

Per informazioni aggiornate sulle procedure di trattamento dei dati di Microsoft, leggi [l'Informativa sulla privacy di Microsoft](#). In questo documento puoi scoprire anche gli strumenti più recenti forniti per l'accesso e il controllo dei dati e come contattare Microsoft per richiedere informazioni sulla privacy.

Informativa sulla privacy di Windows 8 e Windows Server 2012

Elementi di rilievo

Informativa Supplemento sulle funzionalità Supplemento sul server

In questa pagina

Ultimo aggiornamento: **Agosto 2012**

Le informazioni dell'utente

Questi elementi di rilievo dell'informativa completa [Informativa sulla privacy di Windows 8 e Windows Server 2012](#) ("Informativa sulla Privacy di Windows") illustra, in generale, alcune procedure di raccolta e di utilizzo dei dati da parte di Windows 8 e Windows Server 2012 ("Windows"). Si concentrano sulle funzioni di comunicazione con Internet e non intendono costituire una descrizione esaustiva. Non si applicano ad altri siti Microsoft online o offline, prodotti o servizi.

Le tue selezioni

Uso delle informazioni

Come contattare Microsoft

Questa informativa sulla privacy presenta quattro sezioni:

- Elementi di rilievo (in questa pagina)
- Informativa, ovvero l'informativa sulla Privacy completa di Windows che include i collegamenti per le funzionalità di Windows che, a loro volta, hanno informative autonome
- Supplemento sulle funzionalità, che descrive le funzionalità che

hanno un impatto sulla privacy in Windows 8 e Windows Server 2012

- Supplemento sul server, che descrive le funzionalità aggiuntive che hanno un impatto sulla privacy in Windows Server 2012

Per ulteriori informazioni su come proteggere il computer, le informazioni personali e la tua famiglia online, visita il Centro sicurezza e protezione.

Le informazioni dell'utente

- Alcune funzionalità di Windows potrebbero chiederti l'autorizzazione per raccogliere o utilizzare informazioni dal computer, incluse quelle personali. Queste informazioni vengono utilizzate da Windows come descritto nella versione completa [Informativa sulla privacy di Windows](#), e anche in [Supplemento sulle funzionalità](#) e [Supplemento sul server](#).
- Con la tua autorizzazione, alcune funzionalità di Windows possono condividere informazioni personali tramite Internet.
- Se scegli di registrare il software, ti verrà richiesto di fornire informazioni personali.
- Windows richiede l'attivazione per ridurre la pirateria software e per aiutare a garantire che gli utenti ricevano la qualità software auspicata. L'attivazione invia alcune informazioni sul PC a Microsoft.
- È possibile scegliere di accedere a Windows con [Account Microsoft](#), che ti consente di sincronizzare le impostazioni di Windows e accedere automaticamente alle app e ai siti Web. Quando crei un account Microsoft, ti verrà richiesto di fornire alcune informazioni personali.
- [Ulteriori dettagli](#)

[Torna all'inizio](#)

Le tue selezioni

- Windows ti offre diversi modi per controllare come le funzionalità di Windows trasferiscano informazioni tramite Internet. Ulteriori informazioni su come controllare queste funzionalità sono consultabili nel Supplemento sulle funzionalità e nel Supplemento sul server.
- Per migliorare l'esperienza, alcune funzionalità, che utilizzano Internet, sono abilitate per impostazione predefinita.
- [Ulteriori dettagli](#)

[Torna all'inizio](#)

Uso delle informazioni

- Utilizziamo le informazioni raccolte per abilitare le funzionalità usate o fornire i servizi richiesti. Le usiamo anche per migliorare i prodotti e servizi. Per garantire l'erogazione dei nostri servizi, occasionalmente forniamo informazioni ad altre aziende che lavorano per nostro conto. L'accesso viene consentito solo alle aziende che hanno un'esigenza aziendale di utilizzare le informazioni. A tali aziende è stato richiesto di mantenere le informazioni riservate ed è stato vietato di utilizzarle per altri scopi.
- [Ulteriori dettagli](#)

[Torna all'inizio](#)

Come contattare Microsoft

Per ulteriori informazioni sulle procedure di tutela della privacy, accedi a [Informativa sulla privacy di Windows](#). Oppure, è possibile scrivere utilizzando [Modulo Web](#).

[Torna all'inizio](#)

Per informazioni aggiornate sulle procedure di trattamento dei dati di Microsoft, leggi l'[Informativa sulla privacy di Microsoft](#). In questo documento puoi scoprire anche gli strumenti più recenti forniti per l'accesso e il controllo dei dati e come contattare Microsoft per richiedere informazioni sulla privacy.

Informativa sulla privacy di Windows 8 e Windows Server 2012

Elementi di rilievo **Informativa** [Supplemento sulle funzionalità](#) [Supplemento sul server](#)

In questa pagina	Questa informativa si riferisce a Windows 8 e Windows Server 2012 ("Windows"). Determinati componenti di Windows dispongono di informative sulla privacy specifiche, elencate sul lato destro di questa pagina. Inoltre, sono elencate le informative sulla privacy per software e servizi correlati a Windows e per le versioni precedenti.
Raccolta e utilizzo delle informazioni relative all'utente	
Raccolta e utilizzo delle informazioni relative al computer dell'utente	Per informazioni sulle funzionalità specifiche, fare riferimento a Supplemento sulle funzionalità e Supplemento sul server .
Protezione delle informazioni personali	L'informativa è incentrata sulle funzionalità di comunicazione con Internet e non deve essere considerata un elenco esaustivo.
Modifiche apportate alla presente informativa sulla	Raccolta e utilizzo delle informazioni relative all'utente
	Le informazioni personali raccolte saranno utilizzate da Microsoft e dalle sue collegate e consociate per attivare le funzionalità utilizzate dall'utente ed erogare i servizi o per concludere le transazioni richieste o autorizzate dall'utente. Inoltre, le informazioni potranno essere utilizzate per analizzare e migliorare i prodotti e i servizi

privacy	Microsoft.
Ulteriori informazioni	Ad eccezione di quanto descritto nella presente informativa, le informazioni personali fornite non verranno divulgate a terze parti senza l'autorizzazione dell'utente. Occasionalmente Microsoft incarica altre società di offrire servizi limitati per proprio conto, ad esempio per l'esecuzione di analisi statistiche dei servizi offerti. A tali società vengono fornite esclusivamente le informazioni personali necessarie per svolgere il servizio e viene loro imposto di rispettare la riservatezza delle informazioni, che non possono essere utilizzate per scopi diversi da quelli concordati.
Informative sulla privacy aggiuntive	
Internet Explorer	Microsoft può accedere a informazioni personali sull'utente o divulgarle senza previa notifica, ivi compreso il contenuto delle comunicazioni, ai seguenti fini: (a) garantire la conformità alla legge o rispondere a richieste legittime o procedimenti legali; (b) proteggere i diritti o la proprietà di Microsoft o dei suoi clienti, ivi inclusa l'esecuzione forzata dei contratti o dei regolamenti che disciplinano l'utilizzo del software; ovvero (c) agire in buona fede nella convinzione che l'accesso o la divulgazione siano necessari per proteggere la sicurezza personale dei dipendenti Microsoft, dei clienti o del pubblico.
Servizio Segnalazione errori Microsoft	
Microsoft Online	
Strumento di rimozione malware Microsoft Windows	
Servizi di aggiornamento Windows Media Center	
Windows Media Player	
Windows 7	Le informazioni raccolte o inviate a Microsoft da Windows 8 possono essere archiviate ed elaborate negli Stati Uniti o in qualsiasi altro paese in cui abbiano sede Microsoft o le sue affiliate, ausiliarie o provider di servizi. Microsoft si attiene alle direttive "Safe Harbor" secondo quanto stabilito dal Ministero del Commercio statunitense relativamente alla raccolta, all'utilizzo e alla conservazione dei dati dell'Unione Europea, dello Spazio Economico Europeo e della Svizzera.

[Torna all'inizio](#)

Raccolta e utilizzo delle informazioni relative al computer dell'utente

Quando si utilizzano software con funzionalità che sfruttano Internet, vengono inviate delle informazioni sul computer ("informazioni standard sul computer") ai siti visitati ed ai servizi online utilizzati. Normalmente le informazioni standard sul computer includono dati quali l'indirizzo IP, la versione del sistema operativo, la versione del

browser e le impostazioni internazionali e di lingua dell'utente. Talvolta, le informazioni possono includere anche l'ID hardware, che indica produttore, nome e versione del dispositivo. Se una determinata funzionalità o un servizio invia informazioni a Microsoft, verranno inviate anche le informazioni standard sul computer.

I dettagli sulla privacy per ogni funzionalità di Windows 8 in [Supplemento sulle funzionalità](#) e [Supplemento sul server](#), oltre alle funzionalità elencate sul lato di questa pagina, descrivono quali informazioni aggiuntive vengono raccolte e le modalità del loro utilizzo.

Gli amministratori possono utilizzare i Criteri di gruppo per modificare molte delle impostazioni per le funzionalità descritte di seguito. Per ulteriori informazioni, vedere [questo white paper per gli amministratori](#).

[Torna all'inizio](#)

Protezione delle informazioni personali

Microsoft è impegnata a proteggere incondizionatamente la riservatezza delle informazioni personali. Utilizza un'ampia gamma di tecnologie e procedure di protezione per impedire l'accesso, l'uso e la divulgazione non autorizzati dei dati. Le informazioni fornite verranno archiviate, ad esempio, in sistemi di computer ad accesso limitato, collocati in ambienti controllati. Quando si trasmettono informazioni altamente riservate (ad esempio il numero di una carta di credito o di una password) su Internet, queste ultime vengono protette mediante la crittografia, come il protocollo Secure Socket Layer (SSL).

[Torna all'inizio](#)

Modifiche apportate alla presente informativa sulla privacy

Microsoft potrebbe aggiornare occasionalmente questa Informativa sulla privacy per adeguarla agli aggiornamenti applicati ai prodotti, ai servizi e ai commenti forniti dai clienti. In caso di modifiche alla presente informativa, verrà modificata la data di "ultimo aggiornamento" nella parte superiore di questo documento. In caso

di modifiche sostanziali all'informativa o qualora Microsoft decida di modificare le modalità di utilizzo delle informazioni personali, tali modifiche saranno pubblicate in maniera visibile prima dell'effettiva entrata in vigore o notificate direttamente all'utente. È consigliabile rileggere periodicamente l'informativa per essere sempre aggiornati sulle modalità di protezione delle informazioni adottate da Microsoft.

[Torna all'inizio](#)

Ulteriori informazioni

Microsoft è lieta di ricevere commenti in merito alla presente informativa sulla privacy. Per informazioni relative alla presente informativa sulla privacy o se si ritiene che Microsoft non l'abbia rispettata, è possibile contattarci utilizzando [modulo Web](#).

Microsoft Privacy
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052
Stati Uniti

[Torna all'inizio](#)

Per informazioni aggiornate sulle procedure di trattamento dei dati di Microsoft, leggi [l'Informativa sulla privacy di Microsoft](#). In questo documento puoi scoprire anche gli strumenti più recenti forniti per l'accesso e il controllo dei dati e come contattare Microsoft per richiedere informazioni sulla privacy.

Informativa sulla privacy di Windows 8 e Windows Server 2012

Elementi di rilievo Informativa **Supplemento sulle funzionalità** Supplemento sul server

In questa pagina

Ultimo aggiornamento: ottobre 2012

[Attivazione](#)

Questa pagina costituisce un supplemento all' [Informativa sulla privacy di Windows 8 e Windows Server 2012](#) ("Informativa sulla privacy di Windows"), che contiene quattro sezioni:

[Client di Active](#)

[Directory Active](#)

[Directory Rights](#)

[Management Services \(AD RMS\)](#)

[Controllo](#)

[Crittografia unità](#)

[BitLocker](#)

[Individuazione e configurazione di dispositivi](#)

[DirectAccess](#)

[Aggiornamento](#)

- [In primo piano](#)
- Informativa, ovvero l' [Informativa sulla privacy di Windows completa](#) , che include collegamenti alle informative sulla privacy relative a funzionalità di Windows che dispongono di informative specifiche
- [Supplemento sulle funzionalità](#) (questo documento), che descrive le funzionalità che hanno impatto sulla privacy in Windows 8 e Windows Server 2012
- [Supplemento sul server](#), che descrive le funzionalità aggiuntive che hanno impatto sulla privacy in Windows Server 2012

Per comprendere le procedure di raccolta e utilizzo dei dati relative a

dinamico	una particolare funzionalità o un particolare servizio di Windows, è consigliabile leggere sia l'Informativa sulla privacy completa sia il supplemento o l'informativa specifica.
Centro accessibilità	
Visualizzatore eventi	
Family Safety	Attivazione
Fax	Scopo della funzionalità
Personalizzazione riconoscimento grafia: apprendimento automatico	L'attivazione limita i rischi di contraffazione del software per garantire ai clienti Microsoft la qualità del software che si aspettano. Una volta attivato il software, un prodotto specifico viene associato al PC (o all'hardware) in cui è installato il software. Questa associazione impedisce l'utilizzo del codice Product Key per attivare la stessa copia del software su più PC. Alcune modifiche ai componenti o al software del PC possono richiedere la riattivazione di Windows. Alcune modifiche all'hardware o al software del PC possono richiedere la riattivazione di Windows. La funzionalità di attivazione può rilevare e disabilitare exploit di attivazione, ovvero software che cerca di eludere o evitare l'attivazione del software. In presenza di un exploit di attivazione, un fornitore di software o hardware potrebbe aver manomesso software Microsoft originale per creare copie contraffatte del software. Gli exploit di attivazione potrebbero interferire con il normale funzionamento del sistema.
Gruppo Home	
Input Method Editor (IME)	
Analisi utilizzo	
Installazione	
Stampa Internet	
Preferenze lingua	
Servizi di posizione	
Nome e immagine dell'account	Informazioni raccolte, elaborate o trasmesse
Presenza in rete	Durante l'attivazione vengono inviate a Microsoft le informazioni seguenti:
Notifiche, app della schermata di blocco e aggiornamenti dei riquadri	<ul style="list-style-type: none"> • Il codice prodotto Microsoft, ovvero un codice di cinque cifre che identifica il prodotto Windows da attivare. • Un ID di canale o un codice di sito che identifica il modo in cui è stato ottenuto in origine il prodotto Windows. Un ID di canale o un codice di sito, ad esempio, specifica se il prodotto è stato acquistato in origine da un negozio al dettaglio, ottenuto come copia di valutazione, ottenuto tramite un programma di contratti multilicenza o preinstallato da un produttore di PC.
Ordinazione stampe	
Risoluzione problemi compatibilità programmi	
Proprietà	<ul style="list-style-type: none"> • La data di installazione e l'esito dell'installazione.
Prossimità	<ul style="list-style-type: none"> • Informazioni che confermano che il codice Product Key di

Connessioni di Accesso remoto	Windows non è stato alterato.
Connessione RemoteApp e desktop	<ul style="list-style-type: none"> • Marca e modello del PC. • Informazioni sulla versione per sistema operativo e software.
Connessione Desktop remoto	<ul style="list-style-type: none"> • Impostazioni internazionali e della lingua. • Un numero univoco denominato GUID (Globally Unique Identifier) assegnato al PC.
Accesso con un account Microsoft	<ul style="list-style-type: none"> • Codice Product Key (con hash) e ID prodotto.
Sincronizzazione delle impostazioni	<ul style="list-style-type: none"> • Nome BIOS, numero di revisione e data di revisione.
Teredo Technology	<ul style="list-style-type: none"> • Numero di serie del volume dell'unità disco rigido (con hash).
Servizi Trusted Platform Module (TPM)	<ul style="list-style-type: none"> • Risultato del controllo di attivazione. Sono inclusi codici di errore e le informazioni seguenti su eventuali exploit di attivazione e su software correlato dannoso o non autorizzato trovato o disabilitato: <ul style="list-style-type: none"> • Identificatore dell'exploit di attivazione. • Stato corrente dell'exploit di attivazione, ad esempio pulito o in quarantena. • Identificazione del produttore del PC. • Nome del file e hash dell'exploit di attivazione, nonché un hash dei componenti software correlati che potrebbe indicare la presenza di un exploit di attivazione.
Aggiornamento dei certificati radice	
Servizi di aggiornamento	
Analisi utilizzo software Windows	
Windows Defender	
Segnalazione errori Windows	
Associazione file di Windows	<ul style="list-style-type: none"> • Nome e hash del contenuto del file delle istruzioni di avvio del PC. Se la licenza di Windows fa parte di un abbonamento, vengono inviate anche informazioni relative all'abbonamento. Vengono inoltre inviate informazioni standard sul computer, ma l'indirizzo IP del PC viene mantenuto solo temporaneamente.
Guida di Windows	
Assistenza remota	
Windows Search	
Windows Share	
Windows SmartScreen	
Riconoscimento vocale	

Utilizzo delle informazioni

Le informazioni raccolte vengono utilizzate da Microsoft per verificare che la copia del software in uso sia coperta da una regolare licenza. Microsoft non utilizza tali informazioni per contattare l'utente.

[Windows](#)

[Windows Store](#)

[Servizio Ora di Windows](#)

[Risoluzione dei problemi Windows](#)

Scelta e controllo

L'attivazione è necessaria e avviene automaticamente durante la configurazione di Windows. Se non si dispone di una licenza valida per il software, non sarà possibile attivare Windows.

[Inizio pagina](#)

Client di Active Directory Active Directory Rights Management Services (AD RMS)

Scopo della funzionalità

Il client di Active Directory Rights Management Services (AD RMS) è una tecnologia di protezione delle informazioni che interagisce con le applicazioni con supporto AD RMS per contribuire a proteggere le informazioni digitali dall'utilizzo non autorizzato. I proprietari delle informazioni digitali possono definire come le informazioni potranno essere utilizzate dal destinatario, ad esempio chi potrà aprire, modificare, stampare o eseguire altre operazioni su di esse. Per creare o visualizzare un file con autorizzazioni limitate, il PC deve eseguire applicazioni con supporto AD RMS e avere accesso a un server AD RMS.

Informazioni raccolte, elaborate o trasmesse

AD RMS utilizza l'indirizzo di posta elettronica dell'utente per identificarlo in un server AD RMS. Di conseguenza, tale indirizzo viene archiviato nel server e nel PC nelle licenze e nei certificati di identità creati dal server. I certificati di identità e le licenze vengono trasferiti a e verso i server AD RMS quando si tenta di aprire, stampare o eseguire altre azioni su un documento protetto da Rights Management. Se il PC è connesso a una rete aziendale, il server AD RMS è in genere gestito dall'azienda. Se si utilizzano servizi di Windows Live AD RMS, il server è gestito da Microsoft. Per agevolare la protezione della privacy dell'utente, le informazioni inviate ai server Microsoft AD RMS sono crittografate.

Utilizzo delle informazioni

La licenza consente all'utente di accedere ai file protetti. I certificati di identità vengono utilizzati per identificare l'utente in un server AD RMS e consentono di proteggere i file e accedere a quelli protetti.

Scelta e controllo

Le funzionalità AD RMS devono essere abilitate tramite un'app con AD RMS. Per impostazione predefinita, non sono abilitate. È possibile scegliere di non abilitarle o utilizzarle. Tuttavia, se non vengono abilitate, non sarà possibile accedere ai file protetti.

[Inizio pagina](#)

Controllo

Controllo consente a un amministratore di configurare Windows affinché registri l'attività del sistema operativo in un registro sicurezza utilizzando il Visualizzatore eventi e altre applicazioni. Questo registro può aiutare un amministratore a rilevare un accesso non autorizzato al PC o alle risorse nel PC. Ad esempio, questo registro può aiutare gli amministratori a risolvere problemi e determinare se qualcuno ha effettuato l'accesso al PC, creato un nuovo account utente, modificato un criterio di sicurezza o aperto un documento.

Informazioni raccolte, elaborate o trasmesse

Gli amministratori determinano quali informazioni vengono raccolte, per quanto tempo vengono conservate e se vengono trasmesse ad altre parti. Queste informazioni potrebbero includere informazioni personali, come ad esempio nomi utente o nomi di file. Per ulteriori informazioni, consultare l'amministratore. Nessuna informazione viene inviata a Microsoft.

Utilizzo delle informazioni

Gli amministratori determinano anche come controllare le informazioni utilizzate. Generalmente, il registro sicurezza viene utilizzato da auditor e amministratori per tenere traccia dell'attività del PC o per identificare l'accesso non autorizzato al PC o alle risorse nel PC.

Scelta e controllo

Gli amministratori determinano se questa funzionalità è abilitata e le modalità di notifica agli utenti. Gli altri utenti non possono visualizzare il registro sicurezza a meno che l'amministratore non

conceda loro l'autorizzazione. È possibile configurare Controllo nel PC aprendo Criteri di sicurezza locali in Strumenti di amministrazione.

[Inizio pagina](#)

Crittografia unità BitLocker

Scopo della funzionalità

Crittografia unità BitLocker consente di proteggere i dati crittografandoli per impedire a utenti non autorizzati di accedervi. Quando BitLocker è attivato su un'unità supportata, Windows crittograferà i dati sull'unità.

Informazioni raccolte, elaborate o trasmesse

Quando BitLocker viene abilitato utilizzando la crittografia software, le chiavi di crittografia nella memoria crittograferanno e decrittograferanno continuamente i dati quando vengono letti da o scritti nell'unità protetta. Quando BitLocker viene abilitato utilizzando la crittografia dati, la crittografia e decrittografia dei dati viene eseguita dall'unità.

Durante la configurazione di BitLocker, è possibile scegliere di stampare una chiave di ripristino o salvarla in un percorso sulla rete. Se BitLocker viene impostato su un'unità non rimovibile, è inoltre possibile salvare la chiave di ripristino su un'unità flash USB.

Se il PC non appartiene a un dominio, è possibile eseguire il backup della chiave di ripristino di BitLocker, dell'ID della chiave di ripristino e del nome del computer in OneDrive. Per proteggere la privacy dell'utente, le informazioni inviate vengono crittografate tramite SSL.

È possibile configurare BitLocker in modo da crittografare i dati utilizzando un certificato archiviato in una smart card. Quando l'unità dati viene protetta con una smart card, la chiave pubblica e l'identificativo univoco della smart card vengono archiviati non crittografati nell'unità. Queste informazioni possono essere utilizzate per individuare il certificato utilizzato in origine per generare il certificato di crittografia della smart card.

Se il PC dispone di un hardware di sicurezza dotato almeno della versione 1.2 di Trusted Platform Module (TPM), BitLocker utilizza il

TPM per fornire protezione dei dati con hardware migliorato per l'unità in cui è installato Windows. Per ulteriori informazioni, consultare la sezione Servizi Trusted Platform Module (TPM). Nei PC dotati di TPM, è inoltre possibile impostare un PIN personale per aggiungere un ulteriore livello di protezione dei dati crittografati. BitLocker archiverà questo PIN basato su TPM in un modulo crittografato e con hash sull'unità.

Le informazioni raccolte da BitLocker non vengono inviate a Microsoft a meno che non si scelga di eseguire il backup della chiave di ripristino in OneDrive.

Utilizzo delle informazioni

Le chiavi di crittografia e i GUID vengono archiviati nella memoria del PC per supportare le operazioni di BitLocker. Le informazioni di ripristino di BitLocker consentono di accedere ai dati protetti in caso di errori hardware e altri problemi. Queste informazioni di ripristino consentono a BitLocker di distinguere tra utenti autorizzati e non autorizzati.

