1,Microsoft Enhanced Cryptographic Provider v1.0

2,Microsoft Base Cryptographic Provider v1.0

Inserire il testo seguente:

3,Infineon TPM Cryptographic Provider.

Cliccare su **Aggiungi** e quindi su **Applica** per salvare le modifiche apportate al modello di certificato.

L'Autorità di certificazione (CA) può ora procedere alla registrazione degli utenti per i certificati Security Platform.

Nota: per utilizzare con altri modelli i [provider del servizio di crittografia](#) forniti da Security Platform Solution, la procedura richiesta è simile a quella già descritta per i modelli di Active Directory.



Infineon Security Platform Solution

Come registrare i certificati

I certificati rappresentano un meccanismo di sicurezza nell'ambito della relazione tra una chiave pubblica e l'ente che la possiede. Infatti, un certificato è una dichiarazione firmata in modo digitale dall'autorità emittente che garantisce che la chiave pubblica fornita appartiene al soggetto che detiene il certificato. Solitamente, i certificati contengono informazioni sull'identità dell'ente che ha accesso alla chiave privata corrispondente alla chiave pubblica citata nel certificato.

È possibile registrare un certificato utente, associato ad uno dei [provider del servizio di crittografia](#) forniti da Security Platform Solution, mediante:

- Snap-In Certificati di Microsoft Management Console oppure
- L'applicazione Web fornita dai sistemi operativi server di Microsoft Windows



©Infineon

Technologies AG

Infineon Security Platform Solution

Come registrare i certificati utilizzando Microsoft Management Console

Questo metodo è applicabile unicamente se il computer locale e l'Autorità di certificazione appartengono al medesimo dominio Windows.

1. Avvio dello snap-in Certificati di Microsoft Management Console.
Avviare Microsoft Management Console e quindi aggiungere lo snap-in Certificati per poter gestire i certificati per il proprio account utente.
2. Richiesta guidata certificato.
Cliccare con il pulsante destro del mouse sull'archivio logico **Personale** e quindi scegliere **Richiedi nuovo certificato...** per avviare la **Richiesta guidata certificato**.
3. Elaborazione della richiesta di certificato.
Scegliere **Avanti** per continuare.
4. Scegliere il tipo di certificato **Utente** e quindi selezionare l'elemento **Avanzato**. Questa operazione consentirà, in un secondo tempo, di associare il certificato a uno dei [provider del servizio di crittografia](#) (CSP) forniti da Security Platform Solution.

Scegliere **Avanti** per continuare.

5. Selezionare uno dei provider del servizio di crittografia forniti da Security Platform Solution per associarlo al certificato richiesto.
La lunghezza della chiave viene impostata automaticamente al valore predefinito dal provider.



Se i provider forniti da Security Platform Solution non compaiono nell'elenco, verificare che il modello del certificato utente sia stato modificato.

Scegliere **Avanti** per continuare.

6. Selezionare l'Autorità di certificazione a cui inviare la richiesta.
Scegliere **Avanti** per continuare.

7. Immettere il nome e la descrizione del nuovo certificato.
Scegliere **Avanti** per continuare.

8. Scegliere **Fine** per completare la richiesta.

Se la richiesta è stata eseguita correttamente, verrà visualizzato un messaggio di conferma.



©Infineon Technologies AG

Infineon Security Platform Solution

Come registrare i certificati utilizzando un browser Web

Le sezioni seguenti descrivono le procedure di registrazione dei certificati tramite l'Autorità di certificazione standard di Microsoft, che può essere installata nei sistemi operativi server di Microsoft Windows (come Microsoft Windows Server 2003).

Altre Autorità di certificazione pubbliche (CA) potrebbero utilizzare interfacce Web diverse.

1. **Avvio di Internet Explorer** Avviare Internet Explorer e accedere alla pagina iniziale dell'Autorità di certificazione della propria azienda. Selezionare **Richiedi certificato**, quindi scegliere **Avanti** per continuare.
2. **Elaborazione della richiesta di certificato**
Selezionare **Richiesta di certificato utente**, quindi scegliere **Avanti** per continuare.



Se si seleziona **Richiesta avanzata**, è possibile scegliere o impostare un'ampia gamma di parametri che renderanno più agevole la propria richiesta. Generalmente, è necessario selezionare questa opzione per poter scegliere uno dei [provider del servizio di crittografia](#) (CSP) forniti da Security Platform Solution.

Scegliere **Altre opzioni** per associare il provider del servizio di crittografia al certificato richiesto.

Se si sceglie **Invia**, la richiesta di certificato verrà inviata utilizzando i valori predefiniti indicati di seguito.

CSP:	<i>MS Base Cryptographic Provider V1</i>
Lunghezza chiave:	<i>Predefinita dal provider del servizio di crittografia (CSP)</i>
Protezione avanzata chiave privata:	<i>No</i>
Nome contenitore:	<i>Un GUID qualsiasi</i>

Il certificato verrà associato a *MS Base Cryptographic Provider V1*.

Selezionare, tra i provider del servizio di crittografia forniti da Security Platform Solution, quello che verrà utilizzato dal certificato richiesto. La lunghezza della chiave viene impostata automaticamente al valore

predefinito dal provider, mentre il nome del contenitore corrisponde a un GUID qualsiasi.



Se i provider forniti da Security Platform Solution non compaiono nell'elenco, verificare che il modello del certificato utente sia stato modificato.

Scegliere **Invia** per completare la richiesta.

Se la richiesta è stata eseguita correttamente, verrà visualizzato un messaggio di conferma.

Il certificato ricevuto può essere installato nel sistema facendo clic su **Installa questo certificato**.



©Infineon Technologies AG

Infineon Security Platform Solution

Infrastruttura a chiave pubblica (PKI) in PKCS #11

Lo standard PKCS #11 definisce un'interfaccia comune per la creazione, l'uso e l'amministrazione dei certificati e delle chiavi di crittografia. Per ciascuna implementazione dell'interfaccia viene fornito un approccio specifico alla tecnologia sottostante, in quanto lo standard PKCS #11 non fornisce alcuna informazione circa il token di crittografia che esegue le funzionalità principali. Il mercato offre diverse soluzioni basate sia su software che su Smart Card, nonché moduli di crittografia hardware specializzati. Ciascuna libreria compatibile PKCS #11 implementa secondo modalità proprie i metodi di inclusione e l'uso dei dispositivi speciali per la generazione e la gestione dei dati crittografati.

Lo standard PKCS #11 definisce un'interfaccia indipendente dalla piattaforma e consente l'uso di un'ampia gamma di soluzioni essendo supportato da numerose piattaforme e sistemi operativi.

Le librerie compatibili PKCS #11 forniscono le funzionalità attraverso un'interfaccia perfettamente definita. In funzione dell'obiettivo principale dell'implementazione, una libreria PKCS #11 è in grado di supportare solo un sottoinsieme dell'interfaccia definita.

Per la costruzione di un'infrastruttura a chiave pubblica, le applicazioni che utilizzano un modulo PKCS #11 necessitano dell'accesso a una memorizzazione permanente per conservare in modo sicuro e affidabile i certificati utente e le chiavi private. PKCS #11 non fornisce informazioni su questo meccanismo di memorizzazione. Un meccanismo molto diffuso è rappresentato dai servizi di directory, che hanno dimostrato di essere un valido strumento per la gestione delle funzionalità richieste. L'accesso ai servizi di directory avviene generalmente tramite il protocollo LDAP (Lightweight Directory Access Protocol).

Poiché Windows 2000/XP non include una libreria PKCS #11 nativa, è necessario aggiungere questa funzione mediante soluzioni di altri produttori. Il software Infineon Security Platform Solution contiene una libreria per l'implementazione dell'interfaccia PKCS #11 che utilizza Trusted Platform Module per l'esecuzione delle operazioni di crittografia più delicate, come la generazione di chiavi.

Sullo stesso sistema è possibile installare diverse implementazioni indipendenti. Generalmente, le applicazioni che utilizzano queste librerie devono essere configurate tramite una procedura aggiuntiva per poter accedere correttamente

ai rispettivi moduli.

Le applicazioni basate su PKCS #11 devono inoltre implementare tutto il lavoro amministrativo necessario per fornire i dati richiesti per la gestione delle funzionalità PKCS #11.

Gli sviluppatori di applicazioni traggono vantaggio dalle procedure di sicurezza basate su chiave pubblica utilizzando differenti moduli di implementazione PKCS #11, senza la necessità di apportare modifiche alla piattaforma o al software utilizzato. Inoltre, le aziende possono amministrare i rispettivi ambienti e le applicazioni utilizzate mediante strumenti e criteri coerenti in tutta l'organizzazione.

Per abilitare altri utenti alla lettura dei messaggi crittografati o verificare le e-mail con firma, è necessario che i certificati utente siano memorizzati in una directory pubblica. In genere questa directory si trova su un server raggiungibile dall'interno dell'unità organizzativa interessata.

I componenti di base di un'infrastruttura a chiave pubblica includono i certificati digitali, gli elenchi delle revocche dei certificati e le authority di certificazione. Gli amministratori di aziende devono assicurarsi che l'infrastruttura a chiave pubblica sia implementata prima che la crittografia a chiave pubblica venga realmente utilizzata nelle proprie reti.

La configurazione di un'infrastruttura a chiave pubblica all'interno di un'organizzazione include le seguenti fasi:

- Installazione di un server dei certificati
- Definizione di un provider di certificati esterno
- Configurazione di [Mozilla Firefox](#) per l'uso della libreria PKCS #11 di Infineon Security Platform
- Ottenimento dei certificati da un'authority di certificazione per l'autenticazione del client

Questa Guida introduttiva offre una panoramica sugli argomenti sopra elencati e riporta i collegamenti che forniscono ulteriori informazioni su tali argomenti.



Dopo un'aggiornamento del software Security Platform Solution, le applicazioni che utilizzano Security Platform Solution mediante l'interfaccia PKCS#11 potrebbero non funzionare come previsto perché il file DLL relativo (*ifxtpmck.dll*) si trova ora nella directory di installazione del software Security Platform Solution. Nelle versioni precedenti del prodotto, si trovava nella directory *system32*. È necessario riconfigurare

le applicazioni per il caricamento del file *ifxtpmck.dll* dal nuovo percorso.



©Infineon

Technologies AG

Infineon Security Platform Solution

Configurazione di PKCS #11 in Mozilla Firefox

Lo standard PKCS #11 definisce interfacce e tecnologie indipendenti dalla piattaforma per la gestione degli elementi importanti per la sicurezza per l'infrastruttura PKI in ambiente distribuito. Sono disponibili molte soluzioni di produttori diversi. Infineon Security Platform Solution comprende una libreria PKCS #11 di funzioni software che implementa la funzionalità necessaria all'uso di tale software. Questa libreria utilizza Trusted Platform Module per la maggior parte delle operazioni relative alla sicurezza.

Mozilla Firefox supporta più di una libreria PKCS #11. Componente standard del prodotto è una soluzione basata completamente su meccanismi software.

La libreria PKCS #11 contenuta nel software Infineon Security Platform deve essere configurata in Mozilla Firefox. Durante questa procedura è possibile disabilitare la libreria PKCS #11 standard, se non è più necessaria. Questa decisione va presa di comune accordo con l'amministratore di sistema.

Configurazione di Mozilla Firefox

1. Avviare Mozilla Firefox.
2. Selezione **Strumenti > Opzioni**. Il pannello Opzioni si apre.
3. Fare clic sull'icona **Protezione** nel pannello Opzioni.
4. Selezionare **Usa una password master** per definire la password per la protezione del vostro database di certificati.
5. Inserire una **Nuova password** per due volte per confermare. Solo quando i valori inseriti sono identici si attiva il pulsante OK. Il **misuratore di qualità della Password** fornisce un'indicazione sul livello di sicurezza del valore corrente inserito. Per ottenere per questa password un livello di protezione pari a quello consigliato per le password del Software Infineon Security Platform Solution dovranno essere prese in considerazione alcune [linee guida sulle password](#) . Se si desidera modificare una password già impostata è inoltre necessario inserire la **password Corrente**.
6. Fare clic su **OK**.

La configurazione delle e-mail è descritta alla sezione [Configura protezione della posta elettronica](#).

Configurazione della gestione del certificato

Questa sezione spiega la configurazione e le modalità di gestione dei certificati in Mozilla Firefox.

1. Fare clic sull'icona **Avanzato** nel pannello Opzioni per configurare l'ambiente di gestione delle certificazioni.
2. Fare clic sulla scheda **Crittografia**. Per la **Selezione del Certificato** impostare la modalità **Richiedi Ogni Volta**. Ciò garantisce che nessuna autenticazione cliente è effettuata senza che l'utente ne sia a conoscenza.
3. Fare clic sul pulsante **Periferiche di Protezione** per aprire la Gestione Periferiche.
4. Fare clic sul pulsante **Caricamento** per aprire il dialogo di configurazione per un nuovo Modulo PKCS #11.
5. Il **Nome del Modulo** è obbligatorio, il **nome file del Modulo** è stabilito a *IfxTPMCK.dll*. Se il modulo non si trova in una cartella contenuta nella variabile PATH del sistema, è possibile utilizzare il pulsante **Sfoglia** per individuare il file. Confermare le impostazioni con **OK**.
6. Se il nome del modulo specificato è compreso nell'elenco **Moduli Crittografati** successivamente, esso è correttamente configurato per l'uso.



©Infineon

Infineon Security Platform Solution

Come registrare i certificati

I certificati rappresentano un meccanismo di sicurezza nell'ambito della relazione tra una chiave pubblica e l'ente che la possiede. Infatti, un certificato è una dichiarazione firmata in modo digitale dall'autorità emittente che garantisce che la chiave pubblica fornita appartiene alla persona fisica o all'ente che la detiene. Solitamente, i certificati contengono informazioni sull'identità della persona o dell'ente che ha accesso alla chiave privata corrispondente alla chiave pubblica citata nel certificato.

