Aktuelle Informationen über Methoden für die Verarbeitung der Daten von Microsoft, finden Sie in der Datenschutzerklärung von Microsoft. Hier erfahren Sie mehr über die neuesten Tools für den Zugriff auf und die Steuerung Ihrer Daten, und wie Sie uns kontaktieren, wenn Sie eine Abfrage zum Datenschutz haben.

Datenschutzbestimmungen für Windows 8 und Windows Server 2012

Letzte Aktualisierung: **August 2012**

Diese wichtigsten Punkte der vollständigen Datenschutzbestimmungen für Windows 8 und Windows Server 2012 ("Datenschutzbestimmungen zu Windows") erläutern im Detail einige der Datensammlungen und Verwendungszwecke von Windows 8 und Windows Server 2012 ("Windows"). Zentrales Thema der Übersicht sind die Features zur Kommunikation mit dem Internet. Es wird kein Anspruch auf Vollständigkeit erhoben. Sie gelten nicht für andere Online- oder Offlineinhalte von Microsoft-Webseiten, -Produkten oder -Diensten.

Diese Datenschutzbestimmungen sind in vier Abschnitte unterteilt:

- Highlights (diese Seite)
- Bestimmungen – die vollständigen Datenschutzbestimmungen zu Windows mit Links für

Windows-Features, für die eigene Datenschutzbestimmungen vorliegen

- Features – Ergänzung mit Beschreibungen der Features, die Auswirkungen auf den Datenschutz in Windows 8 und Windows Server 2012 haben

- Server – Ergänzung mit Beschreibungen zu zusätzlichen Features, die Auswirkungen auf den Datenschutz in Windows Server 2012 haben

Weitere Informationen, wie Sie Ihren Computer, Ihre persönlichen Daten und die Daten Ihrer Familie online schützen können, finden Sie im Safety & Security Center.

Ihre Informationen

- Bei bestimmten Windows-Features können Sie um Ihre Zustimmung zur Erfassung und Verwendung von Informationen, auch persönlicher Informationen, auf Ihrem PC aufgefordert werden. Windows verwendet diese Informationen, wie in den vollständigen Windows-Datenschutzbestimmungen, ebenso wie in der Features – Ergänzungund den Server – Ergänzung.

- Einige Windows-Features können, mit Ihrer Zustimmung, persönliche Informationen über das Internet freigeben.

- Wenn Sie Ihre Software registrieren möchten, werden Sie aufgefordert, persönliche Informationen anzugeben.

- Windows fordert die Aktivierung, damit Softwarefälschungen reduziert werden und sichergestellt ist, dass Microsoft-Kunden die erwartete Softwarequalität zur Verfügung steht. Bei der Aktivierung werden einige Informationen über Ihren PC an Microsoft gesendet.

- Sie sich bei Windows mit einem Microsoft-Kontoanmelden. So können Sie Windows-Einstellungen synchronisieren und sich automatisch bei Apps und Webseiten automatisch anmelden. Wenn Sie ein Microsoft-Konto erstellen, werden

Sie aufgefordert, einige persönliche Informationen anzugeben.

- Zusätzliche Details

Seitenanfang

Ihre Auswahlmöglichkeiten:

- Windows bietet Ihnen eine Vielzahl von Möglichkeiten, mit denen Sie steuern können, wie Informationen zu Windows-Features über das Internet übertragen werden. Weitere Informationen zum Steuern dieser Features sind in den Ergänzungen zu Features und zum Server enthalten.
- Zur Verbesserung der Benutzerfreundlichkeit sind einige Features, die eine Verbindung mit dem Internet herstellen, standardmäßig aktiviert.
- Zusätzliche Details

Seitenanfang

Verwendung der Informationen

- Wir verwenden die erfassten Informationen, um die von Ihnen verwendeten Features zu aktivieren oder Ihnen die angeforderten Dienste bereitzustellen. Wir verwenden die Informationen auch, um unsere Produkte und Dienste zu verbessern. Um unsere Dienste zu gewährleisten, geben wir gelegentlich Informationen an andere Firmen weiter, die in unserem Auftrag arbeiten. Nur Unternehmen, die die Informationen aufgrund einer Geschäftsanforderung verwenden, erhalten Zugriff auf die Informationen. Diese Unternehmen müssen die Informationen vertraulich halten und dürfen sie nicht für andere Zwecke nutzen.
- Zusätzliche Details

Seitenanfang

So erreichen Sie uns

Weitere Informationen zu unseren Datenschutzrichtlinien finden Sie unter den vollständigen Windows-Datenschutzbestimmungen. Sie können uns auch uns über unsere Webformular.

Seitenanfang

Aktuelle Informationen über Methoden für die Verarbeitung der Daten von Microsoft, finden Sie in der Datenschutzerklärung von Microsoft. Hier erfahren Sie mehr über die neuesten Tools für den Zugriff auf und die Steuerung Ihrer Daten, und wie Sie uns kontaktieren, wenn Sie eine Abfrage zum Datenschutz haben.

Datenschutzbestimmungen für Windows 8 und Windows Server 2012

Auf dieser Seite finden Sie Folgendes:

Zusätzliche Datenschutzbestimmungen

Diese Datenschutzbestimmungen gelten für Windows 8 und Windows Server 2012 ("Windows"). Einige Windows-Komponenten verfügen über eigene Datenschutzbestimmungen, die auf der rechten Seite dieser Seite aufgeführt sind. Datenschutzbestimmungen für Software und Dienste im Zusammenhang mit Windows und für frühere Versionen werden auch dort aufgelisteten.

Weitere Informationen finden Sie in der Features – Ergänzungund Server – Ergänzung.

Die Datenschutzbestimmungen konzentrieren sich auf Features zur Kommunikation mit dem Internet und sind keine vollständige Liste.

Sammlung und Verwendung Ihrer persönlichen Daten

Die Daten, die wir von Ihnen erfassen, werden von

Microsoft Fehlerberichterstattungsdienst

Microsoft Online

Microsoft Windows-Tool zum Entfernen bösartiger Software

Update Services

Windows Media Center

Windows Media Player

Windows 7

Microsoft und den von Microsoft kontrollierten Tochterunternehmen und verbundenen Unternehmen dazu verwendet, die von Ihnen genutzten Features zu aktivieren und den Dienst/die Dienste bereitzustellen bzw. die Transaktion(en) auszuführen, die von Ihnen angefordert oder genehmigt wurden. Ferner können die von uns erfassten Informationen dazu genutzt werden, die Produkte und Dienste von Microsoft zu analysieren und zu verbessern.

Mit Ausnahme der in den vorliegenden Bestimmungen beschriebenen Verwendung werden keine persönlichen Informationen ohne Ihre Zustimmung an Dritte übermittelt. Microsoft beauftragt von Zeit zu Zeit andere Unternehmen mit bestimmten Dienstleistungen, z. B. mit dem Durchführen von statistischen Analysen unserer Dienste. Dabei stellt Microsoft diesen Unternehmen nur die persönlichen Daten bereit, die zur Erbringung der Dienstleistung erforderlich sind. Es ist den Unternehmen untersagt, diese Daten für andere Zwecke zu verwenden.

Microsoft kann auf Ihre Informationen einschließlich der Inhalte unserer Kommunikation zugreifen oder sie offenlegen, um (a) das Gesetz einzuhalten, auf gesetzliche Anforderungen einzugehen oder dem Rechtsweg zu folgen; (b) die Rechte oder das Eigentum von Microsoft sowie von Microsoft-Kunden zu schützen, wozu auch die Durchsetzung von Verträgen oder Richtlinien von Microsoft gehören, denen die Verwendung der Microsoft-Software unterliegt; oder (c) nach Treu und Glauben anzunehmen, dass ein Zugriff oder eine Offenlegung notwendig ist, um die persönliche Sicherheit der Arbeitnehmer oder der Kunden von Microsoft oder der Öffentlichkeit zu schützen.

Informationen, die durch Windows 8 von Microsoft gesammelt oder an Microsoft gesendet wurden, können in den USA und in jedem anderen Land, in dem Microsoft oder dessen Tochtergesellschaften, Niederlassungen und Dienstanbieter Einrichtungen unterhalten, gespeichert

und verarbeitet werden. Microsoft hält sich im Hinblick auf die Sammlung, Verwendung und Aufbewahrung von Daten aus der Europäischen Union, dem Europäischen Wirtschaftsraum und der Schweiz an die Bestimmungen des US-Handelsministeriums („Safe Harbor“).

Seitenanfang

Sammlung und Verwendung von Informationen zum Computer

Wenn Sie Software mit internetfähigen Features verwenden, werden Informationen zu Ihrem Computer ("Standardcomputerinformationen") an von Ihnen besuchte Webseiten und von Ihnen verwendete Onlinedienste gesendet. Zu den Standardcomputerinformationen zählen im Allgemeinen Informationen wie Ihre IP-Adresse, die Betriebssystemversion, die Browserversion sowie Gebietsschema- und Spracheinstellungen. In einigen Fällen können die Standardgeräteinformationen außerdem eine Hardware-ID enthalten, die den Gerätehersteller, den Gerätenamen und die Geräteversion angibt. Wenn eine Funktion oder ein Dienst Informationen an Microsoft sendet, werden gleichzeitig Standardcomputerinformationen gesendet.

Datenschutzbestimmungen für die einzelnen Windows 8-Funktion in der Features – Ergänzungund Server – Ergänzung, sowie die auf dieser Seite aufgeführten Features beschrieben, welche zusätzlichen Daten erfasst werden und wie diese verwendet werden.

Administratoren können eine Gruppenrichtlinie verwenden, um viele der Einstellungen für die unten beschriebenen Features zu ändern. Weitere Informationen finden Sie unter dieses Whitepaper für Administratoren.

Seitenanfang

Sicherheit von Informationen

Microsoft leistet einen wichtigen Beitrag, um die Sicherheit Ihrer persönlichen Informationen zu gewährleisten. Wir verwenden verschiedene Sicherheitstechnologien und -verfahren zum Schutz von persönlichen Informationen vor unberechtigtem Zugriff, unberechtigter Verwendung oder Offenlegung. Ihre Daten werden beispielsweise auf Computersystemen mit beschränktem Zugriff an überwachten Standorten gespeichert. Wenn wir streng vertrauliche Informationen (z. B. eine Kreditkartennummer oder ein Kennwort) über das Internet übertragen, schützen wir sie durch Verschlüsselung, z. B. das Secure Socket Layer (SSL)-Protokoll.

Seitenanfang

Änderungen dieser Datenschutzbestimmungen

Die vorliegenden Datenschutzbestimmungen werden von Microsoft gelegentlich aktualisiert, um Änderungen an Produkten und Diensten sowie Feedback von Kunden Rechnung zu tragen. Wenn wir Änderungen veröffentlichen, geben wir das Datum der letzten Aktualisierung oben im Dokument der Bestimmungen an. Wenn wir wesentliche Änderungen an den Datenschutzbestimmungen vornehmen oder sich die Art und Weise, wie Microsoft Ihre personenbezogenen Daten verwendet, wesentlich ändert, informieren wir Sie entweder durch die Veröffentlichung einer Bekanntmachung dieser Änderungen vor ihrem Inkrafttreten oder durch die direkte Übermittlung einer Benachrichtigung an Sie. Wir empfehlen, die Datenschutzbestimmungen regelmäßig zu lesen, um sich darüber auf dem Laufenden zu halten, wie Microsoft Ihre Daten schützt.

Seitenanfang

Weitere Informationen

Microsoft begrüßt Kommentare zu diesen Datenschutzbestimmungen. Sollten Sie Fragen zu diesen Datenschutzbestimmungen oder Grund zur Annahme haben, dass die Bestimmungen von unserer Seite nicht eingehalten werden, setzen Sie sich bitte mit uns in Verbindung. Verwenden Sie dazu unser Webformular.

Microsoft Privacy- und Datenschutzgesetzte
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052, USA
USA

Seitenanfang

Aktuelle Informationen über Methoden für die Verarbeitung der Daten von Microsoft, finden Sie in der Datenschutzerklärung von Microsoft. Hier erfahren Sie mehr über die neuesten Tools für den Zugriff auf und die Steuerung Ihrer Daten, und wie Sie uns kontaktieren, wenn Sie eine Abfrage zum Datenschutz haben.

Datenschutzbestimmungen für Windows 8 und Windows Server 2012

Auf dieser Seite

Letzte Aktualisierung: Oktober 2012

Diese Seite ist eine Ergänzung der Datenschutzbestimmungen für Windows 8 und Windows Server 2012 ("Windows-Datenschutzbestimmungen") und umfasst vier Abschnitte:

- Highlights
- Bestimmungen, die die vollständigen Windows-Datenschutzbestimmungen darstellen und Links zu Datenschutzbestimmungen für Windows-Features enthalten, für die eigene Datenschutzbestimmungen vorhanden sind.
- „Features – Ergänzung" (dieses Dokument). Hier werden die Features beschrieben, die Auswirkungen auf den Datenschutz in Windows 8 und Windows Server 2012 haben
- Ergänzung zu Servern. Hier werden die zusätzlichen

Ereignisanzeige

Family Safety

Fax

Handschriftanpassung – Automatisches Lernen

Heimnetzgruppe

Eingabemethoden-Editor (IME)

Programm zur Verbesserung der Installation

Internetdrucken

Spracheinstellungen

Positionsdienste

Name und Profilbild

Netzwerkinformationen

Benachrichtigungen, Sperrbildschirm-Apps und Kachelupdates

Abzüge bestellen

Programmkompatibilitäts-Assistent

Eigenschaften

Näherung

RAS-Verbindungen

RemoteApp- und Desktopverbindungen

Remotedesktopverbindung

Anmelden mit einem

Features beschrieben, die sich auf den Datenschutz in Windows Server 2012 auswirken.

Lesen Sie die vollständigen Datenschutzbestimmungen und alle maßgeblichen Ergänzungen oder eigene Bestimmungen, um sich mit den Praktiken der Datensammlung und -verwendung für ein bestimmtes Feature oder einen Dienst von Windows vertraut zu machen.

