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 8.1 e Windows Server 2012 R2

In questa pagina

Ultimo aggiornamento: aprile 2014

I presenti elementi di rilievo tratti dalla versione completa dell'Informativa sulla privacy di Windows 8.1 e Windows Server 2012 R2 (informativa sulla privacy di "Windows") offrono una descrizione di alto livello di alcune delle procedure per la raccolta e l'uso dei dati di Windows 8.1 e Windows Server 2012 R2 ("Windows"). Tali elementi sono incentrati sulle funzionalità online e non sono da intendersi come una descrizione esaustiva. Non si applicano ad altri siti, prodotti o servizi Microsoft online e offline.

La presente informativa sulla privacy è suddivisa nelle sezioni seguenti:

- **In primo piano** (questa pagina)
- Informativa, ovvero l'informativa sulla privacy completa di Windows 8.1, che include collegamenti alle informative sulla privacy relative a funzionalità di Windows per le quali sono disponibili informative specifiche

Supplemento sulle funzionalità, che descrive le funzionalità che hanno impatto sulla privacy in Windows 8.1 e Windows Server 2012 R2

- Supplemento sulle app, che descrive le app che hanno un impatto sulla privacy in Windows 8.1
- Supplemento su Windows Server, che descrive le funzionalità aggiuntive che hanno impatto sulla privacy in Windows Server 2012 R2

Per ulteriori informazioni su come proteggere il PC, le informazioni personali e i familiari online, visitare il Safety and Security Center.

Informazioni personali

- Alcune funzionalità di Windows possono richiedere l'autorizzazione dell'utente per la raccolta o l'utilizzo delle informazioni del PC, incluse le informazioni personali. Windows usa queste informazioni come indicato nella versione completa dell'Informativa sulla privacy di Windows 8.1 Informativa sulla privacy di Windows 8.1 Preview e Windows Server 2012 R2, nonché nelSupplemento sulle funzionalità, nel Supplemento sulle app e nel Supplemento su Windows Server.
- Alcune funzionalità di Windows consentono, con l'autorizzazione dell'utente, di condividere informazioni personali su Internet.
- Se si sceglie di registrare il software in uso, verrà chiesto di fornire informazioni personali.
- Windows richiede l'attivazione per ridurre la pirateria e garantire ai clienti Microsoft la qualità del software che si aspettano. Eseguendo l'attivazione, vengono inviate a Microsoft alcune informazioni sul PC.
- Se si sceglie di accedere a Windows con un account Microsoft, Windows sincronizzerà le impostazioni in tutti i dispositivi ed eseguire automaticamente l'accesso ad alcune app e alcuni siti Web. Windows non richiede di eseguire l'accesso con un account Microsoft per accedere a servizi email o di social network di terze

parti, ma se la terza parte offre un'app tramite lo Store, sarà necessario eseguire l'accesso allo Store con un account Microsoft per installare l'app. Se si crea un account Microsoft, verrà richiesto di fornire alcune informazioni personali, come l'area geografica e la data di nascita.

- Dettagli aggiuntivi

Inizio pagina

Scelte dell'utente

- Windows offre un gran numero di modalità per il controllo del trasferimento delle informazioni via Internet da parte delle funzionalità di Windows. Per informazioni su come controllare queste funzionalità, vedere il Supplemento sulle funzionalità, il Supplemento sulle app e nel Supplemento su Windows Server.

- Al fine di migliorare l'esperienza dell'utente, alcune funzionalità che utilizzano Internet sono attivate per impostazione predefinita.

- Dettagli aggiuntivi

Inizio pagina

Utilizzo delle informazioni

- Microsoft utilizza le informazioni raccolte per abilitare le funzionalità utilizzate dall'utente o fornire i servizi richiesti, nonché per migliorare i suoi prodotti e servizi. Per garantire un'erogazione ottimale dei servizi, vengono occasionalmente fornite informazioni ad altre aziende che lavorano per conto di Microsoft. L'accesso a tali informazioni viene concesso solo alle aziende che devono utilizzarle per esigenze di lavoro. Tali aziende sono tenute a rispettare la riservatezza delle informazioni e non sono autorizzate a utilizzarle per altri scopi.

- Dettagli aggiuntivi

Inizio pagina

Informazioni di contatto

Per altre informazioni sulle politiche per il rispetto della privacy applicate da Microsoft, vedere la versione completa dell'Informativa sulla privacy di Windows 8.1. In alternativa, è possibile scrivere a Microsoft utilizzando l'apposito modulo Web.

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 8.1 e Windows Server 2012 R2

In questa pagina

Ultimo aggiornamento: aprile 2014

La presente informativa sulla privacy si applica a Windows 8.1 e Windows Server 2012 R2 ("Windows"). Per alcuni componenti di Windows sono disponibili informative sulla privacy specifiche, anch'esse elencate in questa pagina. Nell'elenco sono riportate anche le informative sulla privacy per prodotti software e servizi correlati a Windows e per le versioni precedenti.

Per informazioni sulle funzionalità specifiche, fare riferimento al Supplemento sulle funzionalità, nel Supplemento sulle appe il Supplemento su Windows Server. Per informazioni su Windows Embedded Industry Pro e Windows Embedded Industry Enterprise, fare riferimento a questa informativa.

Questa informativa sulla privacy rappresenta una divulgazione preliminare incentrata sulle funzionalità che interagiscono con Internet e non è da intendersi come un elenco esaustivo.

Raccolta e utilizzo delle informazioni dell'utente

Le informazioni personali raccolte dagli utenti verranno utilizzate da Microsoft e dalle sue filiali e consociate per abilitare le funzionalità utilizzate dall'utente e per fornire servizi o effettuare transazioni richieste o autorizzate dall'utente. Le informazioni possono inoltre essere utilizzate per analizzare e migliorare i prodotti e i servizi Microsoft.

Se non altrimenti specificato nella presente informativa, le informazioni personali fornite dall'utente non verranno rese disponibili a terzi senza l'esplicito consenso dell'utente stesso. Saltuariamente vengono incaricate altre aziende di fornire servizi limitati per conto di Microsoft, ad esempio la conduzione di analisi statistiche dei servizi Microsoft. Tali aziende collaboratrici avranno accesso esclusivamente ai dati necessari per la fornitura del servizio e non sarà ad esse consentito l'uso di tali dati per altri scopi.

Microsoft può accedere o divulgare le informazioni sull'utente, incluso il contenuto delle comunicazioni, allo scopo di (a) attenersi a disposizioni di legge o adempiere a richieste giuridiche o a quanto sancito nell'ambito di un'azione legale; (b) tutelare i diritti o la proprietà di Microsoft o dei suoi clienti, inclusa l'applicazione delle condizioni dei contratti di Microsoft o dei criteri che disciplinano l'utilizzo del software o (c) proteggere la sicurezza personale dei dipendenti e dei clienti Microsoft o degli altri utenti, ritenendo in buona fede che l'accesso o la divulgazione sia necessaria a tale scopo.

Le informazioni raccolte da o inviate a Microsoft da Windows 8.1 potrebbero essere archiviate ed elaborate negli Stati Uniti o in altri paesi in cui Microsoft o le sue consociate e affiliate o i suoi provider di servizi dispongono di sedi operative. Microsoft rispetta la convenzione Safe Harbor stabilita dal Ministero del Commercio degli Stati Uniti relativamente alla raccolta, all'uso e alla conservazioni di dati di utenti dei paesi dell'Unione europea, dello Spazio economico europeo e della Svizzera.

Inizio pagina

Raccolta e utilizzo di informazioni relative al computer

Quando si utilizzano prodotti software con funzionalità che sfruttano

Internet, vengono inviate delle informazioni sul computer ("informazioni standard sul computer") ai siti visitati e ai servizi online utilizzati. Le informazioni standard sul computer includono in genere dati quali l'indirizzo IP, la versione del sistema operativo, la versione del browser e le impostazioni internazionali e della lingua. In alcuni casi, possono inoltre includere un ID hardware, che indica il produttore, il nome e la versione del dispositivo. Se una funzionalità o un servizio invia informazioni a Microsoft, verranno incluse anche le informazioni standard sul computer.

I dettagli sulla privacy per ogni funzionalità di Windows nel Supplemento per le funzionalità, nel Supplemento per le app e nel Supplemento per il server, nonché per le funzionalità elencate in altri punti della pagina, descrivono quali ulteriori informazioni vengono raccolte e come vengono utilizzate.

Gli amministratori possono utilizzare Criteri di gruppo per modificare molte delle impostazioni delle funzionalità qui descritte. Per ulteriori informazioni, vedere questo white paper per amministratori.

Inizio pagina

Sicurezza delle informazioni

Microsoft si impegna a proteggere la riservatezza delle informazioni dell'utente. Le diverse tecnologie e procedure di sicurezza utilizzate consentono di impedire l'accesso, l'utilizzo o la divulgazione non autorizzata delle informazioni personali. Ad esempio, le informazioni fornite vengono archiviate su computer ad accesso limitato, situati in strutture controllate. Quando vengono trasmessi su Internet dati altamente riservati (come un numero di carta di credito o una password), questi vengono protetti mediante crittografia, tramite ad esempio il protocollo SSL (Secure Socket Layer).

Inizio pagina

Modifiche alla presente informativa sulla privacy

La presente informativa sulla privacy è soggetta ad aggiornamenti non programmati, in base a corrispondenti variazioni in prodotti e servizi e secondo quanto suggerito dai clienti stessi. In questi casi verrà

modificata la data indicata all'inizio dell'informativa sulla privacy, alla voce "Ultimo aggiornamento". In presenza di modifiche sostanziali alla presente informativa o alle modalità di trattamento dei dati personali da parte di Microsoft, l'utente verrà informato tramite la pubblicazione di una notifica preventiva o l'invio diretto di un avviso. È consigliabile consultare periodicamente questa informativa per mantenersi aggiornati sulle misure adottate da Microsoft per la sicurezza delle informazioni personali raccolte.

Inizio pagina

Per ulteriori informazioni

Microsoft è lieta di ricevere commenti in merito alla presente informativa sulla privacy. Qualora si abbiano domande relativamente all'informativa sulla privacy o si ritenesse che Microsoft non l'abbia rispettata, è possibile scrivere a Microsoft utilizzando l'apposito modulo Web.

Microsoft Privacy
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052
USA

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 8.1 e Windows Server 2012 R2

In questa pagina

Ultimo aggiornamento: aprile 2014

Questa pagina costituisce un supplemento all'Informativa sulla privacy di Windows 8.1 e Windows Server 2012 R2 ("Informativa sulla privacy di Windows"), che contiene quattro sezioni:

- In primo piano
- Informativa, ovvero l'Informativa sulla privacy di Windows 8.1 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 8.1 e Windows Server 2012 R2
- Supplemento sulle app, che descrive le app che hanno un impatto sulla privacy in Windows 8.1
- Supplemento su Windows Server, che descrive le funzionalità

aggiuntive che hanno impatto sulla privacy in Windows Server 2012 R2

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

Attivazione

Scopo della funzionalità

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 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 Microsoft. 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.

Informazioni raccolte, elaborate o trasmesse

Durante l'attivazione vengono inviate a Microsoft le informazioni seguenti:

- 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.

Risoluzione problemi compatibilità programmi

Proprietà

Prossimità

Connessioni di Accesso remoto

Connessione RemoteApp e desktop

Connessione Desktop remoto

Accesso con un account Microsoft

Archiviazione nel cloud OneDrive

Sincronizzazione delle impostazioni

Tecnologia Teredo

Servizi TPM (Trusted Platform Module)

Aggiornamento dei certificati radice

Update Services

Rete privata virtuale

Analisi utilizzo software di Windows

Windows Defender

Segnalazione errori Windows

Associazione file di

- La data di installazione e l'esito dell'installazione.
- Informazioni che confermano che il codice Product Key di Windows non è stato alterato.
- Marca e modello del PC.
- Informazioni sulla versione per sistema operativo e software.
- Impostazioni internazionali e della lingua.
- Un numero univoco denominato GUID (Globally Unique Identifier) assegnato al PC.
- Codice Product Key (con hash) e ID prodotto.
- Nome BIOS, numero di revisione e data di revisione.
- Numero di serie del volume dell'unità disco rigido (con hash).
- Risultato del controllo di attivazione. Sono inclusi codici di errore e informazioni su eventuali exploit di attivazione e su software correlato dannoso o non autorizzato, trovato o disabilitato:
    - 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.
- 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 inviate anche informazioni standard sul computer.
- Se si utilizza una copia di Windows ottenuta tramite contratti multilicenza in cui viene utilizzato un server di attivazione, è possibile che venga inviato a Microsoft. l'indirizzo IP di tale server.

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. Le informazioni sul server licenze vengono utilizzate per verificare che i server licenze siano conformi ai contratti di licenza.

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 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

ID di annuncio

Scopo della funzionalità

Per fornire annunci più pertinenti, Windows consente alle app di accedere a un identificatore univoco per ogni utente di un dispositivo. È possibile ripristinare o disattivare l'accesso a questo identificatore in qualsiasi momento.

Informazioni raccolte, elaborate o trasmesse

Se si consente alle app di accedere all'ID di annuncio, tale ID verrà fornito da Windows a tutte le app che lo richiedono. Le app potrebbero archiviare o trasmettere queste informazioni.