Microsoft non utilizzerà le singole chiavi di ripristino per altri scopi. Quando le chiavi di ripristino vengono inviate a OneDrive, Microsoft potrebbe utilizzare i dati aggregati per analizzare le tendenze e aiutare a migliorare prodotti e servizi.

Scelta e controllo

Per impostazione predefinita, BitLocker è disattivato. Su un'unità removibile, qualsiasi utente può attivare o disattivare BitLocker in qualsiasi momento aprendo Crittografia unità BitLocker nel Pannello di controllo. Un amministratore può disattivare o attivare BitLocker per tutte le unità.

Se si è scelto di eseguire il backup della chiave di ripristino in OneDrive, è possibile accedervi o eliminarla [all'indirizzo seguente](#).

[Inizio pagina](#)

Individuazione e configurazione di dispositivi

Windows dispone di varie funzionalità che consentono di individuare e configurare dispositivi nel PC, ad esempio l'installazione dispositivi,

l'installazione dispositivi Mobile Broadband, l'individuazione rete e l'associazione di dispositivi wireless.

Installazione dispositivi

Scopo della funzionalità

Quando si installa un nuovo dispositivo nel PC, Windows può cercare, scaricare e installare automaticamente il software driver necessario. Windows può inoltre scaricare informazioni sul dispositivo, ad esempio una descrizione, un'immagine e il logo del produttore. Alcuni dispositivi, inclusi particolari tipi di stampanti, webcam, dispositivi Mobile Broadband e dispositivi portatili che eseguono la sincronizzazione con Windows, dispongono di un'app che ne abilita tutte le funzionalità e ne migliora l'utilizzo da parte dell'utente. Se il produttore del dispositivo ha fornito un'apposita app e l'utente è connesso a Windows Store, Windows può scaricarla e installarla automaticamente da Windows Store.

Informazioni raccolte, elaborate o trasmesse

Durante la ricerca dei driver, Windows verifica in primo luogo se nel PC sia già disponibile un driver appropriato. In caso negativo, Windows contatterà il servizio Windows Update online per trovare e scaricare i driver. Per ulteriori informazioni sui dati raccolti da Windows Update e sulla relativa modalità di utilizzo, vedere l'[Informativa sulla privacy relativa ai servizi di aggiornamento](#).

Per recuperare informazioni sul dispositivo e determinare se è disponibile un'app corrispondente, Windows invia a Microsoft dati sul dispositivo, tra cui l'ID dispositivo (ad esempio l'ID hardware o l'ID modello del dispositivo in uso), il paese e la lingua dell'utente e la data dell'ultimo aggiornamento delle informazioni sul dispositivo. Se sono disponibili informazioni o un'app per il dispositivo, Windows le scarica e le installa da Windows Store. L'app sarà disponibile nell'account Windows Store nell'elenco delle app scaricate.

Utilizzo delle informazioni

Le informazioni inviate a Microsoft vengono utilizzate per individuare e scaricare il driver, le informazioni e l'app appropriati per il dispositivo. Microsoft non utilizza le informazioni e le impostazioni per identificare o contattare l'utente, né per inviargli pubblicità

mirata.

Scelta e controllo

Se si scelgono impostazioni rapide durante la configurazione di Windows, vengono attivati il download e l'installazione automatici di driver, informazioni e app per dispositivi. Se si sceglie di personalizzare le impostazioni, è possibile controllare il download e l'installazione automatici di driver, app e informazioni per dispositivi selezionando **Recupera automaticamente driver, app e informazioni per i nuovi dispositivi** in Help protect and update your PC. Dopo la configurazione di Windows è possibile modificare queste impostazioni nel Pannello di controllo selezionando Change device installation settings e quindi **Chiedi ogni volta**.

Le app dei dispositivi possono essere disinstallate in qualsiasi momento senza disinstallare il dispositivo, anche se potrebbero essere necessarie per utilizzare determinate funzionalità. Dopo avere disinstallato l'app di un dispositivo, è possibile reinstallarla accedendo all'elenco delle app di proprietà dell'utente in Windows Store.

Installazione dispositivi Mobile Broadband

Scopo della funzionalità

Se il PC è dotato di hardware Mobile Broadband fornito da alcuni operatori di telefonia mobile, Windows può scaricare e installare automaticamente un'app che consente di gestire l'account e il piano dati dell'operatore di telefonia mobile che ha fornito l'hardware Mobile Broadband al PC. Ulteriori informazioni sul dispositivo vengono scaricate per poter visualizzare la connessione Mobile Broadband negli elenchi di reti.

Informazioni raccolte, elaborate o trasmesse

Per determinare le informazioni e l'app da scaricare, Windows invia una parte dell'identificatore dell'hardware Mobile Broadband che consente di identificare l'operatore di telefonia mobile dell'utente. Per tutelare la privacy, Windows non invia a Microsoft gli identificatori completi.

Se l'operatore di telefonia mobile ha fornito un'app a Microsoft, Windows la scarica da Windows Store e la installa. Quando si apre

l'app al termine dell'installazione, questa avrà accesso all'hardware Mobile Broadband, compresi gli identificatori hardware univoci che l'operatore potrà utilizzare per identificare l'account dell'utente.

Utilizzo delle informazioni

Microsoft utilizza la parte dell'identificatore dell'hardware Mobile Broadband che Windows invia per determinare l'operatore di cui installare l'app nel computer. Una volta installata, l'app può utilizzare gli ID dell'hardware Mobile Broadband. Ad esempio, l'app di un operatore di telefonia mobile potrebbe utilizzare tali identificatori per cercare informazioni su account e piano dati online. L'utilizzo delle informazioni da parte dell'app sarà soggetto alle procedure relative alla privacy dell'operatore.

Scelta e controllo

Se si scelgono impostazioni rapide durante la prima configurazione di Windows, Windows cercherà e scaricherà automaticamente le app dell'operatore di telefonia mobile. È possibile attivare e disattivare questa funzionalità dal Pannello di controllo. Per ulteriori informazioni, vedere la sezione precedente Installazione dispositivi.

È possibile disinstallare l'app di un operatore di telefonia mobile in qualsiasi momento senza disinstallare l'hardware Mobile Broadband.

Individuazione rete

Scopo della funzionalità

Quando si connette il PC a una piccola rete privata come quella domestica, Windows è in grado di individuare automaticamente altri PC e dispositivi condivisi in rete e rendere il PC dell'utente visibile agli altri sulla rete. Quando sono disponibili dispositivi condivisi, Windows è in grado di connettersi automaticamente e installarli. Esempi di dispositivi condivisi sono le stampanti e gli extender multimediali, ma non dispositivi personali come fotocamere e telefoni cellulari.

Informazioni raccolte, elaborate o trasmesse

Quando si attiva la condivisione e la connessione ai dispositivi, le informazioni sul PC, ad esempio nome e indirizzo di rete, potrebbero essere trasmesse sulla rete locale per consentire ai PC di individuarle

e connettersi.

Per determinare se i dispositivi connessi alla rete devono essere installati automaticamente, alcune informazioni sulla rete vengono raccolte e inviate a Microsoft. Le informazioni comprendono il numero di dispositivi in rete, il tipo di rete (ad esempio, una rete privata) e i tipi di nomi di modello dei dispositivi in rete. Non viene raccolta alcuna informazione personale, ad esempio la password o il nome di rete.

A seconda delle impostazioni di installazione del dispositivo, quando Windows installa dispositivi condivisi, Windows potrebbe inviare alcune informazioni a Microsoft e installare software del dispositivo nel PC. Per ulteriori informazioni, vedere la sezione *Installazione dispositivo*.

Utilizzo delle informazioni

Le informazioni inviate a Microsoft sulla rete vengono utilizzate per determinare quali dispositivi in rete devono essere installati automaticamente. Microsoft non utilizza le informazioni e le impostazioni per identificare o contattare l'utente, né per inviargli pubblicità mirata.

Scelta e controllo

Se si sceglie di abilitare la condivisione e di connettersi ai dispositivi quando si entra in una rete, l'individuazione rete viene attivata per tale rete. È possibile modificare questa impostazione per la rete corrente facendo clic sul tipo di rete elencato sotto il nome della rete in Centro connessioni di rete e condivisione.

È possibile scegliere se abilitare l'individuazione rete completamente e se abilitare l'installazione automatica dei dispositivi connessi alla rete selezionando **Modifica impostazioni di condivisione avanzate** in Centro connessioni di rete e condivisione.

Associazione dispositivo wireless

Scopo della funzionalità

Windows consente di associare il PC a dispositivi wireless che utilizzano Bluetooth o Wi-Fi Direct. Wi-Fi Direct è una tecnologia wireless che consente ai dispositivi di comunicare direttamente tra di

loro, senza doversi connettere a una rete Wi-Fi.

Informazioni raccolte, elaborate o trasmesse

Quando si seleziona **Consenti ai dispositivi Bluetooth di trovare il PC in Impostazioni Bluetooth**, Windows trasmette il nome del PC tramite Bluetooth per consentire ai dispositivi Bluetooth di identificare e rilevare il PC.

Quando si seleziona **Aggiungi un dispositivo** in Dispositivi nelle impostazioni PC, Windows trasmette il nome del PC tramite Wi-Fi per consentire ai dispositivi Wi-Fi Direct di identificare e rilevare il PC. Quando si chiude **Aggiungi un dispositivo**, Windows interrompe la trasmissione del nome del PC tramite Wi-Fi.

A seconda delle impostazioni di installazione del dispositivo, quando Windows si associa a dispositivi wireless, Windows potrebbe inviare alcune informazioni a Microsoft e installare software dispositivo nel PC. Per ulteriori informazioni, vedere la sezione precedente Installazione dispositivi.

Utilizzo delle informazioni

Windows trasmette il nome del PC per consentire ad altri dispositivi di identificare e connettersi al PC. Il nome del PC non viene inviato a Microsoft.

Scelta e controllo

Per modificare la modalità di trasmissione del nome del PC di Windows tramite Bluetooth, tenere premuto o fare clic con il pulsante destro del mouse sul PC in Dispositivi e stampanti nel Pannello di controllo, selezionare **Impostazioni Bluetooth**, quindi selezionare **Consenti ai dispositivi Bluetooth di trovare il PC**. Se non si desidera che Windows trasmetta il nome del PC tramite Wi-Fi mentre si aggiungono dispositivi, disattivare temporaneamente il Wi-Fi in Wireless nelle impostazioni PC prima di aggiungere un dispositivo.

[Inizio pagina](#)

DirectAccess

Scopo della funzionalità

DirectAccess consente al PC di connettersi in remoto e in modo semplice alla rete aziendale ogni volta che il PC è connesso a Internet, indipendentemente dalla propria posizione.

Informazioni raccolte, elaborate o trasmesse

Ogni volta che si avvia il PC, DirectAccess tenterà di connettersi alla rete aziendale, indipendentemente dal fatto che ci si trovi sul posto di lavoro o meno. Una volta connesso, il PC scaricherà i criteri aziendali e sarà possibile accedere alle risorse configurate nella rete aziendale. L'amministratore della rete aziendale può sfruttare la connettività di DirectAccess per gestire e monitorare in remoto il PC, compresi i siti Web che si visitano anche quando non ci si trova fisicamente in azienda.

DirectAccess non invia alcuna informazione a Microsoft.

Utilizzo delle informazioni

I criteri aziendali determinano il modo in cui vengono utilizzate le informazioni raccolte dall'amministratore della rete aziendale.

Scelta e controllo

DirectAccess deve essere configurato dall'amministratore della rete aziendale utilizzando Criteri di gruppo. Mentre il proprio amministratore può consentirci di disattivare temporaneamente alcuni elementi di DirectAccess, solo l'amministratore della rete aziendale può interrompere i tentativi di Windows di connettersi alla rete aziendale a scopo di gestione. Se l'utente o l'amministratore della rete aziendale rimuovono il PC dal dominio aziendale, DirectAccess non sarà più in grado di connettersi.

[Inizio pagina](#)

Aggiornamento dinamico

Scopo della funzionalità

Con Aggiornamento dinamico Windows esegue un singolo controllo con Windows Update per ottenere gli aggiornamenti più recenti per il PC durante l'installazione di Windows. Se sono disponibili aggiornamenti, vengono automaticamente scaricati da

Aggiornamento dinamico e installati nel PC in modo che questo venga aggiornato al primo accesso o utilizzo da parte dell'utente.

Informazioni raccolte, elaborate o trasmesse

Per installare driver compatibili, Aggiornamento dinamico invia a Microsoft informazioni relative all'hardware del PC. Tra i tipi di aggiornamenti che possono essere scaricati nel PC da Aggiornamento dinamico sono inclusi:

- **Aggiornamenti dell'installazione.** Importanti aggiornamenti software per i file di installazione per garantire la riuscita dell'installazione.
- **Aggiornamenti dei driver inclusi.** Importanti aggiornamenti dei driver per la versione di Windows che viene installata.

Utilizzo delle informazioni

Aggiornamento dinamico fornisce a Microsoft le informazioni relative all'hardware del PC per consentire l'identificazione dei driver corretti per il sistema. Per ulteriori informazioni sulle modalità di utilizzo delle informazioni raccolte da Aggiornamento dinamico, vedere l'[Informativa sulla privacy relativa ai servizi di aggiornamento](#).

Scelta e controllo

All'inizio dell'installazione di Windows, viene chiesto se si desidera effettuare la connessione online per l'installazione di aggiornamenti.

[Inizio pagina](#)

Centro accessibilità

Scopo della funzionalità

Centro accessibilità consente di attivare le opzioni e le impostazioni di accessibilità per consentire di interagire in modo più semplice con il PC.

Informazioni raccolte, elaborate o trasmesse

Se si utilizza questa funzionalità, verrà chiesto di selezionare le affermazioni appropriate.

Ad esempio:

- Immagini e testo in TV sono difficili da visualizzare.
- Le condizioni della luce rendono difficile visualizzare le immagini sul monitor.
- Non utilizzo una tastiera.
- Sono un non vedente.
- Sono sordo.
- Soffro di un disturbo del linguaggio.

Queste informazioni vengono salvate in formato non leggibile e archiviate localmente nel PC.

Utilizzo delle informazioni

In base alle affermazioni scelte verrà fornito un set di informazioni aggiornate sulla configurazione. Queste informazioni vengono inviate a Microsoft e non sono disponibili ad altri utenti.

Scelta e controllo

È possibile scegliere quali affermazioni selezionare andando a Centro accessibilità nel Pannello di Controllo. È possibile modificare le scelte in qualsiasi momento. È inoltre possibile scegliere quali informazioni configurazione nel PC.

[Inizio pagina](#)

Visualizzatore eventi

Scopo della funzionalità

Gli utenti del PC, principalmente gli amministratori, possono utilizzare il Visualizzatore eventi per visualizzare e gestire i registri eventi. I registri eventi contengono informazioni su hardware, software ed eventi di sicurezza nel PC. È inoltre possibile ottenere informazioni da Microsoft sugli eventi nel registro eventi facendo clic su Guida registro eventi.

Informazioni raccolte, elaborate o trasmesse

I registri eventi contengono anche informazioni generate da tutti gli utenti e app nel PC. Per impostazione predefinita, tutti gli utenti possono visualizzare le voci del registro eventi. Tuttavia, gli amministratori possono scegliere di limitare l'accesso ai registri eventi. È possibile accedere ai registri eventi del PC aprendo il Visualizzatore eventi. Per informazioni sull'apertura del Visualizzatore eventi, vedere Guida e supporto tecnico di Windows.

Se si utilizza Guida registro eventi per cercare ulteriori informazioni su un evento specifico, le informazioni sull'evento vengono inviate a Microsoft.

Utilizzo delle informazioni

Quando si utilizza Guida registro eventi per cercare ulteriori informazioni su un evento, i dati inviati dal PC vengono utilizzati per individuare la posizione dell'utente e fornirgli le informazioni sull'evento. Per eventi Microsoft, i dettagli relativi all'evento verranno inviati a Microsoft. Microsoft non utilizza le informazioni e le impostazioni per identificare o contattare l'utente, né per inviargli pubblicità mirata. Per eventi associati ad applicazioni di terze parti, le informazioni verranno inviate alla posizione specificata dall'autore o produttore di terze parti. Se si inviano informazioni sugli eventi ad autori o produttori di terze parti, l'uso delle informazioni sarà soggetto alle procedure relative alla privacy della terza parte.

Scelta e controllo

Gli amministratori possono scegliere di limitare l'accesso ai registri del Visualizzatore eventi. Gli utenti che hanno completo accesso ai registri del visualizzatore eventi possono cancellarli. A meno che non si abbia precedentemente accettato di inviare automaticamente informazioni sull'evento quando si fa clic sulla Guida registro eventi, verrà chiesto all'utente di confermare che le informazioni visualizzate possono essere inviate tramite Internet. Nessuna informazione relativa al registro eventi verrà inviata tramite Internet senza consenso. Gli amministratori possono utilizzare i Criteri di gruppo per selezionare o modificare il sito al quale vengono inviate le informazioni sull'evento.

[Inizio pagina](#)

Family Safety

Scopo della funzionalità

Family Safety aiuta i genitori a proteggere i loro figli quando utilizzano il PC. I genitori possono controllare le app, i giochi e i siti Web che possono essere utilizzati dai bambini, nonché impostare limiti temporali e ricevere regolari rapporti di attività tramite posta elettronica. La gestione delle restrizioni e la visualizzazione dei rapporti di attività possono essere effettuate localmente sul PC oppure online utilizzando il sito Web Microsoft Family Safety.

Informazioni raccolte, elaborate o trasmesse

Le impostazioni di Family Safety e i rapporti sull'attività dei bambini vengono archiviati nel PC. I rapporti di attività possono contenere informazioni sul tempo trascorso al computer, il tempo di utilizzo delle singole app e dei singoli giochi e i siti Web visitati, inclusi i tentativi di visualizzazione di siti bloccati. Gli amministratori del PC possono modificare le impostazioni e visualizzare il rapporto di attività.

Se si abilita la gestione online per l'account di un figlio, i genitori possono visualizzare il rapporto sull'attività del bambino e modificare le impostazioni nel sito Web Microsoft Family Safety. Per consentire ad altri utenti di visualizzare i rapporti di attività e di modificare le impostazioni, è possibile aggiungerli come genitori nel sito Web Microsoft Family Safety. Se il genitore che configura Family Safety esegue l'accesso a Windows con un account Microsoft, la gestione online viene abilitata automaticamente.

Se si configura Family Safety per l'account di un figlio con la gestione online abilitata, i rapporti settimanali sull'attività del bambino vengono automaticamente inviati al genitore tramite posta elettronica.

Utilizzo delle informazioni

Windows e il sito Web Microsoft Family Safety utilizzano le informazioni raccolte per fornire la funzionalità di protezione famiglia. Microsoft potrebbe analizzare le informazioni dei registri di attività in forma aggregata per finalità di verifica della qualità dei

dati, ma non utilizza le informazioni e le impostazioni per identificare o contattare i singoli utenti, né per inviare loro pubblicità mirata.

Scelta e controllo

Family Safety è disattivata per impostazione predefinita. È possibile accedere a Family Safety aprendo Family Safety nel Pannello di controllo. Solo gli amministratori possono attivare Family Safety ed è possibile monitorare o limitare solo utenti che non dispongono di privilegi amministrativi. I bambini possono visualizzare le proprie impostazioni, ma non possono modificarle. Se Family Safety è attivata, ogni volta che il bambino accede a Windows riceverà una notifica di monitoraggio del suo account. Se durante la creazione di un account si specifica che si tratta dell'account di un bambino, è possibile scegliere di abilitare Family Safety per il determinato account.

Se l'amministratore che configura l'account di un bambino ha eseguito l'accesso a Windows con un account Microsoft, la gestione online viene abilitata automaticamente e si riceveranno ogni settimana i rapporti sull'attività del bambino. È possibile aggiungere o rimuovere account di genitori nel sito Web Microsoft Family Safety. Chiunque venga aggiunto come genitore nel sito Web potrà visualizzare un rapporto sull'attività del bambino e modificare le impostazioni di Family Safety relative al bambino, anche se il genitore non è un amministratore del PC utilizzato dai bambini.

Per un corretto utilizzo di Family Safety, solo i genitori devono essere amministratori dei propri PC e ai bambini non dovrebbero essere concessi privilegi amministrativi. Tenere presente che l'utilizzo di questa funzionalità per monitorare altri utenti (ad esempio adulti) potrebbe costituire una violazione della legge applicabile.

[Inizio pagina](#)

Fax

Scopo della funzionalità

La funzionalità Fax consente di creare e salvare frontespizi fax e inviare e ricevere fax utilizzando il PC e un modem fax incorporato o esterno o un server fax.

Informazioni raccolte, elaborate o trasmesse

Le informazioni raccolte comprendono informazioni personali immesse in un frontespizio fax, nonché gli identificativi contenuti nei protocolli fax standard del settore come ad esempio, Transmitting Subscriber ID (TSID) e Call Subscriber ID (CSID). Per impostazione predefinita, Windows utilizza "Fax" come valore per ogni identificativo.

Utilizzo delle informazioni

Le informazioni immesse nella finestra di dialogo del mittente vengono presentate sul frontespizio fax. Gli identificativi come TSID e CSID potrebbero contenere testo arbitrario e vengono generalmente utilizzati dal fax o dal PC ricevente per identificare il mittente. Nessuna informazione viene inviata a Microsoft.

Scelta e controllo

L'accesso al fax viene determinato dai privilegi dell'account utente nel PC. A meno che un amministratore fax modifichi le impostazioni di accesso, tutti gli utenti possono inviare e ricevere fax. Per impostazione predefinita, tutti gli utenti possono visualizzare i documenti da loro inviati e i fax ricevuti sul PC. Gli amministratori possono visualizzare tutti i documenti inviati tramite fax e configurare le impostazioni relative ai fax, comprese quelle relative a chi può visualizzare o gestire i fax e i valori TSID e CSID.

[Inizio pagina](#)

Personalizzazione riconoscimento grafia: apprendimento automatico

Scopo della funzionalità

Apprendimento automatico è uno strumento per la personalizzazione del riconoscimento della grafia disponibile nei PC touch o con pennino per tablet. Questa funzionalità raccoglie dati sulle parole utilizzate e sul modo in cui vengono scritte. Aiuta il software per il riconoscimento della grafia a riconoscere e migliorare l'interpretazione dello stile e vocabolario della grafia e inoltre migliora la correzione automatica e i suggerimenti per le lingue senza Input Method Editor (IME).

Informazioni raccolte, elaborate o trasmesse

Le informazioni raccolte tramite apprendimento automatico vengono archiviate nel profilo utente di ogni utente nel PC. I dati vengono archiviati in un formato proprietario che non può essere letto utilizzando un'app per la visualizzazione di testo (ad esempio Blocco note o WordPad) e che è disponibile ad altri utenti solo se sono amministratori del PC.

Le informazioni raccolte includono:

- Testo contenuto in messaggi digitati e voci di calendario create utilizzando app di posta elettronica (ad esempio, Office Outlook o Windows Live Mail) compresi tutti i messaggi già inviati.
- Input penna in Pannello di input.
- Testo riconosciuto da input penna scritto in Pannello di input o digitato sulle tastiere su schermo.
- Caratteri alternativi selezionati per correggere il testo riconosciuto.

Utilizzo delle informazioni

Le informazioni raccolte vengono utilizzate per aiutare a migliorare il riconoscimento della grafia creando una versione del software di riconoscimento personalizzata per il proprio stile e vocabolario e per consentire la correzione automatica e i suggerimenti mentre si digita sulle tastiere su schermo.