Aktivierung

Funktionsweise dieses Features

Die Aktivierung reduziert Softwarefälschungen und stellt sicher, dass Microsoft-Kunden die erwartete Softwarequalität erhalten. Nachdem Ihre Software aktiviert wurde, wird dem PC (oder der Hardware), auf dem die Software installiert ist, ein bestimmter Product Key zugeordnet. Diese Zuordnung verhindert, dass mit dem Product Key dieselbe Kopie der Software auf mehreren PCs aktiviert wird. Bei einigen Änderungen an PC-Komponenten oder der Software muss die Software möglicherweise erneut aktiviert werden. Bei einigen Änderungen an der Hardware oder der Software des PCs muss Windows möglicherweise erneut aktiviert werden. Bei der Aktivierung können Aktivierungsexploits (Software, die die Softwareaktivierung umgeht) erkannt und deaktiviert werden. Ist ein Aktivierungsexploit vorhanden, hat ein Drittanbieter möglicherweise die Originalsoftware von Microsoft manipuliert, um Fälschungen der Software zu erstellen. Aktivierungsexploits können die normale Ausführung des Systems beeinträchtigen.

Gesammelte, verarbeitete und übertragene Informationen

Bei der Aktivierung werden beispielsweise die folgenden Informationen an Microsoft gesendet:

- Der Microsoft-Produktcode (ein fünfstelliger Code zur Identifizierung des Windows-Produkts, das Sie aktivieren).
- Eine Kanal-ID oder ein Standortcode, der angibt, wie Sie das Windows-Produkt ursprünglich erhalten haben. Die

Microsoft-Konto

Synchronisieren der Einstellungen

Teredo-Technologie

Trusted Platform Module (TPM)-Dienste

Aktualisierung von Stammzertifikaten

Update Services

Windows-Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP)

Windows Defender

Windows-Fehlerberichterstattung

Windows-Dateizuordnung

Windows-Hilfe

Remoteunterstützung

Windows Search

Windows-Freigabe

Windows SmartScreen

Windows-Spracherkennung

Windows Store

Windows-Zeitdienst

Windows-Problembehandlung

Kanal-ID gibt z. B. Aufschluss darüber, ob das Produkt ursprünglich im Einzelhandel erworben wurde, eine Evaluierungskopie ist, im Rahmen eines Volumenlizenzprogramms erworben oder vom PC-Hersteller vorinstalliert wurde.

- Das Datum der Installation und ob die Installation erfolgreich war.
- Informationen, durch die bestätigt wird, dass der Windows-Product Key nicht geändert wurde.
- Marke und Modell des PCs.
- Versionsinformationen zum Betriebssystem und zur Software.
- Regions- und Spracheinstellungen.
- Eine eindeutige GUID (Globally Unique Identifier), die dem PC zugewiesen ist.
- Product Key (mit Hash) und Produkt-ID.
- BIOS-Name, Revisionsnummer und Revisionsdatum.
- Seriennummer des Festplattenvolumes (mit Hash).
- Das Ergebnis der Aktivierungsprüfung. Dazu gehören Fehlercodes und folgende Informationen zu eventuellen Aktivierungsexploits und ähnlicher schädlicher oder unbefugter Software, die gefunden oder deaktiviert wurde:
    - Der Bezeichner des Aktivierungsexploits.
    - Der aktuelle Zustand des Aktivierungsexploits (z. B. bereinigt oder unter Quarantäne).
    - ID des PC-Herstellers.
    - Dateiname und Hash des Aktivierungsexploits sowie ein Hash der zugehörigen Softwarekomponenten, der auf das Vorhandensein eines Aktivierungsexploits hinweist.

- Der Name und Hash des Inhalts der Startanweisungsdatei für den PC. Falls Sie Windows auf Abonnementbasis lizenziert haben, werden zudem Informationen zum Abonnement gesendet. Darüber hinaus werden Standardcomputerinformationen gesendet. Die IP-Adresse Ihres PCs wird jedoch nur vorübergehend gespeichert.

Verwendung von Informationen

Microsoft verwendet die Informationen, um zu überprüfen, ob Sie über eine lizenzierte Kopie der Software verfügen. Microsoft verwendet diese Informationen nicht, um Kontakt mit einzelnen Kunden aufzunehmen.

Auswahl und Steuerung

Die Aktivierung ist erforderlich und wird automatisch ausgeführt, während Sie Windows einrichten. Wenn Sie nicht über eine gültige Lizenz für die Software verfügen, können Sie Windows. nicht aktivieren.

Seitenanfang

Active Directory Rechteverwaltungsdienste-Client (AD RMS-Client)

Funktionsweise dieses Features

Beim Active Directory Rechteverwaltungsdienste-Client (AD RMS-Client) handelt es sich um eine Technologie zum Schutz von Informationen, die mit AD RMS-fähigen Apps eingesetzt wird, um digitale Informationen vor nicht autorisierter Verwendung zu schützen. Die Besitzer digitaler Informationen können festlegen, wie Empfänger die in einer Datei enthaltenen Informationen verwenden können, z. B. wer die Datei öffnen, ändern, drucken oder anderweitig verwenden kann. Um eine Datei mit eingeschränkten Berechtigungen erstellen oder anzeigen zu können, muss auf Ihrem PC eine AD RMS-fähige App ausgeführt werden, und Sie müssen Zugriff auf einen AD RMS-Server haben.

Gesammelte, verarbeitete und übertragene

Informationen

AD RMS identifiziert Sie bei einem AD-RMS-Server anhand Ihrer E-Mail-Adresse. Daher wird Ihre E-Mail-Adresse auf dem Server und auf Ihrem PC in Lizenzen sowie in vom Server erstellten Identitätszertifikaten gespeichert. Identitätszertifikate werden an und von AD RMS-Servern übertragen, wenn Sie ein durch die Rechteverwaltung geschütztes Dokument öffnen, drucken oder anderweitig verwenden. Wenn Ihr PC mit einem Unternehmensnetzwerk verbunden ist, wird der AD RMS-Server in der Regel vom Unternehmen ausgeführt. Wenn Sie Windows Live AD RMS-Dienste verwenden, wird der Server von Microsoft ausgeführt. Aus Gründen des Datenschutzes werden die an Microsoft AD RMS gesendeten Informationen verschlüsselt.

Verwendung von Informationen

Die Lizenz ermöglicht Ihnen den Zugriff auf geschützte Dateien. Die Identitätszertifikate werden verwendet, um Sie gegenüber einem AD RMS-Server zu identifizieren, und ermöglichen es Ihnen, Dateien zu schützen und auf geschützte Dateien zuzugreifen.

Auswahl und Steuerung

AD RMS-Features müssen über eine AD RMS-fähige App aktiviert werden. Standardmäßig sind sie nicht aktiviert. Sie können wählen, ob Sie die Features aktivieren oder verwenden möchten. Wenn Sie sie nicht aktivieren, können Sie allerdings nicht auf geschützte Dateien zugreifen.

Seitenanfang

Überwachung

Die Überwachung bietet Administratoren die Möglichkeit, Windows so zu konfigurieren, dass Betriebssystemaktivitäten in einem Sicherheitsprotokoll aufgezeichnet werden, auf das über die Ereignisanzeige und andere Apps zugegriffen werden kann. Mithilfe dieses Protokolls können Administratoren nicht autorisierte Zugriffe auf den PC oder Ressourcen auf dem PC erkennen. Administratoren können das Protokoll z. B.

verwenden, um Probleme zu behandeln und festzustellen, ob jemand sich am PC angemeldet, ein neues Benutzerkonto erstellt, eine Sicherheitsrichtlinie geändert oder ein Dokument geöffnet hat.

Gesammelte, verarbeitete und übertragene Informationen

Administratoren bestimmen, welche Informationen gesammelt, wie lange sie aufbewahrt und ob sie an andere Empfänger übertragen werden. Die Informationen können persönliche Informationen wie Benutzer- oder Dateinamen beinhalten. Weitere Informationen erhalten Sie von Ihrem Administrator. Es werden keine Informationen an Microsoft gesendet.

Verwendung von Informationen

Administratoren legen auch fest, wie die Überwachungsinformationen verwendet werden. Im Allgemeinen wird das Sicherheitsprotokoll von Prüfern und Administratoren verwendet, um PC-Aktivitäten nachzuverfolgen oder nicht autorisierte Zugriffe auf den PC oder Ressourcen auf dem PC zu identifizieren.

Auswahl und Steuerung

Administratoren bestimmen, ob dieses Feature aktiviert wird und wie Benutzer benachrichtigt werden. Andere Benutzer können das Sicherheitsprotokoll nur anzeigen, wenn ihnen der Administrator den Zugriff erlaubt. Sie können die Überwachung auf Ihrem PC in „Verwaltung" unter „Lokale Sicherheitsrichtlinie" konfigurieren.

Seitenanfang

BitLocker-Laufwerkverschlüsselung

Funktionsweise dieses Features

Die BitLocker-Laufwerkverschlüsselung schützt Ihre Daten durch Verschlüsselung und kann so verhindern, dass nicht berechtigte Benutzer auf Ihre Daten zugreifen. Wenn BitLocker auf einem unterstützten Laufwerk aktiviert ist, verschlüsselt Windows die

Daten auf dem Laufwerk.

Gesammelte, verarbeitete und übertragene Informationen

Wenn BitLocker mit Softwareverschlüsselung aktiviert wird, werden Daten während Lese- und Schreibvorgängen auf dem geschützten Laufwerk fortlaufend von kryptografischen Schlüsseln im Arbeitsspeicher verschlüsselt und entschlüsselt. Wenn BitLocker mit Hardwareverschlüsselung aktiviert wird, wird die Datenverschlüsselung und -entschlüsselung vom Laufwerk ausgeführt.

Während der Installation von BitLocker haben Sie die Möglichkeit, einen Wiederherstellungsschlüssel auszudrucken oder an einem Netzwerkspeicherort zu speichern. Wenn Sie BitLocker auf einem nicht austauschbarem Laufwerk installieren, können Sie den Wiederherstellungsschlüssel auch auf einem USB-Speicherstick speichern.

Gehört der PC keiner Domäne an, können Sie Ihren BitLocker-Wiederherstellungsschlüssel, die Wiederherstellungsschlüssel-ID und den Computernamen auf __elbasuer__ OneDrive sichern. Aus Datenschutzgründen werden die gesendeten Informationen durch SSL verschlüsselt.

Sie können BitLocker so einrichten, dass Daten mithilfe eines auf einer Smartcard gespeicherten Zertifikats verschlüsselt werden. Wenn Sie ein Datenlaufwerk mit einer Smartcard schützen, werden der öffentliche Schlüssel und der eindeutige Bezeichner (ID) für die Smartcard unverschlüsselt auf dem Laufwerk gespeichert. Anhand dieser Informationen kann das Zertifikat ermittelt werden, das ursprünglich zum Generieren des Verschlüsselungszertifikats der Smartcard verwendet wurde.

Wenn Ihr PC mit Sicherheitshardware mit Version 1.2 oder höher des Trusted Platform Module (TPM) ausgestattet ist, verwendetBitLocker das TPM, um für das Laufwerk, auf dem Windows installiert ist, erweiterten hardwareunterstützten Datenschutz bereitzustellen. Weitere Informationen finden Sie im Abschnitt „Trusted Platform Module (TPM)-Dienste“. Auf PCs mit dem TPM können Sie auch eine PIN (Personal Identification

Number) einrichten, um zusätzlichen Schutz für Ihre verschlüsselten Daten bereitzustellen. BitLocker speichert diese TPM-basierte PIN verschlüsselt und mit Hash auf dem Laufwerk.

Von BitLocker gesammelte Informationen werden nur dann an Microsoft gesendet, wenn Sie den Wiederherstellungsschlüssel auf OneDrive sichern.

Verwendung von Informationen

Kryptografische Schlüssel und GUIDs (Globally Unique Identifiers) werden zur Unterstützung von BitLocker-Vorgängen im Arbeitsspeicher des PC gespeichert. BitLocker-Wiederherstellungsinformationen ermöglichen Ihnen im Fall von Hardwarefehlern oder anderen Problemen den Zugriff auf Ihre geschützten Daten. Anhand dieser Wiederherstellungsinformationen kann BitLocker zwischen autorisierten und nicht autorisierten Benutzern unterscheiden.

Ihre persönlichen Wiederherstellungsschlüssel werden von Microsoft in keiner Weise verwendet. Wenn Wiederherstellungsschlüssel an OneDrive gesendet werden, kann Microsoft aggregierte Daten zu den Schlüsseln zum Analysieren von Trends sowie zum Verbessern unserer Produkte und Dienste verwenden.

Auswahl und Steuerung

BitLocker ist standardmäßig deaktiviert. Auf einem Wechseldatenträger kann BitLocker jederzeit und von jedem Benutzer über die Option „BitLocker-Laufwerkverschlüsselung" in der Systemsteuerung aktiviert oder deaktiviert werden. Administratoren können BitLocker für alle Laufwerke aktivieren oder deaktivieren.

Wenn Sie Ihren Wiederherstellungsschlüssel auf OneDrive gesichert haben, können Sie hierauf den Schlüssel zugreifen oder ihn löschen.

Seitenanfang

Geräteermittlung und -installation

Windows bietet mehrere Features, mit denen Sie Geräte auf Ihrem PC erkennen und installieren können, wie Geräteinstallation, Installation von mobilen Breitbandgeräten, Netzwerkerkennung und Drahtlosgerätekopplung.

Geräteinstallation

Funktionsweise dieses Features

Wenn auf dem PC ein neues Gerät installiert wird, sucht Windows automatisch nach der entsprechenden Treibersoftware, lädt die Software herunter und installiert sie. Windows kann auch Informationen zum Gerät herunterladen, z. B. eine Beschreibung, ein Bild und das Herstellerlogo. Einige Geräte, darunter bestimmte Drucker, Webcams, mobile Breitbandgeräte und tragbare Geräte, die mit Windows synchronisiert werden können, verfügen über Apps, die eine bessere Nutzung der Funktionen des Geräts und eine höhere Benutzerfreundlichkeit ermöglichen. Falls der Gerätehersteller eine App für das Gerät bereitgestellt hat, wird die App automatisch von Windows aus dem Windows Store heruntergeladen und installiert, wenn Sie beim Store angemeldet sind.