Utilizzo delle informazioni

L'ID di annuncio viene utilizzato dagli sviluppatori di app e dalle reti di annunci per fornire annunci più pertinenti in base alle app utilizzate dall'utente e alla modalità di utilizzo delle stesse. Può essere utilizzato inoltre dagli sviluppatori di app per migliorare la qualità del servizio consentendo loro di determinare la frequenza e l'efficacia degli annunci e di individuare truffe e problemi di sicurezza.

Se si consente alle app di accedere all'ID di annuncio, l'uso dell'identificatore in ogni app è soggetto alle procedure relative alla privacy di tale app.

Scelta e controllo

Se si scelgono le impostazioni rapide durante la configurazione di Windows, Windows consentirà alle app di accedere all'ID annunci. Se si sceglie di personalizzare le impostazioni, è possibile controllare l'accesso all'ID annunci selezionando **Consenti alle app di usare il mio ID annunci per le esperienze tra app** in **Condividi informazioni con Microsoft e altri servizi**. Dopo la configurazione di Windows è possibile modificare questa impostazione nella sezione **Privacy** di Impostazioni PC. Se si disattiva questa impostazione, l'ID annunci non viene inviato alle app che lo richiedono. Riattivando l'impostazione invece verrà generato un nuovo ID annunci.

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 decidono quali informazioni vengano raccolte, per quanto siano conservate e se debbano essere inviate a terzi. Le informazioni potrebbero includere informazioni personali come nomi utente o nomi dei file. Per ulteriori informazioni, contattare l'amministratore di sistema. Nessuna informazione viene inviata a Microsoft.

Utilizzo delle informazioni

Gli amministratori gestiscono anche l'utilizzo delle informazioni di controllo. Generalmente, il registro sicurezza viene utilizzato da responsabili del controllo 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 attivata 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

Biometria

Scopo della funzionalità

Se nel PC è disponibile un lettore di impronta digitale, è possibile accedere a Windows con l'impronta digitale per l'identificazione nelle app che supportano questo metodo

Informazioni raccolte, elaborate o trasmesse

Quando si imposta una nuova impronta digitale, le letture dell'impronta vengono archiviate in locale nel PC. Nessuna informazione viene inviata a Microsoft. Quando si utilizza l'impronta digitale per l'identificazione personale in un'app, l'impronta viene confrontata da Windows con quelle salvate nel PC e il sistema comunica all'app se l'impronta digitalizzata corrisponde a quella associata all'account. Windows non fornisce i dati dell'impronta digitalizzata all'app.

Utilizzo delle informazioni

Windows utilizza le informazioni sulle impronte digitali che si sceglie di archiviare nel PC per l'accesso a Windows tramite impronta digitale.

Scelta e controllo

È possibile aggiungere o rimuovere impronte digitali in **Opzioni di accesso** , nella sezione **Account** di Impostazioni PC.

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 MicrosoftOneDrive. 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 archivierà 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. Tali informazioni di ripristino consentono a BitLocker di distinguere fra utenti autorizzati e non.

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.

Le chiavi di ripristino archiviate nell'account OneDrive dell'utente possono essere visualizzate e gestite all'indirizzo.

Inizio pagina

Contatti

Scopo della funzionalità

Se si utilizza l'app Contatti o un'app di terze parti supportata per la gestione dei contatti, è possibile scegliere di condividere determinati contatti con altre app presenti nel PC, di visualizzare le informazioni sui contatti in una scheda contatto oppure di condividere informazioni specifiche sui contatti con altre app presenti nel PC per eseguire un'azione, ad esempio una chiamata o il mapping di un indirizzo.

Informazioni raccolte, elaborate, archiviate e trasmesse

Quando un'app richiede informazioni sui contatti, Windows consente di scegliere determinati contatti da condividere con l'app. I contatti possono provenire dall'app Contatti o da un'app contatti di terze parti supportata. Windows non condivide per intero l'elenco dei contatti con l'app richiedente.

Se un'app ha accesso a un'informazione relativa a un contatto, ad esempio il numero di telefono o l'indirizzo di posta elettronica, Windows è in grado di visualizzare una scheda contatto con le informazioni aggiuntive provenienti dall'app contatti per tale contatto. Windows non condivide le informazioni aggiuntive sul contatto con l'app che visualizza la scheda contatto.

Toccando o facendo clic su un comando come **Chiama**, il **E-mail**o **Mappa** sulla scheda contatto, Windows apre l'app necessaria per il completamento dell'azione e le fornisce i dettagli sul contatto necessari in tal senso, ad esempio il numero di telefono per l'esecuzione di una chiamata.

Utilizzo delle informazioni

Windows utilizza le informazioni sui contatti provenienti dall'app contatti per condividere i contatti specificati, per visualizzare le schede contatto, per aprire le app e condividere le informazioni sui contatti necessarie per completare le azioni elencate sulle schede contatti, nonché per visualizzare i contatti in Windows Search. L'utilizzo di informazioni relative ai contatti da parte dell'app Contatti è illustrato nell' Informativa sulla privacy relativa alle app per le comunicazioni.

Se vengono condivise informazioni sui contatti con un'app di terze parti, la modalità di utilizzo delle informazioni dipende dalle procedure relative alla privacy della terza parte. Se vengono condivise informazioni sui contatti con un'app Microsoft, le procedure relative alla privacy dell'app saranno illustrate nella relativa Informativa sulla privacy.

Scelta e controllo

Windows visualizza e condivide le informazioni sui contatti soltanto quando si sceglie di condividere determinati contatti con un'app, di visualizzare una scheda contatto o di selezionare un'azione della scheda contatto.

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 da parte di Windows, se nel PC non sono disponibili driver appropriati viene automaticamente contattato il servizio Windows Update online per trovare e scaricare i driver dei dispositivi. Per ulteriori informazioni sui dati raccolti da Windows Update e sulla relativa modalità di utilizzo, vedere l' Informativa sulla privacy di Update Services.

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), l’area geografica e la lingua dell'utente e la data dell'ultimo aggiornamento delle informazioni sul dispositivo. Se è disponibile un'app per il dispositivo, Windows la scarica e la installa automaticamente da Windows Store. L'app sarà disponibile nell'account Windows Store, nell'elenco delle app di proprietà

dell'utente.

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 inviate per identificare o contattare l'utente.

Scelta e controllo

Se si scelgono impostazioni rapide durante la configurazione di Windows, si attivano il download e l'installazione automatici di driver, informazioni e app del dispositivo. Se si sceglie di personalizzare le impostazioni, è possibile controllare il download e l'installazione automatici di driver di dispositivo, app e informazioni selezionando **Ottieni automaticamente driver, app e info per i nuovi dispositivi** in **Contribuisci a proteggere e aggiornare il 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 attivare la condivisione e di connettersi ai dispositivi quando si entra in una rete, l'individuazione della 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 attivare l'individuazione della rete completamente e se attivare 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 si desidera che Windows non trasmetta il nome del PC tramite Wi-Fi mentre vengono aggiunti dispositivi, disattivare temporaneamente il Wi-Fi nella sezione Wireless in Impostazioni PC prima di aggiungere un dispositivo.

Inizio pagina

Crittografia del dispositivo

Scopo della funzionalità

La crittografia del dispositivo consente di proteggere i dati crittografandoli tramite la tecnologia Crittografia unità BitLocker, che contribuisce a impedire gli attacchi software offline. Quando si attiva la crittografia del dispositivo, i dati presenti nell'unità in cui è installato Windowsvengono crittografati da Windows.

Informazioni raccolte, elaborate o trasmesse

Se si utilizza la crittografia software, le chiavi crittografiche nella memoria crittograferanno e decrittograferanno continuamente i dati quando vengono letti o scritti nell'unità protetta. Se si utilizza la crittografia hardware, la crittografia e decrittografia dei dati verrà eseguita dall'unità.

Per archiviare e gestire le chiavi crittografiche utilizzate per crittografare l'unità, Windows utilizza il modulo TPM (Trusted Platform Module) presente nel PC. Quando la crittografia dei dispositivi è attivata, Windows crittografa automaticamente l'unità in cui è installato Windows e genera una chiave di ripristino, che può essere utilizzata per accedere ai dati protetti quando si verificano determinati errori hardware o altri problemi.

Il backup della chiave di ripristino di BitLocker del PC viene eseguito automaticamente online nell'account Microsoft OneDrive di ogni account amministratore connesso a un account Microsoft. Anche il backup del nome del computer e dell'identificatore della chiave di ripristino viene eseguito nello stesso account OneDrive. Per proteggere la privacy dell'utente, le informazioni inviate vengono crittografate tramite SSL.

Utilizzo delle informazioni

Le chiavi crittografiche e gli identificatori univoci globali (GUID) vengono memorizzati nel PC per supportare le operazioni di BitLocker. Le informazioni di ripristino consentono di accedere ai dati protetti quando si verificando determinati errori hardware o altri problemi e permettono a BitLocker di distinguere fra utenti autorizzati e non autorizzati

Microsoft esegue il backup delle informazioni di ripristino nell'account OneDrive dell'utente, affinché sia possibile accedervi online. Microsoft

non utilizza le informazioni sulle chiavi di ripristino, né le archivia in posizioni diverse dall'account OneDrive dell'utente. Microsoft potrebbe utilizzare dati aggregati sulle chiavi di ripristino per analizzare le tendenze e contribuire a migliorare i propri prodotti e servizi. Tali informazioni potrebbero essere ad esempio utilizzate per determinare la percentuale di computer in cui è attivata la crittografia del dispositivo.

Scelta e controllo

Se durante la configurazione del PC si sceglie di utilizzare un account Microsoft, verrà automaticamente attivata la crittografia del dispositivo, se supportata dal PC, e verrà eseguito il backup della chiave di ripristino nell'account OneDrive dell'utente. Se invece durante la configurazione del PC si sceglie di utilizzare un account locale, la crittografia del dispositivo verrà disattivata.

Se in seguito si connette un account Microsoft a un account amministratore nel computer, si verifica quanto segue:

- Se la crittografia del dispositivo non è attivata, viene attivata automaticamente da Windows e viene eseguito il backup delle informazioni di ripristino nell'account OneDrive dell'utente.
- Se invece la crittografia del dispositivo è già attivata, verrà eseguito il backup delle informazioni di ripristino per il PC nell'account OneDrive dell'utente.

È possibile visualizzare e gestire le chiavi di ripristino archiviate nell'accountOneDrive all'indirizzo.

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

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 sulla TV sono difficili da vedere.

- L'illuminazione rende difficile la visione di immagini sul monitor.
- Non utilizzo una tastiera.
- Sono non vedente.
- Sono non udente.
- Soffro di un disturbo del linguaggio.

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

Utilizzo delle informazioni

Vengono forniti alcuni consigli sulla configurazione in base alle frasi scelte in precedenza. Queste informazioni non vengono inviate a Microsoft e non sono disponibili per altri utenti, ad eccezione dell'utente corrente e degli amministratori del PC.

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 configurare 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 accedere alle voci dei registri eventi. Gli amministratori possono comunque scegliere di limitarne l'accesso. È possibile

accedere ai registri eventi del PC aprendo il Visualizzatore eventi. Per informazioni sull'avvio 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 con accesso completo ai registri del Visualizzatore eventi sono autorizzati a cancellarne il contenuto. 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. Non verranno inviate informazioni tramite Internet senza il consenso da parte dell'utente. Gli amministratori possono usare i Criteri di gruppo per selezionare o modificare il sito a cui vengono inviate le informazioni sugli eventi.

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 attiva la gestione online per un account bambino, 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 attivata automaticamente.

Se si configura Family Safety per un account bambino 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 dal 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 includono i dati personali immessi in una copertina per fax e gli identificatori contenuti nei protocolli standard per la comunicazione via fax come l'identificativo stazione trasmittente (IDST) e l'identificativo stazione ricevente (IDSR). Per impostazione predefinita, in Windows viene utilizzato "Fax" come valore per ogni identificatore.

Utilizzo delle informazioni

Le informazioni immesse nella finestra di dialogo mittente vengono riportate sulla copertina del fax. Gli identificativi come IDST e IDSR 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. Se non vengono modificate le impostazioni di accesso da parte di un amministratore del fax, 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 fax inviati e ricevuti e configurare le impostazioni fax, compresi i permessi per la visualizzazione o la gestione dei fax e i valori IDST e IDSR.

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. Grazie a questa funzionalità è possibile raccogliere dati sulle parole utilizzate e sul modo in cui vengono scritte. In questo modo il software per il riconoscimento della grafia può migliorare l'interpretazione della grafia e il vocabolario e migliorano anche la correzione automatica e i suggerimenti di testo per le lingue senza IME (Input Method Editor).

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 con tastiere virtuali.
- Caratteri alternativi selezionati per correggere il testo riconosciuto.

Utilizzo delle informazioni

Le informazioni raccolte vengono utilizzate per contribuire a migliorare il riconoscimento della grafia creando una versione del software di riconoscimento personalizzata per il proprio stile e vocabolario e per attivare la correzione automatica e i suggerimenti di testo mentre si digita con tastiere virtuali.