È possibile registrare un certificato utente, associato ad uno dei [provider del servizio di crittografia](#) forniti da Security Platform Solution, mediante:

- [Server dei certificati Sun](#) oppure
- [CA pubbliche con supporto PKCS #11](#).



©Infineon

Technologies AG

Infineon Security Platform Solution

Iscrizione dei certificati con un'authority di certificazione basata sul server dei certificati Sun

Le sezioni seguenti descrivono l'iscrizione dei certificati con l'authority di certificazione iPlanet. Questo prodotto è disponibile per diverse piattaforme (Windows 2000 / XP, Unix, Linux, ...).

L'accesso viene fornito tramite un browser Web che supporta lo standard PKCS #11.

Iscrizione dei certificati con Mozilla Firefox

1. Verificare che Mozilla Firefox sia installato.
2. Avviare Mozilla Firefox.
3. Immettere l'indirizzo Internet del server dei certificati. Se non si conosce l'indirizzo, contattare l'amministratore del sistema.
La comunicazione utilizza un canale protetto con SSL sulla porta predefinita 1025, pertanto l'indirizzo del server dei certificati dovrebbe essere il seguente: *https://your_server_name:1025*.
4. Dopo la visualizzazione di alcuni messaggi, il certificato è pronto per l'iscrizione.
5. Il certificato può essere utilizzato per effettuare l'autenticazione del client presso l'authority di certificazione. La modalità di autenticazione può essere definita dall'utente.
 - Se è necessario recuperare un nuovo certificato per ciascuna nuova sessione, selezionare **Accetta il certificato per questa sessione**.
 - Se si desidera abbandonare il certificato, selezionare **Non accettare il certificato e non effettuare il collegamento**.
 - Se si desidera utilizzare il certificato per l'autenticazione del client finché non scade, selezionare **Accetta il certificato per sempre (finché non scade)**.

Nota: ulteriori informazioni sul livello di sicurezza della comunicazione sono disponibili sul server dell'authority di certificazione.

Per verificare le proprietà di un'authority di certificazione, procedere come segue:

1. Fare clic sull'icona **Avanzato da Strumenti** > Opzioni e fare clic sulla scheda **Crittografia**.
2. Fare clic su **Visualizza Certificati** per aprire il Gestore di Certificati e fare clic sulla scheda **Autorità**.
3. Selezionare la modalità di gestione dell'authority di certificazione che corrisponde ai requisiti o che è stata definita dall'amministratore del sistema.

- Se si desidera utilizzare i certificati rilasciati dall'authority per la certificazione basata sul Web, selezionare **Questo certificato può identificare siti web.**
- Se si desidera accettare i certificati rilasciati dall'authority utilizzati per firmare e/o crittografare le e-mail, selezionare **Questo certificato può identificare utenti mail.**
- Se si desidera utilizzare i certificati rilasciati dall'authority per gestire il software certificato, selezionare **Questo certificato può identificare produttori di software.**



Infineon Security Platform Solution

Registrazione dei certificati tramite CA pubbliche che supportano PKCS #11

In genere, le CA pubbliche offrono un sistema di registrazione dei certificati basato su un'interfaccia Web.

Ad esempio, l'interfaccia utente può essere simile a quella di [Sun Certificate Server](#). La differenza risiede nell'indirizzo del servizio. Inoltre, le CA pubbliche offrono [un'ampia gamma di servizi](#) in materia di sicurezza e certificati.

In alcuni casi, il provider di questi servizi mette a disposizione un software specifico che può essere scaricato e installato per automatizzare la gestione delle comunicazioni e delle richieste dei certificati.



©Infineon

Technologies AG

Soluzione Infineon Security Platform

Introduzione a Personal Secure Drive

Personal Secure Drive (PSD) offre un'area di archiviazione protetta per i dati riservati. È possibile configurare uno o più Personal Secure Drives utilizzando [Inizializzazione utenti guidata](#).

Una volta configurato, Personal Secure Drive funziona come una qualsiasi altra unità del computer, consentendo di creare file e cartelle a cui si accede normalmente, come accade per i file e le cartelle salvate su altre unità. Non esistono limitazioni alle tipologie di file che possono essere salvate su Personal Secure Drive.

Personal Secure Drive si differenzia da una normale unità del computer per due aspetti fondamentali:

1. I dati sono crittografati.
2. L'unità è visibile e accessibile soltanto all'utente.

Crittografia

I dati presenti su Personal Secure Drive vengono automaticamente protetti utilizzando tecniche di crittografia avanzate, tra cui gli algoritmi AES e RSA. I file e le cartelle salvati su Personal Secure Drive vengono immediatamente crittografati. È possibile creare file e cartelle direttamente su Personal Secure Drive o trasferirli da altre unità. Tutti i file sono automaticamente crittografati quando vengono posizionati su Personal Secure Drive. Analogamente, quando si accede o si copiano file o cartelle da Personal Secure Drive a un'altra unità, la decrittografia viene eseguita automaticamente. Quindi, non occorrono operazioni particolari per proteggere file o cartelle: tutte le procedure di crittografia e decrittografia sono gestite automaticamente.



Come proteggere i file e le cartelle esistenti Spostare nell'unità PSD i file e le cartelle che si desidera proteggere.

Se si sceglie di copiarli in PSD senza eliminarli dall'unità di origine, le copie non crittografate rimarranno disponibili nella posizione originaria.

Modalità Server

In [modalità server](#), le impostazioni di PSD sono gestite da Trusted Computing Management Server. Ciò significa che le impostazioni PSD sono la migrazione automaticamente come altre credenziali e certificati utente (consultare [Migrazione delle chiavi verso altri computer](#)).



Il file immagine del drive PSD non sarà migrato.

Si raccomanda di configurare PSD su una unità rimovibile (es. unità flash USB) che consente di portare i file immagine del drive PSD.

Se si desidera configurare PSD sul supporto fisso (ad esempio, disco rigido locale), e si desidera utilizzare su un'altra piattaforma, è necessario fare un backup del file immagine del drive PSD sulla prima piattaforma e ripristinarlo su un'altra piattaforma (consultare [Backup e ripristino dei dati di Security Platform](#)). Si noti che, in questo caso, ci sono copie fisiche multiple di PSD.



©Infineon Technologies AG

Infineon Security Platform Solution

Vantaggi dell'uso di Personal Secure Drive

Quando si lavora con informazioni digitali per uso aziendale o privato, è necessario che i dati confidenziali siano adeguatamente protetti. Personal Secure Drive offre la massima protezione in quanto tutti i file selezionati dall'utente vengono memorizzati su un'unità virtuale crittografata, creando così un archivio ad alta sicurezza per dati importanti. I vantaggi sono i seguenti:

- Crittografia di unità virtuali mediante una chiave AES (Advanced Encryption Standard) memorizzata in modo sicuro.
- Codifica della chiave di crittografia tramite l'algoritmo RSA.
- Sicurezza trasparente: crittografia / decrittografia automatiche dei dati.
- Elaborazione anche di file di grandi dimensioni senza ritardi significativi: infatti le operazioni di crittografia e decrittografia vengono eseguite "al volo".

Protezione dei file semplificata

Personal Secure Drive è progettato per offrire un'interfaccia utente semplice e intuitiva, che permette di concentrare l'attenzione sul lavoro che si sta svolgendo piuttosto che su lunghe procedure di sicurezza. Personal Secure Drive offre:

- Facilità d'uso: Personal Secure Drive funziona come qualsiasi unità Windows standard.
- Interfaccia basata su procedure guidate (wizard) per semplificare l'amministrazione e la configurazione.
- Integrazione con Microsoft EFS (Encrypting File System).

Massime garanzie con TPM (Trusted Platform Module)

Personal Secure Drive è basato sulla più recente iniziativa di Trusted Computing, il TPM (Trusted Platform Module). Personal Secure Drive si basa su TPM come processo di crittografia dei file, garantendo che i dati vengano protetti dall'accesso di personale non autorizzato e contemporaneamente "bloccati" sul PC su cui sono stati crittografati. TPM fornisce la sicurezza hardware per i dati, superando qualsiasi schema di protezione basato su software attualmente disponibile.

Vantaggi di Personal Secure Drive

- Consente la memorizzazione sicura dei dati sul PC locale.
- Protezione dati grazie a TPM (Trusted Platform Module) che fornisce la sicurezza basata su hardware.
- Interfaccia semplice e intuitiva.
- Integrazione completa con l'ambiente Windows; Personal Secure Drive funziona come una qualsiasi unità locale.
- Crittografia/decrittografia automatica di dati per utenti autorizzati; gli utenti finali non devono effettuare operazioni aggiuntive per la protezione dei dati.
- Routine di crittografia e decrittografia altamente efficienti; nessuna perdita di produttività o prestazioni per l'utente finale.



©Infineon

Technologies AG

Soluzione Infineon Security Platform - Caricamento e scaricamento di PSD

SCaricamento e scaricamento Personal Secure Drive

Personal Secure Drive può essere caricato (aperto) e scaricato (chiuso) per limitare l'accesso ai propri dati crittografati.

Prima di poter accedere a una PSD è necessario caricarla. L'operazione di caricamento richiede l'autorizzazione dell'utente. Per il caricamento di una PSD è necessaria un'autorizzazione. Una volta caricata la PSD è possibile accedere ai dati crittografati finché non si scarica esplicitamente la PSD, ci si disconnette o si arresta il computer.

Come caricare PSD

Caricare PSD selezionando [l'icona TNA](#), e quindi la voce **Personal Secure Drive - Carica** (se si è impostata una Personal Secure Drive) o **Personal Secure Drive - <LetteraUnità:EtichettaUnità> - Caricamento** (se si sono impostate più di una Personal Secure Drive).

Una volta completata l'autenticazione, viene avviato Windows Explorer e appare l'unità PSD.

Caricamento automatico di PSD all'avvio

È possibile impostare il caricamento automatico di PSD all'avvio di Windows.

Impostare questa opzione mediante [l'icona TNA](#), selezionando **Personal Secure Drive - Carica all'avvio** (se si è impostata una Personal Secure Drive) o **Personal Secure Drive - <LetteraUnità:EtichettaUnità> - Caricamento** (se si sono impostate più di una Personal Secure Drive). Se l'opzione è attiva, apparirà un segno di spunta accanto alla voce **Carica all'avvio** .

Come Scaricare PSD

Scaricare PSD selezionando [l'icona TNA](#), e quindi la voce **Personal Secure Drive - Scarica** (se si sono impostate più di una Personal Secure Drive) o **Personal Secure Drive - <LetteraUnità:EtichettaUnità> - Scarica** (se si sono impostate più di una Personal Secure Drive).

Finestra di dialogo Carica PSD

Se si è scelto di caricare PSD, viene visualizzata la [finestra di autenticazione](#) che consente di utilizzare le funzionalità di Security Platform.

Finestra di dialogo Scarica PSD

Se la vostra PSD sta per essere scaricata, verrà visualizzato un dialogo contenente lo stato di tutte le Personal Secure Drive attualmente caricate. Se si continua e una PSD da scaricare ha dei file aperti, verrà visualizzato un messaggio di avviso.

Elementi della finestra di dialogo Scarica PSD	Spiegazione
<input type="checkbox"/> <i>Personal Secure Drives</i>	Qui è possibile vedere lo stato di tutte le Personal Secure Drive attualmente caricate. Selezionare tutte le unità che si desidera scaricare. Accertarsi che nessuna delle unità da scaricare sia in uso. È possibile aggiornare questo elenco premendo il tasto "F5".
<input checked="" type="checkbox"/> <i>Chiudi la finestra di dialogo al termine dell'operazione</i>	Spuntare questa casella di controllo se si desidera che il Dialogo di Scaricamento PSD sia chiuso automaticamente dopo che la Personal Secure Drive selezionata è stata scaricata. Se l'operazione non è stata completata correttamente, la finestra di dialogo non verrà chiusa e apparirà una segnalazione di errore.
<input type="checkbox"/> <i>Scarica</i>	Scegliere Scarica per continuare.
<input type="checkbox"/> <i>Chiudi</i>	Cliccare su questo pulsante per chiudere la finestra di dialogo Scarica PSD senza eseguire l'operazione.



Infineon Security Platform Solution

Gestione di Personal Secure Drive

Questa sezione descrive gli aspetti gestionali relativi a Personal Secure Drive.

Criteria

I criteria di Personal Secure Drive appartengono all'[Amministrazione dei criteri di Infineon Security Platform](#).

Mapping delle lettere di unità per Personal Secure Drive

Durante la configurazione di Personal Secure Drive, viene chiesto di scegliere una lettera di unità tra quelle disponibili nell'elenco visualizzato. L'elenco non comprende le lettere di unità attualmente in uso, né quelle precedentemente assegnate a dispositivi sostituibili "a caldo" (dispositivi che possono essere sostituiti mantenendo l'alimentazione del sistema) o a unità rimovibili. In questo modo, si evitano conflitti tra le lettere di unità.

Inoltre, sette lettere non assegnate sono contrassegnate come “non consigliate” al fine di conservarle per l'uso futuro da parte di periferiche con collegamento a caldo non ancora caricate. Si evitano così potenziali conflitti con le lettere di unità che verranno assegnate ad eventuali dispositivi supplementari con collegamento a caldo.

Il numero delle lettere di unità riservate a dispositivi supplementari è impostato nella chiave del registro di sistema di Windows
HKEY_LOCAL_MACHINE\Software\Infineon\TPM
Software\PSD\DLSkip. Per aumentare o diminuire il numero delle lettere riservate, occorre modificare il valore della chiave.