Gesammelte, verarbeitete und übertragene Informationen

Bei der Suche nach Treibern prüft Windows zunächst, ob auf dem PC möglicherweise bereits ein geeigneter Treiber verfügbar ist. Wenn nicht, wird von Windows eine Verbindung mit dem Windows Update-Dienst hergestellt, um Gerätetreiber zu suchen und herunterzuladen. Weitere Informationen zu den von Windows Update gesammelten Informationen und ihrer Verwendung finden Sie in den Datenschutzbestimmungen zu Update Servicesauf den Schlüssel zugreifen oder ihn löschen.

Um Informationen zum Gerät abzurufen und festzustellen, ob eine entsprechende App verfügbar ist, sendet Windows Daten an Microsoft. Zu diesen Daten zählen die Geräte-ID (z. B. die Hardware-ID oder Modell-ID des verwendeten Geräts), Ihre Region und Sprache sowie das Datum der letzten Aktualisierung der Geräteinformationen. Wenn Informationen oder Geräte-Apps verfügbar sind, werden diese von Windows aus dem Windows

Store heruntergeladen und installiert. Die App wird dann in Ihrem Windows Store-Konto in der Liste der heruntergeladenen Apps angezeigt.

Verwendung von Informationen

Die an Microsoft gesendeten Informationen werden verwendet, damit der entsprechende Gerätetreiber, die entsprechenden Geräteinformationen und die Geräte-App schneller ermittelt und heruntergeladen werden können. Microsoft verwendet die Informationen nicht dazu, Sie zu identifizieren, Kontakt zu Ihnen aufzunehmen oder gezielte Werbung zu schalten.

Auswahl und Steuerung

Wenn Sie beim Einrichten von Windows die Expresseinstellungen auswählen, aktivieren Sie das automatische Herunterladen und Installieren von Gerätetreibern, -informationen und -Apps. Wenn Sie sich für das Anpassen der Einstellungen entscheiden, können Sie das automatische Herunterladen und Installieren von Gerätetreibern, Apps und Informationen steuern, indem Sie unter Help protect and update your PC die Option **Automatisch Gerätetreiber, Apps und Infos für neue Geräte abrufen** auswählen. Nach der Einrichtung von Windows können Sie diese Einstellungen in der Systemsteuerung ändern, indem Sie Change device installation settings und dann **Nein, zu installierende Software selbst auswählen**auf den Schlüssel zugreifen oder ihn löschen.

Geräte-Apps können jederzeit deinstalliert werden, ohne das Gerät zu deinstallieren. Möglicherweise ist die App jedoch zur Verwendung bestimmter Features des Geräts erforderlich. Eine Geräte-App kann nach der Deinstallation erneut installiert werden. Rufen Sie dazu im Windows Store die Liste der Ihnen gehörenden Apps auf.

Installation von mobilen Breitbandgeräten

Funktionsweise dieses Features

Falls Ihr PC mit mobiler Breitbandhardware bestimmter Mobilfunkanbieter ausgestattet ist, kann Windows automatisch eine App herunterladen und installieren, mit der Sie Ihr Konto

und Ihren Datentarif beim Mobilfunkanbieter verwalten können. Zudem werden weitere Geräteinformationen heruntergeladen, mit denen Ihre mobile Breitbandverbindung in Netzwerklisten angezeigt werden kann.

Gesammelte, verarbeitete und übertragene Informationen

Um festzustellen, welche Geräteinformationen und Apps heruntergeladen werden sollen, wird von Windows ein Teil der Hardware-IDs von mobilen Breitbandgeräten gesendet, der es ermöglicht, Ihren Mobilfunkanbieter zu identifizieren. Aus Datenschutzgründen werden von Windows nicht die vollständigen IDs von mobilen Breitbandgeräten an Microsoft gesendet.

Falls Ihr Mobilfunkanbieter Microsoft eine App zur Verfügung gestellt hat, lädtWindows die App aus dem Windows Store herunter und installiert sie. Wenn Sie die App nach der Installation öffnen, hat sie Zugriff auf Ihr mobiles Breitbandgerät und damit auch auf die eindeutigen Hardware-IDs, mit deren Hilfe der Mobilfunkanbieter Ihr Konto identifizieren kann.

Verwendung von Informationen

Microsoft verwendet den von Windows gesendeten Teil der ID Ihres mobilen Breitbandgeräts, um den Netzbetreiber zu ermitteln, dessen App auf dem Computer installiert werden soll. Nachdem sie installiert wurde, kann die App die Hardware-IDs Ihres mobilen Breitbandgeräts verwenden. Die App eines Mobilfunkanbieters kann z. B. mithilfe dieser IDs online nach Konto- und Tarifinformationen suchen. Die Verwendung dieser Informationen durch die App unterliegt den Datenschutzpraktiken des Mobilfunkanbieters.

Auswahl und Steuerung

Windows sucht automatisch nach Apps von Mobilfunkanbietern und lädt sie herunter, wenn Sie während der Erstinstallation von Windows die Option „Express-Einstellungen" auswählen. Sie können dieses Feature in der Systemsteuerung aktivieren und deaktivieren. Weitere Informationen finden Sie im Abschnitt

„Geräteinstallation“ weiter oben.

Apps von Mobilfunkanbietern können jederzeit deinstalliert werden, ohne das mobile Breitbandgerät zu deinstallieren.

Netzwerkerkennung

Funktionsweise dieses Features

Wenn Sie Ihren PC an ein kleines privates Netzwerk anschließen (z. B. ein Heimnetzwerk), kann Windows automatisch andere PCs und freigegebene Geräte im Netzwerk erkennen und Ihren PC im Netzwerk für andere sichtbar machen. Sind freigegebene Geräte verfügbar, kann Windows automatisch eine Verbindung mit ihnen herstellen und sie installieren. Beispiele für freigegebene Geräte sind Drucker und Medienextender. Persönliche Geräte wie Kameras und Mobiltelefone fallen nicht in diese Kategorie.

Gesammelte, verarbeitete und übertragene Informationen

Wenn Sie die Freigabe und Verbindungsherstellung mit Geräten aktivieren, können Informationen über Ihren PC (z. B. sein Name und die Netzwerkadresse) über das lokale Netzwerk übertragen werden, damit andere PCs Ihren PC erkennen und eine Verbindung herstellen können.

Um festzustellen, ob mit Ihrem Netzwerk verbundene Geräte automatisch installiert werden sollen, werden einige Informationen über das Netzwerk gesammelt und an Microsoft gesendet. Dazu zählen die Anzahl von Geräten im Netzwerk, der Netzwerktyp (z. B. privates Netzwerk) sowie die Typen und Modellbezeichnungen der Geräte im Netzwerk. Persönliche Informationen wie Netzwerkname oder Kennwort werden nicht gesammelt.

Abhängig von den Geräteinstallationseinstellungen können von Windows einige Informationen an Microsoft gesendet und Gerätesoftware auf Ihrem PC installiert werden, wenn Windows freigegebene Geräte installiert. Weitere Informationen finden Sie im Abschnitt „Geräteinstallation“.

Verwendung von Informationen

Die an Microsoft gesendeten Informationen über das Netzwerk werden dazu verwendet, die automatisch im Netzwerk zu installierenden Geräte zu ermitteln. Microsoft verwendet die Informationen nicht dazu, Sie zu identifizieren, Kontakt zu Ihnen aufzunehmen oder gezielte Werbung zu schalten.

Auswahl und Steuerung

Wenn Sie den PC einem Netzwerk hinzufügen und dabei die Freigabe und Verbindungsherstellung mit Geräten aktivieren, wird die Netzwerkerkennung für dieses Netzwerk aktiviert. Sie können diese Einstellung für das aktuelle Netzwerk ändern, indem Sie in „Netzwerk- und Freigabecenter" auf den unter dem Namen des Netzwerks aufgeführten Netzwerktyp klicken.

Die Netzwerkerkennung und die automatische Installation von Netzwerkgeräten können mit der Option **Erweiterte Freigabeeinstellungen ändern** in „Netzwerk- und Freigabecenter" aktiviert oder deaktiviert werden.

Drahtlosgerätekopplung

Funktionsweise dieses Features

Windows bietet Ihnen die Möglichkeit, Ihren PC mit Drahtlosgeräten mit Bluetooth- oder WiFi Direct-Technologie zu koppeln. WiFi Direct ist eine Drahtlostechnologie, mit deren Hilfe Geräte ohne Verbindung mit einem WiFi-Netzwerk direkt miteinander kommunizieren können.

Gesammelte, verarbeitete und übertragene Informationen

Wenn Sie in „Bluetooth-Einstellungen" die Option **Bluetooth-Geräte können diesen Computer ermitteln**aktivieren, überträgt Windows den Namen Ihres PC über Bluetooth, damit Bluetooth-fähige Geräte Ihren PC erkennen und identifizieren können.

Wenn Sie in „Bluetooth-Einstellungen" die Option **Gerät hinzufügen** aktivieren, überträgt Windows den Namen Ihres PC über WiFi, damit WiFi-fähige Geräte Ihren PC erkennen und identifizieren können. Windows beendet die Übertragung des PC-

Namens über WiFi, wenn Sie **Gerät hinzufügen**schließen.

Abhängig von den Geräteinstallationseinstellungen können von Windows einige Informationen an Microsoft gesendet und Gerätesoftware auf Ihrem PC installiert werden, wenn Windows den PC an Drahtlosgeräte koppelt. Weitere Informationen finden Sie im Abschnitt „Geräteinstallation" weiter oben.

Verwendung von Informationen

Windows überträgt den Namen Ihres PC, damit andere Geräte den PC identifizieren und eine Verbindung mit ihm herstellen können. Der Name Ihres PC wird nicht an Microsoft gesendet.

Auswahl und Steuerung

Um die Einstellung für die Bluetooth-Übertragung Ihres PC-Namens durch Windows zu ändern, klicken Sie in der Systemsteuerung in „Geräte" auf Ihren PC, und halten Sie die Maustaste gedrückt (oder klicken mit der rechten Maustaste auf den PC), und wählen Sie **Bluetooth-Einstellungen**und anschließend **Bluetooth-Geräte können diesen Computer ermitteln**aus. Wenn Windows den Namen Ihres PC beim Hinzufügen von Geräten nicht über WiFi übertragen soll, können Sie WiFi vor dem Hinzufügen eines Geräts in den PC-Einstellungen unter „Drahtlos" vorübergehend deaktivieren.

Seitenanfang

DirectAccess

Funktionsweise dieses Features

DirectAccess ermöglicht es Ihrem PC, unabhängig vom Standort eine nahtlose Remoteverbindung mit Ihrem Arbeitsplatznetzwerk herzustellen, wenn er mit dem Internet verbunden ist.

Gesammelte, verarbeitete und übertragene Informationen

Bei jedem Start des PC versucht DirectAccess, eine Verbindung mit Ihrem Arbeitsplatznetzwerk herzustellen, unabhängig davon, ob Sie sich am Arbeitsplatz befinden oder nicht. Nachdem die Verbindung hergestellt wurde, lädt Ihr PC die

Arbeitsplatzrichtlinie herunter, und Sie können auf konfigurierte Ressourcen im Arbeitsplatznetzwerk zugreifen. Der Arbeitsplatzadministrator kann die DirectAccess-Konnektivität nutzen, um Ihren PC remote zu verwalten und zu überwachen. Dabei hat er auch Zugriff auf die Webseiten, die Sie besuchen, wenn Sie sich nicht am Arbeitsplatz befinden.

DirectAccess sendet keine Informationen an Microsoft.

Verwendung von Informationen

Wie die vom Arbeitsplatzadministrator gesammelten Informationen verwendet werden, hängt von den Richtlinien Ihres Unternehmens ab.

Auswahl und Steuerung

DirectAccess muss vom Arbeitsplatzadministrator mithilfe der Gruppenrichtlinie konfiguriert werden. Ihr Administrator kann Ihnen das vorübergehende Deaktivieren einiger Elemente von DirectAccess erlauben, aber nur der Arbeitsplatzadministrator kann verhindern, dass Windows zu Verwaltungszwecken eine Verbindung mit Ihrem Arbeitsplatz herstellt. Wird Ihr PC von Ihnen oder Ihrem Arbeitsplatzadministrator aus der Arbeitsplatzdomäne entfernt, kann DirectAccess keine Verbindung mehr herstellen.

Seitenanfang

Dynamisches Update

Funktionsweise dieses Features

Das dynamische Update ermöglicht es Windows, während der Installation von Windows eine einmalige Überprüfung mit Windows Update durchzuführen, um die aktuellen Updates für Ihren PC abzurufen. Falls Updates gefunden werden, werden sie automatisch heruntergeladen und installiert, sodass Ihr PC auf dem neuesten Stand ist, wenn Sie sich zum ersten Mal anmelden oder den PC zum ersten Mal verwenden.

Gesammelte, verarbeitete und übertragene Informationen

Beim dynamischen Update werden Informationen über die Hardware Ihres PC an Microsoft gesendet, damit kompatible Treiber installiert werden können. Folgende Arten von Updates können mit dem dynamischen Update auf den PC heruntergeladen werden:

- **Installationsupdatesauf den Schlüssel zugreifen oder ihn löschen.** Wichtige Softwareupdates für Installationsdateien, mit denen eine erfolgreiche Installation sichergestellt wird.

- **Updates für mitgelieferte Treiberauf den Schlüssel zugreifen oder ihn löschen.** Wichtige Treiberupdates für die installierte Windows-Version.

Verwendung von Informationen

Beim dynamischen Update werden Informationen über die Hardware Ihres PCs an Microsoft gesendet, damit die richtigen Treiber für Ihr System ermittelt werden können. Weitere Informationen zur Verwendung der Informationen, die beim dynamischen Update gesammelt werden, finden Sie in den Datenschutzbestimmungen zu Update Servicesauf den Schlüssel zugreifen oder ihn löschen.

Auswahl und Steuerung

Zu Beginn der Installation von Windows werden Sie gefragt, ob Sie in den Onlinemodus wechseln möchten, um Updates zu installieren.

Seitenanfang

Center für erleichterte Bedienung

Funktionsweise dieses Features

Im Center für erleichterte Bedienung können Sie Barrierefreiheitsoptionen und -einstellungen aktivieren, um die Interaktion mit dem PC zu erleichtern.

Gesammelte, verarbeitete und übertragene Informationen

Wenn Sie dieses Feature verwenden, werden Sie aufgefordert, für Sie zutreffende Aussagen auszuwählen.