Gli esempi di testo vengono utilizzati per creare un vocabolario esteso. I campioni di input penna vengono utilizzati per migliorare il riconoscimento della grafia per ogni utente in un PC. Nessuna informazione viene inviata a Microsoft.

Scelta e controllo

L'apprendimento automatico è attivato per impostazione predefinita. È possibile attivare o disattivare l'apprendimento automatico in qualsiasi momento in **Impostazioni avanzate** , nella sezione **Lingue** nel Pannello di controllo. Quando si disattiva l'apprendimento automatico, tutti i dati raccolti e archiviati mediante l'apprendimento automatico 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 attivare 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 a **Gruppo Home** in **Rete** di Impostazioni PC.

Inizio pagina

IME (Input Method Editor)

Gli IME (Input Method Editor) Microsoft vengono utilizzati per convertire gli input da tastiera in ideogrammi di lingue asiatiche. In questa sezione vengono illustrate varie funzionalità, tra cui la regolazione automatica e previsione IME, la segnalazione degli errori di conversione IME e la registrazione delle parole IME.

Candidati dall'IME nel cloud

Scopo della funzionalità

Quando si utilizza l'IME Microsoft Pinyin per l'immissione di caratteri in cinese semplificato, l'IME può utilizzare un servizio online per cercare

ideogrammi candidati per l'input digitato che non esiste in un dizionario locale nel PC in uso.

Informazioni raccolte, elaborate o trasmesse

Durante la digitazione di caratteri in cinese semplificato tramite l'IME Microsoft Pinyin, l'IME suggerisce ideogrammi che potrebbero essere utilizzati. Se l'IME non riesce a trovare un suggerimento valido nel dizionario locale, invierà l'input da tastiera a Microsoft per stabilire se esistono ideogrammi candidati migliori per tale input. Se sono disponibili, gli ideogrammi verranno visualizzati nell'elenco dei candidati e, se selezionati, verranno aggiunti al dizionario locale. Verrà inviato anche un identificatore univoco a generazione casuale per consentire a Microsoft di analizzare l'utilizzo di questa funzionalità. L'identificatore non è associato all'account Microsoft dell'utente e non viene utilizzato per identificare o contattare l'utente, né per inviargli pubblicità mirata.

Utilizzo delle informazioni

Microsoft utilizza le informazioni raccolte per cercare ideogrammi nel cloud e migliorare i suoi prodotti e servizi. Microsoft non utilizzerà tali informazioni per identificare o contattare l'utente, né per inviargli pubblicità mirata.

Scelta e controllo

La ricerca di candidati dall'IME nel cloud è disattivata per impostazione predefinita per l'IME Microsoft Pinyin per il cinese semplificato. Per visualizzare o modificare questa impostazione, aprire Impostazioni PC, fare clic su **Data/ora e lingua**, fare clic su **Area geografica e lingua**, scegliere la propria lingua e quindi fare clic su **Opzioni**.

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

Le funzionalità di apprendimento automatico e di suggerimento del testo sono attive per impostazione predefinita negli IME che le 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 attivare l'invio automatico delle segnalazioni errori conversione in Impostazioni IME.

Registrazione delle parole 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

Condivisione connessione Internet

Scopo della funzionalità

Condivisione connessione Internet consente di condividere la connessione Internet Mobile Broadband con altri dispositivi tramite Wi-Fi. È inoltre possibile avviare Condivisione connessione Internet in remoto nel dispositivo Mobile Broadband dal PC se si utilizza lo stesso account Microsoft per accedere a entrambi.

Informazioni raccolte, elaborate o trasmesse

Alla prima condivisione della connessione Internet, Windows genera e archivia automaticamente un nome di rete e una password. È possibile modificare questi dati in qualsiasi momento.

Se il PC lo supporta ed è stato aggiunto all'account Microsoft come dispositivo attendibile, Windows sincronizza nome di rete e password con l'account Microsoft. Windows sincronizza anche altre informazioni per consentire l'avvio remoto di Condivisione connessione Internet da altri dispositivi attendibili. Tali informazioni includono l'indirizzo hardware della radio Bluetooth e un numero casuale utilizzato per proteggere la connessione.

Utilizzo delle informazioni

Queste informazioni vengono utilizzate per configurare Condivisione connessione Internet. Microsoft non utilizza le informazioni per identificare o contattare l'utente, né per inviargli pubblicità mirata.

Scelta e controllo

Se si accede a un dispositivo che supporta Condivisione connessione Internet con l'account Microsoft personale e si aggiunge tale dispositivo come dispositivo attendibile, le informazioni necessarie per l'avvio remoto di Condivisione connessione Internet verranno sincronizzate in OneDrive. È possibile interrompere la sincronizzazione delle informazioni scegliendo di non sincronizzare le password. Per ulteriori informazioni, vedere la sezione "Sincronizzazione delle impostazioni" di questa pagina.

Inizio pagina

Stampa Internet

Scopo della funzionalità

Stampa Internet consente di stampare da Internet.

Informazioni raccolte, elaborate o trasmesse

Quando si stampa con questa funzionalità, è innanzitutto necessario connettersi a un server di stampa via Internet ed eseguire l'autenticazione. Le informazioni da inviare al server di stampa varieranno in base al livello di sicurezza supportato dal server di stampa (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 da stampanti remote. Se si sceglie di utilizzare un server di stampa ospitato da 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 le lingue preferite da utilizzare all'elenco delle lingue in Windows 8.1. 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 Area geografica nel Pannello di controllo verrà inviata ai siti Web visitati.

Inizio pagina

Servizi di posizione

I servizi di posizione di Windows consentono di decidere quali app, siti Web e funzionalità di Windowssi desidera autorizzare a determinare la posizione del PC. I servizi di posizione di Windows sono costituiti da due componenti. Localizzatore geografico di Windows, che si connette a un servizio online Microsoft per determinare la posizione dell'utente. Piattaforma di localizzazione geografica di Windows, che determina la posizione del PC tramite hardware, ad esempio un sensore GPS, o tramite software, ad esempio il componente 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 e alcune funzionalità di Windows potranno richiedere l'autorizzazione ad accedere alla posizione del PC. Se si consente a un'app di utilizzare la posizione dell'utente, oltre a fornire la posizione mentre viene utilizzata l'app, la piattaforma di localizzazione geografica di Windows può indicare all'app quando il PC si sposta all'interno o all'esterno dei confini geografici definiti per l'app. Un'app ad esempio può consentire di impostare un promemoria per ricordarsi di fare la spesa quando si esce dall'ufficio. A seconda della configurazione del sistema, la piattaforma di localizzazione geografica di Windows può determinare la posizione del PC tramite hardware, ad esempio un sensore GPS, o tramite software, ad esempio Localizzatore geografico di Windows.

La piattaforma di localizzazione geografica di Windows non impedisce alle app di determinare la posizione del PC in altri modi. È ad esempio possibile installare dispositivi (come un ricevitore GPS) in grado di inviare informazioni sulla posizione direttamente a un'app ignorando la piattaforma. Indipendentemente dalle impostazioni della piattaforma di localizzazione geografica di Windows, i servizi online possono utilizzare l'indirizzo IP per determinare 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 Localizzatore geografico di Windows, potrebbero trasmettere dati se richiesti dalla piattaforma di localizzazione geografica di Windows per determinare la posizione del PC. È possibile che anche le app, i siti Web e le funzionalità autorizzati a utilizzare la piattaforma per determinare la posizione del computer trasmettano o archivino tali informazioni. Se in un'app vengono configurati confini geografici da monitorare, tali confini verranno archiviati in forma crittografata nel computer. Tra le informazioni archiviate relative ai confini sono inclusi un nome, una posizione e la presenza del computer all'interno o all'esterno del confine l'ultima volta che ne è stata determinata la posizione. È possibile che le app in cui vengono configurati confini geografici trasmettano o archivino queste informazioni

Utilizzo delle informazioni

Se si attiva la piattaforma di localizzazione geografica di Windows, le app, i siti Web e le funzionalità di Windows autorizzati saranno anche in grado di accedere alla posizione del PC e di 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 a Windows e alle app di richiedere la mia posizione alla piattaforma di localizzazione geografica di Windows in Condividi informazioni con Microsoft e altri servizi. La prima volta che ogni app di Windows Store richiede la posizione del PC, viene richiesto se si desidera consentire all'app di utilizzare la posizione. È possibile visualizzare e modificare questa impostazione per ogni app di Windows Store in Autorizzazioni nelle 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 app in **Privacy** in Impostazioni PC. Gli amministratori possono inoltre scegliere di disattivare la piattaforma di localizzazione per tutti gli utenti utilizzando **Impostazioni posizione** nel Pannello di controllo. Per evitare che le app ricevano notifiche quando vengono attraversati i confini geografici in esse definiti, un utente amministrativo può disattivare Servizio Framework localizzatore Windows nel Pannello di controllo.

Localizzatore geografico di Windows

Scopo della funzionalità

Il Localizzatore geografico di Windows si connette al servizio di rilevamento della posizione Microsoft online, 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 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 archiviato di punti di accesso Wi-Fi nelle vicinanze proveniente da una richiesta precedente di un'app in grado di riconoscere 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 rilevamento della posizione di Microsoft. Il servizio restituisce la posizione approssimativa del PC al localizzatore, che passa l'informazione alla piattaforma di localizzazione geografica di Windows, che a sua volta la fornisce all'app che ha richiesto la posizione del PC. 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 delle reti Wi-Fi, Windows non invia informazioni sui SSID (nomi dei punti di accesso Wi-Fi) o sulle reti Wi-Fi nascoste. Al fine di garantire privacy e sicurezza, le informazioni sulle reti Wi-Fi inviate vengono crittografate tramite SSL.

Se si sceglie di contribuire a migliorare il servizio di localizzazione geografica di Microsoft, Windows potrebbe inviare di nuovo a Microsoft le informazioni sui punti di accesso Wi-Fi vicini dopo che un'app richiede la posizione del PC. Se si utilizza una connessione Internet a consumo, Windows limiterà il numero di volte al giorno in cui vengono inviate queste informazioni, per limitare l'uso della connessione Internet.

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 rilevamento della 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 le impostazioni rapide durante la configurazione di Windows, si sceglie di contribuire a migliorare il servizio di rilevamento della posizione di Microsoft. Se si sceglie di personalizzare le impostazioni, è possibile specificare se si desidera contribuire al miglioramento del servizio di localizzazione geografica di Microsoft selezionando **Invia alcuni dati sulla posizione a Microsoft quando vengono utilizzate app in grado di riconoscere la posizione** in **Contribuisci al miglioramento dei prodotti e**

servizi Microsoft. 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 attivare o disattivare 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

Gestisci le credenziali

Scopo della funzionalità

Windows consente di connettere le app di Windows Store agli account utilizzati per i siti Web. Se in precedenza è stata salvata una password per un sito Web in Internet Explorer, Windows può utilizzare la password salvata per la connessione di un'app a tale sito Web.

Informazioni raccolte, elaborate o trasmesse

Quando un'app richiede le credenziali per l'accesso a un sito Web, è possibile scegliere di salvare tali credenziali. Se è già stato eseguito l'accesso al sito Web in Internet Explorer e si è scelto di salvare le credenziali, Windows inserisce automaticamente le credenziali salvate. Le credenziali vengono archiviate in forma crittografata nel PC. Per ulteriori informazioni su come sincronizzare queste e altre credenziali in OneDrive, vedere la sezione "Sincronizzazione delle impostazioni" di questa pagina.

Utilizzo delle informazioni

Windows utilizza la credenziali salvate esclusivamente per facilitare l'accesso a siti Web selezionati. Se si salvano le credenziali durante la connessione di un'app a un sito Web, le credenziali salvate non verranno utilizzate in Internet Explorer o in altre app.

Scelta e controllo

È possibile gestire le credenziali salvate in Gestione credenziali nel Pannello di controllo. Per ulteriori informazioni su come sincronizzare queste e altre credenziali in OneDrive, vedere la sezione "Sincronizzazione delle impostazioni" di questa pagina.

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 **Account** in 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 Microsoft e altri servizi**. Dopo la configurazione di Windows è possibile modificare questa impostazione in **Privacy** in Impostazioni PC. È possibile modificare l'immagine dell'account nella sezione **Account** in Impostazioni PC. È inoltre possibile scegliere di consentire a determinate 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 impedirebbe il corretto funzionamento di alcune funzionalità di Windows.

Inizio pagina

Notifiche, app della schermata di blocco e aggiornamenti dei riquadri

Le app di Windows Store possono ricevere contenuti e visualizzare notifiche automaticamente in vari modi. Le notifiche ricevute possono, ad esempio, essere visualizzate brevemente 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 in **Notifiche** in **Ricerca e app** in 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 nel PC dell'utente.

App della schermata di blocco

Scopo della funzionalità

Alcune app di Windows Store possono visualizzare informazioni di stato e notifiche sullo schermo mentre il PC è bloccato. Le app della schermata di blocco supportano anche l'esecuzione di operazioni mentre il PC è bloccato, ad esempio la sincronizzazione della posta

elettronica in background o la possibilità di rispondere a telefonate in arrivo. È inoltre possibile utilizzare la fotocamera del PC direttamente dalla schermata di blocco.