I testi di esempio vengono utilizzati per creare un dizionario esteso. I campioni di input penna vengono utilizzati per migliorare il riconoscimento dei caratteri per ogni utente sul PC. Nessuna informazione viene inviata a Microsoft.

Scelta e controllo

L'apprendimento automatico viene abilitato per impostazione predefinita. È possibile attivare o disattivare l'apprendimento automatico in Impostazioni avanzate in Lingue nel Pannello di controllo. Quando si disattiva l'apprendimento automatico, tutti i dati raccolti e archiviati mediante questa funzionalità vengono eliminati.

[Inizio pagina](#)

Gruppo Home

Scopo della funzionalità

In Windows è possibile collegare facilmente i PC della rete domestica così da poter condividere immagini, musica, video, documenti e dispositivi. È inoltre possibile trasmettere flussi multimediali a dispositivi presenti nella rete domestica, ad esempio a un extender multimediale. Questi PC e dispositivi costituiscono il gruppo home dell'utente. Il gruppo home può essere protetto con una password ed è possibile decidere con chi condividerlo.

Informazioni raccolte, elaborate o trasmesse

È possibile accedere ai propri file, come ad esempio immagini, video, musica e documenti da qualsiasi PC nel gruppo home. Quando si partecipa a un gruppo home, le informazioni (inclusi indirizzo di posta elettronica, nome visualizzato e immagine) su tutti gli account Microsoft nel PC verranno condivise con gli altri utenti del gruppo home per abilitare la condivisione.

Utilizzo delle informazioni

Le informazioni raccolte consentono ai PC nel gruppo home di capire con chi condividere i contenuti e come presentarli. Nessuna informazione viene inviata a Microsoft.

Scelta e controllo

È possibile aggiungere o rimuovere PC dal gruppo home e decidere cosa condividere con gli altri membri del gruppo home. È possibile creare un gruppo home e gestire le impostazioni accedendo al gruppo home nelle impostazioni del PC.

[Inizio pagina](#)

Input Method Editor (IME)

I Microsoft IME sono utilizzati con le lingue dell'Asia orientale per convertire l'input da tastiera in ideogrammi. In questa sezione vengono illustrate varie funzionalità, tra cui la regolazione

automatica e previsione IME, la segnalazione errori conversione IME e la registrazione parola IME

Regolazione automatica e previsione IME

Scopo della funzionalità

A seconda dell'IME utilizzato e delle impostazioni, le funzionalità di regolazione automatica e suggerimento di testo degli IME potrebbero registrare parole o sequenze di parole per migliorare la selezione degli ideogrammi visualizzati.

Informazioni raccolte, elaborate o trasmesse

Le funzionalità di regolazione automatica (autoapprendimento) e suggerimento di testo degli IME registrano una parola o una sequenza di parole e la frequenza con cui vengono utilizzate. Le informazioni sulla regolazione automatica (ad eccezione delle sequenze di cifre/simboli) vengono archiviate in file per ogni utente sul PC.

Utilizzo delle informazioni

I dati relativi all'apprendimento automatico e al suggerimento di testo vengono utilizzati dagli IME sul PC per migliorare la selezione degli ideogrammi visualizzati quando si utilizza l'IME. Se si sceglie di inviare questi dati a Microsoft, questi vengono utilizzati per migliorare gli IME e i prodotti e servizi correlati.

Scelta e controllo

Tranne che per l'IME del cinese semplificato (nel quale la funzionalità di stima è disattivata per impostazione predefinita), le funzionalità di apprendimento automatico e di suggerimento di testo sono attive per impostazione predefinita negli IME che li supportano. I dati raccolti non vengono inviati automaticamente a Microsoft. È possibile scegliere se raccogliere o inviare questi dati in Lingua nel Pannello di controllo.

Segnalazione errori conversione IME

Scopo della funzionalità

Se si verificano errori durante la presentazione degli ideogrammi o la conversione degli input da tastiera in ideogrammi, questa funzionalità può raccogliere informazioni sugli errori per aiutare

Microsoft a migliorare i suoi prodotti e servizi.

Informazioni raccolte, elaborate o trasmesse

Segnalazione errori conversione IME raccoglie informazioni sugli errori di conversione IME, ad esempio cosa è stato digitato, il risultato della prima conversione o stima, la stringa alternativa scelta, informazioni sull'IME utilizzato e informazioni su come utilizzarlo. Inoltre, se si utilizza l'IME giapponese, è possibile scegliere se includere informazioni sull'apprendimento automatico nelle segnalazioni errori conversione.

Utilizzo delle informazioni

Microsoft utilizza le informazioni per migliorare prodotti e servizi. Microsoft non utilizza le informazioni e le impostazioni per identificare o contattare l'utente, né per inviargli pubblicità mirata.

Scelta e controllo

Dopo che un determinato numero di errori di conversione viene archiviato, Mis-Conversion Report Tool chiederà se inviare una segnalazione errori conversione. È inoltre possibile scegliere di inviare una segnalazione errori conversione dal Mis-Conversion Report Tool dell'IME in qualsiasi momento. È possibile visualizzare le informazioni contenute in ogni segnalazione prima di scegliere se inviarle o meno. È inoltre possibile abilitare l'invio automatico delle segnalazioni errori conversione in Impostazioni IME.

Registrazione parola IME

Scopo della funzionalità

A seconda dell'IME utilizzato, potrebbe essere possibile utilizzare la registrazione parola per segnalare parole non supportate (parole che potrebbero non essere convertite correttamente in ideogrammi dagli input da tastiera).

Informazioni raccolte, elaborate o trasmesse

Le segnalazioni della registrazione possono includere informazioni fornite nella finestra di dialogo Add Word sulle parole segnalate e sul numero della versione di software per un IME. Queste segnalazioni potrebbero includere informazioni personali, ad esempio, se si aggiungono nomi di persona tramite la registrazione parola. È

possibile controllare i dati che si stanno per inviare in ogni segnalazione prima di scegliere se inviarli.

Utilizzo delle informazioni

Microsoft utilizza le informazioni per migliorare prodotti e servizi. Microsoft non utilizza le informazioni e le impostazioni per identificare o contattare l'utente, né per inviargli pubblicità mirata.

Scelta e controllo

Ogni volta che si crea una segnalazione di registrazione parola, viene chiesto di decidere se inviare la segnalazione a Microsoft. È possibile visualizzare le informazioni contenute in ogni segnalazione prima di scegliere se inviarle o meno.

[Inizio pagina](#)

Analisi utilizzo Installazione

Scopo della funzionalità

Questa funzionalità invia a Microsoft un singolo rapporto contenente le informazioni di base sul PC e sulla modalità di installazione di Windows 8. Microsoft utilizza queste informazioni per migliorare l'esperienza di installazione e creare soluzioni ai problemi comuni relativi all'installazione.

Informazioni raccolte, elaborate o trasmesse

Nel report sono generalmente incluse informazioni relative all'esperienza di installazione, ad esempio la data di installazione, la durata di ciascuna fase dell'installazione, se si è trattato di un aggiornamento o di una nuova installazione del prodotto, i dettagli sulla versione, la lingua del sistema operativo, il tipo di supporto, la configurazione del PC e la riuscita o meno con eventuali codici di errore.

Se si sceglie di partecipare ad Analisi utilizzo Installazione, il rapporto viene inviato a Microsoft durante la connessione a Internet. Analisi utilizzo Installazione genera casualmente un numero denominato identificatore univoco globale (GUID, Globally Unique Identifier) inviato a Microsoft insieme al rapporto. Il GUID consente a Microsoft

di determinare quali dati vengono inviati da un computer specifico nel tempo. Il GUID non contiene informazioni personali e non viene utilizzato per identificare l'utente.

Utilizzo delle informazioni

Microsoft e i suoi partner utilizzano il rapporto per migliorare prodotti e servizi. Il GUID viene utilizzato per correlare i dati con i dati raccolti dal programma Analisi utilizzo software Windows, a cui l'utente può scegliere di partecipare durante l'utilizzo di Windows 8.

Scelta e controllo

È possibile scegliere di partecipare al programma durante l'installazione di Windows 8 selezionando **Voglio contribuire a migliorare l'installazione di Windows**.

Per ulteriori informazioni, vedere la sezione relativa ad Analisi utilizzo software Windows.

[Inizio pagina](#)

Stampa Internet

Scopo della funzionalità

Stampa Internet consente di stampare da Internet.

Informazioni raccolte, elaborate o trasmesse

Quando si stampa utilizzando questa funzionalità, è innanzitutto necessario connettersi e autenticarsi a un server di stampa Internet. Le informazioni da inviare al server di stampa varieranno in base al livello di sicurezza che il server di stampa supporta (ad esempio, potrebbe essere richiesto di fornire un nome utente e una password). Dopo essersi connessi, viene visualizzato un elenco di stampanti compatibili. Se il PC non dispone di un driver di stampa per la stampante selezionata, è possibile scegliere di scaricare un driver dal server di stampa. Poiché i processi di stampa non vengono crittografati, è possibile che altri visualizzino il contenuto che viene inviato.

Utilizzo delle informazioni

Le informazioni raccolte consentono di stampare utilizzando

stampanti remote. Se si sceglie di utilizzare un server di stampa ospitato in Microsoft, le informazioni fornite non verranno utilizzate per identificare o contattare l'utente, né per inviargli pubblicità mirata. Se si inviano informazioni al server di stampa di terze parti, l'utilizzo delle informazioni sarà soggetto alle procedure relative alla privacy della terza parte.

Scelta e controllo

È possibile attivare o disattivare Stampa Internet aprendo Programmi e funzionalità nel Pannello di controllo e quindi selezionando **Attivazione o disattivazione delle funzionalità Windows**.

[Inizio pagina](#)

Preferenze lingua

Scopo della funzionalità

È possibile aggiungere lingue preferite da utilizzare all'elenco delle lingue in Windows 8. App e siti Web vengono visualizzati nella prima lingua disponibile nell'elenco.

Informazioni raccolte, elaborate o trasmesse

Quando si visitano siti Web e si installano app nel PC, l'elenco di lingue preferite viene inviato ai siti Web visitati ed è disponibile per le app utilizzate in modo che possano fornire contenuti nelle lingue preferite.

Utilizzo delle informazioni

L'elenco delle lingue preferite viene utilizzato da siti Web e app Microsoft per fornire il relativo contenuto nelle lingue preferite dall'utente. Microsoft non utilizza le informazioni per identificare o contattare l'utente. Le informazioni sulla lingua inviate o utilizzate da siti Web e app di terze parti sono soggette alle pratiche relative alla privacy dell'entità di pubblicazione del sito Web o dell'app di terze parti.

Scelta e controllo

L'elenco delle lingue preferite è disponibile per le app che vengono

installate e per i siti Web visitati. È possibile aggiungere o rimuovere lingue dall'elenco in Preferenze lingua nel Pannello di controllo. Se non sono presenti lingue in questo elenco, la lingua scelta nella scheda Formati in Paese nel Pannello di controllo verrà inviata ai siti Web visitati.

[Inizio pagina](#)

Servizi di posizione

Nei PC in cui si esegue Windows, per servizi di posizione si intendono il software Windows e il servizio online di Microsoft utilizzati per determinare la posizione fisica approssimativa del PC, fornita alle applicazioni o ai siti Web a cui l'utente consente di accedere. La piattaforma di localizzazione geografica Windows ottiene la posizione dall'hardware dedicato, ad esempio un sensore GPS nel PC o tramite software come il Localizzatore geografico di Windows.

Piattaforma di localizzazione geografica di Windows

Scopo della funzionalità

Se si sceglie di attivare la piattaforma di localizzazione geografica di Windows, le app installate da Windows Store potranno richiedere l'autorizzazione ad accedere alla posizione del PC. A seconda della configurazione del sistema, la piattaforma può determinare la posizione del PC tramite hardware, ad esempio un sensore GPS, o tramite software, ad esempio il Localizzatore geografico di Windows.

La piattaforma non impedisce alle app di accedere alla posizione dell'utente in altri modi. Ad esempio, è possibile installare dispositivi (come un ricevitore GPS) che possono inviare informazioni sulla posizione direttamente a un'app ignorando completamente la piattaforma. Indipendentemente dalle impostazioni della piattaforma di localizzazione geografica di Windows, i servizi online possono utilizzare l'indirizzo IP del PC per determinarne la posizione approssimativa, in genere la città in cui si trova il PC.

Informazioni raccolte, elaborate o trasmesse

La piattaforma di localizzazione geografica di Windows non trasmette alcuna informazione dal PC, ma i singoli localizzatori geografici, ad

esempio il Localizzatore geografico di Windows, potrebbero eseguire il trasferimento durante l'utilizzo di app in grado di rilevare la posizione geografica. Le app autorizzate a utilizzare la piattaforma per determinare la posizione dell'utente potrebbero anche trasmettere o archiviare tale informazioni.

Utilizzo delle informazioni

Se si abilita la piattaforma di localizzazione geografica di Windows, le app autorizzate saranno in grado di accedere alla posizione dell'utente e utilizzarla per fornire contenuto personalizzato. Se si utilizza un'app o un localizzatore geografico di terze parti, l'utilizzo della posizione del PC sarà soggetto alle procedure relative alla privacy della terza parte. Prima di scaricare un'app da Windows Store, sarà possibile verificare nella relativa descrizione se l'app è in grado di rilevare la posizione geografica.

Scelta e controllo

Se si scelgono impostazioni rapide durante la configurazione di Windows, viene attivata la piattaforma di localizzazione geografica di Windows. Se si sceglie di personalizzare le impostazioni, è possibile controllare la piattaforma di localizzazione geografica di Windows selezionando **Consenti alle app di accedere alla mia posizione utilizzando la piattaforma di localizzazione geografica di Windows** in **Condividi informazioni con le app**. La prima volta che ogni app di Windows Store richiede la posizione del PC, in Windows verrà richiesto se si desidera consentire l'operazione. È possibile definire se le app possono accedere alla posizione dell'utente utilizzando Privacy in Impostazioni PC. Per definire se una singola app di Windows Store può utilizzare la posizione dell'utente, si può utilizzare Autorizzazioni nell'accesso alle impostazioni dell'app.

Se si utilizza un'app desktop che fa uso della piattaforma di localizzazione geografica di Windows, dovrebbe essere richiesta l'autorizzazione all'utilizzo della posizione del PC e quando l'app accede alla posizione del PC, nell'area di notifica verrà visualizzata un'icona di avviso di accesso effettuato alla posizione del PC. Ogni utente può controllare le impostazioni di posizione per le tutte le app in Privacy di Impostazioni PC. Gli amministratori possono inoltre scegliere di disattivare la piattaforma di localizzazione geografica di

Windows per tutti gli utenti in Posizione nel Pannello di controllo.

Localizzatore geografico di Windows

Scopo della funzionalità

Il Localizzatore geografico di Windows si connette al servizio di localizzazione geografica di Microsoftonline, che determina la posizione approssimativa del PC in base al suo indirizzo IP e alle reti Wi-Fi presenti nelle vicinanze.

Informazioni raccolte, elaborate o trasmesse

Quando un'app autorizzata dall'utente richiede l'accesso alla posizione del PC, la piattaforma di localizzazione geografica di Windows chiede a tutti i localizzatori geografici installati (incluso il Localizzatore geografico di Windows) di determinare la posizione corrente del PC. Il Localizzatore geografico di Windows controlla innanzitutto se è presente un elenco di punti di accesso Wi-Fi archiviati da una richiesta precedente di un'app in grado di rilevare la posizione. Se non è già disponibile un elenco di punti di accesso Wi-Fi vicini o se l'elenco non è aggiornato, il localizzatore geografico invia le informazioni sui punti di accesso Wi-Fi vicini e i dati GPS, se disponibili, al servizio di localizzazione geografica di Microsoft. Il servizio restituisce la posizione approssimativa del PC al Localizzatore geografico di Windows, il quale passa l'informazione alla piattaforma di localizzazione geografica di Windows, che a sua volta la fornisce all'app che ha richiesto la posizione dell'utente. Il Localizzatore geografico di Windows potrebbe anche aggiornare l'elenco archiviato di punti di accesso Wi-Fi. Il Localizzatore geografico di Windows mantiene questo elenco al fine di determinare la posizione approssimativa del PC senza dover effettuare ogni volta la connessione a Internet. Questo elenco di punti di accesso viene crittografato al momento dell'archiviazione su disco e pertanto non risulta direttamente accessibile alle app.

Le informazioni inviate sui punti di accesso Wi-Fi vicini includono BSSID (indirizzo MAC del punto di accesso Wi-Fi) e potenza del segnale. Le informazioni GPS includono latitudine, longitudine, direzione, velocità e altitudine osservate. Per proteggere la privacy dell'utente, il Localizzatore geografico di Windows non invia alcuna informazione che consenta di identificare univocamente il PC se non i

dati standard sul computer inviati con tutte le connessioni a Internet. Per tutelare la privacy dei proprietari di reti Wi-Fi, Windows non invia i SSID (nomi dei punti di accesso Wi-Fi) o informazioni sulle reti Wi-Fi nascoste. Al fine di garantire privacy e sicurezza, le informazioni sulle reti Wi-Fi inviate vengono crittografate tramite SSL.

Utilizzo delle informazioni

Le informazioni vengono utilizzate dal Localizzatore geografico di Windows per fornire alla piattaforma di localizzazione geografica di Windows la posizione approssimativa del PC quando viene richiesta da un'app autorizzata.

Se si sceglie di contribuire a migliorare il servizio di localizzazione geografica di Microsoft, i dati Wi-Fi e GPS inviati a Microsoft vengono utilizzati per migliorare i servizi di posizione di Microsoft forniti alle app. Microsoft non archivia alcuna informazione raccolta da questo servizio che potrebbe essere utilizzata per identificare o contattare l'utente, inviargli pubblicità mirata, tenere traccia delle posizioni del PC o crearne una cronologia.

Scelta e controllo

Il Localizzatore geografico di Windows viene utilizzato solo se un'app autorizzata ha richiesto la posizione del PC. Per ulteriori informazioni su come definire se le app possono richiedere la posizione del PC, vedere la sezione Piattaforma di localizzazione geografica di Windows. Se si autorizzano le app a richiedere la posizione del PC, l'elenco memorizzato nella cache delle posizioni dei punti di accesso Wi-Fi vicini crittografate e archiviate dal Localizzatore geografico di Windows verrà eliminato e sostituito periodicamente.

Se si scelgono impostazioni rapide durante la configurazione di Windows, si sceglie di contribuire a migliorare il servizio di localizzazione geografica di Microsoft. Se si sceglie di personalizzare le impostazioni, è possibile decidere se contribuire a migliorare il servizio di localizzazione geografica di Microsoft selezionando

Contribuisci a migliorare i servizi Microsoft inviandoci i dati sulla posizione quando utilizzi app in grado di riconoscere la posizione in Invia info a Microsoft per contribuire a migliorare Windows e le app. Dopo la configurazione di Windows è possibile modificare questa impostazione tramite Impostazioni

posizione nel Pannello di controllo. Se si sceglie di non contribuire a migliorare il servizio, sarà comunque possibile utilizzare il Localizzatore geografico di Windows per determinare la posizione approssimativa del PC.

È possibile abilitare e disabilitare il Localizzatore geografico di Windows aprendo **Attivazione o disattivazione delle funzionalità Windows** nel Pannello di controllo. Se si disattiva il Localizzatore geografico di Windows, è comunque possibile utilizzare altri localizzatori geografici (ad esempio GPS) con la piattaforma di localizzazione geografica di Windows.

[Inizio pagina](#)

Nome e immagine dell'account

Scopo della funzionalità

Per fornire contenuto personalizzato, le applicazioni possono richiedere il nome e l'immagine dell'account di Windows. Il nome e l'immagine dell'account sono visualizzati in *Il tuo account*, nella sezione *Utenti di Impostazioni PC*. Se si accede a Windows con un account Microsoft, Windows utilizzerà il nome e l'immagine associati a tale account. Se non è stata scelta un'immagine per l'account, verrà utilizzata un'immagine predefinita fornita da Windows..

Informazioni raccolte, elaborate o trasmesse

Se si consente alle app di accedere al nome e all'immagine dell'account, Windows fornirà tali informazioni a tutte le app che le richiedono. Le app potrebbero archiviare o trasmettere queste informazioni.

Se si accede a Windows con un account di dominio e si sceglie di consentire alle app di utilizzare il nome e l'immagine dell'account, le app che possono utilizzare le credenziali Windows dell'utente potranno accedere ad altre informazioni sull'account di dominio. Tali informazioni includono, ad esempio, il nome dell'entità utente (come `luca@contoso.com`) e il nome di dominio DNS (come `corp.contoso.com\luca`).

Se si accede a Windows con un account Microsoft o se si accede a Windows con un account di dominio connesso a un account

Microsoft, Windows potrà sincronizzare automaticamente l'immagine dell'account nel PC con l'immagine dell'account Microsoft.

Utilizzo delle informazioni

Se si utilizza un'app di terze parti, la modalità di utilizzo del nome e dell'immagine dell'account dipende dalle procedure relative alla privacy della terza parte. Se si utilizza un'app Microsoft, le procedure relative alla privacy dell'app saranno illustrate nella relativa Informativa sulla privacy.

Scelta e controllo

Se si scelgono impostazioni rapide durante la configurazione di Windows, Windows consentirà l'accesso al nome e all'immagine dell'account da parte delle applicazioni. Se si sceglie di personalizzare le impostazioni, è possibile controllare l'accesso al nome e all'immagine dell'account selezionando **Consenti alle app di utilizzare il nome e l'immagine del mio account** in **Condividi informazioni con le app**. Dopo la configurazione di Windows è possibile modificare questa impostazione nella sezione **Privacy** di Impostazioni PC. È possibile modificare l'immagine dell'account nella sezione **Personalizza** di Impostazioni PC. È inoltre possibile scegliere di consentire a particolari app di modificare l'immagine dell'account.

[Inizio pagina](#)

Presenza in rete

Scopo della funzionalità

Se si dispone di un piano di iscrizione per l'accesso alla rete (ad esempio, tramite una connessione Mobile Broadband), questa funzionalità fornisce informazioni sul piano di iscrizione alle app e alle funzionalità di Windows nel PC. Le funzionalità e le app di Windows potranno utilizzare tali informazioni per ottimizzare il proprio funzionamento. Ad esempio, se si è connessi tramite un piano dati a consumo, Windows Update attenderà a inviare aggiornamenti di priorità bassa al PC finché non ci si sarà connessi a un altro tipo di rete. Questa funzionalità inoltre fornisce informazioni sulla connessione di rete, come ad esempio sulla potenza del

segnale e se il PC è connesso a Internet o meno.

Informazioni raccolte, elaborate o trasmesse

Questa funzionalità raccoglie informazioni sulla connettività della rete Internet e Intranet, come ad esempio il suffisso Domain Name Service (DNS) del PC, nome della rete e indirizzo gateway delle reti alle quali si connette il PC. Questa funzionalità inoltre riceve informazioni sul piano di iscrizione, come ad esempio la quantità di dati rimanenti nel piano.

I profili della connettività di rete possono includere una cronologia di tutte le reti visitate e la data e l'ora dell'ultima connessione. Questa funzionalità è in grado di connettersi a un server Microsoft per determinare se l'utente è connesso a Internet. Gli unici dati inviati a Microsoft durante i controlli della connettività di rete sono le informazioni standard sul PC.