Dazu zählen u. a. folgende Aussagen:

- Bilder oder Text im Fernsehen sind schwer zu erkennen.
- Die Beleuchtung erschwert das Erkennen von Bildern auf dem Monitor.
- Ich verwende keine Tastatur.
- Ich bin blind.
- Ich bin taub.
- Ich habe einen Sprachfehler.

Diese Informationen werden in einem nicht lesbaren Format lokal auf Ihrem PC gespeichert.

Verwendung von Informationen

Basierend auf den ausgewählten Aussagen werden Ihnen Konfigurationsempfehlungen vorgeschlagen. Diese Informationen werden nicht an Microsoft gesendet und sind mit Ausnahme von Ihnen und den Administratoren des PC für niemanden zugänglich.

Auswahl und Steuerung

Sie können die gewünschten Aussagen in der Systemsteuerung unter „Erleichterte Bedienung" auswählen. Die Einstellungen können jederzeit geändert werden. Außerdem können Sie die Empfehlungen auswählen, die Sie auf Ihrem PC konfigurieren möchten.

Seitenanfang

Ereignisanzeige

Funktionsweise dieses Features

PC-Benutzer und vor allem Administratoren können die Ereignisanzeige verwenden, um Ereignisprotokolle anzuzeigen

und zu verwalten. Ereignisprotokolle enthalten Informationen über die Hardware, die Software und Sicherheitsereignisse auf dem PC. Sie können zu den Ereignissen in den Protokollen auch Informationen von Microsoft abrufen, indem Sie auf „Onlinehilfe" klicken.

Gesammelte, verarbeitete und übertragene Informationen

Ereignisprotokolle enthalten Ereignisinformationen, die von allen Benutzern und Apps auf dem PC generiert werden. Ereignisprotokolleinträge können standardmäßig von allen Benutzern angezeigt werden, der Zugriff auf die Protokolle kann aber von Administratoren eingeschränkt werden. Um die Ereignisprotokolle für Ihren PC anzuzeigen, öffnen Sie die Ereignisanzeige. Informationen zum Öffnen der Ereignisanzeige finden Sie in „Windows-Hilfe und Support".

Wenn Sie die Onlinehilfe des Ereignisprotokolls verwenden, um nach weiteren Informationen zu einem bestimmten Ereignis zu suchen, werden die Informationen zu dem Ereignis an Microsoft. gesendet.

Verwendung von Informationen

Wenn Sie die Onlinehilfe des Ereignisprotokolls verwenden, um nach weiteren Informationen zu einem Ereignis zu suchen, werden die von Ihrem PC gesendeten Ereignisdaten dazu verwendet, nach weiteren Informationen zum Ereignis zu suchen und sie anzuzeigen. Bei Microsoft-Ereignissen werden die Ereignisdetails an Microsoft gesendet. Microsoft verwendet die Informationen nicht dazu, Sie zu identifizieren, Kontakt mit Ihnen aufzunehmen oder gezielte Werbung zu schalten. Bei Ereignissen, die Apps von Drittanbietern betreffen, werden die Informationen an den vom Herausgeber oder Hersteller angegebenen Ort gesendet. Wenn Sie Informationen über Ereignisse an Drittanbieter senden, unterliegt die Verwendung der Informationen den Datenschutzpraktiken des jeweiligen Herausgebers bzw. Herstellers.

Auswahl und Steuerung

Administratoren können den Zugriff auf Protokolle der Ereignisanzeige einschränken. Benutzer mit Vollzugriff auf Protokolle der Ereignisanzeige können die Protokolle löschen. Sofern Sie dem automatischen Senden von Ereignisinformationen zuvor nicht bereits zugestimmt haben, werden Sie beim Klicken auf „Onlinehilfe" um Ihre Zustimmung gebeten, dass die angezeigten Informationen über das Internet gesendet werden. Nur wenn Sie zustimmen, werden Ereignisprotokollinformationen über das Internet gesendet. Administratoren können die Webseite, an die Ereignisinformationen gesendet werden, mithilfe der Gruppenrichtlinie auswählen oder ändern.

Seitenanfang

Family Safety

Funktionsweise dieses Features

Family Safety ermöglicht es Eltern, ihre Kinder bei der Nutzung eines PCs zu schützen. Eltern können festlegen, welche Apps, Spiele und Webseiten Kinder verwenden dürfen. Eltern können auch Zeitlimits festlegen und regelmäßige Aktivitätsberichte per E-Mail erhalten. Eltern können Einschränkungen verwalten und Aktivitätsberichte lokal auf dem PC oder online über die Microsoft Family Safety-Webseite anzeigen.

Gesammelte, verarbeitete und übertragene Informationen

Family Safety-Einstellungen und -Berichte zur Aktivität von Kindern werden auf dem PC gespeichert. Aktivitätsberichte können Informationen zu der mit dem Computer verbrachten Zeit, zu der mit einzelnen Apps und Spielen verbrachten Zeit sowie zu besuchten Webseiten (auch zu Versuchen, geblockte Webseiten aufzurufen) enthalten. Administratoren am PC können Einstellungen ändern und den Aktivitätsbericht anzeigen.

Wenn die Onlineverwaltung für ein Kinderkonto aktiviert wurde, können die Eltern den Aktivitätsbericht des Kindes anzeigen und die Einstellungen auf der Microsoft Family Safety-Webseite

ändern. Eltern können anderen Personen erlauben, Aktivitätsberichte anzuzeigen und Einstellungen zu ändern, indem Sie diese Personen auf der Microsoft Family Safety-Webseite als Eltern hinzufügen. Wenn sich ein Elternteil, das Family Safety konfiguriert, bei Windows mit einem Microsoft-Konto anmeldet, wird die Onlineverwaltung automatisch aktiviert..

Wenn Family Safety für ein Kinderkonto bei aktivierter Onlineverwaltung konfiguriert wird, werden automatisch wöchentlich Berichte über die Aktivitäten des Kindes per E-Mail an das Elternteil gesendet.

Verwendung von Informationen

Die gesammelten Informationen werden von Windows und der Microsoft Family Safety-Webseite zur Bereitstellung des Family Safety-Features verwendet. Die Informationen des Aktivitätsprotokolls können von Microsoft in zusammengefasster Form zur Sicherstellung der Datenqualität analysiert werden. Die Informationen werden jedoch nicht dazu verwendet, Sie zu identifizieren, Kontakt mit Ihnen aufzunehmen oder gezielte Werbung zu schalten.

Auswahl und Steuerung

Family Safety ist standardmäßig deaktiviert. Sie können in der Systemsteuerung unter „Family Safety" auf dieses Feature zugreifen. Nur Administratoren können Family Safety aktivieren, und nur Benutzer ohne Administratorrechte können überwacht oder im Hinblick auf den Zugriff eingeschränkt werden. Kinder können ihre Einstellungen anzeigen, aber nicht ändern. Wenn Family Safety aktiviert ist, wird das Kind benachrichtigt, dass sein Konto bei jeder Anmeldung bei Windows überwacht wird. Wenn Sie beim Erstellen eines Kontos angeben, dass es sich bei dem Konto um ein Kinderkonto handelt, können Sie für dieses Konto Family Safety aktivieren.

Wenn der Administrator, der ein Kinderkonto einrichtet, bei Windows mit einem Microsoft-Konto angemeldet ist, wird die Onlineverwaltung automatisch aktiviert und Berichte über die Aktivitäten des Kindes werden wöchentlich gesendet.

Elternkonten können auf der Microsoft Family Safety-Webseite hinzugefügt oder entfernt werden. Ein Benutzer, der auf der Webseite als Elternteil hinzugefügt wird, kann den Aktivitätsbericht des Kindes aufrufen und die Family Safety-Einstellungen für das Kind ändern, auch wenn das Elternteil kein Administrator an dem vom Kind verwendeten PC ist.

Damit Family Safety seine Funktion erfüllen kann, sollten nur Eltern Administratoren des PC sein und Kinder keine Administratorrechte besitzen. Die Verwendung dieses Features zur Überwachung anderer Benutzer (Erwachsener) verstößt möglicherweise gegen geltendes Recht.

Seitenanfang

Fax

Funktionsweise dieses Features

Das Faxfeature ermöglicht Ihnen das Erstellen und Speichern von Faxdeckblättern sowie das Senden und Empfangen von Faxen über Ihren PC und ein externes oder integriertes Faxmodem oder einen Faxserver.

Gesammelte, verarbeitete und übertragene Informationen

Zu den gesammelten Informationen zählen alle persönlichen Informationen, die Sie auf einem Faxdeckblatt angeben, und in standardmäßigen Faxprotokollen enthaltene Bezeichner, z. B. Absender-ID (TSID) und Teilnehmer-ID (CSID). Windows verwendet standardmäßig den Wert „Fax" für jeden Bezeichner.

Verwendung von Informationen

Die im Absenderdialogfeld eingegebenen Informationen erscheinen auf dem Faxdeckblatt. Bezeichner wie die TSID und die CSID können beliebigen Text enthalten und werden in der Regel vom empfangenden Faxgerät oder PC zum Identifizieren des Absenders verwendet. Es werden keine Informationen an Microsoft gesendet.

Auswahl und Steuerung

Der Zugriff auf das Faxfeature hängt von Ihren Benutzerkontorechten auf dem PC ab. Sofern die Zugriffseinstellungen nicht von einem Faxadministrator geändert werden, können alle Benutzer Faxe senden und empfangen. Standardmäßig können alle Benutzer die von ihnen gesendeten Dokumente und alle auf dem PC empfangenen Faxe anzeigen. Administratoren können alle gefaxten Dokumente (gesendet oder empfangen) anzeigen und Faxeinstellungen konfigurieren, z. B. Berechtigungen für das Anzeigen und Verwalten von Faxen sowie die TSID- und CSID-Werte.

Seitenanfang

Handschriftanpassung – Automatisches Lernen

Funktionsweise dieses Features

Das automatische Lernen ist ein Handschrifterkennungs-Anpassungstool, das auf PCs mit Toucheingabe oder Tablettstift verfügbar ist. Dieses Feature sammelt Daten über die von Ihnen verwendeten Wörter und deren Schreibweise. So kann die Handschrifterkennungssoftware die Interpretation Ihrer Handschrift und Ihres Vokabulars lernen und verbessern sowie die Autokorrektur- und Wortvorschläge für Sprachen ohne Eingabemethoden-Editoren (IMEs) optimieren.

Gesammelte, verarbeitete und übertragene Informationen

Die beim automatischen Lernen gesammelten Informationen werden im Benutzerprofil jedes Benutzers des PC gespeichert. Die Daten werden in einem proprietären Format gespeichert, das nicht mit einer Textanzeige-App (z. B. Editor oder WordPad) gelesen werden kann, und sind für andere Benutzer nur verfügbar, wenn diese Administratoren Ihres PCs sind.

Folgende Informationen werden gesammelt:

- Text aus Nachrichten und Kalendereinträgen, die Sie mit E-Mail-Apps erstellen (z. B. Office Outlook oder Windows Live Mail). Dies beinhaltet auch alle bereits versendeten Nachrichten.

- Freihandeingaben im Eingabebereich.
- Erkannter Text aus Freihandeingaben im Eingabebereich oder Eingaben über die Bildschirmtastaturen.
- Alternative Zeichen, die Sie zum Korrigieren des erkannten Textes auswählen.

Verwendung von Informationen

Die gesammelten Informationen werden dazu verwendet, die Handschrifterkennung durch Erstellen einer für Ihre Handschrift und Ihr Vokabular angepassten Version der Handschrifterkennungssoftware zu verbessern und Autokorrektur- sowie Wortvorschläge bei der Eingabe über Bildschirmtastaturen zu ermöglichen.

Anhand der Textbeispiele wird ein erweitertes Wörterbuch erstellt. Mithilfe der Freihandbeispiele wird die Zeichenerkennung für jeden Benutzer eines PC verbessert. Es werden keine Informationen an Microsoft gesendet.

Auswahl und Steuerung

Das automatische Lernen ist standardmäßig aktiviert. Sie können das automatische Lernen jederzeit in der Systemsteuerung unter „Sprachen" über die Option „Erweiterte Einstellungen" aktivieren oder deaktivieren. Wenn Sie das Feature deaktivieren, werden alle durch automatisches Lernen gesammelten und gespeicherten Daten gelöscht.

Seitenanfang

Heimnetzgruppe

Funktionsweise dieses Features

Unter Windows können Sie PCs in Ihrem Heimnetzwerk mühelos verbinden, um Bilder, Musik, Videos, Dokumente und Dienste zu teilen. Mithilfe eines Heimnetzwerks können PCs zudem Medien auf Geräte im Heimnetzwerk (z. B. einen Medienextender) streamen. Diese PCs und Geräte bilden die Heimnetzgruppe. Sie

können Ihre Heimnetzgruppe mit einem Kennwort schützen und die Inhalte auswählen, die Sie teilen möchten.

Gesammelte, verarbeitete und übertragene Informationen

Sie können auf jedem PC in der Heimnetzgruppe auf Ihre eigenen Dateien zugreifen, z. B. Bilder, Videos, Musik und Dokumente. Wenn Sie Ihren PC einer Heimnetzgruppe hinzufügen, werden Kontoinformationen (einschließlich E-Mail-Adresse, Anzeigename und Bild) für alle Microsoft-Konten auf Ihrem PC für andere PCs in der Heimnetzgruppe freigegeben, damit Sie Dateien mit diesen Benutzern teilen können.

Verwendung von Informationen

Anhand der gesammelten Informationen können PCs in Ihrer Heimnetzgruppe feststellen, für wen Inhalte freigegeben und wie sie angezeigt werden sollen. Es werden keine Informationen an Microsoft gesendet.

Auswahl und Steuerung

Sie können in Ihrer Heimnetzgruppe PCs hinzufügen oder entfernen und festlegen, welche Inhalte für Mitglieder der Gruppe freigegeben werden. In den PC-Einstellungen können Sie unter „Heimnetzgruppe" eine Heimnetzgruppe erstellen und ihre Einstellungen verwalten.

Seitenanfang

Eingabemethoden-Editor (IME)

Microsoft Eingabemethoden-Editoren (IMEs) werden für ostasiatische Sprachen verwendet, um Tastatureingaben in Ideogramme zu konvertieren. In diesem Abschnitt werden verschiedene Features beschrieben, z. B. IME – Automatische Abstimmung und Vorhersage, IME-Konvertierungsfehlerberichterstattung und IME-Wortregistrierung.