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 Skype vengono impostate automaticamente come app della schermata di blocco. È possibile aggiungere o rimuovere queste o altre app nella schermata di blocco e disattivare l'utilizzo della fotocamera in **Schermata di blocco** in **PC e dispositivi** in 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 stabilire se le app della schermata di blocco possono visualizzare notifiche nella schermata di blocco in **Notifiche** in **Ricerca e app** 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

Ordina 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 inviare un ordine a un servizio di stampa di foto online, le fotografie digitali verranno trasmesse via Internet al servizio scelto dall'utente. 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 Esplora file. 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 nei siti Web dei servizi di stampa di foto online vengono trasmesse allo specifico servizio utilizzato.

Utilizzo delle informazioni

Le informazioni archiviate dalla fotocamera nei file immagine digitali potrebbero essere utilizzate dal servizio di stampa di foto online durante il processo di stampa, ad esempio per regolare l'intensità del 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 sul fronte 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

Con Ordinazione stampe è possibile scegliere quali immagini inviare e

quale servizio utilizzare per la stampa delle 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. È inoltre possibile modificare le proprietà del file per rimuovere dati personali.

Inizio pagina

Prelettura e preavvio

Scopo della funzionalità

In Windows l'avvio di app e funzionalità di Windows viene velocizzato tenendo traccia di quando vengono utilizzate tali app e funzionalità e con quale frequenza, nonché dei file di sistema caricati.

Informazioni raccolte, elaborate o trasmesse

Quando si utilizza un'app o una funzionalità di Windows, Windows salva nel PC alcune informazioni relative ai file di sistema utilizzati, nonché al momento e alla frequenza di utilizzo dell'app o della funzionalità.

Utilizzo delle informazioni

In Windows le informazioni sull'utilizzo dell'app e della funzionalità vengono utilizzate per velocizzarne l'avvio. In alcuni casi, le app potrebbero essere avviate automaticamente in stato sospeso.

Scelta e controllo

Le app avviate e sospese automaticamente vengono visualizzate in Gestione attività e possono essere terminate. Nello stato sospeso, queste app non possono accedere alla webcam o al microfono fino all'avvio, anche se questa funzionalità è stata abilitata in precedenza.

Inizio pagina

Risoluzione problemi compatibilità programmi

Scopo della funzionalità

Se viene rilevato un problema di incompatibilità con un'app desktop 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 organizzare i file ed eseguire ricerche di file rapidamente. 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. Le proprietà includono nome del file, data dell'ultima modifica, dimensioni del file, autore, parole chiave e commenti. Le proprietà vengono archiviate nel file e si spostano insieme al file se questo viene spostato o copiato in un'altra posizione, come accade con una condivisione di file o se viene inviato come allegato di un messaggio di posta elettronica.

Utilizzo delle informazioni

Le proprietà sono utili per effettuare ricerche ed organizzare i file più velocemente. 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 Esplora file e facendo clic su **Proprietà**. Alcune proprietà intrinseche, ad esempio la data dell'ultima modifica, le dimensioni del file, il nome del file e alcune proprietà specifiche per l'app non possono essere rimosse in questo modo. 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 di prossimità NFC

Scopo della funzionalità

Se il PC dispone di hardware NFC (Near Field Communication), è possibile metterlo in contatto fisico con un altro dispositivo o accessorio 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 le informazioni di associazione Bluetooth, gli indirizzi di rete 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 NFC è attivato, è attivata anche la funzionalità Tocco e invio. Per ulteriori informazioni, vedere la sezione Servizio di prossimità NFC.

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. La funzionalità Connessione remota include componenti per la connessione telefonica come il client RAS, Connection Manager e l'utilità RAS Phone, nonché strumenti da 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. Nel caso degli strumenti da riga di comando come Rasdial, non è possibile scegliere di 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.

Se il PC o l'app a cui ci si desidera connettere è ospitato da Microsoft, è possibile che vengano inviate a Microsoft ulteriori informazioni sulla connessione per scopi di supporto.

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 se la connessione remota non è ospitata da 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. Per aggiungere una nuova connessione, fare clic su **Accedi a RemoteApp e desktop**e immettere un URL di 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. Un elenco viene archiviato nel Registro di sistema. Tale elenco viene archiviato in modo permanente a meno che non venga eliminato da un amministratore. Nessuna informazione viene inviata a Microsoft se la connessione remota non è ospitata da 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 per l'accesso ad app, siti e servizi forniti da Microsoft e da partner Microsoft 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 accedere a Windows con un account Microsoft oppure, nei prodotti che lo supportano, scegliere di connettere il proprio 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 visita un sito Web a cui si accede con un account Microsoft, Windowseseguirà l'accesso automaticamente.

Informazioni raccolte, elaborate o trasmesse

Quando si immette un indirizzo di posta elettronica da utilizzare come account Microsoft durante la configurazione del PC oppure in **Account** in 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, come un numero di cellulare utilizzabile per verificare il titolare dell'account. Se non si dispone di un account Microsoft, è possibile crearne uno utilizzando qualsiasi indirizzo di posta elettronica.

Quando si accede con un account Microsoft, Windows invierà a Microsoft anche informazioni standard sul computer, inclusi il produttore, il nome del modello e la versione del dispositivo.

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 l'account Microsoftpersonale o con un account di dominio connesso all'account Microsoft:

- Determinate impostazioni di Windows verranno sincronizzate tra tutti i PC a cui si accede con l'account Microsoft. Per ulteriori informazioni sulle impostazioni sincronizzate e su come controllarle, vedere la sezione "Sincronizzazione delle impostazioni" di questa pagina.

- Le app Microsoft in cui viene utilizzato un account Microsoft per l'autenticazione, ad esempio Mail, Calendario, Contatti, 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 a cui si accede con l'account Microsoft. Se si visita Bing.com, ad esempio, è possibile che l'accesso venga eseguito automaticamente senza dover 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" di questa pagina.

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 sull'impatto prodotto sulla privacy dall'utilizzo di un account Microsoft, leggere l' informativa sulla privacy dell'account Microsoft. Per informazioni sull'utilizzo delle informazioni associate all'account Microsoft nelle singole app Microsoft, vedere le informative sulla privacy delle singole app. L'informativa sulla privacy di un'app Microsoft specifica può essere visualizzata accedendo alle impostazioni dell'app o aprendo la finestra di dialogo Informazioni su.

Le informazioni standard sul dispositivo potrebbero essere utilizzate per personalizzare determinate comunicazioni con l'utente, ad esempio i messaggi di posta elettronica inviati allo scopo di supportare l'utente durante i primi utilizzi del dispositivo.

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" di questa pagina. Per ulteriori informazioni sui dati

raccolti dalle app Microsoft che utilizzano un account Microsoft per l'autenticazione, leggere le informative sulla privacy corrispondenti.

Nei prodotti che lo supportano, è possibile creare un account locale o un account Microsoft in qualsiasi momento nella pagina **Account** , disponibile in Impostazioni del PC. Se si accede a Windows con un account di dominio, è possibile connettere o disconnettere l'account Microsoft in qualsiasi momento nella sezione **Account** 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

Archiviazione nel cloud OneDrive

Scopo della funzionalità

Quando si esegue l'accesso con un account Microsoft nel dispositivo, è possibile scegliere di salvare automaticamente determinati contenuti e impostazioni nei server Microsoft in modo da disporre di un backup in caso di problemi con il dispositivo.

Informazioni raccolte, elaborate o trasmesse

Se durante l'installazione si sceglie di utilizzare OneDrive per l'archiviazione nel cloud, Windows invierà automaticamente ai server Microsoft contenuti quali:

- Foto e video nel dispositivo salvati nella cartella **rullino** .
- Impostazioni specifiche del dispositivo e non condivise tra i dispositivi.
- Informazioni descrittive relative al dispositivo, ad esempio il nome e il tipo.

È inoltre possibile scegliere di salvare contenuto nei server Microsoft e per le app è possibile selezionare i server Microsoft come percorso di salvataggio predefinito per i file.

Utilizzo delle informazioni

In Windows questo contenuto viene utilizzato per fornire il servizio di archiviazione nel cloud. Microsoft non utilizza il contenuto o le informazioni per identificare o contattare l'utente, né per inviargli pubblicità mirata.

Scelta e controllo

Se si sceglie di utilizzare OneDrive durante la configurazione del PC, Windows salverà automaticamente il contenuto descritto in questa sezione in OneDrive. È possibile modificare queste impostazioni in qualsiasi momento nella sezione OneDrive di Impostazioni PC.

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 uno o 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 verranno aggiornate automaticamente 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:

- Il layout della schermata Start
- Le app installate da Windows Store
- 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
- I dizionari del correttore ortografico, IME e personali
- La cronologia del Web browser, i preferiti e i siti Web visitati
- Password salvate per app, siti Web e rete
- Gli indirizzi di stampanti di rete condivise a cui è stata effettuata la connessione

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 che si è scelto di sincronizzare con gli altri PC tramite l'account Microsoft.

Utilizzo delle informazioni

Windows 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, le impostazioni vengono sincronizzate per impostazione predefinita. Per scegliere di sincronizzare le impostazioni e determinare quali

impostazioni sincronizzare, è possibile accedere a **Sincronizzazione delle impostazioni** nella sezione OneDrive di Impostazioni PC. Se si accede a Windows con un account di dominio e si sceglie di connettere tale account a un account Microsoft, in Windows verrà richiesto di specificare quali impostazioni si desidera sincronizzare prima di connettere l'account Microsoft.

Inizio pagina

Tecnologia Teredo

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. Quando viene localizzato il servizio, le informazioni vengono inviate per mantenere la 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 TPM (Trusted Platform Module)

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 del dispositivo, 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. 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, la crittografia del dispositivo 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 anche 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

L'aggiornamento dei certificati radice invia una richiesta al servizio Windows Update online, richiedendo l'elenco aggiornato delle autorità di certificazione radice del programma Microsoft Root Certificate. Se il certificato non attendibile è presente nell'elenco, la funzionalità di aggiornamento dei certificati radice ottiene tale certificato da Windows Update e lo inserisce nell'archivio dei certificati attendibili nel PC. Le informazioni trasferite includono nomi e hash di crittografia dei certificati radice.

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 in un PC.

Inizio pagina

Update Services

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

Update Services raccoglie dal PC dell'utente informazioni che consentono a Microsoft di gestire e migliorare i servizi, ovvero:

- Informazioni sul software Microsoft e gli altri componenti di supporto, quali driver e firmware forniti dai produttori dei dispositivi, installati nel PC e per cui sono disponibili aggiornamenti in Update Services. Le informazioni raccolte consentono di identificare gli aggiornamenti appropriati per l'utente.
- Le impostazioni di configurazione di Windows Update e/o Microsoft Update, ad esempio la possibilità di scaricare o installare automaticamente gli aggiornamenti.
- Operazioni riuscite e non riuscite, oltre agli errori che si verificano quando l'utente accede ai servizi di aggiornamento e li utilizza.

- ID dei dispositivi Plug and Play, ovvero il codice assegnato dal produttore del dispositivo al fine di identificarlo (ad esempio, un particolare tipo di tastiera).
- Identificatore univoco globale (GUID, Globally Unique Identifier), ovvero un 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, fornitore e data di revisione, ovvero informazioni relative al set delle routine software fondamentali per testare l'hardware, avviare il sistema operativo nel PC e trasferire dati tra i dispositivi hardware collegati al PC.
- Produttore, modello, ruolo della piattaforma e numero di SKU, ovvero le informazioni sul PC utilizzate per le indagini diagnostiche relative all'installazione dei driver.

Per utilizzare Update Services è possibile aprire Windows Update nel Pannello di controllo e verificare la disponibilità degli aggiornamenti oppure modificare le impostazioni in modo da consentire a Windows di installare automaticamente gli aggiornamenti appena sono disponibili (scelta consigliata). In Windows Update è possibile scegliere esplicitamente di utilizzare Microsoft Update.

Se si sceglie di scaricare gli aggiornamenti importanti del software per il 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 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 .

Utilizzo delle informazioni

Le informazioni inviate a Microsoft vengono utilizzate per l'esecuzione e gestione di Update Services. Vengono inoltre utilizzate per generare statistiche aggregate che consentono di analizzare le tendenze e

migliorare i prodotti e servizi Microsoft, incluso Update Services.

Per generare le statistiche aggregate, i servizi di aggiornamento utilizzano il GUID raccolto da Update Services per monitorare e registrare il numero di singoli computer che utilizzano Update Services, nonché l'esito positivo o negativo delle operazioni di download e installazione di aggiornamenti specifici. Update Services registra il GUID del computer che ha tentato il download e l'installazione, l'ID dell'elemento richiesto, la disponibilità degli aggiornamenti e informazioni standard sul computer.

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

Aggiornamenti obbligatori

Se si attiva Update Services, per assicurare il funzionamento corretto di tale servizio è necessario aggiornare periodicamente alcuni componenti software del sistema, che formano o sono direttamente correlati a Update Services. Tali aggiornamenti devono essere applicati per consentire al servizio di rilevare, scaricare o installare altri aggiornamenti. Gli aggiornamenti obbligatori correggono errori, forniscono miglioramenti continui e assicurano la compatibilità con i server Microsoft che supportano il servizio.