Nota: Il valore predefinito nella chiave del registro di sistema è 7, che è il valore massimo consentito è 9. Se si imposta la chiave a un valore superiore a 9, viene ripristinato automaticamente il valore predefinito.



Soluzione Infineon Security Platform

Ripristino di Personal Secure Drive

Ripristino di Personal Secure Drive consente di ripristinare i dati dell'unità PSD nel caso in cui siano stato smarrite le credenziali necessarie. Il ripristino dei dati è reso possibile dall'uso di un agente di ripristino. Un agente di ripristino è un [ruolo utente](#) che consente di decrittografare i dati di altri utenti. Se l'utente aggiorna il sistema da un'edizione Home ad un Sistema Operativo superiore, ad es. da Windows XP Home a Windows XP Professional o da Windows Vista Basic Home a Windows Vista Home Premium, gli agenti di recupero Home non sono più validi e l'utente deve configurare il recupero PSD di nuovo come descritto nella tavola "Come configurare ed eseguire un Recupero PSD".



Condizioni preliminari per l'utilizzo di Ripristino di PSD

- Esiste almeno un agente di ripristino PSD.
- Il file immagine PSD è accessibile.

È possibile ripristinare un file immagine PSD perduto, o i dati utente presenti nel file, unicamente da un file [immagine di backup di PSD](#).

Come configurare ed eseguire Ripristino di PSD

Ripristino di PSD	Edizioni di Windows che non supportano EFS	Edizioni di Windows che supportano EFS
Informazioni generali	<ul style="list-style-type: none">• Vengono utilizzati agenti di ripristino PSD dedicati. Gli utenti di Personal Secure Drive dovranno registrare l'agente di ripristino PSD.• Tutte le attività vengono eseguite mediante il tool a riga di comando di Ripristino di PSD.	<ul style="list-style-type: none">• Vengono utilizzati agenti di ripristino EFS.• Gli agenti di ripristino sono gestiti mediante le Impostazioni di protezione Microsoft.• Il ripristino di PSD viene eseguito attraverso il tool a riga di comando di Ripristino di PSD.
Come configurare gli agenti di ripristino:		
Abilitazione di Ripristino di PSD	<ol style="list-style-type: none">1. Configurare PSD.2. Creare il file del certificato di	<ol style="list-style-type: none">1. Configurare PSD.2. Configurare gli agenti di

ripristino e il file PKCS #12 di ripristino.

Verrà chiesto di impostare la password di protezione del file PKCS #12.

Riga di comando:
PSDRecovery /R:nomefile

3. Registrare l'agente di ripristino PSD.

Riga di comando:
PSDRecovery /A:nomefile.CER [/ID:driveID]

Nota: è possibile eseguire prima le operazioni descritte al punto 2 e quindi passare al punto 1.

ripristino EFS utilizzando le Impostazioni di protezione Microsoft.

Riga di comando:
secpol.msc

3. [Caricare PSD](#) per rendere effettive le modifiche apportate.

Nota: è possibile eseguire prima le operazioni descritte al punto 2 e quindi passare al punto 1. In questo caso non è più necessaria l'esecuzione della fase 3. In Windows 2000, EFS crea un agente di ripristino per impostazione predefinita, diversamente da Windows 7, Windows Vista e Windows XP Professional.

Visualizzazione dell'elenco degli agenti di ripristino registrati	Visualizzare l'elenco degli agenti di ripristino registrati in PSD. Riga di comando: PSDRecovery /V [/ID:driveID]	Visualizzazione degli agenti di ripristino EFS mediante le Impostazioni di protezione Microsoft. Riga di comando: secpol.msc	
Eliminazione di un agente di ripristino registrato	È possibile eliminare l'agente di ripristino PSD selezionato. Riga di comando: PSDRecovery /D:[nome] [numero] [/ID:driveID]	È possibile eliminare gli agenti di ripristino EFS mediante le Impostazioni di protezione Microsoft. Riga di comando: secpol.msc	
Come ripristinare PSD:	<ul style="list-style-type: none"> • Assicurarsi di poter accedere sia al certificato digitale dell'agente di ripristino, sia alla chiave privata associata (in altre parole, è necessario importare il file di ripristino PKCS #12). • Verificare che l'applicazione Personal Secure Drive sia installata. • Verificare che i dati crittografati di Personal Secure Drive da ripristinare siano accessibili all'agente di ripristino. 		
Ricerca del file immagine PSD	I dati crittografati di Personal Secure Drive sono situati in un	Ripristino dei dati	Ripristinare in una nuov

unico file con estensione * .FSF.
I file * .FSF sono file di sistema nascosti e normalmente sono accessibili soltanto agli utenti che dispongono dei diritti amministrativi richiesti.

Per conoscere la posizione di questo file, è possibile utilizzare il tool a riga di comando di Ripristino di PSD: PSDRecovery /L

PSD

temporanea
È possibile
questi dati :
Ripristino c
attivo. In qu
i dati PSD j
essere visu
eventualme
in un'altra p
Riga di con
PSDRecov
/M:DriveIn
[X:]

Sintassi del tool a riga di comando di Ripristino di PSD

PSDRecovery.exe è un tool a riga di comando simile a cipher.exe di Encrypting File System.

 Si noti che la sintassi non distingue tra lettere maiuscole e minuscole.

PSDRecovery /A:nomefile.CER [/ID:driveID]

Supportato solo nelle edizioni Windows che non supportano EFS.

Registra un agente recupero dati aggiungendo il certificato del file *.CER specificato all'elenco degli agenti recupero dati a tutte le Personal Secure Drive.

nomefile.CER

Nome del file con estensione .CER

/ID:driveID

Facoltativo: Esegue un'azione specificata solo per la Personal Secure Drive con l'ID unità dato.

PSDRecovery /D:nome[/ID:driveID]

PSDRecovery /D:numero[/ID:driveID]

Supportato solo nelle edizioni Home di Windows.

Elimina l'agente di ripristino selezionato dall'elenco degli agenti di ripristino registrati in PSD. È necessario specificare il nome o il numero progressivo (visualizzati con PSDRecovery /V) dell'agente di ripristino desiderato.

nome

Nome dell'agente di ripristino, come visualizzato con PSDRecovery /V

numero

Numero progressivo assegnato all'agente di ripristino, come visualizzato con PSDRecovery /V

Senza parametro /ID questa azione è eseguita per tutte le Personal Secure Drive.

PSDRecovery /L

ID elenco, file di immagine e percorso file di immagine per tutte le Personal Secure Drive.

PSDRecovery /M:DriveImageFile.FSF [X:]

Ripristina i dati PSD in una nuova unità temporanea non crittografata.

DriveImageFile.FSF	Percorso completo del file immagine PSD, come visualizzato con PSDRecovery /L
--------------------	---

X	Lettera dell'unità logica da assegnare alla nuova unità temporanea in cui verranno salvati i dati recuperati (opzionale). Se non si indica la lettera di unità, viene utilizzata la prima disponibile.
---	--

PSDRecovery /R:nomefile

Supportato solo nelle edizioni Home di Windows.

Genera la chiave e il certificato dell'agente di ripristino PSD e li scrive in un file *.PFX (contenente sia il certificato, sia la chiave privata) e in un file *.CER (che contiene soltanto il certificato).

nomefile	Nome del file privo di estensione con o senza percorso completo. Se si sceglie di indicare il percorso completo, i file di output verranno collocati nella directory specificata. In caso contrario, i file verranno salvati nella directory corrente.
----------	---

PSDRecovery /V [/ID:driveID]

Supportato solo nelle edizioni Home di Windows.

Consente di visualizzare l'elenco degli agenti di ripristino registrati in PSD. Per ciascun agente, vengono indicati i seguenti parametri: numero progressivo, nome dell'agente di ripristino e valore hash del certificato.

Senza parametro /ID questa azione è eseguita per tutte le Personal Secure Drive.



Soluzione Infineon Security Platform

Encrypting File System

La funzionalità EFS (Encrypting File System) fa parte della tecnologia di protezione dei volumi del file system NTFS. L'integrazione è completamente trasparente e non richiede alcun intervento, a parte la configurazione iniziale. La funzionalità EFS consente di proteggere i documenti dall'accesso non autorizzato ai dati memorizzati (ad esempio in caso di furto di un computer portatile). In questa fase iniziale viene crittografato un volume o una cartella. Di conseguenza, vengono crittografati tutti i file e le sottocartelle presenti nel volume selezionato.

L'uso di un volume o di una cartella crittografata non presenta alcuna differenza per l'utente, in quanto la crittografia è del tutto trasparente agli utenti con diritto di accesso al volume o alla cartella.

Nota:

- si raccomanda di utilizzare la crittografia a livello di cartella o volume, non a livello di file. Per semplicità, sono descritti solo questi elementi.
- la funzione EFS non è supportata nelle edizioni Home di Windows.



©Infineon

Technologies AG

Soluzione Infineon Security Platform

Caratteristiche della funzione EFS (Encrypting File System)

Questo è un estratto della Guida in linea Microsoft originale relativo alla funzione EFS. La Guida completa è disponibile alla pagina. Per consultare la Guida in linea Microsoft, ridurre a icona tutte le finestre attualmente aperte in modo da visualizzare il desktop di Windows. Premere F1 ed eseguire la ricerca desiderata utilizzando una parola chiave appropriata.

- Gli utenti possono crittografare i file durante la memorizzazione su disco. La crittografia viene abilitata selezionando una casella di controllo nella finestra di dialogo delle proprietà del file.
- L'accesso ai file crittografati è facile e veloce. All'accesso da disco, gli utenti vedono i dati come testo normale.
- La crittografia dei dati viene eseguita automaticamente ed è completamente trasparente all'utente.
- Gli utenti possono decrittografare un file deselegionando la casella di controllo nella finestra di dialogo delle proprietà del file.
- Gli amministratori possono recuperare i dati crittografati da un altro utente. Questo garantisce l'accesso ai dati anche se l'utente che li ha crittografati non è più disponibile o se ha perso la chiave privata.
- La funzione EFS crittografa solo i dati memorizzati sul disco. Per crittografare i dati trasferiti su una rete TCP/IP sono disponibili due funzioni opzionali: Internet Protocol Security (IPSec) e la crittografia PPTP.

Nota: la funzione EFS non è supportata nelle edizioni Home di Windows.



©Infineon

Technologies AG

Soluzione Infineon Security Platform

Uso del sistema Encrypting File System

Se si utilizza l'Encrypting File System (EFS) è opportuno considerare alcuni fattori. Determinati aspetti riguardano solo gli amministratori di sistema, in quanto sono importanti per l'installazione di EFS.

Aspetti amministrativi

- Possono essere crittografati solo i file e le cartelle sui volumi NTFS
In genere questa non è una limitazione reale, dato che il file system NTFS è quello raccomandato se si utilizza Windows 2000 o XP. Anche un numero considerevole di funzioni non collegate alla soluzione di sicurezza si basano su NTFS.
- Un volume FAT interrompe la crittografia in ogni caso
Ogni volta che un file crittografato viene salvato su un volume FAT, la protezione non esiste più. Questo principio vale soprattutto per i dischetti, utilizzati tipicamente per trasferire i file di piccole dimensioni. Ma anche i dischi rigidi con più partizioni possono essere un anello debole, se una di tali partizioni è un volume FAT e questo volume viene utilizzato per la memorizzazione anche solo temporanea dei file.
- I file di sistema e i file compressi non possono essere crittografati
La cartella di installazione di Windows e alcuni file della cartella principale della partizione di avvio non possono essere protetti dal meccanismo EFS. Ciò non interrompe affatto la protezione, dato che il sistema operativo stesso protegge i file di sistema principali con meccanismi speciali che non possono essere disattivati. Per ulteriori informazioni su questo argomento, vedere la sezione relativa alle [domande frequenti](#).
- I file temporanei sono anche esposti a potenziali attacchi
Per evitare "falle" nella struttura di protezione dei dati, è necessario crittografare anche i file e le cartelle temporanei. La maggior parte delle applicazioni utilizza le cartelle standard per la memorizzazione dei file temporanei. La crittografia di queste cartelle migliora notevolmente il livello di sicurezza di un sistema. L'uso di una cartella temporanea comune per tutti gli utenti è sconsigliata, poiché richiede una gestione amministrativa supplementare.

Aspetti operativi

Gli utenti che utilizzano file e cartelle crittografate dovrebbero tenere in considerazione le informazioni e i suggerimenti riportati di seguito.

- La crittografia è facile da configurare. Informazioni più dettagliate sono disponibili nelle pagine della Guida in linea Microsoft relative a EFS.
- Il file crittografato può essere aperto solo dall'utente che lo ha creato. L'accesso da parte di altri utenti è possibile e deve essere concesso manualmente, file per file.
- Gli utenti devono utilizzare la funzione di copia e incolla per mantenere la crittografia quando spostano i file in una cartella crittografata. Se si utilizza la tecnica "trascina e rilascia" (drag and drop) per spostare i file, questi non vengono automaticamente crittografati nella nuova cartella.
- Se si desidera utilizzare EFS sui sistemi remoti, questa funzionalità deve essere configurata manualmente su tali sistemi.
- Gli utenti devono crittografare la cartella **Documenti** se questa è la posizione in cui salvano la maggior parte dei documenti. Questo garantisce che i documenti personali siano crittografati per impostazione predefinita.

Gli argomenti sopra esposti sono una breve panoramica sull'uso di EFS. Informazioni più dettagliate sono disponibili nelle pagine della Guida in linea Microsoft relative a EFS. Per consultare la Guida in linea Microsoft, ridurre a icona tutte le finestre attualmente aperte in modo da visualizzare il desktop di Windows. Premere F1 ed eseguire la ricerca desiderata utilizzando una parola chiave appropriata.

Alcuni aspetti tecnici di EFS sono trattati nella sezione [risoluzione dei problemi](#).