IME – Automatische Abstimmung und Vorhersage

Funktionsweise dieses Features

Abhängig vom verwendeten IME und von Ihren Einstellungen zeichnen die IME-Features für die automatische Abstimmung und Wortvorschläge möglicherweise Wörter oder Wortfolgen auf, um die Auswahl der angezeigten Ideogramme zu verbessern.

Gesammelte, verarbeitete und übertragene Informationen

Die IME-Features für die automatische Abstimmung (Selbstlernen) und Wortvorschläge zeichnen ein Wort oder eine Wortfolge und die zugehörige Verwendungshäufigkeit auf. Informationen zur automatischen Abstimmung werden in Dateien für jeden Benutzer eines PC gespeichert (Ziffern-/Symbolfolgen werden nicht gespeichert).

Verwendung von Informationen

Der IME auf Ihrem PC verwendet die von den Features für automatisches Lernen und Wortvorschläge aufgezeichneten Daten, um die Auswahl der Ideogramme zu verbessern, die bei der Verwendung des IME angezeigt werden. Wenn Sie diese Daten an Microsoft senden, werden sie dazu verwendet, den IME sowie zugehörige Produkte und Dienste zu verbessern.

Auswahl und Steuerung

Mit Ausnahme des IME für vereinfachtes Chinesisch (bei dem das Vorhersagefeature standardmäßig deaktiviert ist) sind die Features für automatisches Lernen und Wortvorschläge in den IMEs, von denen sie unterstützt werden, standardmäßig aktiviert. Die gesammelten Daten werden nicht automatisch an Microsoft gesendet. Sie können in der Systemsteuerung unter „Sprache" festlegen, ob diese Daten gesammelt oder gesendet werden.

IME-Konvertierungsfehlerberichterstattung

Funktionsweise dieses Features

Wenn beim Anzeigen von Ideogrammen oder Konvertieren von Tastatureingaben in Ideogramme Fehler auftreten, kann dieses Feature Fehlerinformationen sammeln, mit deren Hilfe Microsoft

seine Produkte und Dienste verbessern kann.

Gesammelte, verarbeitete und übertragene Informationen

Die IME-Konvertierungsfehlerberichterstattung sammelt Informationen über IME-Konvertierungsfehler, z. B. Ihre Eingabe, das erste Konvertierungs- oder Vorhersageergebnis, die stattdessen ausgewählte Zeichenfolge, Informationen zum verwendeten IME und dazu, wie Sie ihn verwenden. Beim japanischen IME können Sie außerdem auswählen, ob Informationen zum automatischen Lernen in Konvertierungsfehlerberichten enthalten sein sollen.

Verwendung von Informationen

Microsoft verwendet die Informationen, um unsere Produkte und Dienste zu verbessern. Microsoft verwendet die Informationen nicht dazu, Sie zu identifizieren, Kontakt mit Ihnen aufzunehmen oder gezielte Werbung zu schalten.

Auswahl und Steuerung

Nachdem eine bestimmte Anzahl von Konvertierungsfehlern gespeichert wurde, werden Sie vom Berichterstellungstool für Konvertierungsfehler gefragt, ob Sie einen Konvertierungsfehlerbericht senden möchten. Zudem können Sie jederzeit über das IME-Berichterstellungstool für Konvertierungsfehler einen Konvertierungsfehlerbericht senden. Sie können die in den Berichten enthaltenen Informationen vor dem Senden anzeigen. In den IME-Einstellungen ist auch eine Option verfügbar, mit der Sie Konvertierungsfehlerberichte automatisch senden können.

IME-Wortregistrierung

Funktionsweise dieses Features

Je nach verwendetem IME können Sie möglicherweise mit der Wortregistrierung nicht unterstützte Wörter melden (Wörter, die nicht korrekt von Tastatureingaben in Ideogramme konvertiert werden können).

Gesammelte, verarbeitete und übertragene

Informationen

Registrierungsberichte können die Informationen, die Sie im Dialogfeld „Wort hinzufügen" zu den gemeldeten Wörter eingeben, und die Softwareversionsnummer für einen IME enthalten. Die Berichte können persönliche Informationen enthalten. Dies ist z. B. der Fall, wenn Sie mit der Wortregistrierung Personennamen hinzufügen. Sie können die in den Berichten enthaltenen Daten vor dem Senden überprüfen.

Verwendung von Informationen

Microsoft verwendet die Informationen, um unsere Produkte und Dienste zu verbessern. Microsoft verwendet die Informationen nicht dazu, Sie zu identifizieren, Kontakt mit Ihnen aufzunehmen oder gezielte Werbung zu schalten.

Auswahl und Steuerung

Jedes Mal, wenn Sie einen Wortregistrierungsbericht erstellen, werden Sie gefragt, ob Sie den Bericht an Microsoft senden möchten. Sie können die im Bericht enthaltenen Informationen vor dem Senden anzeigen.

Seitenanfang

Programm zur Verbesserung der Installation

Funktionsweise dieses Features

Dieses Feature sendet einmalig einen Bericht mit grundlegenden Informationen zum PC und zur Installation von Windows 8 an Microsoft. Microsoft verwendet diese Informationen, um die Benutzerfreundlichkeit der Installation zu verbessern und Lösungen für häufige Installationsprobleme zu entwickeln.

Gesammelte, verarbeitete und übertragene Informationen

Der Bericht enthält im Allgemeinen Informationen zum Installationsvorgang (beispielsweise das Datum der Installation, die Dauer der einzelnen Installationsphasen, ob es sich bei der Installation um ein Upgrade oder um eine Neuinstallation des Produkts handelte, Versionsdetails, Sprache des

Betriebssystems, Medientyp und PC-Konfiguration) und zum Ergebnis (Erfolg oder Fehler) sowie gegebenenfalls Fehlercodes.

Wenn Sie am Programm zur Verbesserung der Installation teilnehmen, wird der Bericht an Microsoft gesendet, sobald Sie eine Verbindung mit dem Internet herstellen. Das Programm zur Verbesserung der Installation generiert eine als GUID (Globally Unique Identifier) bezeichnete Zufallsnummer, die zusammen mit dem Bericht an Microsoft gesendet wird. Anhand der GUID kann Microsoft erkennen, welche Daten im Laufe der Zeit von einem bestimmten Computer übermittelt werden. Die GUID enthält keine persönlichen Informationen und wird nicht dazu verwendet, Sie zu identifizieren.

Verwendung von Informationen

Microsoft und unsere Partner verwenden den Bericht dazu, unsere Produkte und Dienste zu verbessern. Anhand der GUID stellen wir eine Verbindung zwischen diesen Daten und den vom Windows-Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) gesammelten Daten her. Am CEIP können Sie teilnehmen, wenn Sie Windows 8 verwenden.

Auswahl und Steuerung

Sie können während der Installation von Windows 8 entscheiden, ob Sie an diesem Programm teilnehmen möchten, indem Sie **Ich möchte zur Verbesserung der Installation von Windows beitragen** auf den Schlüssel zugreifen oder ihn löschen.

Weitere Informationen finden Sie im Abschnitt zum Windows CEIP.

Seitenanfang

Internetdrucken

Funktionsweise dieses Features

Das Feature Internetdrucken ermöglicht Ihnen das Drucken über das Internet.

Gesammelte, verarbeitete und übertragene Informationen

Wenn Sie mit diesem Feature drucken, müssen Sie zunächst eine Verbindung mit einem Internetdruckserver herstellen und sich authentifizieren. Die Informationen, die zum Herstellen einer Verbindung mit dem Druckserver eingegeben werden müssen, hängen von der unterstützten Sicherheitsstufe des Druckservers ab (Sie können z. B. zur Eingabe eines Benutzernamens und Kennworts aufgefordert werden). Nachdem die Verbindung hergestellt wurde, wird eine Liste kompatibler Drucker angezeigt. Falls auf Ihrem PC kein Druckertreiber für den ausgewählten Drucker installiert ist, können Sie einen Treiber vom Druckserver herunterladen. Da Druckaufträge nicht verschlüsselt werden, können andere Benutzer den gesendeten Inhalt möglicherweise sehen.

Verwendung von Informationen

Die gesammelten Informationen ermöglichen Ihnen das Drucken auf Remotedruckern. Wenn Sie einen von Microsoft gehosteten Druckserver nutzen, werden die von Ihnen bereitgestellten Informationen nicht dazu verwendet, Sie zu identifizieren, Kontakt mit Ihnen aufzunehmen oder gezielte Werbung zu schalten. Wenn Sie Informationen an einen Druckserver von Drittanbietern senden, unterliegt die Verwendung der Informationen den Datenschutzpraktiken des Drittanbieters.

Auswahl und Steuerung

Sie können das Internetdrucken aktivieren oder deaktivieren, indem Sie in der Systemsteuerung „Programme und Funktionen" öffnen und dann **Windows-Features aktivieren oder deaktivieren**auf den Schlüssel zugreifen oder ihn löschen.

Seitenanfang

Spracheinstellungen

Funktionsweise dieses Features

Sie können die bevorzugten Sprachen der Sprachenliste in Windows 8 hinzufügen. Apps und Webseiten erscheinen in der

ersten Sprache, die in dieser Liste verfügbar ist.

Gesammelte, verarbeitete und übertragene Informationen

Wenn Sie Webseiten aufrufen und Apps auf dem PC installieren, wird die Liste der bevorzugten Sprachen an die aufgerufenen Webseiten gesendet und steht den verwendeten Apps zur Verfügung, sodass sie ihnen die Inhalte in Ihrer bevorzugten Sprache bereitstellen.

Verwendung von Informationen

Ihre Liste der bevorzugten Sprachen wird von Microsoft-Webseiten und -Apps verwendet, um Inhalte in Ihren bevorzugten Sprachen bereitzustellen. Microsoft verwendet die Informationen nicht dazu, Sie zu identifizieren oder Kontakt mit Ihnen aufzunehmen. Die von Drittanbieterwebseiten und Apps gesendeten oder verwendeten Sprachinformationen unterliegen den Datenschutzbestimmungen der Drittanbieterwebseite oder des App-Herausgebers.

Auswahl und Steuerung

Ihre Liste der bevorzugten Sprachen steht den Apps, die Sie installieren, und den Webseiten, die Sie aufrufen, zur Verfügung. Sie können in der Systemsteuerung in den Spracheinstellungen dieser Liste Sprachen hinzufügen oder daraus entfernen. Falls diese Liste keine Sprachen enthält, wird die Sprache, die Sie in der Systemsteuerung unter „Region" auf der Registerkarte „Formate" auswählen, an die aufgerufenen Webseiten gesendet.

Seitenanfang

Positionsdienste

Bei PCs unter Windows bezeichnet der Begriff „Positionsdienste" die Windows-Software und den Microsoft-Onlinedienst, mit deren Hilfe die ungefähre physische Position Ihres PC ermittelt und für Apps oder Webseiten bereitgestellt wird, denen Sie den Zugriff auf diese Daten erlauben. Die Plattform für Windows Windows-Position ruft die Position von dedizierter Hardware (z. B. einem

GPS-Sensor im PC) oder über Software wie die Windows-Positionssuche ab.

Plattform für Windows-Position

Funktionsweise dieses Features

Wenn Sie die Plattform für Windows-Position aktivieren, können aus dem Windows Store installierte Apps Sie fragen, ob Sie den Zugriff auf die Position Ihres PCs erlauben. Abhängig von der Systemkonfiguration kann die Position des PCs mithilfe von Hardware (z. B. einem GPS-Sensor) oder von Software (z. B. der Windows-Positionssuche) ermittelt werden.

Die Plattform verhindert nicht, dass Apps auf andere Weise auf die Position Ihres PC zugreifen. Sie können z. B. Geräte installieren (z. B. einen GPS-Empfänger), die Positionsinformationen direkt an eine App senden und die Plattform komplett umgehen. Onlinedienste können die Position des PCs (in der Regel die Stadt, in der sich der PC befindet) unabhängig von den Einstellungen der Plattform für Windows-Position anhand der IP-Adresse des PCs ermitteln.

Gesammelte, verarbeitete und übertragene Informationen

Über die Plattform für Windows-Position selbst werden keine Informationen von Ihrem PC übertragen. Dies kann jedoch über einzelne Positionssuchen wie beispielsweise die Windows-Positionssuche geschehen, wenn Sie Apps mit Positionserkennung verwenden. Apps, die Ihre Position mithilfe der Plattform ermitteln dürfen, können diese Informationen ebenfalls übertragen oder speichern.

Verwendung von Informationen

Wenn Sie die Plattform für Windows-Position aktivieren, können Apps auf Ihre Position zugreifen und so personalisierte Inhalte für Sie bereitstellen. Bei Apps oder Positionssuchdiensten von Drittanbietern unterliegt die Verwendung der Informationen zur Position Ihres PCs den Datenschutzpraktiken des Drittanbieters. Bevor Sie eine App aus dem Windows Store herunterladen, können Sie in der App-Beschreibung überprüfen, ob die App

über eine Positionserkennung verfügt.

Auswahl und Steuerung

Wenn Sie beim Einrichten von Windows die Expresseinstellungen auswählen, aktivieren Sie damit die Plattform für Windows-Position. Wenn Sie „Einstellungen anpassen" auswählen, können Sie die Plattform für Windows-Position mit der Option **Apps den Zugriff auf meinen Standort mithilfe der Plattform für Windows-Position gestatten** unter **Informationen für Apps freigeben**aktivieren oder deaktivieren. Wenn eine Store-App zum ersten Mal die Position Ihres PCs anfordert, werden Sie von Windows gefragt, ob Sie den Zugriff erlauben möchten. In den PC-Einstellungen können Sie unter „Datenschutz" festlegen, ob Sie von Apps nach Ihrem Standort gefragt werden möchten. Zudem können Sie über den Charm „Einstellungen" unter „Berechtigungen" festlegen, ob Ihre Positionsinformationen von einzelnen Store-Apps genutzt werden dürfen.