Se Update Services è disattivato, il sistema non riceverà tali aggiornamenti.

Gli aggiornamenti software necessari per installare o aggiornare le app di Windows Store vengono scaricati e installati automaticamente. Questi aggiornamenti devono essere eseguiti per il corretto funzionamento delle app.

Cookie e token

Un token è simile a un cookie. Memorizza informazioni in un piccolo file che viene collocato sul disco rigido dell'utente dal server Update Services e che viene utilizzato quando il computer si connette a tale server per mantenere una connessione valida. Questo file viene

archiviato solo nel computer dell'utente, non nel server. Nel cookie o nel token sono contenute informazioni, come la data e l'ora dell'ultima analisi, che consentono di trovare gli ultimi aggiornamenti disponibili. Sono incluse informazioni che consentono di determinare i contenuti da scaricare nel computer dell'utente e quando scaricarli, oltre a un GUID che consente al server di identificare il computer.

Le informazioni contenute nel cookie o nel token vengono crittografate dal server, ad eccezione della data e ora di scadenza del cookie o del token. Poiché non si tratta di un cookie o di un token del browser, non può essere controllato tramite le impostazioni del browser. Il cookie o il token non può essere rimosso. Tuttavia, se non si utilizza Update Services il cookie o il token non verrà utilizzato.

Scelta e controllo

Se si scelgono le impostazioni rapide durante l'installazione di Windows, il servizio Windows Update viene attivato e impostato per l'installazione automatica degli aggiornamenti.

Indipendentemente dall'impostazione selezionata, se si attiva Update Services gli aggiornamenti obbligatori per alcuni componenti del servizio verranno scaricati e installati automaticamente senza informare l'utente. Se non si desidera ricevere gli aggiornamenti obbligatori, disattivare Update Services.

È inoltre possibile specificare se rilevare o installare automaticamente sia gli aggiornamenti importanti che quelli consigliati per il computer o solo gli aggiornamenti importanti. Gli aggiornamenti facoltativi non vengono mai installati automaticamente. Dopo la configurazione di Windows è possibile modificare le impostazioni di Windows Update nel Pannello di controllo o in Impostazioni PC.

Se è stato scelto di cercare e installare gli aggiornamenti importanti e ricevere lo Strumento di rimozione malware per Microsoft Windows nell'ambito di tali aggiornamenti per il computer, è possibile disattivare le funzionalità di segnalazione dello strumento.

Inizio pagina

Rete privata virtuale

Scopo della funzionalità

Una rete privata virtuale (VPN) consente di connettersi a una rete privata, quale una rete aziendale, attraverso Internet. Una connessione VPN può essere fornita dal client VPN di Windows oppure da un'app VPN di terze parti.

Informazioni raccolte, elaborate o trasmesse

Quando ci si connette a una rete VPN, le credenziali immesse nel client VPN vengono inviate alla rete remota. È possibile archiviare tali credenziali nel PC in uso. Dopo la connessione, a seconda della configurazione della rete VPN, il routing delle attività di rete avverrà interamente o in parte attraverso la rete remota. Gli amministratori possono configurare app specifiche per il routing del traffico attraverso la VPN e per la connessione automatica alla rete VPN all'avvio di tali app. Nessuna informazione viene inviata a Microsoft.

Ulteriori informazioni potrebbero essere raccolte dal software VPN di terze parti. La raccolta e l'utilizzo di queste informazioni sono soggetti alle procedure relative alla privacy della terza parte.

Utilizzo delle informazioni

I client VPN utilizzano le credenziali fornite per l'autenticazione nella rete remota e per il routing del traffico di rete verso e dalla rete remota. Se un client VPN di terze parti raccoglie ulteriori informazioni, l'utilizzo di tali informazioni è soggetto alle procedure relative alla privacy della terza parte.

Scelta e controllo

È possibile aggiungere o rimuovere una connessione VPN e visualizzare lo stato delle connessioni esistenti in **Rete** in Impostazioni PC. Dopo aver configurato una connessione VPN è possibile connettersi o disconnettersi manualmente selezionando la rete nell'elenco in Impostazioni.

Inizio pagina

Analisi utilizzo software di 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 report 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, quali 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 nel PC.

- Informazioni su prestazioni e affidabilità, quali la velocità di risposta di un'app quando si fa clic su un pulsante, il numero di problemi riscontrati con un'app o un dispositivo e la velocità di invio o ricezione delle informazioni su una connessione di rete.

- Informazioni sull'utilizzo delle app, ad esempio 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 report di Analisi utilizzo software possono inoltre contenere 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 iniziare a partecipare al programma. Dato che la maggior parte degli utenti decide di partecipare ad Analisi utilizzo software entro alcuni 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. Se vengono ricevuti identificatori individuali, Microsoft non li utilizza per identificare o contattare l'utente.

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. Alcuni report di Analisi utilizzo software possono anche contenere GUID derivati dall'account Microsoft dell'utente.

Inoltre, Analisi utilizzo software Windows potrebbe scaricare 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 in forma aggregata con i partner Microsoft, affinché possano migliorare i propri prodotti e servizi, ma non possono essere utilizzate per identificare o contattare l'utente, né per inviargli pubblicità mirata.

Tramite il GUID, Microsoft ha la possibilità di stabilire la frequenza con cui vengono forniti specifici commenti, in modo da poter definire le più corrette priorità di intervento. Ad esempio, grazie al GUID Microsoft può distinguere tra un cliente presso cui uno stesso problema si verifica cento volte e cento clienti presso i quali lo stesso problema si è verificato una sola volta. Microsoft non utilizza le informazioni raccolte da Analisi utilizzo software per identificare o contattare l'utente.

Scelta e controllo

Se durante l'installazione di Windows si scelgono le impostazioni rapide viene attivato il programma Analisi utilizzo software Windows, pertanto Windows e le app Microsoft di Windows Store saranno in grado di inviare report di Analisi utilizzo software per tutti gli utenti del PC. Se si sceglie di personalizzare le impostazioni, è possibile controllare Analisi utilizzo software selezionando **Invia a Microsoft le informazioni relative all'uso del PC nell'ambito del programma Analisi utilizzo software** in **Contribuisci al miglioramento dei prodotti e servizi Microsoft**. Dopo la configurazione di Windows gli amministratori possono modificare questa impostazione in **Centro operativo** nel Pannello di controllo.

Per ulteriori informazioni, vedere le domande frequenti relative ad Analisi utilizzo software.

Inizio pagina

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

Se si utilizza Windows Defender, MicrosoftActive Protection Service (MAPS) può contribuire a migliorare la protezione del PC scaricando automaticamente nuove firme per malware appena rilevato e monitorando lo stato della sicurezza del PC. MAPS invierà a Microsoft informazioni sul malware e altro software potenzialmente indesiderato ed eventualmente file contenenti malware. Se rileva che il PC è infettato con alcuni tipi di malware, MAPS può contattare automaticamente l'utente tramite l'account Microsoft per aiutare a risolvere il problema.

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. MAPS può inoltre raccogliere URL completi per indicare l'origine dei file, nonché gli indirizzi IP a cui si connettono i potenziali file malware. 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 rapporti vengono inviati automaticamente a Microsoft quando:

- 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.
- Windows Defender analizza un controllo ActiveX in Internet Explorer.

Se si sceglie di partecipare a MAPS durante l'installazione di Windows, si parteciperà come membri base. I rapporti dei membri base contengono le informazioni descritte in questa sezione. I rapporti dei membri avanzati sono più completi e potrebbero talvolta includere informazioni personali, quali percorsi di file e dump della memoria parziali. Questi rapporti, 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 si partecipa a MAPS, è possibile che Windows Defender invii dal PC file o contenuto Web specifico che Microsoft sospetta possa essere software potenzialmente indesiderato. Il rapporto di esempio viene

utilizzato per ulteriori analisi. Se è probabile che un file contenga informazioni personali, verrà richiesta l'autorizzazione prima dell'invio. Se per un certo periodo di 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.

Per rilevare e correggere alcuni tipi di infezioni malware, Windows Defender invia regolarmente a MAPS alcune informazioni sullo stato di sicurezza del PC, incluse informazioni sulle impostazioni di sicurezza del PC e file di log in cui vengono descritti i driver e altro software caricati all'avvio del PC. Viene inviato anche un numero che identifica il PC in modo univoco.

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.

Le informazioni sullo stato di sicurezza del PC raccolte da MAPS vengono utilizzate per determinare se il PC è stato infettato da alcuni tipi di malware. In questo caso Microsoft utilizzerà le informazioni incluse nell'account Microsoft per contattare l'utente con i dettagli sul problema e le soluzioni per risolverlo.

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 **Quando Microsoft Defender è attivato, puoi aumentare la protezione dal malware inviando informazioni e file a Windows Active Protection Service** in **Condividi informazioni con Microsoft e altri servizi**. 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 **Impostazioni** in Windows Defender.

Se si riceve lo Strumento di rimozione malware tramite Windows Update, è possibile che vengano inviate informazioni di questo tipo a MAPS anche se Windows Defender è disattivato. Per ulteriori informazioni, leggere Strumento di rimozione malware per Windows .

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 della cronologia possono essere eliminati da un amministratore.

Inizio pagina

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. Al fine di evitare problemi e migliorare l'affidabilità del software, alcune soluzioni vengono inoltre incluse nei Service Pack e nelle versioni successive 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 attivare 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. In alcuni casi, il servizio di segnalazione invierà automaticamente informazioni aggiuntive per facilitare la diagnosi del problema, ad esempio uno snapshot parziale della memoria del PC.

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.

Per consentire la diagnosi di alcuni tipi di problemi, è possibile che Segnalazione errori Windows crei una segnalazione contenente informazioni aggiuntive, ad esempio file di log. Prima dell'invio di una segnalazione di questo tipo, Windows richiederà l'autorizzazione dell'utente, anche se è stata attivata la segnalazione automatica.

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, grazie al GUID Microsoft può distinguere tra un cliente presso cui uno stesso problema si verifica cento volte e cento clienti presso i quali lo stesso problema si è verificato 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 correggere 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 online le soluzioni ai problemi** in **Cerca soluzioni online**. Dopo la configurazione di Windows è possibile modificare questa impostazione in Centro operativo nel Pannello di controllo.

Per ulteriori informazioni, vedere l' 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. A Microsoft non verranno inviate informazioni sull'associazione dei tipi di file, a meno che non si decida di utilizzare il servizio.

Inizio pagina

Guida di Windows

Guida e supporto tecnico online di Windows

Scopo della funzionalità

Guida e supporto tecnico online 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 e supporto tecnico online di Windows utilizza inoltre tecnologie Web standard, come 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**e 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 PC 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, grazie al GUID Microsoft può distinguere tra un cliente presso cui uno stesso problema si verifica cento volte e cento clienti presso i quali quel dato problema si è verificato una sola volta.

Il programma 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 le utilizzerà 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 il programma Analisi utilizzo Guida selezionando **Invia a Microsoft le informazioni relative all'uso della Guida nell'ambito del programma Analisi utilizzo Guida** in **Contribuisci al miglioramento dei prodotti e servizi Microsoft**. 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. Tutte le connessioni di Assistenza remota vengono registrate in un file log di sessione.

Utilizzo delle informazioni

Le informazioni vengono utilizzate per stabilire una connessione crittografata e per consentire l'accesso al desktop alla persona che fornisce assistenza. 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 permette di eseguire ricerche nel dispositivo e in Internet da una sola posizione. Per garantire risultati di ricerca ottimali, è possibile che in Windows Search vengano utilizzati Bing e la piattaforma di localizzazione geografica di Windows. Si noti che nel dispositivo sono disponibili ulteriori funzionalità di ricerca separate fornite da Microsoft, ad esempio la ricerca in Windows Store, Internet Explorer e altri prodotti Microsoft.

Informazioni raccolte, elaborate o trasmesse

Se si sceglie di recuperare i risultati della ricerca nel Web, Windows invia i dati digitati in Windows Search a Microsoft. Per migliorare i risultati della ricerca, Windows Search invia a Microsoft anche informazioni sulla modalità di interazione dell'utente con la funzionalità. Windows Search invia inoltre un identificatore per fornire risultati della ricerca personalizzati in base alle interazioni dell'utente con Bing e altri prodotti e servizi Microsoft. Se si accede a Windows con un account Microsoft, l'identificatore verrà associato a tale account Microsoft. È possibile scegliere di non ottenere risultati personalizzati in Windows Windows. In tal caso, l'identificatore non verrà inviato.

Se si consente a Windows Search di utilizzare la propria posizione, nell'ambito di ogni richiesta di ricerca verrà inviata a Microsoft la posizione fisica del dispositivo fornita dalla piattaforma di localizzazione geografica di Windows. In alternativa, è possibile tentare di ricavare la posizione fisica approssimativa in base all'indirizzo IP.

Quando si utilizza Windows Search per eseguire ricerche in un'app, vengono forniti all'app i termini di ricerca.