Nota: la funzione EFS non è supportata nelle edizioni Home di Windows.



Infineon Security Platform Solution

Posta elettronica protetta

La protezione della posta elettronica è una delle applicazioni con chiave pubblica più comunemente utilizzate, in quanto permette agli utenti di condividere informazioni in modo confidenziale garantendo che l'autenticità delle informazioni sia mantenuta durante il trasferimento. Questo risultato viene raggiunto tramite la crittografia e/o la firma digitale specifica della posta elettronica per impedire alle persone non autorizzate di leggere o modificare il contenuto dei messaggi di posta elettronica inviati dall'utente. L'uso di questa funzione garantisce che solo l'autore della posta elettronica e i destinatari specifici possano decrittografare e leggere il messaggio o confermare l'identità del mittente.

Questo documento spiega come utilizzare i [certificati digitali](#) e offre istruzioni dettagliate per configurare [Microsoft Windows Mail/Outlook](#) e [Mozilla Thunderbird](#).



©Infineon

Technologies AG

Infineon Security Platform Solution

Protezione della posta elettronica con Windows Mail/Outlook Express/Outlook

Questa sezione spiega come configurare Windows Mail/Outlook Express/Outlook per proteggere la posta elettronica e come utilizzare il [certificato digitale](#) per inviare una e-mail con firma elettronica e crittografata:

- [Configura protezione della posta elettronica](#)
- [Invia Messaggi con la Firma Digitale](#)
- [Invia Messaggi Crittografati](#)



©Infineon

Technologies AG

Infineon Security Platform Solution

Configura protezione della posta elettronica

Verificare che Outlook/Windows Mail/Outlook Express siano già installati e configurati per l'invio e la ricezione dei messaggi tramite il server di posta elettronica. Inoltre, è richiesta la presenza di almeno un certificato digitale per poter procedere con le operazioni indicate di seguito.

Nota: Se non si dispone di un certificato per la protezione della posta elettronica, è necessario richiederlo prima di iniziare le operazioni di configurazione.

+ Windows Mail/Outlook Express

+ Outlook 2007

+ Outlook 2003

+ Outlook XP

+ Outlook 2000

Infineon Security Platform Solution

Invia Messaggi con la Firma Digitale

⊕ **Windows Mail/Outlook Express**

⊕ **Outlook 2007**

⊕ **Outlook 2003**

⊕ **Outlook XP**

⊕ **Outlook 2000**



©Infineon Technologies AG

Infineon Security Platform Solution

Invia Messaggi Crittografati

Per inviare un messaggio crittografato, innanzi tutto è necessaria una copia della chiave pubblica o del certificato di crittografia del destinatario. Il certificato contiene una copia della chiave pubblica. Verificare di aver ricevuto il certificato di chiave pubblica del destinatario e che quest'ultimo sia presente nell'elenco dei contatti prima di procedere con i passaggi seguenti:

⊕ **Windows Mail/Outlook Express**

⊕ **Outlook 2007**

⊕ **Outlook 2003**

⊕ **Outlook XP**

⊕ **Outlook 2000**

Non è necessario utilizzare la chiave privata per inviare messaggi crittografati perché la crittografia utilizza la chiave pubblica del destinatario. Tuttavia, la chiave privata è necessaria per leggere un messaggio crittografato, in quanto la decrittografia richiede la chiave privata corrispondente alla chiave pubblica utilizzata per crittografare la e-mail.



Infineon Security Platform Solution

Protezione della posta elettronica con Mozilla Thunderbird

Questa sezione spiega come configurare Mozilla Thunderbird Mail per proteggere la posta elettronica e come utilizzare il [certificato digitale](#) per inviare una e-mail con firma elettronica e crittografata:

- [Configura protezione della posta elettronica](#)
- [Invia Messaggi con la Firma Digitale](#)
- [Invia Messaggi Crittografati](#)



©Infineon

Technologies AG

Infineon Security Platform Solution

Configura protezione della posta elettronica

Verificare che Mozilla Thunderbird sia installato e configurato per inviare e ricevere posta elettronica tramite il server di posta elettronica. Occorre almeno un certificato digitale per continuare con la procedura.

Nota: se non si dispone ancora di un certificato da utilizzare per proteggere la posta elettronica, procurarsene uno prima di continuare con i passaggi di configurazione descritti di seguito.

Mozilla Thunderbird

1. Avvio di Mozilla Thunderbird.
2. Fare clic su **Strumenti > Impostazioni Account...** per aprire il pannello Impostazioni Account.
3. Cliccare su **Sicurezza** nel riquadro sinistro nel account nome.
4. Cliccare sul pulsante **Seleziona...** nella sezione **Firma digitale** per definire il certificato da utilizzare per la firma elettronica della posta elettronica. Viene visualizzato un elenco di tutti i certificati disponibili. Selezionare un certificato, quindi apporre la firma utilizzando l'impostazione **Apponi firma digitale ai messaggi (impostazione predefinita)**.
5. Nella sezione **Crittografia** è possibile configurare il comportamento di crittografia predefinito.
 - A. Selezionare **Mai (non usare la crittografia)** se si desidera definire l'uso della crittografia in base alle necessità.
 - B. Se si seleziona **Richiesta (impossibile inviare i messaggi a meno che tutti i destinatari non abbiano i certificati)** tutte la posta elettronica vengono crittografate automaticamente.

La configurazione di PKCS #11 è descritta nella sezione [Configurare PKCS #11 per Mozilla Firefox](#).



©Infineon

Technologies AG

Infineon Security Platform Solution

Invio di messaggi con firma digitale con Mozilla Thunderbird

1. Avvio di Mozilla Thunderbird.
2. Fare clic su **Scrivi**, nella barra delle icone o selezionare **File > Nuovo > Messaggio** nel menu per aprire un modello di messaggio vuoto.
3. Inserire l'indirizzo del destinatario (o dei destinatari) o selezionarlo da un elenco tramite il pulsante **A**.
4. Se si desidera aggiungere allegati, cliccare sull'icona **Allega** nella barra delle icone per aprire una finestra di dialogo per la selezione dei file.
5. Aggiungere il testo nel campo **Oggetto** e nel **corpo** del messaggio.
6. Cliccare sul piccolo **pulsante freccia in corrispondenza dell'icona Sicurezza** o selezionare **Opzioni > Sicurezza** per visualizzare il menu di configurazione della sicurezza. Selezionare **Aggiungi firma digitale al messaggio** per apporre la firma alla e-mail. La firma è rappresentata da un simbolo nella parte destra della barra di stato.



©Infineon

Technologies AG

Infineon Security Platform Solution

Invia Messaggi Crittografati con Mozilla Thunderbird

1. Avvio di Mozilla Thunderbird.
2. Cliccare su **Componi** nella barra delle icone o selezionare **File > Nuovo > Messaggio** nel menu per aprire un modello di messaggio vuoto.
3. Inserire l'indirizzo del destinatario (o dei destinatari) o selezionarlo da un elenco tramite il pulsante **A**.
4. Se si desidera aggiungere allegati, cliccare sull'icona **Allega** nella barra delle icone per aprire una finestra di dialogo per la selezione dei file.
5. Aggiungere il testo nel campo **Oggetto** e nel **corpo** del messaggio.
6. Cliccare sul piccolo **pulsante freccia in corrispondenza dell'icona Sicurezza** o selezionare **Opzioni > Sicurezza** per visualizzare il menu di configurazione della sicurezza. Selezionare **Crittografa il messaggio** per crittografare il messaggio e-mail. È rappresentato da un simbolo di firma nella parte destra della barra di stato.



©Infineon

Technologies AG

Infineon Security Platform Solution

Macro con firma in Microsoft Word

Microsoft Word supporta livelli di sicurezza che consentono agli utenti di eseguire macro basate o meno su macro con firma digitale di uno sviluppatore presente in un elenco di fonti accreditate. Un timbro digitale di identificazione sulla macro conferma che essa proviene dallo sviluppatore che l'ha firmata e che la macro non è stata modificata, garantendone così l'autenticità e confermando che non contiene virus.

Il meccanismo delle macro con firma è supportato da Microsoft Word 2000 e da Microsoft Word XP.



©Infineon

Technologies AG

Infineon Security Platform Solution

Come configurare Microsoft Word per la firma delle macro

Per utilizzare le macro firmate, è necessario configurare appositamente Microsoft Word. Infatti, tale funzionalità di protezione è disponibile soltanto dopo aver configurato l'applicazione.

Microsoft Word offre **tre livelli di protezione** che consentono di ridurre i rischi dovuti all'eventuale presenza di virus delle macro nei documenti, modelli o componenti aggiuntivi caricati nell'applicazione. Se l'amministratore della rete non ha imposto nessun livello di protezione in ambito aziendale, è possibile scegliere il livello di protezione più adatto alle proprie esigenze. Se il livello di protezione di Microsoft Word è impostato a Medio o Alto, è possibile gestire l'elenco delle origini macro attendibili. In questo modo, ogni volta che si apre un documento o si carica un componente aggiuntivo che contiene delle macro, verranno abilitate automaticamente solo quelle sviluppate da una delle fonti giudicate attendibili.



Infineon Security Platform Solution

Firma digitale di un progetto macro in Microsoft Word

Livelli di sicurezza

1. Cliccare su **Strumenti > Macro > Sicurezza ...** per aprire la finestra di dialogo **Sicurezza**.
2. Scegliere il livello di sicurezza appropriato: Alto/Medio/Basso.

Registrazione di una nuova macro

1. Aprire un nuovo documento cliccando su **Nuovo documento vuoto**.
2. Cliccare su **Strumenti > Macro > Registra Nuova Macro ...** .(Nota in **Microsoft Word 2007**: Fare clic **Visualizza > Macro > Registra Nuova Macro...**)
3. Viene visualizzata la finestra di dialogo **Registra macro**.
4. Inserire il nome della macro e cliccare su **OK** per chiudere la finestra di dialogo.
5. Scrivere il testo della macro.
6. Cliccare su **Interrompi registrazione**.

Firma di una (nuova) Macro in Microsoft Word 2007

1. Aprire il documento o il modello che contiene il progetto di macro che si intende firmare se il file non è aperto.
2. Click on **Visualizza > Macro > Visualizza Macro**, comparirà il dialogo **Macros**.
3. Selezionare un **nome Macro** dall'elenco. È possibile eseguire, modificare, creare o eliminare una macro.
4. Fare clic sul pulsante **Modifica** per aprire una finestra **Visual Basic**.
Modificare ora la macro selezionata.
5. Andare in **Gestione Progetto** per selezionare il progetto che si desidera firmare.
6. Fare clic su **Strumenti > Firma Digitale...** nella finestra Visual Basic per aprire il dialogo **Firma Digitale**.
7. Fare clic su **Scegli...** per aprire il dialogo **Seleziona Certificato**.
8. Selezionare un certificato appropriato dall'elenco.
9. Fare clic su **Visualizza Certificato** per visualizzare le informazioni sul certificato nel dialogo **Certificato**.
Nota: Fare clic sulla scheda **Dettagli** per visualizzare le informazioni sul certificato nel dialogo **Certificato**. Fare clic sul pulsante **OK** per chiudere questo dialogo.
10. Fare clic sul pulsante **OK** per chiudere il dialogo **Seleziona Certificato**.
11. Chiudere il dialogo **Firma Digitale** facendo click sul pulsante **OK**.
12. Per salvare la macro fare clic su **Salva** e salvare il documento o il modello come **Documento Word con Attivazione Macro**.
Nota: Poiché **Microsoft Word** utilizza la chiave privata per firmare la macro, è necessario inserire il segreto chiave privata.
13. Fare clic su **File > Chiudi** per ritornare a Microsoft Word.

Firma elettronica di una (nuova) macro

1. Aprire il documento o il modello che contiene il progetto macro da firmare, se il file non è aperto.
2. Cliccare su **Strumenti > Macro > Macro**; viene visualizzata la finestra di dialogo **Macro**.
3. Selezionare un **nome macro** dall'elenco. La macro può essere eseguita, modificata o eliminata.
4. Cliccare sul pulsante **Modifica** per aprire una finestra **Visual Basic**. Modificare la macro selezionata.

Nota: è possibile aprire la finestra **Visual Basic** anche cliccando su **Strumenti > Macro > Visual Basic Editor**.

5. Passare a **Explorer del progetto** per selezionare il progetto che si desidera firmare.
6. Cliccare su **Strumenti > Firma digitale ...** nella finestra Visual Basic per aprire la finestra di dialogo **Firma digitale**.
7. Cliccare su **Scegli** per aprire la finestra di dialogo **Selezione certificato**.
8. Selezionare un certificato dall'elenco.
9. Cliccare su **Visualizza certificato** per visualizzare informazioni sul certificato nella finestra di dialogo **Certificato**.

Nota: cliccare su **Dettagli ...** per visualizzare informazioni sul certificato nella finestra di dialogo **Certificato**. Cliccare su **OK** per chiudere questa finestra di dialogo.

10. Cliccare su **OK** per chiudere questa finestra di dialogo.
11. Chiudere la finestra di dialogo **Selezione certificato** cliccando su **OK**.
12. Chiudere la finestra di dialogo **Firma digitale** cliccando su **OK**.
13. Cliccare su **Salva Normal** per salvare la macro.

Nota: la macro può essere salvata nella cartella di progetto **Normal** (**Tutti i documenti (Normal.dot)**) oppure nella cartella **Documenti**.

Dato che **Microsoft Word** utilizza la chiave privata per firmare la macro, è necessario inserirla.

14. Cliccare su **File > Chiudi** per tornare a Microsoft Word.



©Infineon Technologies AG

Infineon Security Platform Solution

Protezione delle connessioni di rete

Con Security Platform Solution è possibile proteggere le connessioni di rete. Se si utilizzano i servizi integrativi di Security Platform (ad esempio, Cryptographic Service Provider per Crypto-API Microsoft e Crypto-API PKCS #11), le chiavi private dei propri certificati verranno protette da Trusted Platform Module.