Wenn Sie eine Desktop-App verwenden, die die Plattform für Windows-Position nutzt, sollte die App Sie fragen, ob Sie den Zugriff auf die Position Ihres PCs erlauben. Sobald dann eine App auf die Position Ihres PCs zugreift, wird ein Symbol im Infobereich angezeigt, um Sie darauf hinzuweisen. Jeder Benutzer kann die eigenen Standorteinstellungen für alle Apps in den PC-Einstellungen unter „Datenschutz" steuern. Administratoren können außerdem die Windows-Plattform in der Systemsteuerung unter „Standort" für alle Benutzer deaktivieren.

Windows-Positionssuche

Funktionsweise dieses Features

Die Windows-Positionssuche stellt eine Verbindung mit dem online verfügbaren Microsoft-Positionsdienst her. Mit diesem kann der ungefähre Standort Ihres PCs anhand von Informationen zu WiFi-Netzwerken in der Nähe des PCs oder anhand der IP-Adresse des PCs ermittelt werden.

Gesammelte, verarbeitete und übertragene Informationen

Wenn eine App, die Sie für den Zugriff auf Ihre Position

autorisiert haben, Ihre Position anfordert, veranlasst die Plattform für Windows-Position alle installierten Positionssuchdienste (einschließlich der Windows-Positionssuche), Ihre aktuelle Position zu ermitteln. Die Windows-Positionssuche überprüft zuerst, ob eine Liste von WiFi-Zugangspunkten verfügbar ist, die bei einer früheren Anforderung von einer positionsbezogenen App gespeichert wurde. Wenn die Windows-Positionssuche noch nicht über eine Liste mit in der Nähe befindlichen WiFi-Zugriffspunkten verfügt oder wenn die Liste veraltet ist, werden Informationen zu WiFi-Zugriffspunkten in der Nähe sowie gegebenenfalls GPS-Informationen an den Microsoft-Positionsdienst gesendet. Der Dienst gibt die ungefähre Position Ihres PC an die Windows-Positionssuche zurück. Diese gibt die Position an die Plattform für Windows-Position weiter, sodass sie für die anfordernde App verfügbar gemacht werden kann. Die Windows-Positionssuche aktualisiert gegebenenfalls auch die gespeicherte Liste mit den WiFi-Zugangspunkten. Diese Liste wird von der Windows-Positionssuche verwaltet, damit der ungefähre Standort des PCs ohne Internetverbindung ermittelt werden kann. Die Liste der Zugangspunkte wird beim Speichern auf einem Datenträger verschlüsselt, sodass Apps nicht direkt darauf zugreifen können.

Zu den gesendeten Informationen über nahe gelegene WiFi-Zugangspunkte zählen die BSSID (MAC-Adresse des WiFi-Zugangspunkts) und die Signalstärke. Die GPS-Informationen beinhalten die ermittelten Längen- und Breitengrade, die Richtung, Geschwindigkeit und Höhe. Aus Datenschutzgründen sendet die Windows-Positionssuche über die bei allen Internetverbindungen gesendeten Standardcomputerinformationen hinaus keine Informationen, um Ihren PC eindeutig zu identifizieren. Um den Datenschutz von WiFi-Netzwerkeigentümern zu gewährleisten, sendet Windows keine SSIDs (Namen von WiFi-Zugangspunkten) oder ausgeblendete WiFi-Netzwerke. Aus Datenschutz- und Sicherheitsgründen werden über WiFi-Netzwerke gesendete Informationen durch SSL verschlüsselt.

Verwendung von Informationen

Die Windows-Positionssuche verwendet die Informationen, um der Plattform für Windows-Position die ungefähre Position Ihres PC mitzuteilen, wenn diese von einer autorisierten App angefordert wird.

Wenn Sie sich dafür entscheiden, zur Verbesserung des Microsoft-Positionsdiensts beizutragen, werden die an Microsoftgesendeten WiFi- und GPS-Informationen verwendet, um die Positionsdienste von Microsoft und damit wiederum die für Apps bereitgestellten Positionsdienste zu verbessern. Von Microsoft werden keine mit diesem Dienst gesammelten Daten gespeichert, die dazu verwendet werden könnten, Sie zu identifizieren, Kontakt zu Ihnen aufzunehmen, gezielte Werbung zu schalten oder einen Verlauf des PC-Standorts nachzuverfolgen oder zu erstellen.

Auswahl und Steuerung

Die Windows-Positionssuche wird nur verwendet, wenn eine autorisierte App die Position Ihres PCs angefordert hat. Weitere Informationen zum Autorisieren von Apps zum Anfordern der Position Ihres PCs finden Sie im Abschnitt „Plattform für Windows-Position". Wenn Sie Apps autorisieren, den Standort Ihres PCs anzufordern, wird die Liste mit in der Nähe befindlichen WiFi-Zugriffspunkten, die von der Windows-Positionssuche verschlüsselt und gespeichert wird, gelöscht und in regelmäßigen Abständen ersetzt.

Wenn Sie während der Installation von Windows die Option „Express-Einstellungen" auswählen, helfen Sie bei der Verbesserung des Microsoft-Positionsdiensts mit. Wenn Sie „Einstellungen anpassen" auswählen, können Sie mithilfe der Option **Ich möchte die Verbesserung der Microsoft-Dienste unterstützen, indem einige Positionsdaten gesendet werden, sobald ich entsprechende Apps verwende** unter **Senden Sie uns (Microsoft) Infos, damit wir Windows und Apps verbessern können**steuern, ob Sie bei der Verbesserung des Microsoft-Positionsdiensts mithelfen. Sie können diese Einstellung nach der Einrichtung von Windows in der Systemsteuerung unter „Standorteinstellungen" ändern. Auch wenn Sie nicht bei der Verbesserung des Diensts mithelfen,

können Sie die Windows-Positionssuche verwenden, um die ungefähre Position Ihres PCs zu ermitteln.

Sie können die Windows-Positionssuche aktivieren und deaktivieren, indem Sie in der Systemsteuerung die Option **Windows-Features aktivieren oder deaktivieren** öffnen. Wenn Sie die Windows-Positionssuche deaktivieren, können Sie weiterhin andere Positionssuchdienste (z. B. GPS) mit der Plattform für Windows-Position verwenden.

Seitenanfang

Name und Profilbild

Funktionsweise dieses Features

Um personalisierte Inhalte bereitzustellen, können Apps Ihren Namen und Ihr Profilbild von Windows anfordern. Ihr Name und Profilbild werden in den PC-Einstellungen unter Benutzer und Ihr Konto angezeigt. Wenn Sie sich mit einem Microsoft-Konto bei Windows anmelden, werden der Name und das Profilbild dieses Kontos von Windows verwendet. Wurde für das Konto noch kein Profilbild ausgewählt, stellt Windows. ein Standardbild bereit.

Gesammelte, verarbeitete und übertragene Informationen

Wenn Sie Apps den Zugriff auf Ihren Namen und Ihr Profilbild gewähren, stellt Windows diese Informationen allen Apps bereit, die sie anfordern. Apps speichern oder übertragen diese Informationen möglicherweise.

Wenn Sie sich bei Windows mit einem Domänenkonto anmelden und Apps die Verwendung Ihres Namens und Profilbilds erlauben, dürfen Apps, die Ihre Windows-Anmeldeinformationen verwenden können, auf bestimmte Domänenkontoinformationen zugreifen. Diese Informationen enthalten beispielsweise den Benutzerprinzipalnamen (wie „jack@contoso.com“) und den DNS-Domänennamen (wie „corp.contoso.com\jack“).

Wenn Sie sich mit einem Microsoft-Konto bei Windows anmelden oder wenn Sie sich bei Windows mit einem Domänenkonto anmelden, das mit einem Microsoft-Konto verbunden ist, kann

Windows Ihr Profilbild auf dem PC automatisch mit Ihrem Microsoft-Profilbild synchronisieren.

Verwendung von Informationen

Bei Drittanbieter-Apps unterliegt die Verwendung Ihres Namens und Profilbilds den Datenschutzpraktiken des Drittanbieters. Bei Microsoft-Apps werden die Datenschutzpraktiken in den zugehörigen Datenschutzbestimmungen erläutert.

Auswahl und Steuerung

Wenn Sie während der Installation von Windows die Option „Express-Einstellungen" auswählen, gewährt Windows Apps den Zugriff auf Ihren Namen und Ihr Profilbild. Wenn Sie „Einstellungen anpassen" auswählen, können Sie den Zugriff auf Ihren Namen und Ihr Profilbild mit der Option **Apps, die kein Microsoft-Konto verwenden, den Zugriff auf Name und Profilbild gestatten** unter **Informationen für Apps freigeben**steuern. Nach dem Einrichten von Windows können Sie diese Einstellung in den PC-Einstellungen unter **Datenschutz** ändern. Sie können das Profilbild in den PC-Einstellungen unter **Anpassen** ändern. Außerdem können Sie bestimmten Apps das Ändern des Profilbilds erlauben.

Seitenanfang

Netzwerkinformationen

Funktionsweise dieses Features

Wenn Sie über einen Abonnementplan für den Netzwerkzugriff verfügen (z. B. über eine mobile Breitbandverbindung), stellt dieses Feature Informationen über Ihren Abonnementplan für Apps und Windows-Features auf Ihrem PC bereit. Windows-Features und Apps können diese Informationen verwenden, um ihr Verhalten zu optimieren. Bei einem Volumentarif wartet Windows Update z. B., bis Sie mit einem anderen Netzwerktyp verbunden sind, bevor Updates mit niedrigerer Priorität an Ihren PC übermittelt werden. Dieses Feature stellt auch Informationen zur Netzwerkverbindung bereit, z. B. die Signalstärke und ob Ihr PC mit dem Internet verbunden ist.

Gesammelte, verarbeitete und übertragene Informationen

Dieses Feature sammelt Informationen zur Internet- und Intranetkonnektivität, z. B. den Domain Name Service (DNS)-Suffix Ihres PC, den Netzwerknamen und die Gatewayadresse der Netzwerke, mit denen Ihr PC verbunden ist. Außerdem empfängt dieses Feature Informationen zum Abonnementplan wie die verbleibende Datenmenge im Plan.

Netzwerkkonnektivitätsprofile können einen Verlauf aller besuchten Netzwerke sowie das Datum und die Uhrzeit der letzten Verbindung enthalten. Dieses Feature kann versuchen, eine Verbindung mit einem Microsoft-Server herzustellen, um festzustellen, ob Sie mit dem Internet verbunden sind. Die einzigen Daten, die während Netzwerkkonnektivitätsprüfungen an Microsoft gesendet werden, sind standardmäßige PC-Informationen.

Verwendung von Informationen

Wenn Daten an Microsoft gesendet werden, werden sie nur dazu verwendet, den Netzwerkkonnektivitätsstatus bereitzustellen. Der Netzwerkkonnektivitätsstatus wird für Apps und Features auf Ihrem PC verfügbar gemacht, die Informationen zur Netzwerkkonnektivität anfordern. Bei Drittanbieter-Apps unterliegt die Verwendung der gesammelten Informationen den Datenschutzpraktiken des Drittanbieters.

Auswahl und Steuerung

Das Feature Netzwerkinformationen ist standardmäßig aktiviert. Administratoren können es in der Systemsteuerung mit den Dienstoptionen unter „Verwaltung" deaktivieren. Das Deaktivieren dieses Features wird nicht empfohlen, da einige Windows-Features andernfalls nicht einwandfrei funktionieren.

Seitenanfang

Benachrichtigungen, Sperrbildschirm-Apps und Kachelupdates

Windows Store-Apps können automatisch Inhalte empfangen

und Benachrichtigungen auf unterschiedliche Weise anzeigen. Sie können beispielsweise Benachrichtigungen empfangen, die kurz in der Bildschirmecke oder auf Kacheln von Apps angezeigt werden, sofern diese an die Startseite angeheftet sind. Wenn Sie möchten, können Sie diese Benachrichtigungen auch auf dem Sperrbildschirm empfangen. Auf dem Sperrbildschirm können zudem ausführliche oder kurze Statusinformationen für bestimmte Apps angezeigt werden. App-Herausgeber können über den auf Microsoft-Servern ausgeführten Windows-Pushbenachrichtigungsdienst Inhalte an Ihre Windows Store-Apps senden, oder die Apps können Informationen direkt von Servern von Drittanbietern herunterladen.

Benachrichtigungen

Funktionsweise dieses Features

Windows Store-Apps können regelmäßig oder in Echtzeit Informationen an Sie übermitteln, die als Benachrichtigungen kurz in der Ecke Bildschirms angezeigt werden.

Gesammelte, verarbeitete und übertragene Informationen

Apps können in Benachrichtigungen Text, Bilder oder beides anzeigen. Die Inhalte von Benachrichtigungen können von der App lokal bereitgestellt werden (z. B. ein Alarm von einer Uhr-App). Benachrichtigungen können auch vom Onlinedienst einer App über den Windows-Pushbenachrichtigungsdienst (z. B. ein Update eines sozialen Netzwerks) gesendet werden. In Benachrichtigungen angezeigte Bilder können direkt von einem vom App-Herausgeber angegebenen Server heruntergeladen werden. In diesem Fall werden Standardcomputerinformationen an diesen Server gesendet.

Verwendung von Informationen

Microsoft verwendet Benachrichtigungsinformationen nur dazu, Benachrichtigungen von Ihren Apps an Sie zu übermitteln. Die Benachrichtigung kann vor der Übermittlung an Ihren PC temporär vom Windows-Pushbenachrichtigungsdienst gespeichert werden. Wenn eine Benachrichtigung nicht sofort zugestellt werden kann, wird sie nur für einige Minuten

gespeichert und dann gelöscht.

Auswahl und Steuerung

Sie können Benachrichtigungen in den PC-Einstellungen unter **Benachrichtigungen** für alle oder einzelne Apps deaktivieren. Wenn Sie Benachrichtigungen für eine App deaktivieren oder deinstallieren, kann der App-Herausgeber weiterhin Updates an den Windows-Pushbenachrichtigungsdienst senden, diese Benachrichtigungen werden aber auf Ihrem PC nicht angezeigt.

Sperrbildschirm-Apps

Funktionsweise dieses Features

Einige Apps können bei gesperrtem PC Statusinformationen und Benachrichtigungen auf dem Bildschirm anzeigen. Nicht verwendete Sperrbildschirm-Apps können Aufgaben wie etwa das Synchronisieren von E-Mails im Hintergrund ausführen.