Utilizzo delle informazioni

Se si sceglie di utilizzare Windows Search per ottenere risultati della ricerca nel Web, vengono utilizzati il termine di ricerca fornito dall'utente, la cronologia delle ricerche locali e online, le informazioni associate all'account Microsoft e la posizione del dispositivo per fornire suggerimenti di ricerca pertinenti, risultati di ricerca personalizzati ed esperienze personalizzate in altri prodotti e servizi Microsoft. Per ulteriori informazioni sull'utilizzo dei dati dell'utente, leggere l' informativa sulla privacy di Bing.

Se si utilizza Windows Search per eseguire la ricerca in un'app di terze parti, l'utilizzo delle informazioni raccolte 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

Se si scelgono le impostazioni rapide quando si configura Windows, si consente a Windows Search di ottenere suggerimenti per la ricerca e risultati Web e si consente a Microsoft di utilizzare dati di Windows Search (inclusa la posizione) per personalizzare Windows Search e altre esperienze Microsoft. Se si sceglie di personalizzare le impostazioni, è possibile decidere se modificarle per Windows Search. Dopo la configurazione di Windows, è possibile modificare questa impostazione in **Cerca** di Impostazioni PC.

È possibile cancellare la cronologia di ricerca locale e parte della cronologia di ricerca di Bing utilizzata per personalizzare l'esperienza con Windows in **Cerca** , nella sezione **Ricerca e app** in Impostazioni PC. Con la cancellazione della cronologia di ricerca si comunica a Microsoft di non utilizzare la cronologia di ricerca raccolta in precedenza per personalizzare i risultati della ricerca o ordinarli. Non vengono cancellate le informazioni per la pubblicità o altre informazioni di personalizzazione, incluse quelle derivate dalla cronologia di ricerca. Non vengono nemmeno eliminate le informazioni utilizzate da Microsoft in forma aggregata per migliorare i risultati di ricerca e altre esperienze Microsoft. Tali informazioni vengono mantenute e rese anonime come descritto nell' informativa sulla privacy di Bing. È possibile gestire le informazioni di personalizzazione e relative alla pubblicità Microsoft online.

Inizio pagina

Installazione di Windows

In questa sezione vengono descritte le funzionalità disponibili nell'ambito del processo di installazione di Windows.

Aggiornamento dinamico

Scopo della funzionalità

Aggiornamento dinamico consente a Windows di eseguire 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 dei 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.

Se inoltre si installa Windows da Windows Store, con Aggiornamento dinamico verranno scaricati e installati gli ultimi aggiornamenti di Windows, nonché alcuni driver hardware necessari per il PC.

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.

Scelta e controllo

Se si installa Windows da Windows Store, gli aggiornamenti verranno scaricati e installati automaticamente. Se invece si installa Windows da un supporto fisico, verrà chiesto se si desidera accedere a Internet per l'installazione degli aggiornamenti.

Programma 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. 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 di Windows, a cui l'utente può scegliere di partecipare durante l'utilizzo di Windows.

Scelta e controllo

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

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

Installation Compatibility Advisor

Scopo della funzionalità

Quando si installa Windows, il programma di installazione consente di determinare se il PC in uso è pronto per un aggiornamento a Windows 8.1, e fornisce informazioni sulla compatibilità relative ai

programmi e ai dispositivi in uso.

Informazioni raccolte, elaborate o trasmesse

Quando si determina la compatibilità, vengono raccolte alcune informazioni sulla potenziale esperienza di aggiornamento, come le capacità dei componenti hardware, i dispositivi collegati al computer e i programmi installati. Occasionalmente, le informazioni sull'autore del programma potrebbero rivelare dati come il nome o l'indirizzo di posta elettronica dell'autore.

Utilizzo delle informazioni

Le informazioni raccolte vengono utilizzate per individuare i driver più corretti per il PC in uso e per stabilire la compatibilità del PC, dei programmi e dei dispositivi in uso con Windows 8.1, nonché per migliorare i suoi 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

Se si installa Windows da Windows Store o da un supporto fisico all'interno di un'installazione esistente di Windows, le informazioni descritte in questa sezione verranno inviate a Microsoft. Se si esegue l'avvio dal supporto di installazione fisico per installare Windows, il programma di installazione non cercherà informazioni sulla compatibilità online.

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 interrompere l'archiviazione delle informazioni o eliminare tutte le destinazioni archiviate in **Condivisione** in **Ricerca e app** di Impostazioni PC.

Inizio pagina

Windows SmartScreen

Scopo della funzionalità

Windows SmartScreen contribuisce a garantire la sicurezza del PC controllando i file scaricati e il contenuto Web delle app per proteggere l'utente da software dannoso e da contenuto Web potenzialmente non sicuro. Windows visualizzerà un avviso prima dell'apertura di un file scaricato sconosciuto o potenzialmente non sicuro. Se con SmartScreenviene rilevato contenuto Web potenzialmente non sicuro in un'app, Windows visualizzerà un avviso anziché il contenuto.

Informazioni raccolte, elaborate o trasmesse

Se si sceglie di utilizzare Windows SmartScreen per controllare i file scaricati, Windows invia informazioni al servizio online SmartScreen. Tali informazioni potrebbero includere un nome di file, l'identificatore

del file ("hash") e informazioni sul certificato digitale insieme alle 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.

Se si sceglie di utilizzare Windows SmartScreen per bloccare contenuto delle app potenzialmente non sicuro, Windows invia al servizio online SmartScreen informazioni tra cui gli indirizzi e i tipi di contenuto a cui accedono alcune app di Windows Store quando vengono utilizzate. In risposta, il servizio online indica al PC se il contenuto è stato segnalato a Microsoft come non sicuro o sospetto. I rapporti inviati a Microsoft includono informazioni quali il nome o l'identificatore dell'app e gli indirizzi completi del contenuto Web a cui ha avuto accesso l'app.

Per proteggere la privacy dell'utente, le informazioni inviate a Microsoft sono crittografate. Negli indirizzi inviati a Microsoft potrebbero essere incluse informazioni associate a una pagina Web aperta da un'app, ad esempio i termini di ricerca. Se ad esempio si cerca una parola in un'app dizionario, tale parola può essere inclusa nelle informazioni inviate a Microsoft come parte dell'indirizzo completo a cui ha avuto accesso l'app. Microsoft filtra gli indirizzi per tentare di rimuovere le informazioni personali, quando possibile.

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

Utilizzo delle informazioni

Microsoft utilizza le informazioni precedenti per fornire avvisi all'utente relativamente a file scaricati e contenuto di app potenzialmente non sicuri. Se ad esempio SmartScreen rileva una potenziale minaccia in un'app che supporta SmartScreen, Windows visualizzerà un avviso anziché il contenuto. Queste informazioni vengono utilizzate da Microsoft anche per migliorare SmartScreen e altri prodotti e servizi. Microsoft non utilizza le informazioni per inviare all'utente 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 il filtro Windows SmartScreen selezionando **Usa i servizi online SmartScreen per proteggere il sistema dai download pericolosi e dai contenuti dannosi nei siti caricati dalle app di Windows Store e Internet Explorer** in **Proteggi il PC e la tua privacy**. Dopo la configurazione di Windows è possibile modificare questa impostazione in Centro operativo nel Pannello di controllo. Per ulteriori informazioni su Internet ExplorerSmartScreen, vedere la sezione sul filtro SmartScreen dell' informativa sulla privacy di Internet Explorer.

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 migliora la propria precisione acquisendo informazioni sull'uso del linguaggio e su parole e suoni preferiti dall'utente.

Informazioni raccolte, elaborate o trasmesse

Riconoscimento vocale Windows archivia un elenco delle parole e della relativa pronuncia nel PC. Parole e pronunce vengono aggiunte a questo elenco con il dizionario vocale e con l'utilizzo di Riconoscimento vocale Windows per dettare e correggere vocaboli.

Quando la funzionalità di revisione documenti di Riconoscimento vocale Windows è attivata, il testo dei documenti di Microsoft Office Word (con estensione di file doc o docx) e dei messaggi di posta elettronica (di cartelle di posta diverse da Posta eliminata 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 verificare i dati prima dell'invio. 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 utilizzare 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 per la modifica delle parole esistenti nel dizionario vocale per eliminare parole aggiunte al proprio profilo vocale. L'eliminazione del profilo vocale personale non comporta tuttavia l'eliminazione delle parole aggiunte tramite il dizionario vocale.

È possibile gestire i percorsi da cui la revisione del documento raccoglie 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 nel 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**. Qualunque sia la scelta dell'utente, è possibile visualizzare tutti i file di dati prima dell'invio e 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 da Windows Store, 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, vengono archiviate nel PC informazioni sulla licenza per ogni 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 informazioni 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.

Sfogliando Windows Store e utilizzando le app ivi 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.

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 di Windows Store indica il numero degli aggiornamenti disponibili. È quindi possibile 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.

Aggiornamenti automatici delle app

Scopo della funzionalità

Questa funzionalità consente di cercare, scaricare e installare gli aggiornamenti delle app di Windows Store in modo che l'utente disponga delle versioni più recenti. Gli aggiornamenti delle app possono includere aggiornamenti di sicurezza, aggiornamenti delle prestazioni oppure nuove funzionalità o nuovo contenuto. Le app

aggiornate possono utilizzare funzionalità di Windows differenti rispetto alle versioni precedenti, in grado di fornire l'accesso a diverse risorse nel PC. Per informazioni sulle modifiche apportate alle funzionalità, vedere la pagina di descrizione del prodotto relativa all'app in Windows Store.

Informazioni raccolte, elaborate o trasmesse

Per fornire aggiornamenti automatici delle app, Windows Store invia le seguenti informazioni a Microsoft:

- Un elenco di tutte le app installate da Windows Store nel PC da tutti gli utenti
- Le informazioni sulle licenze per le singole app
- La riuscita o meno delle operazioni e gli errori verificatisi durante l'aggiornamento delle app di Windows Store
- Il GUID (Globally Unique Identifier, identificatore univoco globale), ovvero un numero generato in modo casuale che non include informazioni personali
- Nome BIOS, numero di revisione e data di revisione
- Le informazioni di base sul PC, ad esempio il produttore, il modello e l'edizione di Windows in uso

Utilizzo delle informazioni

Queste informazioni vengono utilizzate per fornire il servizio di aggiornamento. Vengono inoltre utilizzate per generare statistiche aggregate che consentono di analizzare le tendenze e migliorare i prodotti e i servizi Microsoft. Non vengono utilizzate invece per identificare o contattare l'utente, né per inviargli pubblicità mirata.

Scelta e controllo

Se si scelgono le impostazioni rapide quando si configura Windows, gli aggiornamenti verranno cercati, scaricati e installati automaticamente da Windows Store, anche se è stata effettuata la disconnessone da Windows Store. Se si disattivano gli aggiornamenti automatici delle app, è possibile scegliere se installare o meno l'aggiornamento di un'app quando si accede a Windows Store.

Per disattivare gli aggiornamenti automatici delle app:

1. Aprire Windows Store.
2. Scorrere rapidamente dal bordo destro della schermata e quindi toccare **Impostazioni**.

   Se si utilizza un mouse, posizionare il puntatore nell'angolo inferiore destro dello schermo e quindi fare clic su **Impostazioni**.
3. Toccare o fare clic su **Aggiornamenti app**.
4. Toccare o fare clic su **Aggiorna automaticamente le mie app** per disattivare gli aggiornamenti automatici delle app.

Per informazioni sulle funzionalità della versione più recente dell'app e sulla data dell'ultimo aggiornamento, vedere la pagina di descrizione del prodotto relativa all'app in Windows Store.

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.

Oltre alle autorizzazioni di cui sopra, se un'app richiede informazioni da un dispositivo che archivia informazioni sull'utente e sui suoi comportamenti, Windows richiederà se si desidera consentire all'app di utilizzarlo. Ad esempio, se ci si connette a un dispositivo per le attività sportive che tiene traccia della posizione, Windows richiederà se si desidera consentire l'accesso all'app.

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, aprire **Impostazioni**, quindi selezionare **Autorizzazioni**.

Risultati di ricerca e suggerimenti per le app

personalizzati in Windows Store

Scopo della funzionalità

Quando si visualizzano o cercano le app in Windows Store, Microsoft offre suggerimenti e risultati di ricerca per facilitare l'individuazione delle app più interessanti per un utente specifico.

Informazioni raccolte, elaborate o trasmesse

Per migliorare i risultati di ricerca, Windows Store invia informazioni a Microsoft sulle interazioni dell'utente con il sito, inclusi gli elementi cercati e i risultati di ricerca selezionati. Windows Store invia inoltre un identificatore associato all'account Microsoft per fornire risultati della ricerca personalizzati in base alle interazioni dell'utente con Bing e altri prodotti e servizi Microsoft. È possibile scegliere di non ottenere risultati personalizzati. In tal caso, l'identificatore non verrà inviato.

Utilizzo delle informazioni

Windows Store utilizza l'identificatore associato all'account Microsoft per offrire risultati di ricerca e suggerimenti personalizzati in base alle interazioni dell'utente con Windows Store e altri prodotti e servizi Microsoft, come Bing e Windows Phone Store. Sono incluse informazioni come le app acquistate, le informazioni sul profilo registrate nell'account Microsoft, oltre alle classificazioni e recensioni delle app. Queste informazioni potrebbero inoltre essere utilizzate per personalizzare altri prodotti e servizi Microsoft.