I tipi di rete supportati sono i seguenti:

- [Browser Web/Connessione server \(autenticazione client\)](#)
- [Rete privata virtuale \(VPN\)](#)
- [Rete locale wireless \(WLAN\) o cablata \(LAN\)](#)

È possibile utilizzare certificati per l'autenticazione dell'utente e certificati per l'autenticazione del computer.

Nelle tabelle seguenti vengono indicati i tipi di rete e di certificato attualmente supportati.

Tipo di rete	Servizio integrativo di Security Platform	Protocollo	Tipo di certificato
Browser Web/Connessione server (autenticazione client)	Infineon TPM Cryptographic Provider o Infineon TPM RSA and AES Cryptographic Provider (CSP utente)	SSL/TLS	Certificato utente
Browser Web/Connessione server (autenticazione client)	Infineon TPM PKCS #11 Provider	SSL/TLS	Certificato utente
VPN	Infineon TPM Cryptographic Provider o Infineon TPM RSA and AES Cryptographic Provider (CSP utente)	IPsec	Certificato utente

VPN	Infineon TPM Platform Cryptographic Provider (Piattaforma CSP)	IPsec	Certificato computer
WLAN o LAN cablata	Infineon TPM Cryptographic Provider o Infineon TPM RSA and AES Cryptographic Provider (CSP utente)	WLAN: IEEE 802.11 EAP-TLS LAN cablata: IEEE 802.1X EAP-TLS	Certificato utente
WLAN o LAN cablata	Infineon TPM Platform Cryptographic Provider (Piattaforma CSP)	WLAN: IEEE 802.11 EAP-TLS LAN cablata: IEEE 802.1X EAP-TLS	Certificato computer

Per altri tipi di rete o aree applicative, contattare il supporto tecnico clienti.



Infineon Security Platform Solution

Autenticazione del client

Fino a poco tempo fa le reti di computer utilizzavano un database centralizzato di account per gestire gli utenti, i relativi privilegi e gli accessi. Questa tecnica è semplice ed efficace per le reti di piccole dimensioni. Nello scenario attuale, in cui sono sempre più frequenti reti molto estese con migliaia di utenti, questa forma di controllo centralizzato è difficile da gestire. La verifica di un account nel database su Internet o la gestione di un lungo elenco di utenti possono risultare problematici. Inoltre, l'avvento di Internet ha esposto le reti di computer all'attacco da parte di entità esterne.

Uso dei certificati

I certificati di chiavi pubbliche forniscono una soluzione che semplifica notevolmente l'amministrazione di numerosi utenti nelle reti estese e riduce al tempo stesso il rischio di attacchi a ID/password. Questi certificati possono essere distribuiti su larga scala, vengono rilasciati da vari soggetti ed enti e sono verificati esaminando il certificato senza dover fare riferimento a un database centralizzato.

I certificati possono essere utilizzati per effettuare comunicazioni sicure e per l'autenticazione degli utenti tra client e server sul Web. I certificati consentono ai client di determinare l'identità del server, poiché quest'ultimo presenta un certificato di autenticazione che rivela la propria origine. Se ci si collega a un sito Web in possesso di un certificato rilasciato da un'authority riconosciuta, si ha la garanzia che tale server sia effettivamente gestito dalla persona o dall'organizzazione identificata dal certificato. In modo analogo, i certificati consentono ai server di determinare l'identità degli utenti. Quando ci si collega a un sito Web, la propria identità viene indicata al server dal certificato del client. Il documento utilizzato per identificare un server viene definito **certificato del server** e il processo effettivo di verifica dell'identità del server viene denominato **autenticazione del server**. Analogamente, il documento utilizzato per verificare l'identità del client viene definito **certificato del client** e il processo è la cosiddetta **autenticazione del client**.

Ad esempio, se un server Web intende limitare l'accesso a informazioni o servizi a utenti o client specifici, richiede il certificato del client quando viene effettuata la connessione sicura (ad esempio, SSL).

Mentre l'autenticazione del server garantisce la trasmissione sicura dei dati, l'autenticazione del client migliora la sicurezza di tali transazioni in linea.

Mappatura dei certificati agli account utente

La tecnologia delle chiavi pubbliche ha fornito soluzioni a molti problemi associati alla sicurezza delle reti di grandi dimensioni. I certificati possono essere utilizzati per determinare l'identità di un soggetto e verificarne l'autenticità senza utilizzare estesi database di utenti ed elenchi di account con i relativi privilegi di accesso.

Tuttavia, i sistemi operativi e i tool di amministrazione esistenti sono strutturati solo per l'uso degli account utente e non dei certificati. La soluzione più semplice per conservare i vantaggi derivanti dai certificati e dagli account utente consiste nel creare un'associazione, o mappatura, tra certificato e account utente. In questo modo, il sistema operativo continua a utilizzare gli account, mentre il sistema più grande e gli utenti utilizzano i certificati.

In questo modello un certificato che deve essere rilasciato a un utente viene mappato all'account di tale utente sulla rete. Quando un utente presenta il proprio certificato, il sistema verifica la mappatura e stabilisce quale account collegare.

La presente Guida introduttiva delinea diversi approcci a questo argomento. Spiega come preparare il servizio di informazioni Internet (IIS) e la Active Directory per autenticare i client, nonché l'uso dell'autenticazione client in Internet Explorer.

- [Mappatura dei certificati per gli account utente in IIS e Active Directory](#)
- Autenticazione dei client con Internet Explorer

La mappatura dei certificati utente e l'autenticazione dei client viene trattata anche per l'ambiente PKCS #11 con Mozilla Firefox.

- [Mappatura dei certificati per gli account utente in Mozilla Firefox](#)
- [Autenticazione dei client con Mozilla Firefox](#)



Infineon Security Platform Solution

Autenticazione del client con Internet Explorer

Se il server Web richiede un certificato client, Internet Explorer firmerà un messaggio con la chiave privata associata al certificato client fornito, allo scopo di garantire che l'utente attuale sia effettivamente il proprietario del certificato client.

Ulteriori informazioni sull'autenticazione dei client con Internet Explorer sono disponibili sul sito Microsoft TechNet.



©Infineon

Technologies AG

Infineon Security Platform Solution

Mapping dei certificati agli account utente in IIS e Active Directory

La mappatura dei certificati agli utenti di Windows 2000/XP viene eseguita sia attraverso il servizio Active Directory di Windows 2000/XP, sia mediante le regole definite nel componente Internet Information Services (IIS).

È quindi possibile scegliere se mappare i certificati agli account utente con IIS oppure con Active Directory, in base al tipo di autenticazione client (per tutti gli utenti del dominio oppure per entità esterne che non appartengono al proprio dominio). Si dovrà invece utilizzare la mappatura di IIS per autenticare utenti che non appartengono al proprio dominio.

Nota: L'autenticazione client con IIS richiede l'utilizzo della funzionalità SSL (Secure Socket Layer) del server Web, il che significa che è necessario richiedere un certificato server da una CA. Infatti, l'autenticazione del server mediante un apposito certificato è obbligatoria nel caso di connessioni protette SSL e l'autenticazione del client rappresenta una misura di protezione aggiuntiva.

Consultare il sito Microsoft TechNet per ulteriori informazioni sulla mappatura dei certificati agli account utente con IIS e Active Directory e su Internet Information Services.



©Infineon

Technologies AG

Infineon Security Platform Solution

Autenticazione dei client con Mozilla Firefox

Se il server Web richiede un certificato al client, Mozilla Firefox firma un messaggio con la chiave privata corrispondente al certificato client fornito per assicurare che l'utente sia il vero proprietario del certificato.

In base alla configurazione della cache della password, può essere necessario immettere la password del database dei certificati ogni volta che viene richiesto il certificato del client per l'autenticazione. In caso contrario, la password viene richiesta solo per la prima autenticazione.

Se è già stato rilasciato un certificato per l'uso con una pagina Web specifica, tale certificato viene assunto automaticamente. In caso contrario, viene richiesto di fornire il certificato corretto. La descrizione della [mappatura dei certificati per l'account utente e le pagine Web](#) illustra la procedura per configurare correttamente l'ambiente protetto.



©Infineon

Technologies AG

Infineon Security Platform Solution

Mappatura dei certificati per gli account utente in Mozilla Firefox

La mappatura di un certificato a un account utente viene eseguita automaticamente sulla scorta del fatto che il certificato è memorizzato nel database locale dei certificati dell'utente. L'accesso a questo database è protetto da una password utente specifica. Se non viene sostituito il computer, sono disponibili i certificati presenti nel database locale.

In una rete aziendale di grandi dimensioni può essere necessario disporre dei certificati non solo sul computer locale, ma anche su ciascun sistema della rete. Se le strutture amministrative non mettono a disposizione cartelle condivise per memorizzare i profili utente, i certificati utente devono essere esportati dal computer dell'utente in una directory aziendale. Questo servizio di directory fornisce quindi l'autenticazione centrale o consente di reimportare un certificato utente su un altro computer.

Approccio alternativo: la memorizzazione dei profili utente in una cartella condivisa (profili di roaming) riduce al minimo il carico amministrativo. Unitamente all'accesso al database dei certificati utente e a TUTTI gli altri dati specifici dell'utente memorizzati in tale cartella, è garantito l'accesso coerente da qualsiasi punto della rete aziendale.

Nota: l'autenticazione del client implica l'uso del Secure Sockets Layer (SSL) del server Web, il che comporta la necessità di ottenere un certificato per il server da un'autorità di certificazione. Questo perché l'autenticazione del server tramite un certificato del server è obbligatoria per una connessione SSL, mentre l'autenticazione del client è solo una misura di sicurezza supplementare.



©Infineon

Technologies AG

Infineon Security Platform Solution

Virtual Private Network (VPN)

Una VPN è una rete privata che utilizza una rete pubblica (normalmente Internet) per collegare siti o utenti remoti. Anziché utilizzare una connessione fisica dedicata, come una linea noleggiata, una VPN sfrutta le connessioni "virtuali" instradate su Internet dalla rete privata dell'azienda verso un suo sito remoto o un suo dipendente che lavora a distanza.

L'accesso remoto, chiamato anche VPDN (virtual private dial-up network) o rete commutata privata virtuale, rappresenta una connessione "User-to-LAN", ossia da utente a rete locale, utilizzata spesso dalle aziende. Ad esempio per i dipendenti che hanno bisogno di collegarsi alla rete privata da varie sedi distaccate. Normalmente, un'azienda che desidera creare una grande rete VPN ad accesso remoto si rivolgerà a un ESP, ovvero un fornitore di servizi per le aziende. L'ESP crea un server di accesso alla rete (NAS - network access server) e fornisce agli utenti remoti il software per client desktop da installare sui computer utilizzati a questo scopo.



©Infineon

Technologies AG

Infineon Security Platform Solution

Protocollo di autenticazione estendibile (EAP)

Il protocollo EAP (Extensible Authentication Protocol) viene utilizzato per creare configurazioni di reti private virtuali più sicure.

EAP aggiunge infatti un livello di sicurezza alle tecnologie VPN. EAP è un componente tecnologico importante per la protezione delle connessioni VPN, perché rispetto ad altri metodi di autenticazione offre maggior sicurezza nei confronti delle tecniche di violazione o di attacco basate su dizionari e su identificazioni fraudolente delle password.

EAP abilita questa funzionalità attraverso le tecnologie offerte dall'Authority di certificazione (CA) e da Security Platform. Per utilizzare il protocollo EAP con una rete VPN, il server e il client devono essere configurati per accettare l'autenticazione EAP come un metodo di autenticazione valido e devono possedere inoltre un certificato utente (X.509).



©Infineon

Technologies AG

Soluzione Infineon Security Platform

Come configurare una rete privata virtuale (VPN) per utilizzare EAP

Infineon Security Platform Solution utilizza il protocollo di autenticazione dei certificati EAP (Extensible Authorization Protocol) per autenticare i client. Prima di procedere alla configurazione, il client deve disporre di un [certificato](#) approvato da un'Autorità di certificazione. Il client e il server devono utilizzare la medesima Autorità di certificazione oppure autorità diverse ordinate secondo una gerarchia "trusted". Inoltre, il client deve disporre di Trusted Platform Module.



Durante la richiesta del certificato, è necessario scegliere uno dei [provider del servizio di crittografia](#) forniti da Security Platform Solution. Lo scopo del certificato è quello di consentire l'**autenticazione del client**. Nelle organizzazioni di grandi dimensioni, è possibile che l'amministratore abbia già installato i certificati necessari allo scopo.

Per ulteriori informazioni sulle reti private virtuali (VPN), consultare il sito Microsoft TechNet oppure la Guida in linea Microsoft sulle reti virtuali. Per consultare la Guida in linea Microsoft, ridurre a icona tutte le finestre attualmente aperte in modo da visualizzare il desktop di Windows. Premere F1 ed eseguire la ricerca desiderata utilizzando una parola chiave appropriata.

Per funzionare, una rete privata virtuale (VPN) necessita di Internet o di una rete Intranet. Prima di stabilire la connessione alla rete VPN, accertarsi di disporre di funzionalità Internet o Intranet per accedere al server VPN.

Per utilizzare EAP, la connessione iniziale deve essere effettuata dal client. Per la configurazione delle connessioni VPN, è possibile utilizzare anche le **Connessioni di rete** del proprio sistema operativo. Per ottenere maggiore assistenza sui passaggi necessari per il sistema operativo, consultare la Guida in linea di Microsoft Windows oppure il sito Microsoft TechNet.

Una volta creata la connessione, è necessario configurarla per EAP. A tale scopo, procedere come indicato di seguito.