Gesammelte, verarbeitete und übertragene Informationen

Sperrbildschirm-Apps können Statusaktualisierungen vom App-Herausgeber über den Windows-Pushbenachrichtigungsdienst oder direkt von den Servern des App-Herausgebers (oder eines anderen Drittanbieters) empfangen. Sperrbildschirm-Apps können zudem auch andere Informationen übertragen oder verarbeiten, die nicht mit Benachrichtigungen und Updates im Zusammenhang stehen.

Verwendung von Informationen

Die von den Sperrbildschirm-Apps bereitgestellten Status- und Benachrichtigungsinformationen werden von Windows zum Aktualisieren des Sperrbildschirms verwendet.

Auswahl und Steuerung

Nach dem Einrichten von Windows werden die E-Mail-, Kalender- und Nachrichten-Apps automatisch als Sperrbildschirm-Apps festgelegt. Diese oder andere Apps können Sie in den PC-Einstellungen unter „Anpassen" auf dem Sperrbildschirm hinzufügen oder entfernen. Sie können auch eine App auswählen, für die permanent ausführliche Statusinformationen

(z. B. Details für den nächsten Termin im Kalender) auf dem Sperrbildschirm angezeigt werden.

In den PC-Einstellungen können Sie unter „Benachrichtigungen" festlegen, ob Sperrbildschirm-Apps Benachrichtigungen auf dem Sperrbildschirm anzeigen können.

Kachelupdates

Funktionsweise dieses Features

Windows Store-Apps können regelmäßig oder in Echtzeit Informationen an Sie übermitteln, die auf der Startseite als Updates Ihrer App-Kacheln angezeigt werden.

Gesammelte, verarbeitete und übertragene Informationen

Store-Apps, die an die Startseite angeheftet sind, können ihre Kacheln mit Text und/oder Bildern aktualisieren. Der in einer App-Kachel angezeigte Inhalt kann lokal von der App bereitgestellt, regelmäßig von einem vom App-Herausgeber angegebenen Server heruntergeladen oder vom Onlinedienst der App über den Windows-Pushbenachrichtigungsdienst gesendet werden. Wenn Kachelinhalt direkt von einem vom App-Herausgeber angegebenen Server heruntergeladen wird, werden Standardcomputerinformationen an diesen Server gesendet.

Verwendung von Informationen

Microsoft verwendet Kachelinformationen nur dazu, Kachelupdates von Ihren Apps an Sie zu übermitteln. Die Informationen können vor der Übermittlung an Ihren PC temporär vom Windows-Pushbenachrichtigungsdienst gespeichert werden. Wenn ein Kachelupdate nicht sofort zugestellt werden kann, wird es nur für einige Tage gespeichert und dann gelöscht.

Auswahl und Steuerung

Nachdem der Empfang von Kachelupdates in einer App gestartet wurde, können Sie die Updates deaktivieren, indem Sie die Kachel der App im Menü „Start" auswählen und in den für die App verfügbaren Befehlen auf **Live-Kachel deaktivieren**

klicken. Wenn Sie die Kachel einer App von „Start“ lösen, werden die entsprechenden Kachelupdates nicht mehr angezeigt. Wenn Sie eine App deinstallieren, kann der App-Herausgeber weiterhin Updates an den Windows-Pushbenachrichtigungsdienst senden, diese Benachrichtigungen werden aber auf Ihrem PC nicht angezeigt.

Um die aktuell auf den Kacheln im Menü „Start“ angezeigten Updates zu löschen, wischen Sie vom rechten Rand nach innen, oder zeigen Sie auf die obere rechte Ecke des Menüs „Start“, und tippen oder klicken Sie auf **Einstellungen**und dann erneut auf **Kacheln**. Tippen oder klicken Sie unter **Persönliche Informationen aus meinen Kacheln löschen** auf die Schaltfläche **Löschen**. Nach dem Löschen der aktuellen Updates bereitgestellte Kachelupdates werden weiterhin angezeigt.

Seitenanfang

Abzüge bestellen

Funktionsweise dieses Features

Mit „Abzüge bestellen“ können Sie auf Ihrem PC oder einem Netzlaufwerk gespeicherte digitale Bilder an einen Online-Fotodruckdienst Ihrer Wahl senden. Je nach Dienst können Sie die Bilder drucken und sich dann per Post zusenden lassen oder in einer Filiale abholen.

Gesammelte, verarbeitete und übertragene Informationen

Wenn Sie Fotos bei einem Online-Fotodruckdienst bestellen, werden Ihre digitalen Fotos über das Internet an den jeweiligen Dienst gesendet. Der Dateipfad der ausgewählten digitalen Bilder (der u. U. Ihren Benutzernamen enthält) kann an den Dienst gesendet werden, damit dieser die Bilder anzeigen und hochladen kann. Digitale Bilddateien können Daten zum Bild enthalten, die von der Kamera zusammen mit der Datei gespeichert wurden, z. B. das Datum und die Uhrzeit der Aufnahme oder den Ort der Aufnahme, wenn die Kamera über GPS-Funktionen verfügt. Die Dateien können auch persönliche

Informationen (z. B. Beschriftungen) enthalten, die der Datei mithilfe von Verwaltungs-Apps für digitale Bilder und Windows-Explorer zugeordnet wurden. Weitere Informationen finden Sie im Abschnitt „Eigenschaften" weiter unten.

Nachdem Sie über „Abzüge bestellen" einen Online-Fotodruckdienst ausgewählt haben, werden Sie im Fenster „Abzüge bestellen" zur Webseite des Diensts umgeleitet. Informationen, die Sie auf der Webseite des Online-Fotodruckdiensts eingeben, werden an den Dienst übermittelt.

Verwendung von Informationen

Die von der Kamera in digitalen Bilddateien gespeicherten Informationen können beim Herstellen der Abzüge vom Online-Fotodruckdienst verwendet werden, um z. B. die Farbe oder Schärfe des Bilds vor dem Drucken anzupassen. Von Verwaltungs-Apps für digitale Bilder gespeicherte Informationen können vom Online-Fotodruckdienst verwendet werden, um sie als Beschriftungen auf die Vorder- oder Rückseite des Fotos zu drucken. Die Verwendung dieser und anderer von Ihnen für die Dienste bereitgestellter Informationen (z. B. Informationen, die Sie auf den Webseiten der Dienste eingeben) durch Online-Fotodruckdienste unterliegt den Datenschutzpraktiken der Dienste.

Auswahl und Steuerung

Mit „Abzüge bestellen" können Sie Bilder und den Dienst, an den Sie die Bilder zum Drucken senden möchten, auswählen. Bei einigen Bildverwaltungs-Apps ist es möglich, gespeicherte persönliche Informationen vor dem Senden der Bilder zu entfernen. Möglicherweise können Sie auch die Eigenschaften der Datei bearbeiten, um gespeicherte persönliche Informationen zu entfernen.

Seitenanfang

Programmkompatibilitäts-Assistent

Funktionsweise dieses Features

Wenn ein Kompatibilitätsproblem mit einer App festgestellt wird,

die Sie ausführen möchten, versucht der Programmkompatibilitäts-Assistent, Sie bei der Behebung des Problems zu unterstützen.

Gesammelte, verarbeitete und übertragene Informationen

Wenn ein Kompatibilitätsproblem mit einer App festgestellt wird, die Sie auszuführen versuchen, wird ein Bericht generiert, der Informationen wie den Namen und die Version der App, die erforderlichen Kompatibilitätseinstellungen und Ihre bisherigen Aktionen mit der App enthält. Probleme mit inkompatiblen Apps werden Microsoft über die Windows-Fehlerberichterstattung oder das Windows-Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) gemeldet.

Verwendung von Informationen

Fehlerberichte werden dazu verwendet, Antworten für Probleme bereitzustellen, die Sie für Ihre Apps melden. Antworten enthalten (sofern verfügbar) Links zur Webseite des App-Herausgebers, auf der Sie sich über mögliche Lösungen informieren können. Aufgrund von App-Fehlern erstellte Fehlerberichte werden zum Ermitteln der erforderlichen Einstellungen verwendet, wenn unter dieser Windows-Version Kompatibilitätsprobleme mit den ausgeführten Apps auftreten. Mit den über das CEIP gemeldeten Informationen werden App-Kompatibilitätsprobleme identifiziert.

Microsoft verwendet die mit diesem Feature gesammelten Informationen nicht dazu, Sie zu identifizieren, Kontakt mit Ihnen aufzunehmen oder gezielte Werbung zu schalten.

Auswahl und Steuerung

Für die von der Windows-Fehlerberichterstattung gemeldeten Probleme wird nur dann ein Fehlerbericht generiert, wenn Sie die Option zur Onlinesuche nach Lösungen auswählen. Sofern Sie zuvor nicht bereits zugestimmt haben, dass Probleme automatisch gemeldet werden, werden Sie gefragt, ob Sie den Fehlerbericht senden möchten. Weitere Informationen finden Sie im Abschnitt „Windows-Fehlerberichterstattung“.

Einige Probleme werden automatisch über Windows-CEIP gemeldet, sofern Sie dieses Feature aktiviert haben. Weitere Informationen finden Sie im Abschnitt „Windows Programm zur Verbesserung der Benutzerfreundlichkeit".

Seitenanfang

Eigenschaften

Funktionsweise dieses Features

Eigenschaften sind Dateiinformationen, mit deren Hilfe Sie Ihre Dateien schnell finden und organisieren können. Einige Eigenschaften gelten speziell für die Datei (z. B. die Dateigröße), wohingegen andere eine App oder ein Gerät betreffen (z. B. die beim Aufnehmen eines Fotos verwendeten Kameraeinstellungen oder die für das Foto von der Kamera aufgezeichneten Positionsdaten).

Gesammelte, verarbeitete und übertragene Informationen

Die gespeicherten Informationen hängen vom Dateityp und den Apps ab, von denen die Datei verwendet wird. Beispiele für Eigenschaften sind Dateiname, Änderungsdatum, Dateigröße, Autor, Schlüsselwörter und Kommentare. Eigenschaften werden in der Datei gespeichert und mit ihr verschoben, wenn die Datei an einen anderen Speicherort verschoben oder kopiert wird (wenn sie z. B. in eine Dateifreigabe kopiert oder als E-Mail-Anhang versendet wird).

Verwendung von Informationen

Eigenschaften können die Suche nach Dateien und ihre Organisation erleichtern. Sie können auch von Apps zum Ausführen app-spezifischer Aufgaben verwendet werden. Es werden keine Informationen an Microsoft gesendet.

Auswahl und Steuerung

Sie können einige Eigenschaften einer Datei bearbeiten oder entfernen, indem Sie die Datei in Windows-Explorer auswählen und auf „Eigenschaften" klicken. Einige spezifische Eigenschaften

wie Änderungsdatum, Dateigröße und Dateiname sowie einige app-spezifische Eigenschaften können nicht auf diese Weise entfernt werden. App-spezifische Eigenschaften können nur dann bearbeitet oder entfernt werden, wenn die zum Generieren der Datei verwendete App diese Features unterstützt.

Seitenanfang

Näherung

Nahfeldnäherungsdienst

Funktionsweise dieses Features

Wenn Ihr PC mit Nahfeldkommunikations-Hardware (NFC-Hardware) ausgestattet ist, können Sie ihn physisch an ein anderes Gerät mit NFC-Hardware koppeln, um Links, Dateien und andere Informationen zu teilen. Zwei Arten von Näherungsverbindungen sind verfügbar: "Koppeln und Aktion" und "Koppeln und Halten". . Mit "Koppeln und Aktion" können Sie über WiFi, WiFi Direct oder Bluetooth eine kurz- oder langfristige Verbindung zwischen Geräten herstellen. Bei „Tippen und halten“ ist die Verbindung so lange aktiv wie sich die Geräte nebeneinander befinden.

Gesammelte, verarbeitete und übertragene Informationen

Wenn Sie näherungsfähige Geräte koppeln, tauschen sie Informationen aus, um eine Verbindung miteinander herzustellen. Je nach Gerätekonfiguration können diese Daten Bluetooth- und WiFi-Netzwerkadressen sowie den Namen Ihres PC beinhalten.

Nachdem eine Verbindung hergestellt wurde, können abhängig vom verwendeten Näherungsfeature oder von der verwendeten App weitere Informationen zwischen den Geräten ausgetauscht werden. Windows kann über eine Näherungsverbindung Dateien, Links und andere Informationen zwischen Geräten senden. Apps, die das Näherungsfeature verwenden, können alle Informationen senden und empfangen, auf die sie Zugriff haben. Diese Informationen können über Ihre Netzwerk- oder

Internetverbindung oder direkt über eine Drahtlosverbindung von Gerät zu Gerät gesendet werden.

Verwendung von Informationen

Über eine Näherungsverbindung ausgetauschte Netzwerk- und PC-Informationen werden dazu verwendet, eine Netzwerkverbindung herzustellen und die Geräte füreinander zu identifizieren. Daten, die über eine in einer App initiierte Näherungsverbindung übertragen werden, können von der jeweiligen App in beliebiger Weise verwendet werden. Es werden keine Informationen an Microsoft gesendet.

Auswahl und Steuerung

Der Nahfeldnäherungsdienst ist standardmäßig aktiviert. Administratoren können ihn in der Systemsteuerung mit den Optionen unter „Geräte und Drucker" deaktivieren.

Tippen und senden

Funktionsweise dieses Features

Mit dem Windows-Feature „Tippen und senden" können Sie ausgewählte Informationen mühelos mit einem Freund, der neben Ihnen steht, oder mit einem anderen Gerät (z. B. Ihrem Mobiltelefon) teilen. In einem Browser können Sie „Tippen und senden" z. B. über den Bereich „Geräte" starten. Das nächste Gerät, auf das Sie tippen, empfängt einen Link zur momentan angezeigten Webseite. Dies funktioniert auch bei allen Apps, die die Freigabe von Informationen wie Bildern, Text oder Dateien unterstützen.

Gesammelte, verarbeitete und übertragene Informationen

„Tippen und senden" verwendet die von Ihnen freigegebenen Informationen und die im Abschnitt „Nahfeldnäherungsdienst" weiter oben beschriebenen Informationen.

Verwendung von Informationen

Die Informationen werden nur dazu verwendet, die Verbindung zwischen den beiden Geräten herzustellen. Die geteilten Informationen werden nicht von „Tippen und senden"

gespeichert. Es werden keine Informationen an Microsoft gesendet.