Utilizzo delle informazioni

Se i dati vengono inviati a Microsoft, vengono utilizzati solo per fornire lo stato di connettività della rete. Lo stato di connettività della rete viene reso disponibile ad app e funzionalità nel PC che richiedono informazioni sulla connettività della rete. Se si utilizza un'app di terze parti, l'uso delle informazioni sarà soggetto alle procedure relative alla privacy della terza parte.

Scelta e controllo

Questa impostazione è attiva per impostazione predefinita. Un amministratore può disattivarla utilizzando le opzioni Servizi in Strumenti di amministrazione nel Pannello di controllo. Non è consigliabile disattivare questa funzionalità perché potrebbe impedire ad alcune funzionalità di Windows di funzionare correttamente.

[Inizio pagina](#)

Notifiche, app della schermata di blocco e aggiornamenti dei riquadri

Le app di Windows Store possono automaticamente ricevere contenuti e visualizzare notifiche in vari modi. Le notifiche ricevute possono, ad esempio, essere visualizzate in breve nell'angolo dello schermo o in riquadri di app nel caso in cui siano stati aggiunti a

Start. Se lo si desidera, queste notifiche possono inoltre essere ricevute nella schermata di blocco. Nella schermata di blocco può essere visualizzato anche lo stato dettagliato o breve di determinate app. Gli autori di app possono inviare contenuti alle app di Windows Store dell'utente tramite Servizi notifica Push Windows in esecuzione nei server Microsoft oppure le app possono scaricare informazioni direttamente dai server di terze parti.

Notifiche

Scopo della funzionalità

Le app di Windows Store possono fornire su base periodica o in tempo reale informazioni che l'utente visualizzerà come notifiche all'angolo dello schermo.

Informazioni raccolte, elaborate o trasmesse

Nelle notifiche delle app può essere visualizzato testo, immagini o entrambi. Il contenuto delle notifiche può essere fornito localmente dall'app, ad esempio la sveglia di un'app di orologio. Le notifiche possono inoltre essere inviate dal servizio online di un'app tramite Servizi notifica Push Windows, ad esempio l'aggiornamento di un social network. È possibile che le immagini visualizzate nelle notifiche vengano scaricate direttamente da un server specificato dall'autore dell'app. In questo caso, a tale server verranno inviate le informazioni standard sul computer.

Utilizzo delle informazioni

Microsoft utilizza le informazioni delle notifiche esclusivamente per fornire notifiche dalle app all'utente. Tali informazioni possono essere archiviate temporaneamente tramite Servizi notifica Push Windows prima del trasferimento sul PC in uso. Se non è possibile trasferire immediatamente la notifica, questa verrà archiviata solo per alcuni minuti prima di essere eliminata.

Scelta e controllo

È possibile disattivare le notifiche per tutte le app o per singole app nella sezione **Notifiche** di Impostazioni PC. Se si disattivano le notifiche per un'app o si disinstalla un'app, l'autore dell'app potrebbe comunque inviare gli aggiornamenti a Servizi notifica Push Windows, ma tali notifiche non verranno visualizzate sul PC dell'utente.

App della schermata di blocco

Scopo della funzionalità

Alcune app possono visualizzare informazioni di stato e notifiche sullo schermo mentre il PC è bloccato. Anche se non sono in uso, le app della schermata di blocco possono eseguire attività in background, ad esempio la sincronizzazione della posta elettronica.

Informazioni raccolte, elaborate o trasmesse

Le app della schermata di blocco possono ricevere aggiornamenti dello stato dall'autore tramite Servizi notifica Push Windows o direttamente tramite i server dell'autore o di un'altra terza parte. Possono inoltre trasmettere o elaborare altre informazioni non correlate alle notifiche e agli aggiornamenti.

Utilizzo delle informazioni

Windows utilizza le informazioni di stato e delle notifiche fornite dalle app della schermata di blocco per aggiornare tale schermata.

Scelta e controllo

Dopo aver configurato Windows, le app Mail, Calendario e Messaggi sono impostate automaticamente come app della schermata di blocco. È possibile aggiungere o rimuovere queste e altre app dalla schermata di blocco utilizzando Personalizza di Impostazioni PC. È inoltre possibile scegliere che un'app visualizzi costantemente lo stato dettagliato, ad esempio i dettagli del successivo appuntamento del calendario dell'utente, nella schermata di blocco.

È possibile definire se le app della schermata di blocco possono visualizzare notifiche nella schermata di blocco utilizzando Notifiche di Impostazioni PC.

Aggiornamenti dei riquadri

Scopo della funzionalità

Le app di Windows Store possono fornire informazioni su base periodica o in tempo reale, che l'utente visualizzerà come aggiornamenti nei riquadri delle app in Start.

Informazioni raccolte, elaborate o trasmesse

Le app di Windows Store aggiunte a Start possono aggiornare i relativi riquadri con testo, immagini o entrambi. Il contenuto visualizzato nel riquadro di un'app può essere fornito localmente dall'app, scaricato periodicamente da un server specificato dall'autore dell'app o inviato da un servizio online dell'app tramite Servizi notifica Push Windows. Se il contenuto del riquadro viene scaricato direttamente da un server specificato dall'autore dell'app, a tale server verranno inviate le informazioni standard sul computer.

Utilizzo delle informazioni

Microsoft utilizza le informazioni dei riquadri esclusivamente per fornire gli aggiornamenti delle app all'utente. Tali informazioni possono essere archiviate temporaneamente tramite Servizi notifica Push Windows prima del trasferimento sul PC in uso. Se non è possibile trasferire immediatamente l'aggiornamento di un riquadro, questo verrà archiviato solo per alcuni giorni prima di essere eliminato.

Scelta e controllo

Dopo che un'app ha iniziato a ricevere aggiornamenti dei riquadri, è possibile disattivarli selezionando il riquadro dell'app in Start e scegliendo **Disattiva riquadro animato** nei comandi disponibili per l'app. Se si rimuove il riquadro di un'app da Start, i relativi aggiornamenti non verranno visualizzati. Se si disinstalla un'app, l'autore dell'app potrebbe comunque inviare gli aggiornamenti a Servizi notifica Push Windows, ma Tali aggiornamenti non verranno visualizzati sul PC dell'utente.

Per cancellare gli aggiornamenti correnti visualizzati nei riquadri di Start, scorrere rapidamente dal bordo destro o posizionare il puntatore nell'angolo superiore destro di Start, toccare o fare clic su **Impostazioni** e quindi scegliere **Riquadri**. Toccare o fare clic sul pulsante **Cancella** in **Cancella info personali dai miei riquadri**. Gli aggiornamenti dei riquadri forniti dopo la cancellazione degli aggiornamenti correnti continueranno a essere visualizzati.

[Inizio pagina](#)

Ordinazione stampe

Scopo della funzionalità

Ordinazione stampe consente di inviare immagini digitali archiviate nel PC o in un'unità di rete a un servizio di stampa online scelto dall'utente. A seconda del servizio, è possibile mandare in stampa le immagini e riceverle utilizzando tramite posta o in alternativa, è possibile ritirare le stampe da un rivenditore locale.

Informazioni raccolte, elaborate o trasmesse

Se si decide di effettuare un ordine con un servizio di stampa di foto online, le foto digitali vengono inviate tramite Internet al servizio selezionato. Il percorso dei file (che potrebbe includere il nome utente) delle immagini digitali selezionate potrebbe essere inviato al servizio per consentire allo stesso di visualizzare e caricare le immagini. I file delle immagini digitali potrebbero contenere dati sulle immagini archiviati dalla fotocamera, ad esempio data e ora in cui l'immagine è stata scattata o il luogo in cui è stata scattata se la fotocamera dispone di funzionalità GPS. I file potrebbero inoltre contenere informazioni personali (ad esempio, didascalie) che potrebbero essere associate al file attraverso l'utilizzo di app per la gestione delle immagini digitali e di Windows Explorer. Per ulteriori informazioni, vedere più avanti la sezione Proprietà.

Dopo aver selezionato un servizio di stampa di foto online da Ordinazione stampe, l'utente verrà reindirizzato al sito Web del servizio nella finestra Ordinazione stampe. Le informazioni immesse sul sito Web del servizio di stampa di foto online vengono trasmesse al servizio.

Utilizzo delle informazioni

Le informazioni archiviate nei file delle immagini digitali dalla fotocamera potrebbero essere utilizzate dal servizio di stampa di foto online durante il processo di stampa, ad esempio, per regolare il colore o la nitidezza dell'immagine prima della stampa. Le informazioni archiviate dalle app di gestione delle immagini digitali potrebbero essere utilizzate dal servizio di stampa di foto online per stampare didascalie sulla copertina o sul retro della stampa. L'utilizzo di queste informazioni da parte dei servizi di stampa di foto online e di altre informazioni fornite ai servizi, come ad esempio le informazioni immesse sui siti Web, sarà soggetto alle rispettive

procedure relative alla privacy.

Scelta e controllo

È possibile utilizzare Ordinazione stampe per scegliere quali immagini inviare e quale servizio utilizzare per stampare le immagini. Alcune app per la gestione delle immagini potrebbero essere in grado di rimuovere le informazioni personali archiviate prima dell'invio delle immagini da stampare. Potrebbe inoltre essere possibile modificare le proprietà del file per rimuovere le informazioni personali archiviate.

[Inizio pagina](#)

Risoluzione problemi compatibilità programmi

Scopo della funzionalità

Se viene rilevato un problema di incompatibilità per un'app che si tenta di eseguire, Risoluzione problemi compatibilità programmi tenterà di risolverlo.

Informazioni raccolte, elaborate o trasmesse

Se viene rilevato un problema di incompatibilità con un'app che si tenta di eseguire, viene generato un report che include informazioni come ad esempio il nome e la versione dell'app, le impostazioni di compatibilità necessarie e le azioni intraprese con l'app fino a quel momento. I problemi relativi alle app incompatibili vengono segnalati a Microsoft tramite Segnalazione errori Windows o il programma Analisi utilizzo software Windows.

Utilizzo delle informazioni

Le segnalazioni degli errori vengono utilizzate per fornire all'utente risposte ai problemi segnalati per le app. Le risposte contengono collegamenti (se disponibili) al sito Web dell'autore dell'app per poter ulteriori informazioni sulle possibili soluzioni. Le segnalazioni create a causa di errori delle app vengono utilizzate per cercare di determinare quali sono le impostazioni da modificare quando si verificano problemi di compatibilità per le app eseguite in questa versione di Windows. Le informazioni segnalate tramite il programma Analisi utilizzo software vengono utilizzate per

identificare problemi di compatibilità dell'app.

Microsoft non utilizza alcuna informazione raccolta attraverso questa funzionalità per identificare o contattare l'utente, né per inviargli pubblicità mirata.

Scelta e controllo

Per i problemi segnalati tramite Segnalazione errori Windows, la segnalazione di errore viene creata solo quando si seleziona l'opzione per la ricerca di una soluzione online. A meno che l'utente non abbia precedentemente accettato di segnalare i problemi automaticamente per la ricerca di soluzioni, viene chiesto all'utente se desidera inviare la segnalazione errore. Per ulteriori informazioni, vedere la sezione relativa a Segnalazione errori Windows.

Alcuni problemi verranno segnalati automaticamente tramite il programma Analisi utilizzo software Windows se si è scelto di attivarlo. Per ulteriori informazioni, vedere la sezione sul programma Analisi utilizzo software Windows.

[Inizio pagina](#)

Proprietà

Scopo della funzionalità

Le proprietà sono informazioni sui file che consentono di cercare e organizzare rapidamente i file. Alcune proprietà sono intrinseche al file (ad esempio, la dimensione del file) mentre altre potrebbero essere specifiche per un'app o un dispositivo (ad esempio, le impostazioni della fotocamera quando si scatta una foto o i dati sulla posizione registrati dalla fotocamera per la foto).

Informazioni raccolte, elaborate o trasmesse

Il tipo di informazioni archiviate dipende dal tipo di file e app che le utilizzano. Tra le proprietà ci sono il nome di file, data ultima modifica, la dimensione del file, l'autore, le parole chiave e i commenti. Le proprietà vengono archiviate nel file e si spostano insieme al file se questo viene spostato o copiato in un altro percorso, come accade con una condivisione di file o se viene inviato come allegato di un messaggio di posta elettronica.

Utilizzo delle informazioni

Le proprietà consentono di cercare e organizzare velocemente i file. Inoltre possono essere utilizzate dalle app per eseguire attività specifiche per l'app. Nessuna informazione viene inviata a Microsoft.

Scelta e controllo

È possibile modificare o rimuovere alcune proprietà di un file selezionando il file in Windows Explorer e facendo clic su Proprietà. Alcune proprietà, ad esempio data dell'ultima modifica, nome del file e alcune proprietà specifiche per l'app non possono essere rimosse seguendo tale procedura. Per quanto riguarda le proprietà specifiche dell'app, è possibile modificarle se l'app utilizzata per generare il file supporta queste funzionalità.

[Inizio pagina](#)

Prossimità

Servizio prossimità near field

Scopo della funzionalità

Se il PC dispone di hardware near-field communication (NFC), è possibile toccarlo e unirlo a un altro dispositivo con hardware NFC per condividere collegamenti, file e altre informazioni. Esistono due tipi di connessioni di prossimità: Tocca e attiva e Tocca e tieni premuto. Con Tocca e attiva, è possibile creare una connessione a breve o lungo termine tra dispositivi tramite Wi-Fi, Wi-Fi Direct o Bluetooth. Con Tocca e tieni premuto, la connessione è attiva solo fino a quando i dispositivi rimangono in contatto.

Informazioni raccolte, elaborate o trasmesse

Quando vengono toccati e uniti, due dispositivi dotati della funzionalità di prossimità si scambiano informazioni per stabilire una connessione. A seconda del modo in cui sono configurati i dispositivi, questi dati possono includere gli indirizzi di rete Bluetooth e Wi-Fi e il nome del PC.

Dopo che la connessione è stata stabilita, altre informazioni potrebbero essere scambiate tra i dispositivi, a seconda della specifica funzionalità di prossimità o dell'app utilizzata. Windows è

in grado di scambiare file, collegamenti e altre informazioni tra i dispositivi utilizzando una connessione di prossimità. Le app che utilizzano la prossimità sono in grado di inviare e ricevere le informazioni alle quali hanno accesso. Le informazioni potrebbero essere inviate tramite la rete o connessione Internet o direttamente tramite una connessione wireless da dispositivo a dispositivo.

Utilizzo delle informazioni

Le informazioni su rete e PC scambiate tramite una connessione di prossimità vengono utilizzate per stabilire una connessione di rete e per identificare i dispositivi che si connettono tra di loro. I dati trasferiti attraverso una connessione di prossimità avviata all'interno di un'app possono essere utilizzati da tale app in qualsiasi modo. Nessuna informazione viene inviata a Microsoft.

Scelta e controllo

Il servizio di prossimità near field è attivo per impostazione predefinita. Un amministratore può disattivarlo utilizzando le opzioni in Dispositivi e stampanti nel Pannello di controllo.

Tocco e invio

Scopo della funzionalità

Tocco e invio di Windows facilita la condivisione delle informazioni selezionate con gli amici vicini o con un altro dispositivo, come ad esempio un telefono cellulare. Ad esempio, quando l'utente è in un browser, può avviare Tocco e invio dal pannello Dispositivi. Il dispositivo che viene toccato riceverà un collegamento alla pagina Web correntemente visualizzata. Funziona anche con un'app che supporta la condivisione di informazioni, come immagini, testo o file.

Informazioni raccolte, elaborate o trasmesse

Tocco e invio utilizza le informazioni che si stanno condividendo e quelle descritte nella sezione precedente Servizio prossimità near field.

Utilizzo delle informazioni

Tali informazioni vengono utilizzate esclusivamente per stabilire la connessione tra i due dispositivi. Le informazioni condivise non vengono archiviate da Tocco e invio. Nessuna informazione viene

inviata a Microsoft.

Scelta e controllo

Se il servizio di prossimità near field è abilitato, anche Tocco e invio lo sarà. Per ulteriori informazioni, vedere la sezione Servizio prossimità near field.

[Inizio pagina](#)

Connessioni di Accesso remoto

Scopo della funzionalità

Le connessioni di Accesso remoto consentono all'utente di connettersi a reti private utilizzando una connessione a una rete privata virtuale (VPN) e al Servizio di accesso remoto (RAS). RAS è un componente che connette un PC client (generalmente il PC dell'utente) a un PC host (noto anche come server di accesso remoto) utilizzando protocolli standard del settore. Le tecnologie VPN consentono agli utenti di connettersi a una rete privata, come una rete aziendale, tramite Internet.

Un componente delle connessioni Accesso remoto, Connessione remota, consente di accedere a Internet utilizzando un modem per linea telefonica o una tecnologia di banda larga, come ad esempio un modem via cavo o DSL. Connessione remota comprende componenti di connessione come ad esempio client RAS, Connection Manager e RAS Phone, come connessioni della riga di comando come rasdial.

Informazioni raccolte, elaborate o trasmesse

I componenti di connessione raccolgono informazioni dal PC, come ad esempio nome utente, password e nome del dominio. Queste informazioni vengono inviate al sistema al quale l'utente sta tentando di connettersi. Per proteggere la privacy dell'utente e la sicurezza del PC, le informazioni correlate alla sicurezza come nome utente e password vengono crittografate e archiviate nel PC.

Utilizzo delle informazioni

Le informazioni sulla connessione vengono utilizzate per consentire

al PC di connettersi a Internet. Un server di accesso remoto potrebbe conservare il nome utente e le informazioni relative all'indirizzo IP per scopi legati alla contabilità e conformità, ma nessuna informazione verrà inviata a Microsoft.

Scelta e controllo

Per connessioni non della riga di comando, è possibile scegliere di salvare la password selezionando **Salva nome utente e password**. È possibile annullare l'opzione in qualsiasi momento per eliminare la password precedentemente salvata dalla connessione. Poiché tale impostazione è disattivata per impostazione predefinita, potrebbe essere chiesto di fornire la password per connettersi a Internet o a una rete. Per connessioni della riga di comando come rasdial, non è possibile salvare la password.

[Inizio pagina](#)

Connessione RemoteApp e desktop

Scopo della funzionalità

Connessione RemoteApp e desktop consente di accedere ad app e desktop su PC remoti che sono stati resi disponibili online per l'accesso remoto.

Informazioni raccolte, elaborate o trasmesse

Quando si abilita una connessione, i file di configurazione vengono scaricati nel PC dall'URL remoto specificato. Questi file di configurazione si collegano ad app e desktop su PC remoti in modo da poterli eseguire dal proprio PC. Periodicamente il PC cercherà e scaricherà automaticamente aggiornamenti per questi file di configurazione. Le app vengono eseguite su PC remoti e le informazioni immesse vengono trasmesse attraverso la rete ai PC remoti con cui si sceglie di connettersi.

Utilizzo delle informazioni

Gli aggiornamenti per i file di configurazione potrebbero includere modifiche alle impostazioni, ad esempio l'accesso a nuove app. Tuttavia, le nuove app verranno eseguite solo se l'utente sceglie di eseguirle. Questa funzionalità invia inoltre informazioni ai PC remoti

nei quali vengono eseguite le app. L'utilizzo di questi dati da parte delle app remote è soggetto alle pratiche relative alla privacy dei fornitori delle app e degli amministratori dei PC remoti. Nessuna informazione viene inviata a Microsoft.

Scelta e controllo

È possibile scegliere se utilizzare Connessione RemoteApp e desktop. È possibile aggiungere o rimuovere Connessione RemoteApp e desktop andando a Connessione RemoteApp e desktop nel Pannello di controllo. È possibile aggiungere una nuova connessione facendo clic su **Configurare una nuova connessione con Connessione RemoteApp e desktop**, quindi immettere un URL connessione nella finestra di dialogo. È inoltre possibile utilizzare l'indirizzo di posta elettronica per recuperare l'URL di connessione. È possibile rimuovere una connessione e i relativi file di connessione facendo clic su **Rimuovi** nella finestra di dialogo contenente le descrizioni delle connessioni. Se si interrompe una connessione senza chiudere tutte le app aperte, tali app rimarranno aperte nel PC remoto. Connessione RemoteApp e desktop non viene visualizzata nell'elenco Installazione programmi nel Pannello di controllo

[Inizio pagina](#)

Connessione Desktop remoto

Scopo della funzionalità

Connessione Desktop remoto offre un modo per stabilire una connessione remota con un PC host che sta eseguendo Servizi Desktop remoto.

Informazioni raccolte, elaborate o trasmesse

Le impostazioni di Connessione Desktop remoto vengono archiviate in un archivio di app locale o in un file Remote Desktop Protocol (RDP) nel PC. Le impostazioni riportate includono il nome del dominio in uso e le impostazioni di configurazione della connessione, ad esempio il nome del PC remoto, nome utente, informazioni di visualizzazione, informazioni sul dispositivo locale, informazioni audio, Appunti, impostazioni di connessione, nomi di app remote e l'anteprima o l'icona delle sessioni.

Le credenziali per queste connessioni e per Gateway Desktop remoto unitamente a un elenco dei nomi dei server Gateway Desktop remoto vengono archiviati localmente nel PC. Tale elenco viene archiviato in modo permanente a meno che non venga eliminato da un amministratore. Nessuna informazione viene inviata a Microsoft.

Utilizzo delle informazioni

Le informazioni raccolte dalla connessione Desktop remoto consentono all'utente di connettersi a PC host che eseguono Servizi Desktop remoto mediante le impostazioni preferite. Nome utente, password e informazioni sul dominio vengono raccolti per consentire all'utente di salvare le impostazioni di connessione e di fare doppio clic su un file RDP o di selezionare un elemento preferito per avviare la connessione senza dover immettere nuovamente le informazioni.

Scelta e controllo

È possibile scegliere se utilizzare o meno la connessione Desktop remoto. Se si sceglie di utilizzarla, le impostazioni di connessione preferite dei file RDP e di Desktop remoto contengono le informazioni necessarie per connettersi a un PC remoto, tra cui le opzioni e le impostazioni configurate durante il salvataggio automatico della connessione. È possibile personalizzare i file RDP e i preferiti, che includono i file per la connessione allo stesso PC con impostazioni differenti. Per modificare le credenziali salvate, aprire Gestione credenziali in Account utente nel Pannello di controllo.

[Inizio pagina](#)

Accesso con un account Microsoft

Scopo della funzionalità

Un account Microsoft (precedentemente denominato Windows Live ID) è una singola combinazione di indirizzo di posta elettronica e password, utilizzabile come credenziale per l'accesso ad app, siti e servizi forniti da Microsoft e da partner Microsoftt selezionati. Per ottenere un account Microsoft, è possibile effettuare l'iscrizione in Windows o nei siti Web Microsoft che richiedono un account Microsoft per l'accesso.

È possibile scegliere di accedere a Windows con un account Microsoft o di connettere l'account locale o di dominio a un account Microsoft. In questo modo, sarà possibile per Windows sincronizzare automaticamente le impostazioni e le informazioni disponibili in Windows e nelle app Microsoft, al fine di applicare la stessa combinazione di funzionalità e aspetto a tutti i PC utilizzati. Se si passa alla pagina di accesso di questi siti Web, sarà inoltre possibile accedere automaticamente ai siti Web che utilizzano account Microsoft per l'accesso.