Scelta e controllo

Quando si esegue l'accesso a Windows con un account Microsoft, i risultati di ricerca e i suggerimenti personalizzati di Windows Store sono attivati per impostazione predefinita. È possibile scegliere di non ricevere risultati e suggerimenti personalizzati da Windows Store nella sezione **Preferenze** delle impostazioni di Windows Store.

Contribuire al miglioramento di Windows Store inviando URL per il contenuto Web utilizzato 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 da Microsoft, 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 proteggere la 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 **Usa i servizi online SmartScreen per proteggere il sistema dai download pericolosi e dai contenuti dannosi nei siti caricati dalle app di Windows Store e Internet Explorer** in **Contribuisci al miglioramento dei prodotti e servizi Microsoft**. 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 ad un server di riferimento ora su Internet o nella rete locale utilizzando il protocollo standard NTP (Network Time Protocol). Per impostazione predefinita, il servizio effettua 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.

Scelta e controllo

Il servizio Ora di Windows è attivato per impostazione predefinita. È possibile disattivare questa funzionalità in **Data e ora** in Impostazioni PC. La disattivazione di Servizio Ora di Windows non ha alcun impatto diretto sulle app o su altri servizi, tuttavia senza un'origine ora affidabile l'orologio del PC potrebbe 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 causare errori o impedire il corretto funzionamento.

Inizio pagina

Risoluzione dei problemi di Windows

Scopo della funzionalità

Risoluzione dei problemi di 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 problemi di Windows è utile nella ricerca di soluzioni per i problemi in Guida e supporto tecnico di Windows e nelle community Windows online. Le parole chiave associate al problema verranno inviate a Microsoft per trovare una soluzione. 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

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

Cartelle di lavoro

Scopo della funzionalità

Le cartelle di lavoro sono cartelle nel PC che vengono mantenute automaticamente sincronizzate con il file server della rete aziendale.

Informazioni raccolte, elaborate, archiviate o trasmesse

Quando si salva un file in una cartella di lavoro, il file viene sincronizzato automaticamente con un file server gestito dalla rete aziendale. I file salvati nella cartella di lavoro da altri PC verranno sincronizzati nel PC in uso.

Utilizzo delle informazioni

Windows invia e riceve i file nelle cartelle di lavoro per mantenere sincronizzate le cartelle. L'utilizzo delle informazioni archiviate nei server della rete aziendale è soggetto ai criteri per la privacy della rete aziendale.

Scelta e controllo

È possibile gestire la connessione del PC alle cartelle di lavoro in **Rete aziendale** di Impostazioni PC.

Inizio pagina

Rete aziendale

Rete aziendale consente di connettere il dispositivo a Windows Intune (è richiesto un abbonamento separato da Microsoft) o a un altro servizio di gestione dei dispositivi di terze parti. Se si sceglie di consentire all'amministratore della società di gestire il PC tramite Rete aziendale, questo deve poter eseguire attività quali imporre criteri di sicurezza nel PC, installare app, visualizzare informazioni di configurazione specifiche e di altro tipo nel PC, oltre ad altre attività di gestione. Per informazioni su come la società utilizza questa funzionalità, leggere l'informativa sulla privacy aziendale oppure rivolgersi all'amministratore di sistema.

Informazioni raccolte, elaborate o trasmesse

Durante la configurazione e l'utilizzo di Rete aziendale, il PC comunica

con il servizio di gestione dei dispositivi utilizzato dall'azienda, che potrebbe essere ospitato da Microsoft. Le credenziali immesse per connettersi alla rete aziendale vengono inviate al servizio.

Utilizzo delle informazioni

Le informazioni inviate al servizio di gestione dei dispositivi vengono utilizzate per stabilire una connessione tra il servizio e il PC e per consentire all'utente di installare un'app self-service da Windows Store. Per informazioni sull'app self-service, leggere l'informativa sulla privacy aziendale oppure rivolgersi all'amministratore di sistema.

Scelta e controllo

Se la società utilizza Rete aziendale, è possibile connettersi o disconnettersi in Rete aziendale in Impostazioni PC in **Rete**. Dopo aver connesso il PC al servizio, è possibile visualizzare in qualsiasi momento informazioni sulla connessione oppure disconnettersi.

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 8.1 e Windows Server 2012 R2

Elementi di rilievo Informativa Funzionalità App Server

Questa pagina costituisce un supplemento all'informativa sulla privacy di Windows 8.1 e Windows Server 2012 R2 ("informativa sulla privacy di Windows"), che contiene le sezioni seguenti:

- In primo piano
- Informativa, ovvero l'informativa sulla privacy completa di Windows 8.1, che include collegamenti alle informative sulla privacy relative a funzionalità di Windows per le quali sono disponibili informative specifiche
- Supplemento sulle funzionalità, che descrive le funzionalità che hanno impatto sulla privacy in Windows 8.1 e Windows Server 2012 R2
- **Supplemento sulle app** (questa pagina), che descrive le app che hanno un impatto sulla privacy in Windows 8.1 e include collegamenti alle informative sulla privacy specifiche per ogni app
- Supplemento su Windows Server, che descrive le funzionalità

aggiuntive che hanno impatto sulla privacy in Windows Server 2012 R2

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

Se si sceglie di partecipare al programma Analisi utilizzo software al momento dell'installazione del PC, queste app raccoglieranno informazioni in un rapporto sulle modalità di utilizzo di ogni app, oltre a dati sulle prestazioni e l'affidabilità dell'app. Microsoft utilizza queste informazioni per migliorare prodotti e servizi. Questi dati non verranno utilizzati per identificare o contattare l'utente, né per inviargli pubblicità mirata. È possibile disattivare Analisi utilizzo software in Impostazioni PC. Per ulteriori informazioni, vedere l' informativa sulla privacy del programma Analisi utilizzo software.

I collegamenti seguenti consentono di passare alle informative sulla privacy specifiche per ognuna delle app elencate:

Sveglia

Calcolatrice

Calendario

Fotocamera

Finanza

Cibo

Giochi

Salute

Guida e suggerimenti

Mail

Mappe

Musica

Notizie

Contatti

Lettore

Elenco di lettura

Scanner

Skype

Registratore di suoni

Sport

Viaggi

Video

Meteo

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 8.1 e Windows Server 2012 R2

In questa pagina

Questa pagina costituisce un supplemento all'Informativa sulla privacy di Windows 8.1 e Windows Server 2012 R2 ("Informativa sulla privacy di Windows"). L'informativa sulla privacy è suddivisa nelle sezioni seguenti:

- In primo piano
- Informativa, ovvero l'informativa sulla privacy completa di Windows 8.1, che include collegamenti alle informative sulla privacy relative a funzionalità di Windows per le quali sono disponibili informative specifiche
- Supplemento sulle funzionalità, che descrive le funzionalità che hanno impatto sulla privacy in Windows 8.1 e Windows Server 2012 R2
- Supplemento sulle app, che descrive le app che hanno un impatto sulla privacy in Windows 8.1
- **Supplemento su Windows Server** (questa pagina), che

Windows

Registrazione dell'inventario software

descrive le funzionalità aggiuntive che hanno un impatto sulla privacy in Windows Server 2012 R2

Per comprendere le procedure di raccolta e utilizzo dei dati relative a una particolare funzionalità o un particolare servizio di Windows, è consigliabile leggere sia l'Informativa sulla privacy completa di Windows sia eventuali supplementi applicabili. Leggere inoltre questo white paper per amministratori.

Per informazioni sull'impatto sulla privacy delle funzionalità incluse in Windows Server 2012 R2 Essentials, vedere l' Informativa sulla privacy per Windows Server 2012 R2 Essentials ed Esperienza Windows Server Essentials.

Registrazione accesso utenti

Scopo della funzionalità

Registrazione accesso utenti raccoglie e aggrega i record relativi alle richieste dei client di ruoli server (richieste sia degli utenti che dei dispositivi) e ai prodotti installati (se registrati con questa funzionalità) nel server locale. Questi dati, nella forma di indirizzi IP, nomi utente e, in alcuni casi, nomi host e/o identità di macchine virtuali, vengono archiviati nei database ESE (Extensible Storage Engine) locali e sono accessibili solo agli amministratori. Registrazione accesso utenti dispone di un provider WMIv2 e di cmdlet di Windows PowerShell associati per il recupero dei dati di accesso degli utenti necessari per la gestione dei diritti di licenza CAL (Client Access License) per gli utenti offline, in cui i record effettivi delle richieste client univoche sono critici.

Informazioni raccolte, elaborate o trasmesse

Gli indirizzi IP, i nomi utente e, in alcuni casi, i nomi host (se è installato il ruolo DNS) e le identità di macchine virtuali (se è installato il ruolo Hyper-V) vengono raccolti localmente nel server quando Registrazione accesso utenti è attivato. Nessuno dei dati raccolti viene inviato a Microsoft.

Utilizzo delle informazioni

I dati di Registrazione accesso utenti vengono resi disponibili agli

amministratori tramite i database ESE locali, il provider WMI e i cmdlet di Windows PowerShell. Windows utilizza questi dati esclusivamente nell'ambito della funzionalità Registrazione accesso utenti.

Scelta e controllo

Il servizio Registrazione accesso utenti è abilitato per impostazione predefinita. Può essere arrestato e avviato mentre il server è in esecuzione. Per disabilitarlo in modo permanente, apri Windows PowerShell, digita Disable-UAL e riavvia il server. Un amministratore può eliminare tutti i dati cronologici raccolti arrestando il servizio, disabilitando Registrazione accesso utenti e quindi eliminando tutti i file nella cartella %SystemRoot%\System32\LogFiles\SUM\.

Inizio pagina

Server Manager

Scopo della funzionalità

Server Manager è uno strumento di gestione che consente a un 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.

Informazioni raccolte, elaborate o trasmesse

Server Manager raccoglie i tipi di informazioni seguenti da un server gestito dall'amministratore:

- **Informazioni generali sul server:** nome NetBios e nome di dominio completo (FQDN), credenziali dell'account immesse nella funzionalità “Account di gestione”, indirizzo IPv4, indirizzo IPv6, stato di gestibilità, descrizione, versione del sistema operativo, tipo, ultimo aggiornamento, processori, memoria, nome cluster, tipo di oggetto cluster, stato di attivazione, SKU, architettura del sistema operativo, produttore, configurazione di Analisi utilizzo software e configurazione di Segnalazione errori Windows.
- **Eventi:** ID, gravità, origine, log, data e ora di ogni evento di Windows e altri log scelti dall'amministratore.
- **Tutti i servizi:** nome, stato e tipo di avvio.

- **Informazioni sui ruoli server:** risultati di Best Practice Analyzer (BPA) per i ruoli installati nel server.
- **Informazioni sulle prestazioni:** campioni dei contatori delle prestazioni e notifiche relative all'utilizzo della CPU e alla memoria disponibile.

Utilizzo delle informazioni

Queste informazioni vengono archiviate in Server Manager e non vengono inviate a Microsoft. Vengono visualizzate in Server Manager per facilitare agli amministratori le attività di monitoraggio dei sistemi.

Scelta e controllo

Un amministratore può acconsentire o rifiutare esplicitamente la raccolta di dati da qualsiasi server ad eccezione del server locale aggiungendo o rimuovendo il server in Server Manager. Un amministratore può esplicitamente fornire le credenziali per la connessione a un server remoto. All'amministratore viene chiesto di acconsentire esplicitamente all'archiviazione delle credenziali localmente in Server Manager e l'amministratore stesso può eliminare queste credenziali in qualsiasi momento.

Inizio pagina

Active Directory Federation Services (ADFS)

Scopo della funzionalità

Active Directory Federation Services (ADFS) è una soluzione aziendale di federazione e Single Sign-On per app locali o di rete. ADFS viene utilizzato dagli amministratori per consentire la collaborazione fra utenti di diverse organizzazioni e per facilitare l'accesso ad app locali o su altre reti senza comprometterne la sicurezza. ADFS utilizza un servizio token di sicurezza che utilizza a sua volta Servizi di dominio Active Directory per autenticare gli utenti e rilasciare loro token di sicurezza con vari protocolli. Il token è firmato digitalmente e contiene attestazioni relative all'utente, che derivano da una o più combinazioni di Servizi di dominio Active Directory, Lightweight Directory Access Protocol (LDAP), SQL Server o un archivio personalizzato.

Informazioni raccolte, elaborate o trasmesse

Quando un utente viene autenticato con ADFS, ne vengono raccolte le credenziali. Le credenziali vengono inviate immediatamente a Servizi di dominio Active Directory per l'autenticazione e non vengono archiviate localmente da ADFS. Gli attributi dell'utente in Servizi di dominio Active Directory potrebbero essere utilizzati per generare attestazioni in uscita, a seconda delle regole di attestazione configurate da un amministratore di ADFS. Le attestazioni in uscita verranno inviate a partner attendibili con cui un amministratore di ADFS ha stabilito una relazione di trust. Nessuna informazione viene inviata a Microsoft.

Utilizzo delle informazioni

Microsoft non avrà accesso a queste informazioni. L'utilizzo di tali informazioni è riservato esclusivamente all'utente.