- Fare clic con il tasto destro sulla nuova connessione VPN per visualizzarne le proprietà.
- Configurare le impostazioni di autenticazione nella scheda Protezione per utilizzare il protocollo EAP (Extensible Authentication Protocol) con

l'opzione per l'utilizzo di una SmartCard o di un altro certificato.

- Configurare le proprietà EAP per utilizzare un certificato sul computer.



Se si dispone di più certificati per l'autenticazione del client e per la crittografia, accertarsi di utilizzare il certificato corretto per la connessione VPN. All'avvio della connessione, specificare il certificato associato a uno dei [provider del servizio di crittografia](#) forniti da Security Platform Solution.

È necessario che l'utente sia connesso al computer per utilizzare EAP con un certificato utente.



©Infineon

Technologies AG

Infineon Security Platform Solution

Reti locali wireless (WLAN)

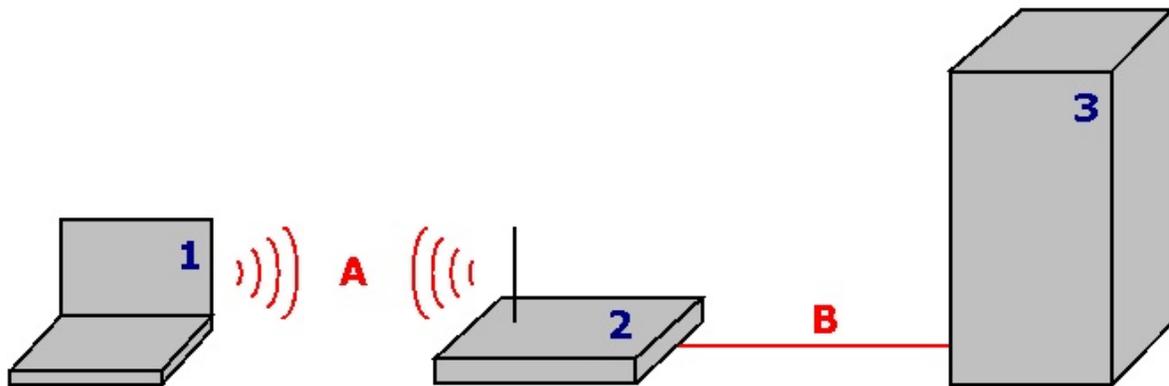
Con Security Platform Solution, è possibile proteggere le chiavi private dei certificati che vengono utilizzati per le reti LAN, sia wireless (IEEE 802.11 EAP-TLS), sia cablate (IEEE 802.1X EAP-TLS). Tale protezione viene fornita grazie ad uno dei provider del servizio di crittografia (CSP) disponibile nel software Security Platform Solution.

La descrizione seguente è dedicata alle reti LAN wireless (WLAN).

Introduzione alle reti WLAN

Le reti LAN wireless (WLAN) utilizzano onde radio ad alta frequenza, al posto dei tradizionali cavi, per comunicare con i vari nodi. Quindi, non è necessaria la visibilità reciproca ("line of sight") tra trasmettitore e ricevitore. I punti di accesso wireless (stazioni base) sono collegati via cavo a una rete Ethernet e trasmettono frequenze radio entro un determinato raggio. Le reti LAN wireless funzionano come i sistemi di telefonia cellulare. In particolare, nei sistemi concepiti per l'ufficio, gli utenti possono passare liberamente tra i vari punti di accesso senza dover interrompere la connessione.

Lo standard **IEEE 802.11** (wireless fidelity, "Wi-Fi") specifica le tecnologie richieste per le reti LAN wireless. Tale standard comprende i metodi di crittografia **WPA** (Wi-Fi Protected Access) e **WEP** (Wired Equivalent Privacy).



1	Client WLAN	PC Security Platform. Trusted Platform Module protegge la chiave privata del certificato in uso. I client WLAN sono connessi al punto di accesso (A) senza l'uso di cavi.
2	Punto di accesso	È chiamato anche "stazione base". Il punto di accesso collega i client WLAN a una rete cablata (B).
3	Server RADIUS	Ad esempio, il Servizio di autenticazione Internet (IAS) disponibile nel server Microsoft Windows 2003. Il server RADIUS gestisce l'autenticazione utente.

Ulteriori informazioni

Per ulteriori informazioni sulle reti WLAN, è possibile consultare la documentazione disponibile su Internet:

- Microsoft Developer Network (MSDN) e la Guida in linea di Microsoft Windows (ricercare "rete senza fili")
- Wi-Fi Alliance
- Wireless LAN Association (WLANA)

Come proteggere una rete WLAN con Security Platform Solution



Condizioni preliminari

- Oltre ai normali requisiti hardware e software delle reti WLAN, è necessario che il client WLAN sia un PC Security Platform con Trusted Platform Module.
- È necessario registrare il certificato protetto da Security Platform.

[Le reti WLAN passo dopo passo](#)



©Infineon Technologies AG

Infineon Security Platform Solution

Le reti WLAN passo dopo passo

La descrizione seguente è dedicata alle reti LAN wireless (WLAN). Rispetto alla configurazione delle reti LAN cablate (IEEE 802.1X), l'unica operazione specifica per Security Platform (la selezione del provider del servizio di crittografia) è uguale a quella richiesta per le reti WLAN.

Istruzioni passo dopo passo per configurare e utilizzare una rete WLAN

Operazione	Eseguita da...
1. Richiesta del certificato di autenticazione del client	Tutti gli utenti di Security Platform che utilizzano la rete WLAN
2. Installazione del software WLAN	Un amministratore
3. Connessione al client WLAN	Tutti gli utenti di Security Platform che utilizzano la rete WLAN

Richiesta del certificato di autenticazione del client

Per proteggere la connessione alla rete WLAN, occorre un [certificato](#) approvato da un'Autorità di certificazione. Sia il client WLAN, sia il server RADIUS devono utilizzare un'Autorità di certificazione attendibile. Assicurarsi di utilizzare un modello di richiesta del certificato adatto per l'*autenticazione del client*.



Selezione del provider del servizio di crittografia

In sede di richiesta del certificato, è necessario scegliere il provider del servizio di crittografia (CSP) che verrà utilizzato dal certificato stesso.

- Se si vuole autenticare se stessi per questa funzione, selezionare un CSP utente (*Infineon TPM Cryptographic Provider* o *Infineon TPM RSA and AES Cryptographic Provider*).
- Per autenticare il proprio computer, selezionare la Piattaforma CSP (*Infineon TPM Platform Cryptographic Provider*). Per utilizzare questa piattaforma è necessario disporre dei privilegi di amministratore o essere un membro del gruppo di amministratori.

Installazione del software WLAN

Consultare la documentazione fornita dal rivenditore WLAN in merito alla configurazione generale della rete. In alcuni casi, il rivenditore fornisce anche un software client per configurare le connessioni WLAN.

Per la configurazione delle connessioni WLAN, è possibile utilizzare anche le **Connessioni di rete** del proprio sistema operativo.

- Configurare la connessione alla rete wireless sul client WLAN come descritto nella Guida in linea di Microsoft Windows (ricercare "rete senza fili").
- Assicurarsi di utilizzare le seguenti impostazioni nella scheda **Autenticazione**:
 - Selezionare **Abilita autenticazione IEEE 802.1x per questa rete**.
 - Alla voce **Tipo EAP**, selezionare **Smart Card o un altro certificato**.
 - Scegliere **Proprietà** e selezionare **Utilizza un certificato su questo computer**.
 - Se si desidera specificare il certificato ad ogni avvio della connessione wireless, deselezionare l'opzione **Utilizza selezione certificati semplice**.



Solo l'amministratore o un membro del gruppo di amministratori può configurare le impostazioni della scheda **Autenticazione**.

Connessione al client WLAN

Consultare la documentazione fornita dal rivenditore WLAN in merito alle connessioni di rete.

Per connettersi al client WLAN, è possibile utilizzare le **Connessioni di rete** del proprio sistema operativo.

- Connettersi al client WLAN come descritto nella Guida in linea di Microsoft Windows (ricercare "reti senza fili").
- Assicurarsi di utilizzare il certificato richiesto in precedenza (vedere "Richiesta del certificato di autenticazione del client").



Infineon Security Platform Solution

Domande frequenti e Risoluzione dei problemi

[Domande frequenti \(FAQ\)](#)

[Risoluzione dei problemi](#)

Technologies AG



Soluzione Infineon Security Platform

Domande frequenti (FAQ)

[Come si elimina un utente di Infineon Security Platform?](#)

[Esistono problemi di protezione quando si memorizzano i dati di ripristino di emergenza su un computer remoto?](#)

[È possibile disinstallare Infineon Security Platform Solution? Se sì, qual è la procedura?](#)

[Quali dati rimarranno nel sistema dopo la disinstallazione?](#)

[Non è possibile utilizzare un certificato registrato con Internet Explorer. Viene visualizzato un messaggio di errore.](#)

[La funzionalità di compressione delle cartelle del sistema operativo consente di archiviare i dati degli utenti. È possibile attivare EFS per le cartelle compresse? Le funzioni possono essere combinate tra loro?](#)

[Devo modificare il certificato assegnato a una cartella EFS. È possibile farlo senza rischi per i dati presenti nella cartella? Posso assegnare un certificato arbitrario alla cartella?](#)

[Come si prepara Infineon Security Platform per eseguire correttamente il backup di sistema? Quali file sono necessari per un ripristino corretto del software utilizzando i meccanismi del sistema?](#)

[Come configurare e gestire l'archivio del backup, in particolare con riferimento alle impostazioni dei criteri?](#)

[Come creare un file di archivio della chiave pubblica da un file token?](#)



I commenti sull'EFS sono rilevanti solo per le edizioni di Windows che supportano EFS.

Come si elimina un utente di Infineon Security Platform?

Esistono due modi diversi per eseguire l'eliminazione:

- **L'eliminazione completa di un account utente dal sistema operativo è un'operazione immediata supportata da Windows. Quando si elimina un account utente, è necessario selezionare la casella di controllo per l'eliminazione del profilo corrispondente. Con questa operazione, vengono rimossi dal sistema tutti i dati relativi all'account utente.**

- **Per eliminare soltanto le informazioni di un utente di Infineon Security Platform, lasciando inalterato l'account utente del sistema, occorre eliminare la cartella `%AppData%\Infineon\TPM Software 2.0`.**

Se si vogliono rimuovere tutti i dati di un utente di Security Platform, fare riferimento alle indicazioni riportate più avanti in questa sezione alla voce [Quali dati rimarranno nel sistema dopo la disinstallazione?](#) .



Se nel sistema esistono dati che sono stati crittografati con una chiave utente specifica di Infineon Security Platform, non sarà più possibile decrittografarli una volta eliminato l'account utente.



Esistono problemi di protezione quando si memorizzano i dati di ripristino di emergenza su un computer remoto?

No, nessun problema. I dati sono protetti dal token di ripristino di emergenza, che è a sua volta protetto da una password.



In [modalità server](#) non c'è problema di sicurezza, poiché il Recupero di Emergenza è gestito dal Trusted Computing Management Server.



È possibile disinstallare Infineon Security Platform Solution? Se sì, qual è la procedura?

È possibile disinstallare il software seguendo la normale procedura di rimozione dei programmi disponibile nel sistema operativo. Prima di iniziare la disinstallazione, occorre salvare tutti i dati dell'utente protetti da Security Platform. Senza tale operazione, non sarà più possibile accedere ai dati, una volta rimosso il software dal sistema. L'ultima operazione necessaria è la disattivazione di Trusted Platform Module nel BIOS del computer.

La nuova versione del software può essere installata sulla versione precedente, senza doverla rimuovere. In questo caso, non occorre eseguire il backup completo dei dati dell'utente.



Quali dati rimarranno nel sistema dopo la disinstallazione?

Quando il software Security Platform Solution viene disinstallato, alcune

informazioni restano archiviate nel sistema. In particolare, vengono mantenute le impostazioni e le credenziali della piattaforma e degli utenti, per permettere di reinstallare il software ripristinando lo stato precedente del sistema. In questo modo, una volta reinstallato Infineon Security Platform, saranno disponibili tutti i dati crittografati in precedenza.

Tuttavia, se tali informazioni non fossero più necessarie e si volesse ripulire il sistema, occorre eliminare i seguenti dati.

Archivi di backup: La posizione degli archivi di backup generati automaticamente viene specificata dagli amministratori del sistema. Si noti che l'archivio di backup generato automaticamente viene rappresentato nel file system da un file XML e da una cartella con lo stesso nome (ad esempio, file `SPSystemBackup.xml` nella cartella `SPSystemBackup`). Possono essere presenti anche archivi di backup creati in modalità manuale.

Token di ripristino di emergenza: la posizione di questi file viene specificata dal proprietario di Security Platform in fase di inizializzazione del software.