Informazioni raccolte, elaborate o trasmesse

Quando si immette un indirizzo di posta elettronica da utilizzare come account Microsoft durante la configurazione del PC oppure nella sezione Utenti di Impostazioni PC, l'indirizzo di posta elettronica viene inviato da Windows a Microsoft per stabilire se esiste già un account Microsoft associato a tale indirizzo. Se si utilizza già l'indirizzo di posta elettronica specificato come account Microsoft, è possibile utilizzarlo insieme alla password per l'account Microsoft per accedere a Windows. Se non sono ancora disponibili informazioni di sicurezza sufficienti per l'account Microsoft, è possibile che vengano innanzitutto richieste ulteriori informazioni per la sicurezza, ad esempio un numero di cellulare utilizzabile per verificare il titolare dell'account in caso di problemi di accesso. Se non si dispone di un account Microsoft, è possibile crearne uno utilizzando qualsiasi indirizzo di posta elettronica.

Ogni volta che si accede a Windows con un account Microsoft mentre il PC è connesso a Internet, Windows verifica l'indirizzo di posta elettronica e la password nei server Microsoft. Se si accede a Windows con un account Microsoft o si accede con un account di dominio connesso a un account Microsoft:

- Determinate impostazioni di Windows verranno sincronizzate tra tutti i PC a cui si accede con un account Microsoft. Per ulteriori informazioni sulle impostazioni sincronizzate e su come controllarle, vedere la sezione Sincronizzazione delle impostazioni.
- Le app Microsoft in cui viene utilizzato un account Microsoft per l'autenticazione, ad esempio Mail, Calendario, Foto, Contatti,

Messaggi, OneDrive, Microsoft Office e altre app, possono avviare automaticamente il download delle informazioni dell'utente. L'app Mail, ad esempio, scaricherà automaticamente i messaggi inviati al proprio indirizzo Outlook.com oppure Hotmail.com, se disponibile.

- I Web browser possono connettersi automaticamente ai siti Web accessibili con l'account Microsoft. Se si visita OneDrive.com, ad esempio, sarà possibile effettuare l'accesso automaticamente senza immettere di nuovo la password dell'account Microsoft.

Prima di consentire ad app di terze parti di utilizzare le informazioni del profilo o altre informazioni personali associate all'account Microsoft, in Windows verrà richiesta l'autorizzazione dell'utente. Se si accede a Windows con un account di dominio connesso a un account Microsoft, le impostazioni e le informazioni selezionate verranno sincronizzate con l'account di dominio e si potrà accedere automaticamente alle app e ai siti Web come indicato in precedenza. Poiché gli amministratori di dominio possono accedere a tutte le informazioni disponibili nel PC dell'utente, sono in grado di accedere anche a tutte le impostazioni e informazioni che si è scelto di sincronizzare con gli altri PC tramite l'account Microsoft. Sono incluse impostazioni quali nome, immagine dell'account e cronologia del browser. Per ulteriori informazioni sulle impostazioni sincronizzate e su come controllarle, vedere la sezione Sincronizzazione delle impostazioni.

Utilizzo delle informazioni

Se si crea un nuovo account Microsoft in Windows, le informazioni fornite verranno utilizzate per creare e proteggere l'account. Le informazioni sulla sicurezza specificate, ad esempio il numero di telefono o l'indirizzo di posta elettronica alternativo, vengono utilizzate esclusivamente se non è possibile accedere all'account personale. Se l'utente effettua l'accesso a Windows con un account Microsoft, le informazioni dell'account Microsoft verranno utilizzate da Windows per accedere automaticamente ad app e siti Web. Per ulteriori informazioni su come il possesso di un account Microsoft influisce sulla privacy degli utenti, leggere [l'informativa sulla privacy](#)

visualizzata quando si sceglie Iscriviti per un nuovo indirizzo e-mail. Per informazioni sulla modalità con cui le singole app Microsoft utilizzano le informazioni associate all'account Microsoft, vedere le informative sulla privacy delle singole app. L'informativa sulla privacy di un'app Microsoft specifica può essere visualizzata nell'accesso alle impostazioni o nella finestra di dialogo Informazioni su dell'app.

Scelta e controllo

Quando si accede a Windows con un account Microsoft, alcune impostazioni vengono sincronizzate automaticamente. Per informazioni su come modificare le impostazioni di Windows sincronizzate o come interrompere la sincronizzazione, vedere la sezione Sincronizzazione delle impostazioni. Per ulteriori informazioni sui dati raccolti dalle app Microsoft che utilizzano un account Microsoft per l'autenticazione, leggere le informative sulla privacy corrispondenti. Le informative sulla privacy per le app Windows Live (Mail, Calendario, Foto, Contatti, Messaggi, OneDrive) sono disponibili all'indirizzo go.microsoft.com/fwlink/?LinkId=257483, mentre quelle per Microsoft Office sono disponibili all'indirizzo go.microsoft.com/fwlink/?LinkId=257484. L'informativa sulla privacy di un'app specifica può essere visualizzata anche nell'accesso alle impostazioni o nella finestra di dialogo Informazioni su dell'app.

Non è necessario accedere a Windows con un account Microsoft. Quando si aggiunge un utente al PC durante la configurazione oppure nella sezione **Utenti** di Impostazioni PC, è possibile scegliere di utilizzare un account locale o un account Microsoft. È possibile modificare la scelta tra account locale e account Microsoft in qualsiasi momento nella sezione **Utenti** di Impostazioni PC. Se si accede a Windows con un account di dominio, è possibile connettere o disconnettere l'account Microsoft in qualsiasi momento nella sezione **Utenti** di Impostazioni PC.

Quando si utilizza InPrivate Browsing in Internet Explorer, non viene eseguito automaticamente l'accesso ai siti Web che utilizzano account Microsoft.

[Inizio pagina](#)

Sincronizzazione delle impostazioni

Scopo della funzionalità

Se si accede a Windows con un account Microsoft, alcune impostazioni e informazioni dell'utente vengono automaticamente sincronizzate da Windows con i server Microsoft per consentire un'esperienza personalizzata in più PC. Se si accede a più PC con un account Microsoft, la prima volta che si effettua l'accesso a un altro PC con lo stesso account Microsoft, le impostazioni e le informazioni che si è scelto di sincronizzare dagli altri PC vengono scaricate e applicate automaticamente da Windows. Le impostazioni che si sceglie di sincronizzare vengono automaticamente aggiornate nei server Microsoft e negli altri PC dell'utente a mano a mano che vengono utilizzati.

Informazioni raccolte, elaborate o trasmesse

Se si sceglie di accedere a Windows con un account Microsoft, Windows sincronizza alcune impostazioni con i server Microsoft. Queste impostazioni includono:

- Preferenze lingua
- Preferenze di Accessibilità
- Impostazioni di personalizzazione come l'immagine dell'account, l'immagine della schermata di blocco, lo sfondo e le impostazioni del mouse
- Impostazioni per le app di Windows Store
- Dizionari del correttore ortografico e IME
- Cronologia e Preferiti del Web browser
- Password salvate per app, siti Web e rete

Per proteggere la privacy dell'utente, tutte le impostazioni sincronizzate vengono inviate in forma crittografata tramite SSL. Alcune di queste impostazioni non verranno sincronizzate nel PC finché quest'ultimo non verrà aggiunto all'account Microsoft come PC attendibile.

Se si accede a Windows con un account di dominio connesso a un account Microsoft, le impostazioni e le informazioni selezionate

verranno sincronizzate con l'account di dominio. Le password salvate dopo avere effettuato l'accesso a Windows con un account di dominio connesso a un account Microsoft non vengono mai sincronizzate. Poiché gli amministratori di dominio possono accedere a tutte le informazioni disponibili nel PC dell'utente, sono in grado di accedere anche a tutte le impostazioni e informazioni, inclusa la cronologia delle esplorazioni, che si è scelto di sincronizzare con gli altri PC tramite l'account Microsoft.

Utilizzo delle informazioni

Windows 8 utilizza queste impostazioni e informazioni per fornire il servizio di sincronizzazione. Microsoft non utilizza le informazioni e le impostazioni sincronizzate per identificare o contattare l'utente, né per inviargli pubblicità mirata.

Scelta e controllo

Quando si accede a Windows con un account Microsoft, la funzionalità di sincronizzazione delle impostazioni verrà attivata. Per scegliere di sincronizzare le impostazioni e determinare quali impostazioni sincronizzare, è possibile accedere a **Sincronizzazione delle impostazioni** in Impostazioni PC. Se si accede a Windows con un account di dominio e si sceglie di connettere tale account a un account Microsoft, verrà richiesto in Windows di specificare quali impostazioni si desidera sincronizzare prima di connettere l'account Microsoft.

[Inizio pagina](#)

Teredo Technology

Scopo della funzionalità

Teredo Technology (Teredo) consente a PC e reti di comunicare su più protocolli di rete.

Informazioni raccolte, elaborate o trasmesse

A ogni avvio del PC, Teredo tenterà di individuare un servizio del protocollo Internet versione 6 (IPv6) pubblico su Internet.

L'operazione viene eseguita automaticamente quando il PC è connesso a una rete pubblica o privata, ma non su reti gestite, quali

domini aziendali. Se si utilizza un'app per cui è necessario che Teredo utilizzi la connettività IPv6 o se si configura il firewall affinché abiliti sempre la connettività IPv6, Teredo contatterà periodicamente il servizio Teredo di Microsoft su Internet. Le uniche informazioni inviate a Microsoft sono informazioni su PC standard e il nome del servizio richiesto (ad esempio, teredo.ipv6.microsoft.com).

Utilizzo delle informazioni

Le informazioni inviate dal PC tramite Teredo vengono utilizzate per stabilire se il PC in uso è connesso a Internet e se è possibile individuare un servizio IPv6 pubblico. Una volta individuato il servizio, le informazioni vengono inviate per mantenere una connessione con il servizio IPv6.

Scelta e controllo

Utilizzando lo strumento dalla riga di comando netsh, è invece possibile modificare la query che il servizio invia tramite Internet per utilizzare server non Microsoft o è possibile disattivarla. Per istruzioni dettagliate, consultare la sezione relativa al protocollo Internet versione 6, Teredo e tecnologie relative di questo white paper tecnico.

[Inizio pagina](#)

Servizi Trusted Platform Module (TPM)

Scopo della funzionalità

Il modulo Trusted Platform Module (TPM) è un hardware di sicurezza integrato in alcuni PC che, se presente e sottoposto a provisioning, consente al PC di usufruire di funzionalità di sicurezza avanzate. Tra le funzionalità Windows che utilizzano il TPM sono inclusi Crittografia unità BitLocker, Smart card virtuale, Avvio protetto, Windows Defender e TPM Based Certificate Storage.

Informazioni raccolte, elaborate o trasmesse

Per impostazione predefinita, Windows diventa proprietario del TPM e archivia le informazioni complete di autorizzazione per il proprietario del TPM, in modo che siano disponibili solo per gli amministratori Windows. I valori di autorizzazione limitata vengono

creati per eseguire azioni amministrative tipiche e azioni di utenti standard. Inoltre sono gestiti da Windows.

La console di gestione TPM consente all'utente di effettuare il provisioning in modo interattivo e di salvare il valore di autorizzazione del proprietario del TPM in supporti esterni, quali un'unità flash USB, dopo che il TPM sia stato sottoposto a provisioning. Un file salvato contiene informazioni di autorizzazione per il proprietario del TPM per il TPM. Il file contiene inoltre informazioni relative al nome del PC, alla versione del sistema operativo, all'utente e alla data di creazione, per assistere l'utente nel riconoscimento del file.

In un ambiente di dominio, la password completa del proprietario del TPM può essere configurata dall'amministratore del dominio per l'archiviazione in Active Directory in un oggetto del TPM durante il provisioning del TPM.

Ciascun TPM dispone di una chiave di verifica dell'autenticità crittografica e univoca, utilizzata per indicare l'autenticità. La chiave di verifica dell'autenticità può essere creata e archiviata nel TPM dal produttore del PC oppure per i PC meno recenti e Windows potrebbe dover attivare la creazione della chiave di verifica dell'autenticità nel TPM. La parte privata della chiave di verifica dell'autenticità non è mai esposta all'esterno del TPM e una volta creata, solitamente, non è possibile reimpostarla. Un certificato della chiave di verifica dell'autenticità verrà archiviato nel TPM della maggior parte dei computer Windows 8. Il certificato della chiave di verifica dell'autenticità indica che nel TPM di un hardware esiste una chiave di verifica dell'autenticità. Il certificato è utile agli utenti che verificano da remoto la conformità del TPM alle specifiche del TPM. Il certificato della chiave di verifica dell'autenticità è solitamente firmato dal produttore del TPM o della piattaforma.

Utilizzo delle informazioni

Una volta inizializzato, il TPM può essere utilizzato dalle app per creare e proteggere ulteriori chiavi crittografiche univoche. Ad esempio, Crittografia unità BitLocker utilizza il TPM per proteggere la chiave che consente di crittografare l'unità.

Se si sceglie di salvare la password del proprietario del TPM in un

file, il PC aggiuntivo e le informazioni relative all'utente salvate nel file consentono all'utente di identificare il PC e il TPM corrispondenti. La chiave di verifica dell'autenticità del TPM viene utilizzata da Windows durante l'inizializzazione del TPM per crittografare il valore di autorizzazione del proprietario del TPM prima di inviarlo al TPM. Windows non trasmette chiavi crittografiche all'esterno del PC. Windows fornisce un'interfaccia per app di terze parti come software antimalware per utilizzare la chiave di verifica dell'autenticità per determinati scenari del TPM, ad esempio per l'avvio di misurazioni con attestazione. Per software antimalware, la chiave di verifica dell'autenticità e il certificato della chiave di verifica dell'autenticità sono utili per confermare che le misurazioni di avvio siano fornite tramite TPM da un produttore specifico. Per impostazione predefinita, solo gli amministratori o le app con diritti amministrativi possono utilizzare la chiave di verifica dell'autenticità del TPM.

Scelta e controllo

Gli utenti o amministratori acconsentono all'utilizzo del TPM attivando una funzionalità Windows o eseguendo un'app che utilizza il TPM.

È possibile scegliere di cancellare il TPM e di reimpostarlo alle impostazioni di fabbrica. Cancellando il TPM vengono rimosse le informazioni sul proprietario così come tutte le chiavi basate sul TPM, ad eccezione della chiave di verifica dell'autenticità, o le informazioni crittografiche che le app potrebbero aver creato quando il TPM era in uso.

[Inizio pagina](#)

Aggiornamento dei certificati radice

Scopo della funzionalità

I certificati vengono utilizzati principalmente per verificare l'identità di una persona o di un dispositivo, autenticare un servizio o crittografare file. Le autorità di certificazione radice attendibili sono organizzazioni che emettono certificati. La funzionalità di aggiornamento dei certificati radice consente di contattare il servizio Windows Update online per verificare se Microsoft ha aggiunto un'autorità di certificazione al proprio elenco di autorità attendibili,

ma solo quando per un'app viene visualizzato un certificato emesso da un'autorità di certificazione non direttamente attendibile (un certificato che non è archiviato in un elenco di certificati attendibili sul PC). Se l'autorità di certificazione è stata aggiunta all'elenco Microsoft delle autorità attendibili, il certificato verrà aggiunto automaticamente all'elenco dei certificati attendibili sul PC.

Informazioni raccolte, elaborate o trasmesse

La funzionalità di aggiornamento dei certificati radice consente di inviare una richiesta al servizio Windows Update online che richiede l'elenco corrente delle autorità di certificazione radice nel programma Microsoft Root Certificate. Se in elenco sono presenti certificati non attendibili, la funzionalità di aggiornamento dei certificati radice ne ottiene il certificato da Windows Update e lo inserisce nell'archivio dei certificati attendibili sul PC. Le informazioni trasferite includono nomi e hash di crittografia dei certificati radice.

Per ulteriori informazioni sul rapporto tra privacy dell'utente e Windows Update, vedere l' [Informativa sulla privacy relativa ai servizi di aggiornamento](#).

Utilizzo delle informazioni

Le informazioni vengono utilizzate da Microsoft per aggiornare l'elenco dei certificati attendibili sul PC. Microsoft non utilizza le informazioni e le impostazioni per identificare o contattare l'utente, né per inviargli pubblicità mirata.

Scelta e controllo

La funzionalità di aggiornamento dei certificati radice è attiva per impostazione predefinita. Gli amministratori possono configurare Criteri di gruppo per disattivare la funzionalità di aggiornamento dei certificati radice su un PC.

[Inizio pagina](#)

Servizi di aggiornamento

Scopo della funzionalità

I servizi di aggiornamento per Windows includono Windows Update

e Microsoft Update:

- **Windows Update** è un servizio che fornisce aggiornamenti software per Windows e altri programmi software di supporto, ad esempio i driver forniti dai produttori di dispositivi.
- **Microsoft Update** è un servizio che fornisce aggiornamenti software per Windows, nonché per altri programmi software Microsoft come ad esempio Microsoft Office.

Informazioni raccolte, elaborate o trasmesse

Se si sceglie di ottenere importanti aggiornamenti software per PC, è possibile che lo Strumento di rimozione malware per Windows sia incluso con gli aggiornamenti. Questo strumento controlla il PC per rilevare eventuali infezioni da parte di malware specifico e agevolare la rimozione di tali infezioni. Se viene eseguito, vengono rimossi i [malware elencati](#) nel sito Web del Supporto tecnico Microsoft.

Durante una verifica del malware, verrà inviato a Microsoft un rapporto contenente informazioni specifiche sul malware rilevato, sugli errori e sul PC. Per ulteriori informazioni, leggere l' [Informativa sulla privacy dello Strumento di rimozione malware per Windows](#) .

Per informazioni su altri dati raccolti da Update Services, vedere l' [Informativa sulla privacy relativa ai servizi di aggiornamento](#).

Utilizzo delle informazioni

Le informazioni dello Strumento di rimozione malware per Microsoft Windows vengono utilizzate per migliorare i prodotti e i servizi antimalware e quelli relativi alla sicurezza di Microsoft. Nessuna informazione presente nei report dello Strumento di rimozione malware per Microsoft Windows verrà utilizzata per identificare o contattare l'utente.

Per informazioni sulla modalità di utilizzo di altre informazioni da parte di Update Services, vedere l' [Informativa sulla privacy relativa ai servizi di aggiornamento](#).

Scelta e controllo

Se si scelgono impostazioni rapide durante la configurazione di Windows, si attiva Update Services e si imposta Windows Update per l'installazione automatica degli aggiornamenti. Se si sceglie di

personalizzare le impostazioni, è possibile controllare Update Services in **Windows Update** in **Contribuisci a proteggere e aggiornare il PC**. Dopo l'installazione di Windows, è possibile modificare le impostazioni per Update Services nel Pannello di controllo. Per ulteriori informazioni, vedere l'Informativa sulla privacy di Update Services.

Se si è scelto di cercare e installare gli aggiornamenti importanti e ricevere lo Strumento di rimozione malware per Microsoft Windows come parte di questi aggiornamenti per il PC, è possibile disattivare le funzionalità di segnalazione dello strumento attenendosi alle [istruzioni](#) disponibili nel Supporto tecnico Microsoft.

[Inizio pagina](#)

Analisi utilizzo software Windows

Scopo della funzionalità

Il programma Analisi utilizzo software Windows può raccogliere informazioni sulla modalità con cui l'utente usa le app, i PC, i dispositivi connessi e Windows. Può inoltre raccogliere informazioni sugli eventuali problemi di prestazioni e affidabilità. Se si sceglie di partecipare ad Analisi utilizzo software Windows, Windows invierà tali dati a Microsoft e scaricherà periodicamente un file per raccogliere informazioni più rilevanti sulla modalità di utilizzo di Windows e delle app. I rapporti di Analisi utilizzo software vengono inviati a Microsoft per contribuire a migliorare le funzionalità utilizzate più spesso dai clienti e per creare soluzioni per i problemi comuni.

Informazioni raccolte, elaborate o trasmesse

Nei report di Analisi utilizzo software possono essere incluse informazioni quali:

- Informazioni di configurazione. Ad esempio il numero di processori presenti nel PC, il numero di connessioni di rete in uso, le risoluzioni dello schermo per i dispositivi di visualizzazione e la versione di Windows in esecuzione.
- Informazioni su prestazioni e affidabilità, ad esempio la velocità

con cui una determinata app risponde quando si fa clic su un pulsante, il numero dei problemi riscontrati con un'app o un dispositivo specifico e la velocità di invio o ricezione delle informazioni su una connessione di rete.

- Informazioni sull'utilizzo delle app, ad esempio le funzionalità utilizzate più spesso, la frequenza di apertura delle app, la frequenza di utilizzo di Guida e supporto tecnico di Windows, i servizi utilizzati per accedere alle app e il numero di cartelle generalmente create sul desktop.

I rapporti di Analisi utilizzo software contengono inoltre informazioni sugli eventi (dati del registro eventi) del PC che si sono verificati fino a un massimo di sette giorni prima della data in cui si decide di partecipare al programma. Dato che la maggior parte degli utenti decide di partecipare ad Analisi utilizzo software entro diversi giorni dalla configurazione di Windows, Microsoft utilizza queste informazioni per analizzare e migliorare l'esperienza di configurazione di Windows.

Queste informazioni vengono inviate a Microsoft quando è disponibile una connessione a Internet. I report di Analisi utilizzo software non contengono intenzionalmente informazioni di contatto, quali nome, indirizzo o numero di telefono. Alcuni report, tuttavia, potrebbero involontariamente contenere identificatori individuali, ad esempio il numero di serie di un dispositivo connesso al PC. Microsoft filtra le informazioni contenute nei report di Analisi utilizzo software per tentare di rimuovere eventuali identificatori individuali contenuti.

Analisi utilizzo software genera un numero casuale denominato identificatore univoco globale (GUID, Globally Unique Identifier), che viene inviato a Microsoft con ogni report di Analisi utilizzo software. Il GUID consente a Microsoft di determinare quali dati vengono inviati da un computer specifico nel tempo. Le app Microsoft preinstallate e concesse in licenza con Windows possono creare propri identificatori univoci, da utilizzare con Analisi utilizzo software Windows, che potrebbero essere basati sulle informazioni dell'account Microsoft dell'utente.

Inoltre, Analisi utilizzo software Windows scarica periodicamente un

file per raccogliere informazioni più rilevanti sulla modalità di utilizzo di Windows e delle app. Tale file consente a Windows di raccogliere ulteriori informazioni per aiutare Microsoft a trovare soluzioni per i problemi più comuni e a comprendere in modo più preciso gli schemi di utilizzo di Windows e delle app.

Utilizzo delle informazioni

Microsoft utilizza le informazioni di Analisi utilizzo software per migliorare i propri prodotti e servizi, oltre ai componenti hardware e software di terze parti progettati per l'uso con tali prodotti e servizi. Le informazioni di Analisi utilizzo software potrebbero essere inoltre condivise con i partner Microsoft, affinché possano migliorare i propri prodotti e servizi, ma si tratta di informazioni condivise in forma aggregata e non possono essere utilizzate per identificare o contattare l'utente, né per inviargli pubblicità mirata.

Il GUID viene utilizzato per determinare quanto siano diffusi i commenti e suggerimenti ricevuti e come classificarli in ordine di priorità. Ad esempio, tramite il GUID Microsoft è in grado di distinguere un cliente che riscontra un problema centinaia di volte da cento clienti che riscontrano lo stesso problema una sola volta. Microsoft non utilizza le informazioni raccolte da Analisi utilizzo software per identificare o contattare l'utente.