Scelta e controllo

Utilizzare ADFS per raccogliere o inviare dati a partner attendibili.

Inizio pagina

Gestione indirizzi IP

Scopo della funzionalità

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

Informazioni raccolte, elaborate o trasmesse

Il server di Gestione indirizzi IP raccoglie log ed eventi di controllo da server DHCP, controller di dominio e server dei criteri di rete, quindi archivia localmente l'indirizzo IP, il nome host, l'identificatore client e il nome utente dell'utente che ha effettuato l'accesso. Un amministratore del server può eseguire ricerche nei log raccolti in base all'indirizzo IP, l'identificatore client, il nome host e il nome utente utilizzando la console di Gestione indirizzi IP. Nessuna di queste informazioni viene inviata a Microsoft.

Utilizzo delle informazioni

Microsoft non ha accesso a queste informazioni. L'utilizzo di tali informazioni è riservato esclusivamente all'utente.

Scelta e controllo

Gestione indirizzi IP non è installato per impostazione predefinita e deve essere installato dall'amministratore del server. Dopo l'installazione di Gestione indirizzi IP, il controllo degli indirizzi IP viene abilitato automaticamente. Per disabilitare il controllo degli indirizzi IP in un server in cui è installato Gestione indirizzi IP, avviare Utilità di pianificazione nel server di Gestione indirizzi IP, individuare Attività di controllo in Microsoft\Windows\IPAM e quindi disabilitare l'attività.

Inizio pagina

Accesso remoto unificato

Scopo della funzionalità

Accesso remoto unificato consente agli utenti remoti di connettersi a una rete privata, quale una rete aziendale, attraverso Internet. Accesso remoto unificato utilizza DirectAccess per garantire ai computer client remoti che eseguono Windows 8 una connettività ininterrotta e trasparente alle reti aziendali. Fornisce inoltre la funzionalità Servizio di accesso remoto (RAS), che offre servizi VPN tradizionali, inclusa la connettività da sito a sito locale o ad altre reti.

Informazioni raccolte, elaborate o trasmesse

Per il monitoraggio degli utenti di Accesso remoto unificato, il server DirectAccess archivia i dettagli relativi agli utenti remoti che si connettono alla rete privata. I dati raccolti includono informazioni quali il nome host dell'utente remoto, il nome utente di Active Directory e l'indirizzo IP pubblico del client remoto (se il client è dietro NAT (Network Address Translation), sarà l'indirizzo IP pubblico). Tali dati possono inoltre essere archiviati nei server di Database interno di Windows o RADIUS, ma solo con il consenso dell'amministratore. Solo un amministratore di DirectAccess (un utente di dominio con un account amministratore locale) che accede a un server può accedere a queste informazioni e visualizzarle.

Utilizzo delle informazioni

Queste informazioni verranno utilizzate dall'amministratore per la risoluzione dei problemi di connettività dei client nonché ai fini del controllo e della conformità. Nessuna informazione viene inviata a Microsoft.

Scelta e controllo

Il monitoraggio dei client remoti è attivato per impostazione predefinita e non può essere disabilitato. I dati di monitoraggio vengono archiviati nei server di Database interno di Windows/RADIUS solo se un amministratore ha configurato l'accounting per l'uso di queste opzioni. Se un amministratore non ha configurato l'accounting, nessuna di queste informazioni verrà archiviata. Un amministratore può inoltre configurare l'accounting su un server di accesso remoto in modo da non archiviare le informazioni relative a nome utente e indirizzo IP.

Inizio pagina

Servizi Desktop remoto

Scopo della funzionalità

Servizi Desktop remoto offre alle aziende una piattaforma che facilita l'implementazione di una strategia desktop centralizzata e la gestione di desktop e app, oltre a migliorare i livelli di flessibilità e conformità rafforzando al contempo la sicurezza dei dati.

Informazioni raccolte, elaborate o trasmesse

Per il monitoraggio degli utenti di Servizi Desktop remoto, il server Host sessione Desktop remoto archivia le informazioni sugli utenti remoti che si connettono a risorse di Servizi Desktop remoto. I dati raccolti includono informazioni quali il nome host dell'utente remoto, il nome utente di Active Directory e l'indirizzo IP pubblico del client remoto (se il client è dietro NAT (Network Address Translation), sarà l'indirizzo IP pubblico). Questi dati vengono archiviati automaticamente nei server di Database interno di Windows e/o di SQL Server alla connessione degli utenti. A Microsoft non viene inviata alcuna informazione. Solo un utente di dominio con un account amministratore locale può accedere a queste informazioni e visualizzarle.

Utilizzo delle informazioni

Queste informazioni verranno utilizzate dall'amministratore per la risoluzione dei problemi di connettività dei client nonché ai fini del controllo interno e della conformità. Nessuna informazione viene inviata a Microsoft.

Scelta e controllo

Il monitoraggio dei client è attivato per impostazione predefinita e non può essere disabilitato. Le informazioni sul monitoraggio vengono archiviate nel server di Database interno di Windows/SQL Server.

Inizio pagina

Analisi utilizzo software di Windows e Segnalazione errori Windows

Scopo della funzionalità

Per ulteriori informazioni su queste funzionalità, vedere la scheda Supplemento sulle funzionalità o questo white paper per amministratori.

Informazioni raccolte, elaborate o trasmesse

Per informazioni sui dati specifici che vengono raccolti, elaborati e trasmessi da queste funzionalità, vedere Analisi utilizzo software e Segnalazione errori Windows nella scheda Supplemento sulle funzionalità .

Utilizzo delle informazioni

Per informazioni sulle modalità di utilizzo dei dati raccolti da queste funzionalità, vedere Analisi utilizzo software e Segnalazione errori Windows nella scheda Supplemento sulle funzionalità .

Scelta e controllo

Per impostazione predefinita, Analisi utilizzo software è disattivato mentre Segnalazione errori Windows è impostato in modo da chiedere conferma all'utente prima di inviare segnalazioni di arresto anomalo a Microsoft. È possibile attivare e disattivare Analisi utilizzo software da Server Manager e dal Pannello di controllo, oltre che mediante i metodi di controllo da riga di comando. Segnalazione errori Windows può

invece essere controllato solo mediante i metodi da riga di comando.

Per attivare o disattivare Analisi utilizzo software mediante il Pannello di controllo, fare clic su **Sistema e manutenzione**e quindi su **Segnalazioni di problemi e soluzioni**. In **Vedere anche**, fare clic su **Impostazioni di Analisi utilizzo software** e selezionare l'opzione appropriata per attivare o disattivare Analisi utilizzo software.

Controlli di Server Manager

Server locale

- Abilitare Analisi utilizzo software
  Aprire Server Manager e selezionare **Server locale**. Fare clic sul collegamento Analisi utilizzo software, selezionare **Sì, desidero partecipare al programma Analisi utilizzo software** nella finestra di dialogo e quindi fare clic su **OK**.

- Disabilitare Analisi utilizzo software
  Aprire Server Manager e selezionare **Server locale**. Fare clic sul collegamento Analisi utilizzo software, selezionare **Non desidero partecipare** nella finestra di dialogo e quindi fare clic su **OK**.

- Abilitare Segnalazione errori Windows
  Aprire Server Manager e selezionare **Server locale**. Fare clic sul collegamento Segnalazione errori Windows, selezionare **Sì, invia automaticamente rapporti brevi**e quindi fare clic su **OK**.

- Disabilitare Segnalazione errori Windows
  Aprire Server Manager e selezionare **Server locale**. Fare clic sul collegamento Segnalazione errori Windows, selezionare **Non desidero partecipare. Non visualizzare più questo messaggio**e quindi fare clic su **OK**.

Più computer

- Abilitare Analisi utilizzo software
  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 scegliere **Configura Commenti e suggerimenti automatici per Windows** . Nella scheda 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 in Selezione dei server e quindi fare clic su **OK**.

- Disabilitare Analisi utilizzo software
  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 scegliere **Configura Commenti e suggerimenti automatici per Windows** . Nella scheda Analisi utilizzo software selezionare **Non desidero partecipare**. Applicare questa impostazione a tutti i server selezionando la casella di controllo accanto a Nome server in Selezione dei server e quindi fare clic su **OK**.

- Abilitare Segnalazione errori Windows
  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 scegliere **Configura Commenti e suggerimenti automatici per Windows** . Nella scheda Segnalazione errori Windows selezionare **Sì, invia automaticamente segnalazioni sintetiche (scelta consigliata)**. Applicare questa impostazione a tutti i server selezionando la casella di controllo accanto a Nome server in Selezione dei server e quindi fare clic su **OK**.

- Disabilitare Segnalazione errori Windows
  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 scegliere **Configura Commenti e suggerimenti automatici per Windows** . Nella scheda Segnalazione errori Windows selezionare **Non desidero partecipare**. Applicare questa impostazione a tutti i server selezionando la casella di controllo accanto a Nome server in Selezione dei server e quindi fare clic su **OK**.

Inizio pagina

Registrazione dell'inventario software

Scopo della funzionalità

La funzionalità di registrazione dell'inventario software offre un nuovo

set di classi WMI e cmdlet di PowerShell per semplificare l'inventario di base dell'edizione Windows Server del sistema operativo, del software installato in Windows Server e delle caratteristiche del server in cui è in esecuzione il software. La registrazione dell'inventario software consente inoltre, se abilitata da un amministratore, di raccogliere con frequenza oraria dati dal provider WMI corrispondente e inoltrarli tramite la rete a un server di aggregazione, nel caso ne venga specificato uno tramite il cmdlet Set-SilLogging - TargerUri.

Informazioni raccolte, elaborate o trasmesse

I dati possono essere trasmessi a un server di aggregazione attraverso la rete, se questa funzionalità è configurata da un amministratore. Per impostazione predefinita, nessuna informazione viene raccolta, elaborata o trasmessa. Questi dati includono:

- Nome ed edizione di Windows Server del sistema operativo installato.
- Un elenco di nomi, versioni ed editori di tutto il software installato nel server e la data di installazione di tale software.
- Il nome di dominio completo del sistema server.
- Il numero, il tipo e il produttore di processori, processori logici e core installati o assegnati nel sistema server.

Dati raccolti ed elaborati, ma non trasmessi per impostazione predefinita, anche se l'attività oraria è abilitata e viene specificato un server di aggregazione di destinazione dall'amministratore:

- La classe MsftSil_UalAccess e il cmdlet Get-SilUalAccess elaborano il numero totale di utenti e dispositivi univoci per ogni ruolo o prodotto registrato per la funzionalità Registrazione accesso utenti a partire da due giorni prima della query. Si tratta di semplici conteggi e non vengono prodotte o trasmesse informazioni sugli utenti o sui dispositivi. La registrazione dell'inventario software deve elaborare le informazioni sugli utenti e sui dispositivi, dalle classi di Registrazione accesso utenti, per il calcolo dei conteggi stessi. Questi dati sono accessibili solo per un amministratore del computer locale. La registrazione dell'inventario software non modifica i requisiti per

l'accesso alle API di Registrazione accesso utenti.

Nessuno dei dati raccolti viene inviato a Microsoft.

Utilizzo delle informazioni

I provider WMI della registrazione dell'inventario software aggregano i dati forniti da altre API già esistenti nel sistema. I dati possono essere trasmessi a un server per ulteriori operazioni di aggregazione tramite la rete, se un amministratore configura questa funzionalità. Per impostazione predefinita, nessuna informazione viene raccolta, elaborata o trasmessa. Nel caso della classe MsftSil_UalAccess e del cmdlet Get-SilUalAccess, i dati elaborati forniscono il numero totale di utenti e dispositivi univoci per ogni ruolo o prodotto registrato per la funzionalità Registrazione accesso utenti a partire da due giorni prima della raccolta, ma l'output non include alcun dato che consenta l'identificazione degli utenti o dei dispositivi. E sebbene questa classe WMI e questo cmdlet esistano nel sistema, non fanno parte del payload di dati di registrazione dell'inventario software raccolto e inoltrato a un server di aggregazione ogni ora quando questa funzionalità è configurata a questo scopo da un amministratore di sistema.

Scelta e controllo

L'attività oraria di registrazione dell'inventario software è disabilitata per impostazione predefinita. Tutte le API di registrazione dell'inventario software sono disponibili per le query per impostazione predefinita per gli amministratori del sistema locale. L'attività oraria di registrazione dell'inventario software può essere avviata e interrotta mentre il server è in esecuzione tramite i cmdlet Start-SilLogging e Stop-SilLogging . Tramite il cmdlet Set-SilLogging gli amministratori del server possono impostare la data e l'ora di avvio dell'attività oraria (per impostazione predefinita le ore 3 del sistema locale), l'URI (Uniform Resource Identifier) di un server di aggregazione di destinazione e l'identificazione personale certificato necessaria per garantire la trasmissione attendibile dei dati.

Tutte le impostazioni di configurazione della registrazione dell'inventario software, inclusi l'avvio e l'interruzione dell'attività oraria, possono essere modificate nel Registro di sistema, opzione progettata per l'utilizzo solo quando il sistema è una macchina virtuale

e solo prima del primo avvio del sistema.

Inizio pagina