Archivio di ripristino di emergenza:

i) Windows 7 e Vista: `\\%ALLUSERSPROFILE%\Infineon\TPM Software 2.0\RestoreData\<Machine SID>\Users\<User SIDs>\SHTempRestore.xml`

ii) Windows XP Professional, Windows 2000 e altri sistemi operativi supportati: `\\%ALLUSERPROFILE%\<Application Data>\Infineon\TPM Software 2.0\RestoreData\<Machine SID>\Users\<User SIDs>\SHTempRestore.xml`

File dei dati e delle chiavi di sistema:

i) Windows 7 e Vista: `\\%ALLUSERSPROFILE%\Infineon\TPM Software 2.0\PlatformKeyData`
`IFXConfigSys.xml`
`IFXFeatureSys.xml`
`TCSps.xml`
`TPMCPSys.xml`

ii) Windows XP Professional, Windows 2000 e altri sistemi operativi supportati: `\\%ALLUSERPROFILE%\<Application Data>\Infineon\TPM Software 2.0\ PlatformKeyData`
`IFXConfigSys.xml`
`IFXFeatureSys.xml`
`TCSps.xml`

TPMCPSys.xml

File di backup locali replicati:

i) Windows 7 e Vista:

\\%ALLUSERSPROFILE%\Infineon\TPM Software 2.0\BackupData\<Machine SID>\System\SHBackupSys.xml

\\%ALLUSERSPROFILE%\Infineon\TPM Software 2.0\BackupData\<Machine SID>\Users\<User SIDs\SHBackup.xml

ii) Windows XP Professional, Windows 2000 e altri sistemi operativi supportati:

\\%ALLUSERPROFILE%\<Application Data>\Infineon\TPM Software 2.0\BackupData\<Machine SID>\System\SHBackupSys.xml

\\%ALLUSERPROFILE%\<Application Data>\Infineon\TPM Software 2.0\BackupData\<Machine SID>\Users\<User SIDs\SHBackup.xml

File delle chiavi utente: \\%AppData%\Infineon\TPM Software 2.0\UserKeyData\TSPps.xml

Contenitore di TPM Cryptographic Service Provider:

\\%AppData%\Infineon\TPM Software 2.0\UserKeyData\TPMcp.xml

File di TPM PKCS #11 Provider: \\%AppData%\Infineon\TPM Software 2.0\UserKeyData\TPMck.xml

File di configurazione dell'utente: \\%AppData%\Infineon\TPM Software 2.0\UserKeyData\
IFXConfig.xml
IFXFeature.xml

Chiavi del registro di sistema:

HKEY_LOCAL_MACHINE\SOFTWARE\Infineon\TPM Software

HKEY_CURRENT_USER\Software\Infineon\TPM software

Le chiavi del registro di **Personal Secure Drive** indicate di seguito devono essere eliminate manualmente quando si disinstalla la funzionalità di protezione Personal Secure Drive:

[HKEY_LOCAL_MACHINE\SOFTWARE\Infineon\TPM Software\PSD]

[HKEY_CURRENT_USER\SOFTWARE\Infineon\TPM Software\PSD]

Personal Secure Drive Directory: anche le directory indicate di seguito devono essere eliminate manualmente.

x:\Security Platform\Personal Secure Drive\System Data

dove x è l'unità di Personal Secure Drive. L'unità viene selezionata durante la creazione di Personal Secure Drive e può essere un qualsiasi disco rigido locale; in alternativa, l'unità può essere definita dai criteri utente locali di Personal Secure Drive.

Varie:

Certificati registrati basati su Trusted Platform Module

Attività di backup pianificate (es.: C:\WINDOWS\Tasks\Security Platform Backup Schedule)



Non è possibile utilizzare un certificato registrato con Internet Explorer. Viene visualizzato un messaggio di errore.

Il certificato è stato bloccato da Internet Explorer, anche se è già stato memorizzato nell'archivio certificati dell'utente. Chiudere Internet Explorer e quindi riaprirlo per sbloccare il certificato.



La funzionalità di compressione delle cartelle del sistema operativo consente di archiviare i dati degli utenti. È possibile attivare EFS per le cartelle compresse? Le funzioni possono essere combinate tra loro?

La combinazione non è possibile, dal momento che il sistema operativo non consente di proteggere con EFS le cartelle compresse. Innanzitutto, occorre disattivare la funzione di compressione. Successivamente, sarà possibile attivare la funzionalità EFS per la cartella selezionata.



Devo modificare il certificato assegnato a una cartella EFS. È possibile farlo senza rischi per i dati presenti nella cartella? Posso assegnare un certificato arbitrario alla cartella?

Normalmente, l'assegnazione di un certificato aggiuntivo a una cartella EFS non comporta alcun problema. La condizione fondamentale è che tutti i certificati siano controllati dal medesimo [Provider del servizio di crittografia](#). Se esiste un certificato assegnato in precedenza, i dati crittografati saranno ancora leggibili. Se si elimina dal sistema il certificato di protezione di un file posizionato in una cartella EFS, tutti i dati contenuti nel file andranno perduti.



Come si prepara Infineon Security Platform per eseguire correttamente il backup di sistema? Quali file sono necessari per un ripristino corretto del software utilizzando i meccanismi del sistema?

I file principali di Infineon Security Platform non contengono le applicazioni del software. Quindi, è possibile reinstallarlo dopo aver ripristinato un backup di sistema.

I dati specifici del software Infineon Security Platform Solution possono essere salvati utilizzando il [Backup guidato di Infineon Security Platform](#).

Durante il backup guidato, non vengono salvati i dati protetti, come file o messaggi di posta elettronica crittografati. Per farlo, è necessario utilizzare altri strumenti di backup. È consigliabile includere nella routine di backup generale dei dati anche l'archivio di backup ottenuto utilizzando la procedura guidata.

Se si sceglie di non utilizzare il backup guidato per creare una copia dei dati specifici del software Security Platform Solution, si raccomanda di eseguire il backup di tutti i dati elencati nella presente sezione, alla voce [Quali dati rimarranno nel sistema dopo la disinstallazione?](#).



- I backup automatici del sistema, configurati dall'amministratore di Security Platform comprendono anche i dati di ripristino di emergenza.
- In [modalità server](#) il Backup e il Ripristino sono gestiti dal Trusted Computing Management Server.



Come configurare e gestire l'archivio del backup, in particolare con riferimento alle impostazioni dei criteri?

È possibile configurare tutte le Security Platform aziendali perché utilizzino un archivio comune del backup impostando il [criterio](#) *posizione archivio del backup*.

Qualora debba essere creato un nuovo archivio del backup, è molto importante non importare i criteri prima dell'inizializzazione della Infineon Security Platform.

Successivamente, è necessario accedere all'amministrazione dei criteri e configurarli correttamente specificando la posizione dell'archivio di backup creato in precedenza. Il file configurato sarà infine utilizzato automaticamente dopo l'inizializzazione di tutte le altre Security Platform aziendali.

 Questa sezione non si applica in [modalità server](#) poiché il backup e il ripristino vengono gestite da Trusted Computing Management Server.



Come creare un file di archivio della chiave pubblica da un file token?

Nelle impostazioni dei criteri di gruppo è possibile specificare che la chiave pubblica di un Token di ripristino di emergenza o un Token di reimpostazione password esistente venga utilizzata da un file di archivio (vedere [Criteri di sistema](#) *Utilizza la chiave pubblica del token di ripristino di emergenza presente in archivio* e *Utilizza la chiave pubblica del token di reimpostazione password presente in archivio*). Per creare tale file di archivio da un file di token esistente, procedere come segue:

- Inizializzare completamente la piattaforma (incluso il ripristino di emergenza e la reimpostazione della password) con le impostazioni dei criteri predefinite sul primo sistema (ad es. un sistema di test).
Inizializzazione guidata rapida crea un file di token generico sia per il ripristino di emergenza sia per la reimpostazione della password.
Inizializzazione guidata di Security Platform crea un file di token per il ripristino di emergenza e uno per la reimpostazione della password.
- Eseguire lo script allegato di seguito sullo stesso sistema per creare il file di archivio della chiave pubblica necessario dal file di token corrispondente.
- Copiare il file di archivio della chiave pubblica in un percorso appropriato e abilitare i criteri indicati in precedenza.

Script **GeneratePubKeyArchive.vbs**:

```
'GeneratePubKeyArchive.vbs <percorso completo di Token.xml> <percorso completo di PubKeyArchive.xml>
```

'Il <percorso completo di Token.xml> può essere uno dei seguenti token:

' - SPPwdResetToken.xml

' - SPEmRecToken.xml

' - SPGenericToken.xml

'Il <percorso completo di PubKeyArchive.xml> è l'output, che contiene la chiave pubblica estratta dal token di input:

```

' - SPPwdResetTokenPubKeyArchive.xml
' - SPEmRecTokenPubKeyArchive.xml
' - SPGenericTokenPubKeyArchive.xml
'Per l'utilizzo con il criterio "Utilizza la chiave pubblica del token di ripristino di
emergenza presente in archivio":
' - SPEmRecTokenPubKeyArchive.xml
' - SPGenericTokenPubKeyArchive.xml
"Per l'utilizzo con il criterio "Utilizza la chiave pubblica del token di
reimpostazione password presente in archivio":
' - SPPwdResetTokenPubKeyArchive.xml
' - SPGenericTokenPubKeyArchive.xml
'Specificare il percorso completo, ad es.:
' GeneratePubKeyArchive.vbs "c:\tmp\SPGenericToken.xml"
"c:\tmp\SPGenericTokenPubKeyArchive.xml"
If WScript.Arguments.Count <> 2 Then
    WScript.Echo "Utilizzo: " & Wscript.ScriptName & " ""<percorso completo
di Token.xml>"" ""<percorso completo di PubKeyArchive.xml>""
    WScript.Quit
End If
Set MPBase = WScript.CreateObject("IfxSpMgtPrv.MgmtProvider")
Set MPToken = MPBase.GetInterface(10)
' CreationFlags: mantenere file esistente = 0, sovrascrivere file esistente = 1
CreationFlags = 0
ReservedFlag = 0
MPToken.CreatePublicKeyFile WScript.Arguments(0), WScript.Arguments(1),
CreationFlags, ReservedFlag
'gestione errori in caso di problema da aggiungere qui
WScript.Echo "Done"

```



Questa sezione non si applica in [modalità server](#) poiché il ripristino di emergenza e la reimpostazione della password vengono gestiti da Trusted Computing Management Server.



Soluzione Infineon Security Platform

Risoluzione dei problemi

La sezione seguente descrive le procedure da eseguire per risolvere i problemi più comuni che potrebbero verificarsi durante l'uso di Infineon Security Platform:

[È necessario configurare la piattaforma ma esiste già un proprietario di Trusted Platform Module.](#)

[Infineon Security Platform è stato configurato ma è cambiato il proprietario della piattaforma.](#)

[Quali aspetti occorre considerare per eseguire il ripristino di emergenza utilizzando l'Inizializzazione guidata di Infineon Security Platform?](#)

[È necessario ripristinare da un backup di sistema un documento archiviato in una cartella protetta con EFS. Non esiste nessun utente di Infineon Security Platform nel sistema di destinazione. Come risolvere questa situazione?](#)

[Un'applicazione di uso comune crea dei file temporanei al di fuori delle normali cartelle Temp. In genere, queste cartelle non vengono protette da EFS. È possibile proteggere questi file temporanei, considerando il fatto che restano sul disco rigido anche dopo aver chiuso l'applicazione?](#)

[Quando un utente di Infineon Security Platform accede per la prima volta a una cartella EFS, viene richiesta la password della chiave utente di base. Se si chiude la finestra di dialogo senza specificare la password ed è configurato un agente di ripristino, si può comunque accedere ai dati contenuti nella cartella. Si tratta di un errore del sistema?](#)



I commenti sull'EFS non sono rilevanti per le edizioni Home di Windows poiché l'EFS non è supportato in questi sistemi.

È necessario configurare la piattaforma ma esiste già un proprietario di Trusted Platform Module.

In questi casi, per l'inizializzazione della piattaforma, si utilizza il proprietario attuale di Security Platform. Richiede la conoscenza della Password Proprietario esistente o l'accesso al corrispondente File di Backup della Password Proprietario.

Questa è una situazione tipica degli ambienti multisistema, in cui sullo stesso computer esistono più sistemi operativi. Il Proprietario di Infineon Security

Platform ("Chiave Radice di Archiviazione", SRK) non può abbandonare Trusted Platform Module e non può essere introdotto dall'esterno perciò l'operazione di importazione non è possibile.

Quando le chiavi utente di base sono già presenti, occorre adottare approcci diversi durante l'[Inizializzazione di Security Platform](#).

Se non è stata creata nessuna chiave utente di base in Security Platform, è possibile generare un nuovo archivio di backup (contenente i dati di ripristino di emergenza). In questo modo, Infineon Security Platform è pronto per le operazioni successive.

Se le chiavi utente di base sono già presenti ed è stato configurato un archivio di backup (con i dati di ripristino di emergenza), è importante non sovrascriverlo durante l'inizializzazione di Security Platform.



In [modalità server](#), è necessario inizialmente azzerare il proprietario, se già presente, prima di effettuare la connessione del sistema al Trust Domain. La Security Platform sarà successivamente registrata nel Trust Domain (vedere [Registrazione Piattaforma](#)).



Infineon Security Platform è stato configurato ma è cambiato il proprietario della piattaforma.

Se Security Platform è stato impostato con il ripristino di emergenza, è possibile riattivare le credenziali della piattaforma utilizzando il [Supporto del ripristino di emergenza](#) di Soluzione Security Platform.



In [modalità server](#), il Trusted Platform Module non dovrebbe avere un proprietario prima che venga eseguita la connessione del sistema al Trust Domain, non deve cioè essere già stata eseguita l'inizializzazione (né mediante il TPM Professional Package Infineon in modalità autonoma né dal Server Trusted Domain in modalità server o da qualsiasi altro software quale il *Trusted Platform Module (TPM) Management di Windows Vista*).



Quali aspetti occorre considerare per eseguire il ripristino di emergenza utilizzando l'Inizializzazione guidata di Infineon Security Platform?

Il ripristino di emergenza del sistema può essere seguito nel caso in cui Trusted

Platform Module sia stato sostituito o reimpostato e sia disponibile un'immagine di backup che consenta di ripristinare i dati. I dati specifici degli utenti di Security Platform e i dati di ripristino di emergenza vengono salvati durante il backup automatico del sistema.

L'amministratore di Infineon Security Platform deve poter accedere all'archivio di backup e al token di ripristino di emergenza che viene generato durante l'installazione del sistema; inoltre, l'amministratore deve conoscere la password che protegge il token.

Per ripristinare il sistema, l'amministratore di Infineon Security Platform deve eseguire il [Backup guidato di Infineon Security Platform](#).