Scelta e controllo

Se si scelgono impostazioni rapide durante la configurazione di Windows, viene attivato il programma Analisi utilizzo software Windows, pertanto Windows e le app Microsoft concesse in licenza con Windows saranno in grado di inviare rapporti di Analisi utilizzo software per tutti gli utenti del PC. Se si sceglie di personalizzare le impostazioni, è possibile controllare Analisi utilizzo software selezionando **Contribuisci a migliorare il software e i servizi Microsoft partecipando ad Analisi utilizzo software** in **Invia info a Microsoft per contribuire a migliorare Windows e le app**. Dopo la configurazione di Windows gli amministratori possono modificare questa impostazione nella sezione Centro operativo del Pannello di controllo.

Per ulteriori informazioni, vedere le [domande frequenti relative ad Analisi utilizzo software](#) online.

Windows Defender

Windows Defender esegue la ricerca di malware e altro software potenzialmente indesiderato nel PC in uso. Include le funzionalità Microsoft Active Protection Service e Cronologia

Microsoft Active Protection Service

Scopo della funzionalità

Microsoft Active Protection Service (MAPS) è una community antimalware volontaria a livello mondiale che include utenti di Windows Defender. Tramite MAPS, gli utenti possono inviare a Microsoft informazioni su malware e altro software potenzialmente indesiderato in un report. MAPS può contribuire alla protezione del PC scaricando automaticamente nuove firme per il malware più recente.

Informazioni raccolte, elaborate o trasmesse

I report MAPS includono informazioni sui file di malware potenziale, ad esempio nomi di file, hash di crittografia, autore del software, dimensione e indicatore di data. Il servizio MAPS potrebbe inoltre raccogliere URL completi per indicare l'origine dei file. Questi URL potrebbero occasionalmente contenere informazioni personali, come termini di ricerca o dati immessi nei moduli. I report potrebbero inoltre includere le azioni eseguite dopo aver ricevuto notifica da Windows Defender del rilevamento di software potenzialmente indesiderato. Il servizio MAPS include queste informazioni per consentire a Microsoft di misurare l'efficacia con cui Windows Defender rileva e rimuove malware o software potenzialmente indesiderato e tenta di identificare il nuovo malware.

I report vengono automaticamente inviati a Microsoft nei casi seguenti:

- Windows Defender rileva la presenza di software non ancora analizzato per i rischi.
- Windows Defender rileva la presenza di modifiche apportate al PC da software non ancora analizzato per i rischi.

- Windows Defender intraprende azioni sul malware al momento del rilevamento (come parte del suo processo di monitoraggio e aggiornamento automatico).
- Windows Defender completa un'analisi pianificata e intraprende automaticamente azioni sul software rilevato, in base alle impostazioni.

È possibile partecipare a MAPS come membri base o avanzati. Se si sceglie di abilitare MAPS durante la configurazione di Windows, si parteciperà come membri base. I report dei membri base contengono le informazioni descritte in questa sezione. I report dei membri avanzati sono più completi e potrebbero talvolta includere informazioni personali, quali percorsi di file e dump della memoria parziali. Questi report, unitamente a quelli di altri utenti di Windows Defender che partecipano a MAPS, sono utili ai ricercatori Microsoft per scoprire nuove minacce più rapidamente. Vengono quindi create definizioni di malware e tali definizioni aggiornate vengono rese disponibili a tutti gli utenti tramite Windows Update.

Se l'utente partecipa a MAPS come membro base o avanzato:

- Microsoft potrebbe richiedere un report di invio file, contenente file specifici del PC che Microsoft sospetta essere software potenzialmente indesiderato. Tale report viene utilizzato per approfondire l'analisi. All'utente verrà ogni volta chiesto se si desidera inviare questo report di invio file a Microsoft..
- Se per qualche tempo Windows Update non è riuscito a ottenere firme aggiornate per Windows Defender, Windows Defender tenterà di utilizzare MAPS per scaricare le firme da una posizione di download alternativa.

Per proteggere la privacy dell'utente, tutte le informazioni inviate a MAPS vengono crittografate tramite SSL.

Utilizzo delle informazioni

I report inviati a MAPS vengono utilizzati per migliorare il software e i servizi Microsoft. I report potrebbero anche essere utilizzati per fini statistici, di test o di analisi e per la generazione di definizioni. Il servizio MAPS non raccoglie intenzionalmente informazioni personali.

Se MAPS dovesse raccogliere accidentalmente informazioni personali, Microsoft non utilizzerà tali informazioni per identificare o contattare l'utente, né per inviargli pubblicità mirata.

Scelta e controllo

Se si scelgono impostazioni rapide durante la configurazione di Windows, viene attivato MAPS. Se si sceglie di personalizzare le impostazioni, è possibile controllare MAPS selezionando **Partecipa a Microsoft Active Protection Service (MAPS) per aiutare Microsoft a proteggermi da app dannose e malware** in **Invia info a Microsoft per contribuire a migliorare Windows e le app**. Dopo la configurazione di Windows è possibile modificare il tipo di appartenenza o le impostazioni di MAPS, ed eventualmente disattivare il servizio, tramite il menu Strumenti di Windows Defender.

Funzionalità di cronologia

Scopo della funzionalità

La funzionalità di cronologia fornisce un elenco di tutte le app del PC rilevate da Windows Defender, nonché delle azioni intraprese al momento del rilevamento.

È possibile anche visualizzare un elenco delle app non monitorate da Windows Defender durante la loro esecuzione nel PC (elementi consentiti). È inoltre possibile visualizzare le app la cui esecuzione non è consentita da Windows Defender finché non si sceglie di rimuoverle o di consentire nuovamente loro l'esecuzione (prendono il nome di elementi in quarantena).

Informazioni raccolte, elaborate o trasmesse

L'elenco dei programmi software rilevati da Windows Defender, le azioni intraprese dagli utenti e quelle intraprese da Windows Defender vengono automaticamente archiviati nel PC. Tutti gli utenti possono visualizzare la cronologia in Windows Defender per vedere i tentativi di installazione o esecuzione, anche da parte di un altro utente, di malware e altro software potenzialmente indesiderato. Ad esempio, in caso di minaccia da parte di un nuovo malware, è possibile verificare la cronologia per vedere se Windows Defender ha evitato che il PC venisse infettato. Nessuna informazione viene

inviata a Microsoft.

Scelta e controllo

Gli elenchi di cronologia possono essere eliminati da un amministratore.

[Inizio pagina](#)

Segnalazione errori Windows

Scopo della funzionalità

Segnalazione errori Windows consente a Microsoft e ai partner Microsoft di diagnosticare i problemi che si verificano nel software in uso e fornire soluzioni. Le soluzioni non sono disponibili per tutti i problemi, ma quando lo sono vengono offerte come procedure per la risoluzione del problema segnalato o come aggiornamenti da installare. Per prevenire i problemi e rendere il software più affidabile, alcune soluzioni sono inoltre incluse nei Service Pack e nelle future versioni del software.

Informazioni raccolte, elaborate o trasmesse

Molti prodotti software sono progettati per interagire con Segnalazione errori Windows. Se si verifica un problema in uno di questi prodotti, potrebbe venire richiesto se si desidera segnalarlo.

Segnalazione errori Windows raccoglie informazioni utili per diagnosticare e risolvere un problema, ad esempio in quale parte del software o dell'hardware si è verificato il problema, il tipo o la gravità del problema, i file che ne agevolano la descrizione, informazioni di base sul software e l'hardware o possibili problemi relativi alle prestazioni e alla compatibilità del software. Se si utilizza Windows per ospitare macchine virtuali, le segnalazioni degli errori inviate a Microsoft potrebbero includere informazioni sulle macchine virtuali.

Segnalazione errori Windows raccoglie inoltre informazioni su app, driver e dispositivi per aiutare Microsoft a comprendere e risolvere i problemi di compatibilità di app e dispositivi. Le informazioni sulle app possono includere i nomi dei relativi file eseguibili. Le informazioni su dispositivi e driver possono includere i nomi dei dispositivi installati nel PC e i file eseguibili associati ai driver di tali

dispositivi. Potrebbero essere raccolte informazioni sulla società che ha pubblicato un'app o un driver.

Se si sceglie di abilitare la segnalazione automatica durante l'installazione di Windows, il servizio di segnalazione invierà automaticamente informazioni di base sulla posizione in cui si verificano gli errori. Alcune segnalazioni errori potrebbero contenere involontariamente informazioni personali. Una segnalazione che contiene uno snapshot della memoria del PC, ad esempio, potrebbe includere il nome dell'utente, parte di un documento in uso o dati recentemente inviati a un sito Web. Se è probabile che una segnalazione contenga questo tipo di informazioni, Windows chiederà all'utente se desidera inviare le informazioni, anche se è stata abilitata la segnalazione automatica. Le segnalazioni che includono file e dati potrebbero essere archiviate nel PC fino all'invio o all'eliminazione.

Dopo l'invio di una segnalazione, il servizio di segnalazione potrebbe richiedere ulteriori informazioni sul problema che si è verificato. Se si sceglie di fornire numero di telefono o indirizzo di posta elettronica in queste informazioni, la segnalazione di errore consentirà l'identificazione personale Microsoft potrebbe contattare l'utente per richiedere informazioni aggiuntive per facilitare la risoluzione del problema segnalato.

Segnalazione errori Windows genera un numero casuale denominato identificatore univoco globale (GUID, Globally Unique Identifier) che viene inviato a Microsoft con ogni segnalazione errori. Il GUID consente a Microsoft di determinare quali dati vengono inviati da un computer specifico nel tempo. Tale GUID non contiene informazioni personali.

Per proteggere la privacy dell'utente, le informazioni inviate vengono crittografate tramite SSL.

Utilizzo delle informazioni

Microsoft utilizza le informazioni sugli errori e sui problemi inviati dagli utenti di Windows per migliorare i prodotti e i servizi Microsoft, nonché i componenti hardware e software di terze parti progettati per l'uso con tali prodotti e servizi. Il GUID viene utilizzato per determinare quanto siano diffusi i commenti e i suggerimenti ricevuti

da Microsoft e come classificarli in ordine di priorità. Ad esempio, tramite il GUID Microsoft è in grado di distinguere un cliente che riscontra un problema centinaia di volte da cento clienti che riscontrano lo stesso problema una sola volta.

Microsoft può consentire ai propri dipendenti, collaboratori, fornitori e partner di accedere a parti rilevanti delle informazioni raccolte, ma essi sono autorizzati a utilizzare le informazioni esclusivamente per riparare o migliorare i prodotti e i servizi Microsoft o il software e l'hardware di terze parti progettati per l'uso con prodotti e servizi Microsoft. Se una segnalazione di errore contiene informazioni personali, Microsoft non utilizza tali informazioni per identificare o contattare l'utente, né per inviargli pubblicità mirata. Se si sceglie di inviare informazioni di contatto come descritto in precedenza, tuttavia, Microsoft potrebbe utilizzare tali informazioni per contattare l'utente.

Scelta e controllo

Se si scelgono impostazioni rapide durante la configurazione di Windows, Segnalazione errori Windows invierà automaticamente le segnalazioni di base per controllare se sono disponibili soluzioni ai problemi online. Se si sceglie di personalizzare le impostazioni, è possibile controllare Segnalazione errori Windows, selezionando **Utilizza Segnalazione errori Windows per cercare soluzioni a problemi** in **Cerca soluzioni ai problemi online**. Dopo la configurazione di Windows è possibile modificare questa impostazione nella sezione Centro operativo del Pannello di controllo.

Per ulteriori informazioni, vedere le [Informativa sulla privacy del servizio Segnalazione errori Microsoft](#) .

[Inizio pagina](#)

Associazione file di Windows

Scopo della funzionalità

Associazione file di Windows consente agli utenti di associare tipi di file ad app specifiche. Se si tenta di aprire un tipo di file a cui non è associata nessuna app, Windows richiederà all'utente se preferisce utilizzare Associazione file di Windows per individuare un'app per il

file, che include la ricerca di un'app compatibile in Windows Store. Verranno visualizzate le app solitamente associate all'estensione di file.

Informazioni raccolte, elaborate o trasmesse

Se si sceglie di utilizzare Associazione file di Windows, l'estensione di file (ad esempio, docx o pdf) e la lingua di visualizzazione del PC vengono inviati a Microsoft. La parte rimanente del nome del file non viene inviata a Microsoft. Quando si esegue un'associazione di file con una determinata app, viene inviato un identificatore univoco dell'app per identificare l'app predefinita per ciascun tipo di file.

Utilizzo delle informazioni

Quando si invia un'estensione di file, il servizio restituisce un elenco di tutte le app conosciute da Microsoft in grado di aprire file con tali estensioni. A meno che non si scelga di scaricare e installare un'app, le associazioni dei tipi di file non cambieranno.

Scelta e controllo

Quando si tenta di aprire un tipo di file senza un'app associata, è possibile scegliere se utilizzare Associazione file di Windows. Nessuna informazione sull'associazione di file viene inviata a Microsoft a meno che non si decida di utilizzare il servizio.

[Inizio pagina](#)

Guida di Windows

Guida online e supporto tecnico di Windows

Scopo della funzionalità

Guida online e supporto tecnico di Windows, quando attivato e quando l'utente è connesso a Internet, consente di scaricare i contenuti della guida e del supporto tecnico più aggiornati a disposizione.

Informazioni raccolte, elaborate o trasmesse

Quando si utilizza Guida online e supporto tecnico di Windows, le query di ricerca della guida vengono inviate a Microsoft insieme alle richieste di contenuti della guida, quando si seleziona un

collegamento. Per agevolare l'individuazione di contenuto della Guida più rilevante, Windows invia alcune informazioni sulla configurazione del PC. Guida online e supporto tecnico di Windows utilizza inoltre tecnologie Web standard, come ad esempio i cookie.

Utilizzo delle informazioni

Microsoft utilizza le informazioni per restituire gli argomenti della Guida in risposta alle query di ricerca, per restituire i risultati più rilevanti, per sviluppare nuovi contenuti e per migliorare quelli esistenti. Le informazioni sulla configurazione del PC vengono utilizzate da Microsoft per visualizzare il contenuto della Guida appropriato per la configurazione specifica. I cookie e altre tecnologie Web vengono utilizzati per agevolare la navigazione nel contenuto della Guida e per consentire a Microsoft di comprendere meglio le modalità di utilizzo della Guida online di Windows.

Scelta e controllo

La funzionalità Guida online e supporto tecnico è attivata per impostazione predefinita. Per modificare l'impostazione, toccare o fare clic sull'icona **Impostazioni** nella parte superiore della finestra di dialogo Guida e supporto tecnico, quindi selezionare o deselezionare **Accedi alla Guida online**. Per cancellare i cookie utilizzati dalla Guida di Windows, aprire Opzioni Internet nel Pannello di controllo, toccare o fare clic sul pulsante **Elimina** in **Cronologia esplorazioni**, selezionare **Cookie e dati di siti Web** quindi toccare o fare clic su **Elimina**. Se si sceglie di bloccare tutti i cookie (nella sezione Privacy di Opzioni Internet), la Guida di Windows non imposterà alcun cookie.

Analisi utilizzo Guida

Scopo della funzionalità

Il programma Analisi utilizzo Guida consente a Microsoft di individuare tendenze nella modalità di utilizzo di Guida online e supporto tecnico di Windows per migliorare i risultati delle ricerche e la rilevanza del contenuto.

Informazioni raccolte, elaborate o trasmesse

Analisi utilizzo Guida invia a Microsoft informazioni sulla versione di Windows in esecuzione nel PC e sulla modalità di utilizzo di Guida e

supporto tecnico di Windows, incluse le query immesse per le ricerche in Guida e supporto tecnico di Windows ed eventuali classificazioni o commenti e suggerimenti sugli argomenti della Guida presentati all'utente. Quando si cerca, si sfoglia o si forniscono classificazioni o commenti e suggerimenti sugli argomenti della Guida presentati all'utente, queste informazioni vengono inviate a Microsoft.

Analisi utilizzo Guida genera un numero casuale denominato identificatore univoco globale (GUID, Globally Unique Identifier) che viene inviato a Microsoft con ogni report di Analisi utilizzo Guida. Il GUID consente a Microsoft di determinare quali dati vengono inviati da un computer specifico nel tempo. Tale GUID non contiene informazioni personali. È inoltre diverso da quelli utilizzati per Segnalazione errori Windows e Analisi utilizzo software Windows.

Utilizzo delle informazioni

I dati raccolti sono utilizzati per identificare tendenze e modelli di utilizzo per consentire a Microsoft di migliorare la qualità del contenuto fornito e la rilevanza dei risultati di ricerca. Il GUID viene utilizzato per determinare quanto siano diffusi i problemi segnalati e come classificarli in ordine di priorità. Ad esempio, tramite il GUID Microsoft è in grado di distinguere un cliente che riscontra un problema centinaia di volte da cento clienti che riscontrano lo stesso problema una sola volta.

Analisi utilizzo Guida non raccoglie intenzionalmente alcuna informazione che possa essere utilizzata per identificare personalmente l'utente. Le informazioni di questo tipo eventualmente digitate nelle caselle di ricerca o in quelle dei commenti e suggerimenti verranno inviate a Microsoft, che tuttavia non utilizzerà queste e altre informazioni raccolte per identificare o contattare l'utente, né per inviargli pubblicità mirata.

Scelta e controllo

Se si scelgono impostazioni rapide durante la configurazione di Windows, si sceglie automaticamente di partecipare ad Analisi utilizzo Guida. Se si sceglie di personalizzare le impostazioni, è possibile controllare le impostazioni di Analisi utilizzo Guida selezionando **Contribuisci a migliorare il contenuto della Guida**

di Windows inviando info al programma Analisi utilizzo Guida in Invia info a Microsoft per contribuire a migliorare Windows e le app. Dopo la configurazione di Windows è possibile modificare tale impostazione in Guida e supporto tecnico di Windows.

[Inizio pagina](#)

Assistenza remota

Scopo della funzionalità

È possibile utilizzare Assistenza remota per invitare un utente a connettersi al proprio PC e ricevere assistenza per un problema relativo al PC, ovunque ci si trovi. Dopo aver eseguito la connessione, il secondo utente potrà visualizzare il PC in uso. Con l'autorizzazione dell'utente, l'assistente potrà utilizzare il proprio mouse e la propria tastiera per eseguire un controllo sul PC e indicare come risolvere il problema.

Informazioni raccolte, elaborate o trasmesse

Assistenza remota imposta una connessione crittografata tra i due PC tramite Internet o tramite la rete locale. Quando un utente utilizza Assistenza remota per connettersi a un altro PC, questi è in grado di visualizzarne il desktop, qualsiasi documento aperto ed eventuali informazioni private visibili. Inoltre, se si consente a un secondo utente di assumere il controllo del PC tramite mouse o tastiera, tale utente potrà eseguire operazioni quali l'eliminazione di file o la modifica delle impostazioni. Dopo aver stabilito una connessione, Assistenza remota consentirà di effettuare lo scambio delle informazioni di contatto, tra cui nome utente, nome PC e immagine dell'account. Il file di registro sessione registra tutte le connessioni di Assistenza remota.

Utilizzo delle informazioni

Le informazioni vengono utilizzate per stabilire una connessione crittografata e per consentire l'accesso al desktop a un secondo utente. Nessuna informazione viene inviata a Microsoft.

Scelta e controllo

Prima di consentire a un altro utente di connettersi al proprio PC, chiudere eventuali app o documenti aperti che non si desidera vengano visualizzati. Se in qualsiasi momento si preferisce evitare che la persona connessa visualizzi dati o esegua operazioni nel PC, premere il tasto ESC per terminare la sessione. È possibile disattivare la registrazione della sessione e lo scambio delle informazioni di contatto deselezionando tali opzioni nelle impostazioni di Assistenza remota.

[Inizio pagina](#)

Windows Search

Scopo della funzionalità

Windows Search offre all'utente un punto di ingresso rapido e coerente per eseguire la ricerca di app, impostazioni, file o contenuto all'interno di app.

Informazioni raccolte, elaborate o trasmesse

Quando si utilizza Windows Search, i caratteri digitati nel campo di ricerca (così come vengono digitati) e la query di ricerca finale inviata vengono forniti esclusivamente a Windows e all'eventuale app in cui si esegue la ricerca, affinché Windows o l'app possa offrire suggerimenti per la ricerca e mostrare i risultati ottenuti. Windows archivia le query di ricerca e i dati relativi alla frequenza di ricerca nelle app.

Utilizzo delle informazioni

Windows utilizza le ricerche precedentemente archiviate, per fornire suggerimenti per la ricerca nel riquadro Ricerca. Le informazioni archiviate relative alla frequenza di ricerca nelle app vengono utilizzate per ordinare l'elenco delle app disponibili per la ricerca nel riquadro Ricerca in ordine di frequenza. Se si esegue la ricerca in un'app di terze parti, l'uso delle informazioni sarà soggetto alle procedure relative alla privacy della terza parte. Se si esegue la ricerca in un'applicazione Microsoft, le procedure relative alla privacy dell'app saranno illustrate nella relativa Informativa sulla privacy.

Scelta e controllo

Windows archivia le informazioni per impostazione predefinita. È possibile disattivare l'archiviazione delle informazioni o eliminare tutte le ricerche precedentemente archiviate utilizzando Cerca in Impostazioni PC.

[Inizio pagina](#)

Windows Share

Scopo della funzionalità

Windows Share consente la condivisione di contenuti tra le app di Windows Store che supportano la condivisione. Consente inoltre di condividere contenuti con gli amici.

Informazioni raccolte, elaborate o trasmesse

Durante la condivisione, l'app di origine passa contenuti all'app di destinazione solo dopo che l'utente ha selezionato la destinazione nel riquadro Condividi. Se l'app di origine non ha implementato la condivisione, l'utente potrà condividere un'immagine o ciò che viene visualizzato sullo schermo. Le app di destinazione e le persone con cui si condividono frequentemente contenuti verranno visualizzate in un elenco nel riquadro Condividi. In questo modo l'utente potrà accedervi più facilmente. Nessuna informazione viene inviata a Microsoft.

Utilizzo delle informazioni

Le informazioni archiviate relative alla frequenza di condivisione di contenuti con app di destinazione e persone vengono utilizzate per ordinare l'elenco nel riquadro Condividi in ordine di frequenza. Se si condividono informazioni con un'app di terze parti, l'uso delle informazioni sarà soggetto alle procedure relative alla privacy della terza parte. Se si condivide un'app Microsoft, le procedure relative alla privacy dell'app saranno illustrate nella relativa Informativa sulla privacy.

Scelta e controllo

Per impostazione predefinita, Windows archivia le informazioni sull'utilizzo di Windows. È possibile disattivare l'archiviazione delle informazioni o eliminare tutte le destinazioni archiviate utilizzando

Cerca in Impostazioni PC.

[Inizio pagina](#)

Windows SmartScreen

Scopo della funzionalità

Windows SmartScreen aiuta a proteggere la sicurezza del PC chiedendo a Microsoft di controllare file e app prima della loro apertura o esecuzione per proteggere l'utente da file e app potenzialmente non sicuri. Windows chiederà quale azione intraprendere prima di aprire un file o un'app non nota o potenzialmente non sicura.

Informazioni raccolte, elaborate o trasmesse

Se si sceglie di utilizzare questa funzionalità, vengono inviate a Microsoft informazioni su alcune app utilizzate e su alcuni file scaricati da Internet. Tali informazioni possono includere nome di file, identificatore di file ("hash") e informazioni sul certificato digitale unitamente a informazioni standard sul PC e al numero di versione del filtro Windows SmartScreen. Per proteggere la privacy dell'utente, le informazioni inviate a Microsoft vengono crittografate tramite SSL.

Windows SmartScreen genera un numero casuale denominato identificatore univoco globale (GUID, Globally Unique Identifier) che viene inviato a Microsoft con i dati di utilizzo di SmartScreen. Il GUID consente a Microsoft di determinare quali dati vengono inviati da un PC specifico nel tempo. Tale GUID non contiene informazioni personali.

Utilizzo delle informazioni

Microsoft utilizza le informazioni descritte sopra per fornire avvisi all'utente relativamente a file e applicazioni potenzialmente non sicuri. Le informazioni vengono inoltre utilizzate per analizzare le prestazioni della funzionalità e migliorare la qualità di prodotti e servizi. Il GUID viene utilizzato per determinare quanto siano diffusi i commenti e i suggerimenti ricevuti da Microsoft e come classificarli in ordine di priorità. Ad esempio, tramite il GUID Microsoft è in grado di distinguere un cliente che riscontra un problema centinaia di volte

da cento clienti che riscontrano lo stesso problema una sola volta. Microsoft non utilizza le informazioni e le impostazioni per identificare o contattare l'utente, né per inviargli pubblicità mirata.

Scelta e controllo

Se si scelgono impostazioni rapide durante la configurazione di Windows, viene attivato Windows SmartScreen. Se si sceglie di personalizzare le impostazioni, è possibile controllare Windows SmartScreen selezionando **Usa il filtro Windows SmartScreen e consenti a Microsoft di controllare i file e le app** in **Contribuisci a proteggere il PC e la tua privacy**. Dopo la configurazione di Windows è possibile modificare questa impostazione nella sezione Centro operativo del Pannello di controllo.

[Inizio pagina](#)

Riconoscimento vocale Windows

Scopo della funzionalità

Riconoscimento vocale Windows è una funzionalità di riconoscimento vocale in Windows e in tutte le app per le quali è abilitata.

Riconoscimento vocale Windows è in grado di aumentare il proprio livello di precisione, apprendendo dall'utente l'uso della lingua, nonché i suoni e le parole che si utilizzano di frequente.

Informazioni raccolte, elaborate o trasmesse

Riconoscimento vocale Windows archivia un elenco delle parole e della relativa pronuncia nel PC. Le parole e la relativa pronuncia vengono aggiunte all'elenco utilizzando il dizionario vocale e Riconoscimento vocale Windows per dettare e correggere le parole.

Quando la funzionalità di revisione documenti di Riconoscimento vocale Windows è attiva, il testo dei documenti Microsoft Office Word (con estensione di file doc o docx) e dei messaggi di posta elettronica (di cartelle di posta diverse da Elementi eliminati o Posta indesiderata) presenti nel PC e nelle condivisioni file connesse incluse nei percorsi dell'indice di ricerca di Windows viene raccolto e archiviato in frammenti da una, due o tre parole. I frammenti da una parola includono solo le parole aggiunte ai dizionari personalizzati,

mentre quelli da due o tre parole includono solo le parole trovate nei dizionari standard.

Tutte le informazioni raccolte vengono archiviate nel profilo vocale personale nel PC. I profili vocali vengono archiviati per ciascun utente e gli utenti possono accedere solo ai propri profili sul PC. Tuttavia, gli amministratori possono accedere a qualsiasi profilo presente sul PC. Le informazioni sul profilo non vengono inviate a Microsoft a meno che non si scelga di inviarle quando richiesto da Riconoscimento vocale Windows. È possibile esaminare i dati prima di inviarli. Se si sceglie di inviare le informazioni, vengono inviati anche i dati di adattamento acustico utilizzati per l'adattamento alle caratteristiche audio.

Se si completa una sessione di formazione vocale, Riconoscimento vocale Windows chiederà all'utente se inviare o meno le informazioni sul profilo vocale a Microsoft. È possibile esaminare le informazioni prima di inviarle. Le informazioni possono includere le registrazioni della voce dell'utente ottenute durante il completamento della sessione di formazione e altre informazioni dal profilo vocale personale.

Utilizzo delle informazioni

Riconoscimento vocale Windows utilizza le parole contenute nel profilo vocale per convertire i comandi vocali in testo. Microsoft utilizza le informazioni sul profilo vocale personale per migliorare prodotti e servizi. Microsoft non utilizza le informazioni e le impostazioni per identificare o contattare l'utente, né per inviargli pubblicità mirata.

Scelta e controllo

È possibile scegliere se eseguire o meno Riconoscimento vocale Windows. Se si esegue Riconoscimento vocale Windows, per impostazione predefinita viene attivata la revisione dei documenti. È possibile scegliere di modificare le impostazioni di revisione dei documenti alla prima esecuzione di Riconoscimento vocale Windows. È possibile modificare le impostazioni di revisione dei documenti o eliminare i profili vocali personali (e la maggior parte delle informazioni di revisione dei documenti), da Riconoscimento vocale in Pannello di controllo, facendo clic su **Opzioni avanzate**

riconoscimento vocale. È inoltre possibile utilizzare l'opzione di modifica delle parole esistenti nel dizionario vocale, per eliminare le parole aggiunte al profilo vocale. L'eliminazione del profilo vocale personale non consente tuttavia l'eliminazione delle parole aggiunte al profilo tramite il dizionario vocale.

È possibile controllare i percorsi da cui la revisione dei documenti raccoglierà i frammenti di parole modificando i percorsi inclusi nell'indice di ricerca di Windows. Per visualizzare o modificare i percorsi inclusi nell'indice di ricerca di Windows, aprire Opzioni di indicizzazione dal Pannello di controllo.

Al termine di ogni sessione di formazione, l'utente potrà scegliere se inviare o meno le informazioni di formazione e altre informazioni sul profilo a Microsoft. È inoltre possibile inviare le informazioni all'avvio di Riconoscimento vocale Windows, facendo clic con il pulsante destro del mouse su **Microfono**, quindi scegliendo **Contribuisci a migliorare il riconoscimento vocale**. In entrambi i casi, è possibile visualizzare tutti i dati dei file prima che vengano inviati. Inoltre è possibile scegliere di non inviarli.

[Inizio pagina](#)

Windows Store

Windows Store ti consente di individuare, gestire e installare le app per il PC. Nelle sezioni riportate è descritto l'impatto delle funzionalità di Windows Store e delle app ottenute tramite Windows Store, sulla privacy, nonché le operazioni da eseguire per verificarlo.

Servizi e app di Windows Store

Scopo della funzionalità

Windows Store ti consente di individuare e installare le app per il PC. Consente inoltre di tenere traccia delle app di Windows Store installate, in modo da ricevere gli aggiornamenti relativi e installarli su più di un PC.

Informazioni raccolte, elaborate o trasmesse

Per individuare e installare le app, è necessario accedere a Windows Store con un account Microsoft. Ciò consente a Windows Store di

accedere alle informazioni contenute nel profilo dell'account Microsoft, quali il nome, l'indirizzo di posta elettronica e l'immagine dell'account. Windows Store raccoglie e associa le seguenti informazioni aggiuntive all'account Windows Store dell'utente:

- Pagamenti effettuati in Windows Store. Le informazioni su cosa è stato acquistato, quanto è stato pagato e le modalità di pagamento durante l'acquisto di app o in-app con l'account Windows Store.
- App installate. L'elenco delle app installate, i criteri di licenza per ciascuna app (licenza permanente o versione di valutazione per un periodo di tempo limitato) e un elenco degli acquisti effettuati con l'account Windows Store in ogni app. Oltre ad archiviare le informazioni online con l'account Windows Store, l'archivio memorizza sul PC le informazioni sulla licenza per ciascuna app installata. Tali informazioni identificano l'utente come proprietario della licenza.
- PC in cui sono state installate app. La marca, il modello e il nome del computer di ciascun PC su cui sono state installate app e il numero che identifica il PC in modo univoco. Tale numero viene generato alla configurazione hardware del PC e non contiene informazioni sull'utente.
- Valutazioni, recensioni e segnalazioni di errori. Una volta installata un'app, è possibile scrivere una recensione o lasciare una valutazione in Windows Store. L'account Microsoft viene associato a queste valutazioni. Se si scrive una recensione, insieme ad essa verrà pubblicato il nome e l'immagine dell'account Microsoft dell'utente.
- Preferenze per Windows Store. Le preferenze impostate per la visualizzazione di app in Windows Store, ad esempio la visualizzazione delle sole app disponibili nella lingua di origine.

Con l'account Windows Store, è possibile scegliere di archiviare le informazioni di pagamento, tra cui il numero di carta di credito. Per motivi di sicurezza, le impostazioni vengono trasmesse tramite SSL. Inoltre, tutte le cifre del numero di carta di credito, ad eccezione delle ultime quattro, sono crittografate.

Windows Store raccoglie alcune informazioni sulla copia di Windows in uso, per stabilire se è stata acquistata da un negozio al dettaglio, ottenuta come copia di valutazione, ottenuta tramite un programma di contratti multilicenza o preinstallata da un produttore di PC.

Quando ci si connette a Windows Store per la prima volta, viene inviato un elenco di tutte le app preinstallate nel PC e le relative licenze vengono associate all'account Windows Store dell'utente.

Windows Store verifica automaticamente la presenza di aggiornamenti per le app e invia una notifica all'utente quando sono disponibili nuovi aggiornamenti. Per fornire nuovi aggiornamenti, Windows Store invia le seguenti informazioni a Microsoft:

- Un elenco di tutte le app installate nel PC da Windows Store da tutti gli utenti
- Le informazioni sulla licenza per ciascuna app, tra cui il proprietario di ciascuna licenza
- Le impostazioni di configurazione di Windows Update e/o Microsoft Update, ad esempio la possibilità di scaricare o installare automaticamente gli aggiornamenti.
- La riuscita o meno delle operazioni e gli errori verificatisi durante l'aggiornamento delle app di Windows Store.
- Globally Unique Identifier (GUID): numero generato in modo casuale che non contiene informazioni personali. I GUID vengono utilizzati per identificare PC singoli senza identificarne l'utente.
- Nome BIOS, numero di revisione e data di revisione: informazioni relative all'insieme di operazioni principali eseguite dal software per eseguire verifiche dell'hardware, avviare il sistema operativo sul computer e trasferire dati tra dispositivi hardware collegati al computer.

Sfogliando Windows Store e utilizzando le app contenute, Microsoft raccoglie alcune informazioni per comprendere tendenze e modelli di utilizzo, analogamente al modo in cui molti siti Web analizzano i dati relativi alla navigazione dei visitatori. Nessuno di questi dati dell'attività viene utilizzato per identificare o contattare l'utente.

Utilizzo delle informazioni

Microsoft utilizza le informazioni di contatto per inviare all'utente e-mail necessarie per la fornitura di servizi di Windows Store, ad esempio le ricevute per le app acquistate. Utilizza le informazioni sul pagamento archiviate per consentire all'utente di pagare gli acquisti, senza dover immettere i dati ogni volta. Microsoft utilizza le informazioni sugli acquisti dell'utente per le operazioni su Windows Store e per fornire supporto tecnico ai clienti.

Windows Store tiene traccia di tutte le app installate. È possibile utilizzare Windows Store per gestire l'elenco dei dispositivi su cui sono installate app, inoltre, il supporto tecnico aiuta il cliente nella gestione di queste informazioni. Una volta installata un'app, l'utente può sempre visualizzarla nella cronologia degli acquisti in Windows Store, anche se si sceglie di disinstallarla. Windows Store utilizza inoltre l'elenco per consentire l'applicazione del limite del numero di PC su cui l'utente può installare app, come descritto nelle condizioni per l'utilizzo di Windows. Quando si scrive una recensione per un'app, il nome e l'immagine dell'account associati all'account Windows verranno pubblicati accanto alla recensione in Windows Store. Se si segnala un problema con un'app, la segnalazione è resa disponibile ai rappresentanti di Windows Store affinché possano valutare il problema e prendere misure. I rappresentanti possono utilizzare il nome e l'indirizzo di posta elettronica associati all'account Windows Store per contattare l'utente, se necessario, durante la revisione del report.

Quando sono disponibili aggiornamenti per le app installate, viene visualizzato un messaggio di notifica in Windows Store e il riquadro dell'app di Windows Store indica il numero degli aggiornamenti disponibili. È possibile quindi visualizzare l'elenco degli aggiornamenti disponibili e scegliere quali installare. Le app aggiornate possono utilizzare funzionalità Windows differenti rispetto alle versioni precedenti, in grado di fornire l'accesso a diverse risorse sul PC. È possibile visualizzare gli elenchi aggiornati delle funzionalità nelle pagine Descrizione app collegate alle pagine degli elenchi degli aggiornamenti disponibili.

Windows Store utilizza le informazioni raccolte sulla copia di

Windows in uso per stabilire la modalità di installazione di Windows nel PC (ad esempio, se preinstallata nel PC dal produttore). Tali informazioni permettono a Windows Store di consentire all'utente di accedere alle app fornite esclusivamente dal produttore ai propri clienti. Vengono inoltre utilizzate per fornire a Microsoft (e talvolta in forma aggregata al produttore) dati circa i modelli di utilizzo di Windows.

Microsoft utilizza alcuni dati sull'acquisto e l'utilizzo e di app in forma aggregata per ottenere informazioni sulle modalità di utilizzo di Windows Store da parte degli utenti, ad esempio il modo in cui trovano le app che installano. Microsoft può condividere alcune delle statistiche in forma aggregata con gli sviluppatori delle app. Microsoft non condivide nessuna informazione personale con gli sviluppatori delle app. I dati di navigazione e di utilizzo raccolti da Windows Store vengono utilizzati per comprendere la modalità di utilizzo del servizio da parte degli utenti, nonché per migliorare le funzionalità e i servizi di Windows Store.

Scelta e controllo

Se si sceglie di utilizzare Windows Store, le informazioni riportate nella presente sezione verranno inviate a Microsoft come descritto in precedenza.

Se si desidera rimuovere una recensione che lo stesso utente ha pubblicato per un'app, accedere alla descrizione dell'app in Windows Store, modificare la recensione ed eliminare tutto il testo.

Autorizzazione per le app di Windows Store

Scopo della funzionalità

Molte delle app installate da Windows Store sono progettate per sfruttare le funzionalità specifiche di hardware e software del PC in uso. Ad esempio, potrebbe essere necessario disporre di una webcam per utilizzare un'app per le foto, così come potrebbe essere necessario conoscere l'ubicazione dell'utente per ottenere consigli su dove mangiare nelle vicinanze da una guida gastronomica.

Informazioni raccolte, elaborate o trasmesse

Di seguito sono riportate le funzionalità utilizzate dalle app da comunicare all'utente:

- Connessione Internet dell'utente. Consente all'app di connettersi a Internet.
- Connessioni in ingresso tramite firewall. Consente all'app di inviare informazioni a o dal PC tramite un firewall.
- Rete domestica o aziendale. Consente all'app lo scambio di informazioni tra il PC in uso e altri PC connessi alla stessa rete.
- Librerie di immagini, video, musica o documenti personali. Consente all'app di accedere, modificare o eliminare i file nelle librerie. La funzionalità consente inoltre di accedere a tutti i dati aggiuntivi incorporati in questi file, ad esempio le informazioni sul percorso delle foto.
- Archivio rimovibile. Consente all'app di accedere, aggiungere, modificare o eliminare i file su unità disco rigido esterne, unità flash USB o dispositivi portatili.
- Credenziali Windows dell'utente. Consente all'app di utilizzare le credenziali dell'utente per eseguire l'autenticazione e garantire l'accesso alla Intranet aziendale.
- Certificati archiviati nel PC o nella smart card. Consente all'app di utilizzare i certificati per la connessione sicura a organizzazioni quali banche, enti pubblici o alla società in cui lavora l'utente.
- Funzionalità di messaggistica del PC dell'utente. Consente all'app di inviare e ricevere messaggi di testo.
- Webcam e microfono. Consente all'app di scattare foto e registrare file audio e video.
- Posizione dell'utente. Consente all'app di stabilire la posizione approssimativa dell'utente in base al sensore GPS o alle informazioni di rete.
- Funzionalità per la comunicazione NFC del PC. Consente all'app di connettersi a dispositivi vicini su cui è in esecuzione la stessa app.

- Dispositivi portatili. Consente all'app di comunicare con dispositivi quali telefoni cellulari, fotocamere digitali o lettori musicali portatili.
- Informazioni in un dispositivo portatile. Consente all'app di accedere, aggiungere, modificare o eliminare contatti, calendari, attività, note, stato o suonerie sul dispositivo portatile.
- Account Mobile Broadband. Consente all'app di gestire l'account Mobile Broadband.

Le funzionalità che un'app utilizza verranno elencate nella relativa pagina Descrizione app. Se si installa un'app, Windows consentirà l'utilizzo di tali funzionalità, ad eccezione di quelle relative a posizione, messaggistica, webcam e microfono, che sono considerate particolarmente sensibili. Alla prima richiesta di accesso dell'app a una di queste funzionalità sensibili, Windows chiederà all'utente se consentirne o meno l'utilizzo. È possibile modificare l'opzione di utilizzo in qualsiasi momento.

Utilizzo delle informazioni

L'utilizzo di queste funzionalità da parte di ogni app sarà soggetto alle procedure relative alla privacy dei relativi sviluppatori. Se un'app utilizza una delle funzionalità sensibili descritte sopra, nella relativa pagina Descrizione app di Windows Store sarà disponibile un collegamento all'Informativa sulla privacy dello sviluppatore dell'app.

Scelta e controllo

È possibile visualizzare le funzionalità richieste da un'app in Windows Store prima dell'installazione dell'app. Windows chiederà se consentire o negare l'accesso alla maggior parte delle funzionalità sensibili (ubicazione, messaggistica, webcam e microfono) prima del primo utilizzo di queste da parte di ciascuna app.

Nella parte inferiore della colonna sinistra della pagina Descrizione applicazione di un'app in Windows Store, verrà visualizzato un elenco abbreviato delle funzionalità. È possibile visualizzare l'elenco completo nella pagina Dettagli di Descrizione app. Dopo aver installato un'app, è possibile visualizzare l'elenco completo delle

funzionalità utilizzate in qualsiasi momento ed è possibile controllarne l'accesso a quelle particolarmente sensibili. A tale scopo, aprire l'app, toccare o fare clic sull'accesso alle impostazioni e quindi selezionare **Autorizzazioni**.

Contribuire a migliorare Windows Store inviando URL per il contenuto Web usato dalle app

Scopo della funzionalità

Alcune app ottenute da Windows Store sono come siti Web e possono esporre il computer a software potenzialmente non sicuro, ad esempio malware. Se si sceglie di attivare questa funzionalità, le informazioni sul contenuto Web utilizzato dalle app verranno raccolte per aiutare Microsoft nella diagnosi di comportamenti potenzialmente non sicuri. Queste informazioni potrebbero essere utilizzate, ad esempio, per rimuovere un'app da Windows Store.

Informazioni raccolte, elaborate o trasmesse

Se si sceglie di inviare informazioni relative al contenuto Web utilizzato dalle app, Microsoft raccoglierà i dati sugli URL e i tipi di contenuto a cui accedono le app durante l'utilizzo. Ciò può agevolare l'individuazione di quali app possono ricevere contenuto da siti Web dannosi o non sicuri. I report inviati a Microsoft includono informazioni quali il nome o l'identificatore dell'app, gli URL completi degli indirizzi a cui accedono le app e gli URL completi che indicano la posizione di qualsiasi JavaScript a cui accede l'app. Windows genera un numero casuale denominato identificatore univoco globale (GUID, Globally Unique Identifier) che viene inviato a Microsoft con ogni report. Il GUID consente a Microsoft di determinare quali dati vengono inviati da un computer specifico nel tempo. Il GUID non contiene informazioni personali e non viene utilizzato per identificare l'utente.

Per agevolare la protezione della privacy dell'utente, le informazioni inviate a Microsoft sono crittografate. È possibile che vengano incluse informazioni associate a una pagina Web a cui accedono le app, ad esempio termini di ricerca o dati immessi nelle app. Ad esempio, se si cerca una parola in un'applicazione di dizionario, tale parola può essere inclusa nelle informazioni inviate a Microsoft come

parte dell'URL completo a cui accede l'app. Microsoft filtra gli indirizzi per tentare di rimuovere le informazioni personali, quando possibile.

Utilizzo delle informazioni

Microsoft esamina periodicamente le informazioni inviate per agevolare l'individuazione delle app che potrebbero interagire con contenuto Web non sicuro, ad esempio indirizzi Web o script dannosi. Queste informazioni potrebbero essere utilizzate per prendere misure per la protezione da app potenzialmente dannose. Gli indirizzi del contenuto Web possono involontariamente contenere informazioni personali, che tuttavia non vengono utilizzate per identificare o contattare l'utente né per l'invio di pubblicità. Il GUID viene utilizzato per determinare quanto siano diffusi i commenti e i suggerimenti ricevuti da Microsoft e come classificarli in ordine di priorità. Ad esempio, il GUID consente a Microsoft di distinguere tra comportamenti potenzialmente non sicuri che si verificano 100 volte su un solo PC e lo stesso comportamento che si verifica una volta su 100 PC diversi.

Scelta e controllo

Se si scelgono impostazioni rapide durante la configurazione di Windows, Windows invierà informazioni sul contenuto Web utilizzato dalle app di Windows Store scritte in JavaScript. Se si sceglie di personalizzare le impostazioni, è possibile controllare questa impostazione selezionando **Contribuisci a migliorare Windows Store inviando URL per il contenuto Web usato dalle app** in **Invia info a Microsoft per contribuire a migliorare Windows e le app**. Dopo l'installazione, è possibile modificare questa impostazione nella sezione Privacy di Impostazioni PC.

[Inizio pagina](#)

Servizio Ora di Windows

Scopo della funzionalità

Servizio Ora di Windows sincronizza automaticamente l'ora del PC con un server di riferimento ora in rete.

Informazioni raccolte, elaborate o trasmesse

Il servizio si connette a un server di riferimento ora tramite Internet o a una rete locale utilizzando un server NTP standard del settore. Per impostazione predefinita, il servizio esegue la sincronizzazione con time.windows.com una volta a settimana. Nessuna informazione diversa da quelle del PC standard viene inviata al server di riferimento ora.

Utilizzo delle informazioni

Servizio Ora di Windows utilizza le informazioni per eseguire la sincronizzazione automatica dell'ora del PC locale.

Scelta e controllo

Servizio Ora di Windows viene attivato per impostazione predefinita. È possibile disattivare la funzionalità o scegliere il tipo di origine ora che si preferisce, in Data e ora dal Pannello di controllo, scegliendo la scheda Ora Internet, quindi facendo clic su **Modifica impostazioni**. La disattivazione di Servizio Ora di Windows non ha alcun impatto diretto sull'app o su altri servizi, tuttavia senza un tipo di origine ora affidabile l'orologio del PC locale può perdere la sincronizzazione con altri PC in rete o su Internet. Nelle app e i servizi dipendenti dall'orario, una discrepanza significativa nell'ora tra i PC collegati alla rete potrebbe comportare il verificarsi di errori o l'impedimento del corretto funzionamento.

[Inizio pagina](#)

Risoluzione dei problemi Windows

Scopo della funzionalità

Risoluzione dei problemi Windows consente di effettuare la diagnosi e di correggere i problemi comuni del PC.