Se il ripristino viene eseguito su un computer il cui nome è stato modificato, è necessario conoscere il nome precedente o l'ID della piattaforma (SID). È possibile che l'archivio di backup contenga i dati di ripristino di più computer. In questi casi, occorre selezionare il computer che si desidera ripristinare dall'archivio di backup.



In [modalità server](#) il Recupero di Emergenza è gestito dal Trusted Computing Management Server.



È necessario ripristinare da un backup di sistema un documento archiviato in una cartella protetta con EFS. Non esiste nessun utente di Infineon Security Platform nel sistema di destinazione. Come risolvere questa situazione?

Se la chiave utente di base non è più disponibile e non esiste un certificato per l'agente di ripristino, il documento è irrimediabilmente perduto.

In caso contrario, la prima operazione da eseguire è il ripristino del file dal backup. Il ripristino viene eseguito senza alterare in alcun modo le proprietà di protezione del file. Successivamente, occorre utilizzare il certificato di ripristino per abilitare un agente di ripristino a decrittografare il file.



Un'applicazione di uso comune crea dei file temporanei al di fuori delle normali cartelle Temp. In genere, queste cartelle non vengono protette da EFS. È possibile proteggere questi file temporanei, considerando il fatto che restano sul disco rigido anche dopo aver chiuso l'applicazione?

Questo è un problema comune a molte applicazioni. In base al tipo di programma, è possibile che vengano creati dei file temporanei al di fuori delle cartelle EFS configurate. Se la cartella Temp utilizzata non è la tipica cartella %AppData% presente nel profilo utente (di solito si chiama "Application Data"), si tratta di una caratteristica specifica dell'applicazione in uso e quindi non è possibile indicare una soluzione vera e propria a questo problema. In generale, una volta individuata la posizione dei file temporanei (dopo aver verificato che l'applicazione non supporta la configurazione delle cartelle), è possibile impostare la protezione EFS per la cartella corrispondente. Se questa soluzione non è praticabile, si consiglia di eliminare i file alla chiusura dell'applicazione.

Ulteriori informazioni sulla risoluzione dei problemi di Encrypting File System sono disponibili sul sito Microsoft MSDN (Microsoft Developer Network).



Quando un utente di Infineon Security Platform accede per la prima volta a una cartella EFS, viene richiesta la password della chiave utente di base. Se si chiude la finestra di dialogo senza specificare la password ed è configurato un agente di ripristino, si può comunque accedere ai dati contenuti nella cartella. Si tratta di un errore del sistema?

Questo comportamento è corretto, considerando la struttura dell'agente di ripristino. Infatti, se è stato configurato un certificato di ripristino per una cartella EFS, tale certificato verrà utilizzato dall'agente di ripristino la prima volta che si accede a quella cartella. Le soluzioni possono essere diverse, in funzione del fatto che il computer appartenga o meno a un dominio.

Il computer è parte di un dominio: in questo caso, l'amministratore dovrà assegnare il certificato. Se non è stato assegnato nessun certificato a un utente di Infineon Security Platform, il comportamento descritto in precedenza non si verifica.

Il computer utilizza Windows 2000 e non è parte di un dominio: Un modo possibile è accertarsi che la chiave privata dell'agente recupero dati non sia disponibile per i normali utenti Security Platform.

Il computer utilizza un altro sistema operativo supportato e non è parte di un dominio: in questo caso, non esiste un certificato di ripristino e quindi il comportamento descritto non si verifica.





©Infineon Technologies AG

Infineon Security Platform Solution - Visualizzatore certificati e Selezione certificati

Visualizzatore certificati e Selezione certificati di Infineon Security Platform

Queste utilità di Infineon Security Platform vengono utilizzate per la gestione dei certificati.

Differenze rispetto allo snap-in Certificati di Microsoft Management Console

Rispetto allo [snap-in Certificati di Microsoft Management Console](#), le utilità Visualizzatore certificati e Selezione certificati consentono di collegare i certificati a Security Platform.

- Le chiavi private possono essere protette mediante Trusted Platform Module.
- È possibile selezionare i certificati da utilizzare per la crittografia di file e cartelle con Encrypting File System (EFS) e Personal Secure Drive (PSD).

Differenze tra Visualizzatore certificati e Selezione certificati

Entrambe le utilità dispongono di funzioni comuni per la gestione dei certificati; ad esempio, consentono di visualizzare l'elenco dei certificati, di accedere ad informazioni dettagliate sulle chiavi private e sui certificati e di importare i certificati PKCS #12 in Security Platform.

Le differenze tra Visualizzatore certificati e Selezione certificati sono indicate di seguito.

Visualizzatore certificati. è uno strumento specifico di Security Platform Solution per la gestione dei certificati; consente, ad esempio, di proteggere le chiavi private mediante Trusted Platform Module.

Selezione certificati. lo scopo di questa utilità è quello di selezionare un certificato per la crittografia di file e cartelle mediante EFS o PSD; è possibile creare certificati autofirmati o richiedere un certificato a un'Autorità di certificazione (CA).

Come registrare e selezionare i certificati

Per registrare e selezionare i **certificati EFS** con **Selezione certificati**, procedere come indicato di seguito.

- Scegliere **Richiedi...** per richiedere un certificato a un'Autorità di certificazione (CA) esterna.
- Scegliere **Crea** per richiedere un certificato a un'Autorità di certificazione all'interno del dominio oppure creare un certificato autofirmato.
- Scegliere **Seleziona** per selezionare il certificato da utilizzare per EFS o PSD.

I comandi **Richiedi...** e **Crea** dipendono dal criterio [Registrazione e tipo di certificato EFS](#).

I certificati EFS vengono utilizzati non solo per Encrypting File System, ma anche per Personal Secure Drive.

La registrazione di **certificati per usi diversi** può essere eseguita mediante l'Inizializzazione utenti guidata, alla pagina [Richiesta certificato](#).

Questa operazione dipende dal criterio [URL per la registrazione dei certificati durante la procedura guidata](#).

[Ulteriori informazioni sulla registrazione dei certificati](#)

Elementi delle finestre di dialogo

Elementi comuni	Spiegazione
<input type="checkbox"/> <i>Mostra certificati e scopi designati</i>	<p>Selezionare uno scopo designato per filtrare l'elenco dei certificati.</p> <p>Ad esempio, è possibile visualizzare soltanto i certificati di protezione della posta elettronica oppure tutti i certificati.</p> <p> In Selezione certificati, questa opzione è impostata su <i>Encrypting File System</i> ed è disabilitata. Si noti che l'impostazione viene utilizzata sia per EFS, sia per PSD.</p>
<input type="checkbox"/> Elenco dei certificati	<p>L'elenco visualizza i certificati presenti sul PC che soddisfano i criteri impostati (ovvero, <i>gli scopi designati</i>).</p> <p> Questo simbolo contraddistingue i certificati le cui chiavi private sono accessibili.</p> <p> Questo simbolo contraddistingue i certificati le cui chiavi private non sono più accessibili.</p> <p> Questo simbolo viene visualizzato quando non è noto se la chiave privata del certificato sia accessibile o meno, ad esempio, quando la chiave è memorizzata su una smart card. In questo caso, occorre inserire la smart card e quindi selezionare il certificato desiderato.</p> <p> Questo simbolo contraddistingue i certificati che non dispongono della chiave privata corrispondente.</p> <p>I certificati EFS o PSD attualmente in uso vengono visualizzati in grassetto in Selezione certificati.</p>
<input type="checkbox"/> <i>Visualizza...</i>	Cliccare su questo pulsante per visualizzare informazioni dettagliate sul certificato selezionato.
<input type="checkbox"/> <i>Importa...</i>	Cliccare su questo pulsante per importare un certificato PKCS #12. Viene avviata l'Importazione

	<p>guidata PKCS #12 di Security Platform. La chiave privata del certificato verrà protetta da Trusted Platform Module.</p> <p> L'abilitazione di questo pulsante dipende dal criterio Consenti agli utenti di importare le chiavi.</p>
<input type="checkbox"/> <i>Chiave privata</i>	Se il certificato selezionato contiene una chiave privata, vengono visualizzate le proprietà della chiave.
Elementi aggiuntivi della finestra di dialogo Visualizzatore certificati	Spiegazione
<input checked="" type="checkbox"/> <i>Mostra certificati di altri provider</i>	Selezionare questa casella di controllo per visualizzare i certificati di altri provider, oltre a quelli forniti da <i>Infineon TPM Cryptographic Provider</i> .
<input checked="" type="checkbox"/> <i>Mostra anche i certificati privati PKCS #11</i>	Se si seleziona questa opzione, sarà necessario eseguire l'autenticazione in Security Platform ogni volta che si accedere a un certificato privato PKCS #11 dal Visualizzatore certificati.
<input type="checkbox"/> <i>Proteggi</i>	<p>Cliccare su questo pulsante per proteggere la chiave privata del certificato selezionato utilizzando Trusted Platform Module.</p> <p> La protezione di una chiave privata non può essere annullata. Se si desidera ripristinare una versione non protetta della chiave, occorre esportare il certificato utilizzando la finestra dei certificati di Microsoft.</p>
<input type="checkbox"/> <i>Elimina</i>	<p>Cliccare su questo pulsante per eliminare dal proprio PC il certificato selezionato e la chiave privata corrispondente.</p> <p>Il pulsante è abilitato unicamente se il certificato selezionato non è utilizzato per EFS o PSD e la chiave privata corrispondente è protetta da Trusted Platform Module.</p>

	 Verificare se il certificato da eliminare sia attualmente in uso. Una volta rimosso, non sarà più possibile utilizzarlo.
<input type="checkbox"/> <i>Chiudi</i>	Cliccare su questo pulsante per chiudere il Visualizzatore certificati.
Elementi aggiuntivi della finestra di dialogo Selezione certificati	Spiegazione
<input type="checkbox"/> <i>Richiedi...</i>	<p>Cliccare su questo pulsante per richiedere un certificato a un'Autorità di certificazione (CA). Verrà visualizzata la finestra di dialogo per la richiesta dei certificati. Seguire le istruzioni visualizzate per completare correttamente la procedura. Al termine dell'operazione, chiudere la finestra di richiesta dei certificati utilizzando il pulsante Chiudi situato nella barra del titolo.</p> <p> Il pulsante Richiedi... è disabilitato se l'indirizzo Web per la richiesta dei certificati non è stato definito durante l'impostazione del criterio Registrazione e tipo di certificato EFS.</p>
<input type="checkbox"/> <i>Crea</i>	<p>Cliccare su questo pulsante per ottenere un certificato di dominio o creare un certificato autofirmato. Il software Security Platform Solution tenterà di ottenere un certificato da un'Autorità di certificazione Microsoft (CA) all'interno del dominio. Se non è disponibile nessuna CA di dominio, verrà creato un certificato autofirmato.</p> <p> Nota:</p> <ul style="list-style-type: none"> • A seconda delle impostazioni della CA di dominio, è possibile che il certificato richiesto non venga concesso direttamente. Possibili cause: CA utilizzata in modalità manuale;

	<p>consegna del certificato a mezzo posta. In questo caso, contattare l'Autorità di certificazione in merito alla disponibilità del certificato richiesto.</p> <ul style="list-style-type: none"> • A seconda dell'impostazione attuale del criterio Registrazione e tipo di certificato EFS, la creazione di certificati autofirmati potrebbe non essere consentita. <p>Se non è disponibile una CA di dominio e i certificati autofirmati non sono consentiti dai criteri, non sarà possibile ottenere il certificato mediante il comando <i>Crea</i>.</p> <ul style="list-style-type: none"> • La validità dei certificati EFS auto-dichiarati può essere definita durante l'impostazione del criterio Periodo di validità dei certificati auto-dichiarati EFS.
<input type="checkbox"/> <i>Seleziona</i>	<p>Cliccare su questo pulsante per poter utilizzare con EFS o PSD il certificato selezionato nella finestra dei certificati. L'utilità Selezione certificati verrà chiusa e si ritornerà alla pagina "Certificato di crittografia" dell'Inizializzazione utenti guidata.</p>
<input type="checkbox"/> <i>Annulla</i>	<p>Cliccare su questo pulsante per chiudere la finestra di Selezione Certificati e ritornare alla pagina "Certificato di crittografia" dell'Inizializzazione utenti guidata senza modificare il certificato EFS o PSD.</p>

Avvio dell'applicazione

Visualizzatore certificati. Per avviare l'utilità Visualizzatore certificati di Security Platform, occorre accedere al Tool di configurazione ([Tool di configurazione - Impostazioni utente - Gestione...](#)).

Selezione certificati. Per avviare l'utilità Selezione certificati di Security Platform, cliccare su **Seleziona...** durante la configurazione della crittografia di file e cartelle con EFS o PSD ([Inizializzazione utenti guidata - Certificato di crittografia](#)).



©Infineon Technologies AG

Infineon Security Platform Solution - Reimpostazione guidata password

Ignora dispositivo di autenticazione

Questa pagina della procedura guidata consente di non aggiornare la configurazione del dispositivo di autenticazione con la nuova frase password utente di base. Ciò può essere utile quando il dispositivo non è in funzione o non è al momento disponibile.



Disponibilità della pagina: Questa pagina è disponibile soltanto se si è scelto di configurare l'autenticazione avanzata.

Elementi della pagina	Spiegazione
<input checked="" type="checkbox"/> <i>Ignora dispositivo di autenticazione</i>	Non aggiornare la configurazione del dispositivo di autenticazione con la nuova frase password utente di base. In questo caso, sarà necessario aggiornare le impostazioni del dispositivo di autenticazione non appena questo viene riattivato o reso nuovamente disponibile. L'operazione può essere eseguita tramite il Tool di configurazione: Selezionare Tool di configurazione - Impostazioni utente - Configura...