Informazioni raccolte, elaborate o trasmesse

Dopo aver eseguito un pacchetto di risoluzione dei problemi, i risultati vengono salvati nel PC. Tali risultati possono contenere informazioni personali, ad esempio il nome utente o il nome di un dispositivo. Risoluzione dei problemi Windows può agevolare la ricerca di soluzioni dei problemi nella Guida di Windows e nelle community online di Windows. Le parole chiave associate al

problema verranno inviate a Microsoft per trovare una soluzione al problema. Ad esempio, se la stampante non funziona correttamente e l'utente cerca assistenza, le parole "printer", "print" e "printing" vengono inviate a Microsoft.

Utilizzo delle informazioni

Microsoft utilizza le informazioni raccolte da Risoluzione dei problemi Windows per risolvere i problemi riscontrati dagli utenti.

Scelta e controllo

Se si scelgono impostazioni rapide durante la configurazione di Windows, Risoluzione dei problemi Windows eseguirà la ricerca online di pacchetti di risoluzione dei problemi per impostazione predefinita. Per modificare le impostazioni, per eliminare i risultati della risoluzione dei problemi passare a Risoluzione dei problemi nel Pannello di controllo. Fare clic su **Visualizza cronologia**, selezionare un risultato, quindi fare clic su **Elimina**.

[Inizio pagina](#)

Per informazioni aggiornate sulle procedure di trattamento dei dati di Microsoft, leggi [l'Informativa sulla privacy di Microsoft](#). In questo documento puoi scoprire anche gli strumenti più recenti forniti per l'accesso e il controllo dei dati e come contattare Microsoft per richiedere informazioni sulla privacy.

Informativa sulla privacy di Windows 8 e Windows Server 2012

Elementi di rilievo Informativa Supplemento sulle funzionalità **Supplemento sul server**

In questa pagina Ultimo aggiornamento: **Agosto 2012**

Registrazione accesso utenti	<p>Questa pagina è un supplemento a Informativa sulla privacy di Windows 8 e Windows Server 2012 ("Informativa sulla privacy di Windows"). L'informativa sulla privacy include quattro sezioni:</p> <ul style="list-style-type: none">• Elementi di rilievo• L'informativa, che è Informativa completa sulla privacy di Windows che include i collegamenti per le funzionalità di Windows, che possiedono informative autonome• Supplemento sulle funzionalità, che descrive le funzionalità che hanno un impatto sulla privacy in Windows 8 e Windows Server 2012• Il Supplemento sul server (questo documento) descrive le funzionalità aggiuntive che hanno un impatto sulla privacy in Windows Server 2012
Server Manager	
Active Directory	
Federation Services	
Gestione indirizzi IP	
Accesso remoto unificato	
Servizi Desktop remoto	
Programma Analisi utilizzo software Windows (CEIP) e	

Segnalazione errori Windows (WER) Per comprendere le procedure rilevanti per la raccolta e l'utilizzo dei dati per una determinata funzionalità o servizio di Windows, è consigliabile leggere l'informativa completa sulla Privacy e qualsiasi supplemento applicabile. Inoltre, è consigliabile leggere [questo white paper per gli amministratori](#).

Registrazione accesso utenti

Descrizione della funzionalità

La Registrazione accesso utenti (UAL) raccoglie e unisce i record delle richieste del client dei ruoli server (richieste dell'utente e del dispositivo) e dei prodotti installati (se registrati con Registrazione accesso utenti) nel server locale. Questi dati, in forma di indirizzi IP, nomi utente e, in alcuni casi, nomi host e/o identità macchina virtuali, vengono archiviati nei database locali ESE (Extensible Storage Engine) e sono accessibili solo dagli amministratori. La Registrazione accesso utenti ha un provider WMIv2 e cmdlet associati di Windows PowerShell per il recupero dei dati di accesso utente che sono progettati per la gestione offline del diritto di licenza di accesso client (CAL), in cui sono di importanza fondamentale i record reali di richieste client univoche.

Dati raccolti, elaborati o trasmessi

Gli indirizzi IP, i nomi utente e, in alcuni casi, i nomi host (se è installato il ruolo DNS) e le identità macchina virtuali (se è installato il ruolo Hyper-V) vengono raccolti, in locale, nel server quando la Registrazione accesso utenti è abilitata. Nessun dato raccolto viene inviato a Microsoft.

Uso delle informazioni

I dati della Registrazione accesso utenti sono disponibili per gli amministratori tramite i database locali ESE, il provider WMI e i cmdlet di Windows PowerShell. Windows non utilizza questi dati al di fuori della funzionalità della Registrazione accesso utenti stessa.

Scelta e controllo

La Registrazione accesso utenti è abilitata per impostazione predefinita. Il servizio Registrazione accesso utenti può essere arrestato e avviato mentre il server è in esecuzione. Per disabilitare la Registrazione accesso utenti in modo permanente, aprire Windows

PowerShell, digitare Disable-UAL e riavviare il server. Un amministratore può eliminare tutti i dati cronologici raccolti, interrompendo prima il servizio, disabilitando la Registrazione accesso utenti, poi eliminando tutti i file nella cartella %SystemRoot%\System32\LogFiles\SUM\.

[Torna all'inizio](#)

Server Manager

Descrizione della funzionalità

Il Server Manager è uno strumento di gestione che consente all'amministratore di monitorare uno o più server e di visualizzare lo stato generale o specifico del ruolo, per eseguire attività di gestione e accedere ad altri strumenti di gestione del server.

Dati raccolti, elaborati o trasmessi

Server Manager raccoglie le seguenti tipologie di informazioni da un server gestito dall'amministratore:

- **Informazioni generali sul server:** Il nome NetBios e il nome di dominio completo (FQDN), le credenziali dell'account immesse nella funzionalità "Gestisci come", l'indirizzo IPv4, l'indirizzo IPv6, lo stato di gestibilità, la descrizione, la versione del sistema operativo, il tipo, l'ultimo aggiornamento, i processori, la memoria, il nome del cluster, il tipo di oggetto cluster, lo stato di attivazione, lo SKU, l'architettura del sistema operativo, il produttore, la configurazione del Programma analisi utilizzo software (CEIP) e la configurazione di Segnalazione errori Windows (WER).
- **Eventi:** L'ID, la gravità, l'origine, il registro, la data e l'ora per ogni evento da Windows e da altri registri che l'amministratore sceglie.
- **Tutti i servizi:** Nome, stato e tipo di avvio.
- **Informazioni sul ruolo server:** I risultati di Best Practice Analyzer (BPA) per i ruoli installati nel server.
- **Informazioni sulle prestazioni:** Esempi per i contatori delle prestazioni e notifiche per l'utilizzo della CPU e della memoria

disponibile.

Uso delle informazioni

Queste informazioni vengono archiviate nel Server Manager e non vengono inviate a Microsoft. Vengono visualizzate nel Server Manager per consentire agli amministratori di monitorare i sistemi.

Scelta e controllo

Un amministratore può decidere di partecipare o meno alla raccolta dei dati da qualsiasi server, ad eccezione del server locale, aggiungendo o rimuovendo il server in Server Manager. Un amministratore può fornire in modo esplicito le credenziali per connettersi ad un server remoto. Il Server Manager richiede all'amministratore di acconsentire in modo esplicito all'archiviazione delle credenziali in locale in Server Manager e l'amministratore stesso può eliminare tali credenziali in qualsiasi momento.

[Torna all'inizio](#)

Active Directory Federation Services

Descrizione della funzionalità

L'Active Directory Federation Services (AD FS) è una federazione dedicata alle aziende e una soluzione Single Sign-On per le applicazioni locali o basate su altre reti. L'AD FS permette agli amministratori di consentire agli utenti di collaborare tra organizzazioni e accedere facilmente alle applicazioni in locale o tramite altre reti, mantenendo la sicurezza dell'applicazione. L'AD FS utilizza un servizio token di sicurezza che utilizza l'Active Directory Domain Services (AD DS) per autenticare gli utenti e fornire loro token di sicurezza, utilizzando vari protocolli. Il token ha una firma digitale e contiene le attestazioni relative all'utente, che provengono da ogni o qualsiasi combinazione di dominio di Active Directory Domain Services, di Lightweight Directory Access Protocol (LDAP), del SQL Server o di un archivio personalizzato.

Dati raccolti, elaborati o trasmessi

Le credenziali dell'utente vengono raccolte quando l'utente esegue l'autenticazione con AD FS. Le credenziali vengono inviate immediatamente all'Active Directory Domain Services per

l'autenticazione e l'AD FS non le archivia in locale. Gli attributi dell'utente in Active Directory Domain Services potrebbero essere utilizzati per generare attestazioni in uscita, a seconda delle regole di attestazione configurate da un amministratore di AD FS. Le attestazioni in uscita verranno inviate a partner attendibili, con i quali un amministratore di AD FS ha stabilito una relazione di trust. Nessuna informazione viene inviata a Microsoft.

Uso delle informazioni

A Microsoft non sarà possibile accedere a queste informazioni. Queste informazioni sono destinate solo all'uso del cliente.

Scelta e controllo

Usare AD FS se si desidera che AD FS raccolga o invii i dati a partner attendibili.

[Torna all'inizio](#)

Gestione indirizzi IP

Descrizione della funzionalità

La Gestione indirizzi IP (IPAM) consente agli amministratori di server di tenere traccia dell'indirizzo IP, del nome host e dell'identificatore del client (ad esempio, l'indirizzo MAC in IPv4 e DUID in IPv6) dei computer o dei dispositivi in una rete con informazioni sull'accesso utente.

Dati raccolti, elaborati o trasmessi

Il server di Gestione indirizzi IP (IPAM) raccoglie i log di controllo e gli eventi dai server DHCP, i controller di dominio e i server dei criteri di rete, e poi archivia in locale l'indirizzo IP, il nome host, l'identificatore client e il nome utente dell'utente connesso. Un amministratore del server può cercare i log raccolti in base all'indirizzo IP, all'identificatore client, al nome host e al nome utente, utilizzando la console di Gestione indirizzi IP (IPAM). Nessuna di queste informazioni viene inviata a Microsoft.

Uso delle informazioni

A Microsoft non sarà possibile accedere a queste informazioni. Queste informazioni sono destinate solo all'uso del cliente.

Scelta e controllo

La Gestione indirizzi IP (IPAM) non è installata per impostazione predefinita e deve essere installata dall'amministratore del server. Dopo l'installazione della Gestione indirizzi IP (IPAM), il controllo dell'indirizzo IP viene abilitato automaticamente. Per disabilitare il controllo dell'indirizzo IP in un server in cui la Gestione indirizzi IP (IPAM) è stata installata, bisogna avviare l'Utilità di pianificazione nel server di Gestione indirizzi IP, passare all'attività di controllo in Microsoft\Windows\Gestione indirizzi IP e poi disabilitare l'applicazione.

[Torna all'inizio](#)

Accesso remoto unificato

Descrizione della funzionalità

L'Accesso remoto unificato consente agli utenti remoti di connettersi a una rete privata, come ad esempio, una rete aziendale tramite Internet. L'Accesso remoto unificato utilizza DirectAccess per fornire ai computer client remoti che eseguono Windows 8 con connettività senza interruzioni e trasparente verso le reti aziendali. Inoltre, fornisce la funzionalità del servizio Accesso remoto (RAS), che è uno dei servizi VPN tradizionali, compresa la connettività locale da sito a sito o ad altre reti.

Dati raccolti, elaborati o trasmessi

Per monitorare l'utente di Accesso remoto unificato, il server DirectAccess archivia i dettagli degli utenti remoti connessi alla rete privata. Sono incluse informazioni come nome host dell'utente remoto, nome utente di Active Directory e indirizzo IP pubblico del client remoto (se il client è protetto dai servizi di conversione degli indirizzi di rete (NAT), si tratterà dell'indirizzo IP pubblico). Questi dati possono essere archiviati anche nel Database interno di Windows (WID)/server RADIUS, solo con il consenso dell'amministratore. Solo un amministratore di DirectAccess (un utente di dominio con un account amministratore locale), con accesso ad un server, può accedere e visualizzare queste informazioni.

Uso delle informazioni

Queste informazioni verranno utilizzate dall'amministratore per la risoluzione dei problemi di connettività del client e anche per scopi di controllo o di conformità. Nessuna informazione viene inviata a Microsoft.

Scelta e controllo

Il monitoraggio del client remoto è abilitato per impostazione predefinita e non può essere disabilitato. I dati di monitoraggio vengono archiviati nei server del database interno di Windows(WID)/RADIUS solo se un amministratore ha configurato l'accounting per usare una qualsiasi di queste opzioni. Se un amministratore non ha configurato l'accounting, nessuna di queste informazioni verrà archiviata. Inoltre, un amministratore può configurare l'accounting in un server di accesso remoto in modo tale che non archivi le informazioni sul nome utente e sull'indirizzo IP.

[Torna all'inizio](#)

Servizi Desktop remoto

Descrizione della funzionalità

I Servizi Desktop remoto (RDS) offrono una piattaforma per consentire alle aziende di implementare una strategia desktop centralizzata, gestire i desktop e le applicazioni e migliorare la flessibilità e la conformità, migliorando al contempo la sicurezza dei dati.

Dati raccolti, elaborati o trasmessi

Per il monitoraggio dell'utente di Servizi Desktop remoto (RDS), il server della sessione Desktop remoto archivia le informazioni sugli utenti remoti che si connettono alle risorse di Servizi Desktop remoto. Sono incluse informazioni come il nome host dell'utente remoto, il nome utente di Active Directory e l'indirizzo IP pubblico del client remoto (se il client è protetto dai servizi di conversione degli indirizzi di rete (NAT), si tratterà dell'indirizzo IP pubblico). Questi dati vengono archiviati automaticamente nel Database interno di Windows (WID)/SQL server quando gli utenti si connettono. Nessuna informazione viene inviata a Microsoft. Solo un utente di dominio che dispone di un account amministratore locale può accedere e visualizzare queste informazioni.

Uso delle informazioni

Queste informazioni verranno utilizzate dall'amministratore per la risoluzione dei problemi di connettività del client e anche per scopi di controllo interno o di conformità. Nessuna informazione viene inviata a Microsoft.

Scelta e controllo

Il monitoraggio del client remoto è abilitato per impostazione predefinita e non può essere disabilitato. Le informazioni sul monitoraggio vengono archiviate nel database interno di Windows/SQL server.

[Torna all'inizio](#)

Programma Analisi utilizzo software Windows (CEIP) e Segnalazione errori Windows (WER)

Descrizione della funzionalità

Per ulteriori informazioni su queste funzionalità, vedere [Supplemento sulle funzionalità](#) o [questo white paper per gli amministratori](#).

Dati raccolti, elaborati o trasmessi

Per ulteriori informazioni sugli specifici dati raccolti, elaborati e trasmessi da queste funzionalità, vedere Programma analisi utilizzo software (CEIP) e Segnalazione errori Windows (WER) in [Supplemento sulle funzionalità](#) .

Uso delle informazioni

Per ulteriori informazioni sulle modalità di utilizzo delle informazioni raccolte da queste funzionalità, vedere Programma analisi utilizzo software (CEIP) e Segnalazione errori Windows (WER) in [Supplemento sulle funzionalità](#) .

Scelta e controllo

L'Analisi utilizzo software (CEIP) è disabilitata per impostazione predefinita, e Segnalazione errori Windows (WER) viene configurata per impostazione predefinita affinché richieda l'autorizzazione dell'utente prima di inviare segnalazioni di arresto anomalo a Microsoft. È possibile abilitare o disabilitare l'Analisi utilizzo software (CEIP) dal Server Manager e dal Pannello di controllo, utilizzando i metodi della riga di comando del controllo. La Segnalazione errori

Windows (WER) può essere controllata utilizzando solo i metodi della riga di comando.

Per abilitare e disabilitare l'Analisi utilizzo software (CEIP) tramite il Pannello di controllo, fare clic su **Sistema e manutenzione** e quindi su **Segnalazioni di problemi e soluzioni**. Quindi, nel riquadro a sinistra, in Vedere anche, fare clic su **Impostazioni Analisi utilizzo software** per l'opzione per attivare o disattivare il programma Analisi utilizzo software (CEIP).

Controlli di Server Manager

Server locale

- Abilitare Analisi utilizzo software (CEIP)
Aprire Server Manager e selezionare **Server locale**. Fare clic sul collegamento al programma Analisi utilizzo software, selezionare **Sì, desidero partecipare al programma Analisi utilizzo software (CEIP)** nella finestra di dialogo e quindi fare clic su **OK**.
- Disabilitare Analisi utilizzo software (CEIP)
Aprire Server Manager e selezionare **Server locale**. Fare clic sul collegamento al programma Analisi utilizzo software e selezionare **No, non desidero partecipare** nella finestra di dialogo e quindi fare clic su **OK**.
- Abilitare Segnalazione errori Windows (WER)
Aprire Server Manager e selezionare **Server locale**. Fare clic sul collegamento a Segnalazione errori Windows, selezionare **Sì, invia automaticamente rapporti brevi** e quindi fare clic su **OK**.
- Disabilitare Segnalazione errori Windows (WER)
Aprire Server Manager e selezionare **Server locale**. Fare clic sul collegamento a Segnalazione errori Windows, selezionare **Non desidero partecipare e Non visualizzare più questo messaggio** e quindi fare clic su **OK**.

Più computer

- Abilitare Analisi utilizzo software (CEIP)
Aprire Server Manager e selezionare **Tutti i server**. Nel riquadro Server, selezionare tutti i server (Ctrl+A), fare clic con

il pulsante destro del mouse e selezionare **Configurare Commenti e suggerimenti automatici per Windows** . Fare clic sul collegamento al programma Analisi utilizzo software, selezionare **Sì, desidero partecipare (scelta consigliata)**. Applicare questa impostazione a tutti i server, selezionando la casella di controllo accanto a Nome server nel controllo Selezione dei server, quindi fare clic su **OK**.

- Disabilitare Analisi utilizzo software (CEIP)
Aprire Server Manager e selezionare Tutti i server. Nel riquadro Server, selezionare tutti i server (Ctrl+A), fare clic con il pulsante destro del mouse e selezionare **Configurare Commenti e suggerimenti automatici per Windows** . Fare clic sul collegamento al programma Analisi utilizzo software, selezionare **No, non desidero partecipare**. Applicare questa impostazione a tutti i server, selezionando la casella di controllo accanto a Nome server nel controllo Selezione dei server, quindi fare clic su **OK**.
- Abilitare Segnalazione errori Windows (WER)
Aprire Server Manager e selezionare **Tutti i server**. Nel riquadro Server, selezionare tutti i server (Ctrl+A), fare clic con il pulsante destro del mouse e selezionare **Configurare Commenti e suggerimenti automatici per Windows** . Fare clic sulla scheda Segnalazione errori Windows, selezionare **Sì, invia automaticamente rapporti brevi (scelta consigliata)**. Applicare questa impostazione a tutti i server, selezionando la casella di controllo accanto a Nome server nel controllo Selezione dei server, quindi fare clic su **OK**.
- Disabilitare Segnalazione errori Windows (WER)
Aprire Server Manager e selezionare **Tutti i server**. Nel riquadro Server, selezionare tutti i server (Ctrl+A), fare clic con il pulsante destro del mouse e selezionare **Configurare Commenti e suggerimenti automatici per Windows** . Fare clic sulla scheda Segnalazione errori Windows, selezionare **No, non desidero partecipare**. Applicare questa impostazione a tutti i server, selezionando la casella di controllo accanto a Nome server nel controllo Selezione dei server, quindi fare clic su **OK**.

Per informazioni aggiornate sulle procedure di trattamento dei dati di Microsoft, leggi l'[Informativa sulla privacy di Microsoft](#). In questo documento puoi scoprire anche gli strumenti più recenti forniti per l'accesso e il controllo dei dati e come contattare Microsoft per richiedere informazioni sulla privacy.

Informativa sulla privacy di Windows 8 e Windows Server 2012

Elementi di rilievo Informativa Supplemento sulle funzionalità Supplemento sul server

In questa pagina

Ultimo aggiornamento: **Agosto 2012**

Le informazioni dell'utente

Questi elementi di rilievo dell'informativa completa [Informativa sulla privacy di Windows 8 e Windows Server 2012](#) ("Informativa sulla Privacy di Windows") illustra, in generale, alcune procedure di raccolta e di utilizzo dei dati da parte di Windows 8 e Windows Server 2012 ("Windows"). Si concentrano sulle funzioni di comunicazione con Internet e non intendono costituire una descrizione esaustiva. Non si applicano ad altri siti Microsoft online o offline, prodotti o servizi.

Le tue selezioni

Uso delle informazioni

Come contattare Microsoft

Questa informativa sulla privacy presenta quattro sezioni:

- Elementi di rilievo (in questa pagina)
- Informativa, ovvero l'informativa sulla Privacy completa di Windows che include i collegamenti per le funzionalità di Windows che, a loro volta, hanno informative autonome
- Supplemento sulle funzionalità, che descrive le funzionalità che

hanno un impatto sulla privacy in Windows 8 e Windows Server 2012

- Supplemento sul server, che descrive le funzionalità aggiuntive che hanno un impatto sulla privacy in Windows Server 2012

Per ulteriori informazioni su come proteggere il computer, le informazioni personali e la tua famiglia online, visita il Centro sicurezza e protezione.

Le informazioni dell'utente

- Alcune funzionalità di Windows potrebbero chiederti l'autorizzazione per raccogliere o utilizzare informazioni dal computer, incluse quelle personali. Queste informazioni vengono utilizzate da Windows come descritto nella versione completa [Informativa sulla privacy di Windows](#), e anche in [Supplemento sulle funzionalità](#) e [Supplemento sul server](#).
- Con la tua autorizzazione, alcune funzionalità di Windows possono condividere informazioni personali tramite Internet.
- Se scegli di registrare il software, ti verrà richiesto di fornire informazioni personali.
- Windows richiede l'attivazione per ridurre la pirateria software e per aiutare a garantire che gli utenti ricevano la qualità software auspicata. L'attivazione invia alcune informazioni sul PC a Microsoft.
- È possibile scegliere di accedere a Windows con [Account Microsoft](#), che ti consente di sincronizzare le impostazioni di Windows e accedere automaticamente alle app e ai siti Web. Quando crei un account Microsoft, ti verrà richiesto di fornire alcune informazioni personali.
- [Ulteriori dettagli](#)

[Torna all'inizio](#)

Le tue selezioni

- Windows ti offre diversi modi per controllare come le funzionalità di Windows trasferiscano informazioni tramite Internet. Ulteriori informazioni su come controllare queste funzionalità sono consultabili nel Supplemento sulle funzionalità e nel Supplemento sul server.
- Per migliorare l'esperienza, alcune funzionalità, che utilizzano Internet, sono abilitate per impostazione predefinita.
- [Ulteriori dettagli](#)

[Torna all'inizio](#)

Uso delle informazioni

- Utilizziamo le informazioni raccolte per abilitare le funzionalità usate o fornire i servizi richiesti. Le usiamo anche per migliorare i prodotti e servizi. Per garantire l'erogazione dei nostri servizi, occasionalmente forniamo informazioni ad altre aziende che lavorano per nostro conto. L'accesso viene consentito solo alle aziende che hanno un'esigenza aziendale di utilizzare le informazioni. A tali aziende è stato richiesto di mantenere le informazioni riservate ed è stato vietato di utilizzarle per altri scopi.
- [Ulteriori dettagli](#)

[Torna all'inizio](#)

Come contattare Microsoft

Per ulteriori informazioni sulle procedure di tutela della privacy, accedi a [Informativa sulla privacy di Windows](#). Oppure, è possibile scrivere utilizzando [Modulo Web](#).

[Torna all'inizio](#)