Auswahl und Steuerung

Wenn der Nahfeldnäherungsdienst aktiviert ist, ist auch „Tippen und senden" aktiviert. Weitere Informationen finden Sie im Abschnitt „Nahfeldnäherungsdienst".

Seitenanfang

RAS-Verbindungen

Funktionsweise dieses Features

RAS-Verbindungen ermöglichen es Ihnen, über eine VPN (Virtuelles Privates Netzwerk)-Verbindung und den RAS-Dienst (Remote Access Service) eine Verbindung mit privaten Netzwerken herzustellen. RAS ist eine Komponente, die mit Standardprotokollen eine Verbindung zwischen einem Client-PC (normalerweise Ihr PC) und einem Host-PC (bezeichnet als RAS-Server) herstellt. VPN-Technologien ermöglichen es Benutzern, über das Internet eine Verbindung mit einem privaten Netzwerk herzustellen, z. B. einem Firmennetzwerk.

Mit der RAS-Verbindungskomponente Einwählnetzwerk können Sie über ein Modem oder Breitbandtechnologie (z. B. ein Kabelmodem oder DSL) auf das Internet zugreifen. Das Einwählnetzwerk umfasst Wählprogrammkomponenten wie RAS-Client, Verbindungs-Manager und RAS-Telefon sowie Befehlszeilen-Wählprogramme wie rasdial.

Gesammelte, verarbeitete und übertragene Informationen

Die Wählprogrammkomponenten sammeln Informationen wie Benutzername, Kennwort und Domänenname von Ihrem PC. Diese Informationen werden an das System gesendet, mit dem Sie eine Verbindung herstellen möchten. Aus Gründen des Datenschutzes und zum Gewährleisten der Sicherheit Ihres PC werden sicherheitsbezogene Informationen wie Ihr Benutzername und Kennwort verschlüsselt und auf Ihrem PC gespeichert.

Verwendung von Informationen

Wählprogramminformationen werden dazu verwendet, Ihren PC mit dem Internet zu verbinden. Ein RAS-Server kann den Benutzernamen und die IP-Adresse zu Abrechnungszwecken und zur Einhaltung der geltenden Bestimmungen speichern, es werden aber keine Informationen an Microsoft gesendet.

Auswahl und Steuerung

Bei Wählprogrammen, die nicht über die Befehlszeile ausgeführt werden, können Sie **Benutzernamen und Kennwort speichern**aktivieren, um Ihr Kennwort zu speichern. Sie können diese Option jederzeit deaktivieren, um das zuvor gespeicherte Kennwort aus dem Wählprogramm zu löschen. Da diese Option standardmäßig deaktiviert ist, müssen Sie möglicherweise Ihr Kennwort angeben, um eine Verbindung mit dem Internet oder einem Netzwerk herzustellen. Bei Befehlszeilen-Wählprogrammen wie rasdial ist es nicht möglich, das Kennwort zu speichern.

Seitenanfang

RemoteApp- und Desktopverbindungen

Funktionsweise dieses Features

RemoteApp- und Desktopverbindungen ermöglichen Ihnen den Zugriff auf Apps und Desktops auf Remote-PCs, die online für den Remotezugriff verfügbar gemacht wurden.

Gesammelte, verarbeitete und übertragene Informationen

Wenn Sie eine Verbindung aktivieren, werden von der angegebenen Remote-URL Konfigurationsdateien auf Ihren PC heruntergeladen. Diese Konfigurationsdateien verknüpfen Apps und Desktops auf Remote-PCs, sodass Sie sie auf Ihrem PC ausführen können. Ihr PC überprüft automatisch in regelmäßigen Abständen, ob Updates der Konfigurationsdateien verfügbar sind und lädt sie herunter. Diese Apps werden auf Remote-PCs ausgeführt, und die von Ihnen in den Apps eingegebenen

Informationen werden über das Netzwerk an die verbundenen Remote-PCs übertragen.

Verwendung von Informationen

Updates für die Konfigurationsdateien können Einstellungsänderungen enthalten, durch die Sie Zugriff auf neue Apps erhalten. Neue Apps werden allerdings nur ausgeführt, wenn Sie sie zur Ausführung auswählen. Dieses Feature sendet auch Informationen an die Remote-PCs, auf denen die Remote-Apps ausgeführt werden. Die Verwendung der Daten durch die Remote-Apps unterliegt den Datenschutzrichtlinien der App-Anbieter und der Administratoren der Remote-PCs. Es werden keine Informationen an Microsoft gesendet.

Auswahl und Steuerung

Sie können wählen, ob Sie RemoteApp- und Desktopverbindungen verwenden möchten. RemoteApp- und Desktopverbindungen können in der Systemsteuerung unter „RemoteApp- und Desktopverbindungen" hinzugefügt oder entfernt werden. Sie können eine neue Verbindung hinzufügen, indem Sie auf **Neue Verbindung mit RemoteApp- und Desktopverbindungen einrichten**klicken und im Dialogfeld eine Verbindungs-URL eingeben. Sie können die Verbindungs-URL auch mit Ihrer E-Mail-Adresse abrufen. Um eine Verbindung und die zugehörigen Verbindungsdateien zu entfernen, klicken Sie im Dialogfeld mit der Verbindungsbeschreibung auf **Entfernen** . Wenn Sie eine Verbindung trennen, ohne alle geöffneten Apps zu schließen, bleiben diese Apps auf dem Remote-PC geöffnet. RemoteApp- und Desktopverbindungen werden nicht in der Systemsteuerung in der Liste unter „Software" angezeigt.

Seitenanfang

Remotedesktopverbindung

Funktionsweise dieses Features

Die Remotedesktopverbindung ermöglicht es Ihnen, eine Remoteverbindung mit einem Host-PC herzustellen, auf dem

Remotedesktopdienste ausgeführt werden.

Gesammelte, verarbeitete und übertragene Informationen

Die Einstellungen für die Remotedesktopverbindung werden in einem lokalen App-Speicher oder in einer Remotedesktopprotokoll (RDP)-Datei auf Ihrem PC gespeichert. Diese Einstellungen enthalten den Namen Ihrer Domäne und Verbindungskonfigurationseinstellungen, z. B. den Namen des Remote-PC, den Benutzernamen, Anzeigeinformationen, Informationen zum lokalen Gerät, Audioinformationen, Zwischenablage, Verbindungseinstellungen, Namen von Remote-Apps und ein Sitzungssymbol oder eine Miniaturansicht.

Die Anmeldeinformationen für diese Verbindungen, die Anmeldeinformationen für das Remotedesktopgateway sowie eine Liste mit vertrauenswürdigen Remotedesktopgateway-Servernamen werden lokal auf Ihrem PC gespeichert. Diese Liste wird permanent gespeichert, sofern sie nicht von einem Administrator gelöscht wird. Es werden keine Informationen an Microsoft gesendet.

Verwendung von Informationen

Die von der Remotedesktopverbindung gesammelten Informationen ermöglichen es Ihnen, mit Ihren bevorzugten Einstellungen eine Verbindung mit Host-PCs herzustellen, auf denen Remotedesktopdienste ausgeführt werden. Benutzername, Kennwort und Domäneninformationen werden gesammelt, damit Ihre Verbindungseinstellungen gespeichert werden können und Sie per Doppelklick auf eine RDP-Datei oder über einen Favoriten eine Verbindung initiieren können, ohne diese Informationen erneut eingeben zu müssen.

Auswahl und Steuerung

Sie können wählen, ob Sie die Remotedesktopverbindung verwenden möchten. Wenn Sie dieses Feature verwenden, enthalten Ihre RDP-Dateien und Remotedesktopverbindungs-Favoriten Informationen, die zum Herstellen einer Verbindung mit einem Remote-PC benötigt werden. Dazu zählen auch die

Optionen und Einstellungen, die beim automatischen Speichern der Verbindung konfiguriert wurden. Sie können die RDP-Dateien und Favoriten anpassen. Es ist auch möglich, Dateien mit unterschiedlichen Einstellungen für die Verbindung mit demselben PC zu verwenden. Gespeicherte Anmeldeinformationen können in der Systemsteuerung unter „Anmeldeinformationsverwaltung" geändert werden.

Seitenanfang

Anmelden mit einem Microsoft-Konto

Funktionsweise dieses Features

Ein Microsoft-Konto (ehemals Windows Live ID) besteht aus einer E-Mail-Adresse und einem Kennwort. Mit diesen Anmeldeinformationen können Sie sich bei Apps, Webseiten und Diensten von Microsoft und ausgewählten Microsoft-Partnern anmelden. Sie können sich bei einem Microsoft-Konto in Windows oder auf Microsoft-Webseiten anmelden, die eine Anmeldung mit einem Microsoft-Konto voraussetzen.

Sie können sich mit einem Microsoft-Konto bei Windows anmelden oder Ihr lokales Konto oder Domänenkonto mit einem Microsoft-Konto verbinden. In diesem Fall kann Windows automatisch die Einstellungen und Informationen in Windows und Microsoft-Apps synchronisieren, sodass Ihre PCs das gleiche Aussehen und Verhalten besitzen. Wenn Sie zur Anmeldeseite dieser Webseiten wechseln, werden Sie automatisch auch bei Webseiten angemeldet, die Microsoft-Konten für die Anmeldung verwenden.

Gesammelte, verarbeitete und übertragene Informationen

Wenn Sie eine E-Mail-Adresse eingeben, die beim Einrichten des PCs oder in den PC-Einstellungen unter „Benutzer" für ein Microsoft-Konto verwendet wird, sendet Windows die E-Mail-Adresse an Microsoft. Dabei wird festgestellt, ob dieser E-Mail-Adresse bereits ein Microsoft-Konto zugeordnet ist. Wird diese E-Mail-Adresse bereits für ein Microsoft-Konto verwendet, können

Sie sich mit dieser Adresse und dem Kennwort für das Microsoft-Konto bei Windows anmelden. Falls die Sicherheitsinformationen für das Microsoft-Konto nicht bereits ausreichen, werden Sie gegebenenfalls nach weiteren Sicherheitsinformationen gefragt (z. B. der Handynummer). Wir können dann bei Anmeldeproblemen überprüfen, ob das Konto tatsächlich Ihnen gehört. Wenn Sie kein Microsoft-Konto besitzen, können Sie mit einer beliebigen E-Mail-Adresse ein Konto erstellen.

Wenn der PC mit dem Internet verbunden ist, überprüft Windows bei jeder Anmeldung bei Windows mit einem Microsoft-Konto E-Mail-Adresse und Kennwort mit Servern von Microsoft. Bei der Anmeldung bei Windows mit einem Microsoft-Konto oder einem Domänenkonto, das mit dem Microsoft-Konto verbunden ist:

- Bestimmte Einstellungen von Windows werden zwischen den PCs synchronisiert, bei denen Sie sich mit einem Microsoft-Konto anmelden. Weitere Informationen zu den synchronisierten Einstellungen und deren Steuerung finden Sie im Abschnitt „Synchronisieren der Einstellungen".

- Microsoft-Apps, die zur Authentifizierung ein Microsoft-Konto verwenden (wie Mail, Kalender, Fotos, Kontakte, Nachrichten, OneDrive, Microsoft Office und andere Apps), können automatisch mit dem Herunterladen Ihrer Informationen beginnen. Die Mail-App lädt beispielsweise automatisch die an Ihre Outlook.com- oder Hotmail.com-Adresse gesendeten Nachrichten herunter (sofern vorhanden).

- Webbrowser können automatisch die Anmeldung bei Webseiten ausführen, bei denen Sie sich mit Ihrem Microsoft-Konto anmelden. Wenn Sie z. B. "OneDrive.com" besuchen, werden Sie automatisch angemeldet, ohne das Kennwort für Ihr Microsoft-Konto erneut eingeben zu müssen.

Sie werden von Windows um Ihre Zustimmung gebeten, bevor Drittanbieter-Apps Profilinformationen oder andere persönliche Informationen im Zusammenhang mit Ihrem Microsoft-Konto

verwenden dürfen. Wenn Sie sich bei Windows mit einem Domänenkonto anmelden, das mit einem Microsoft-Konto verbunden ist, werden die von Ihnen ausgewählten Einstellungen und Informationen mit dem Domänenkonto synchronisiert. Zudem werden Sie automatisch wie oben beschrieben bei Apps und Webseiten angemeldet. Da Domänenadministratoren auf alle Informationen auf Ihrem PC zugreifen können, besitzen sie auch Zugriff auf alle Einstellungen und Informationen, für die Sie die Synchronisierung mit anderen PCs über Ihr Microsoft-Konto ausgewählt haben. Dazu gehören Einstellungen wie der Name, das Profilbild und der Browserverlauf. Weitere Informationen zu den synchronisierten Einstellungen und deren Steuerung finden Sie im Abschnitt „Synchronisieren der Einstellungen".

Verwendung von Informationen

Wenn Sie ein neues Microsoft-Konto in Windows erstellen, verwenden wir die von Ihnen bereitgestellten Informationen zum Erstellen und Sichern des Kontos. Beispielsweise werden die angegebenen Sicherheitsinformationen (wie Telefonnummer oder alternative E-Mail-Adresse) nur verwendet, falls Sie sich nicht bei Ihrem Konto anmelden können. Wenn Sie mit einem Microsoft-Konto bei Windows angemeldet sind, verwendet Windows Ihre Microsoft-Kontoinformationen, um Sie automatisch bei Apps und Webseiten anzumelden. Weitere Informationen zu den Auswirkungen eines Microsoft-Kontos auf den Datenschutz erhalten Sie in den Datenschutzbestimmungen , die bei der Auswahl von „Für neue E-Mail-Adresse registrieren" angezeigt werden. Details dazu, wie einzelne Microsoft-Apps mit dem Microsoft-Konto zusammenhängende Informationen verwenden, finden Sie in den Datenschutzbestimmungen der Apps. Die Datenschutzbestimmungen für eine Microsoft-App können Sie über den Charm „Einstellungen" oder im Dialogfeld „Info" der App anzeigen.

Auswahl und Steuerung

Wenn Sie sich bei Windows mit einem Microsoft-Konto anmelden, werden einige Einstellungen automatisch synchronisiert. Weitere Informationen dazu, wie Sie die

Synchronisierung der Windows-Einstellungen ändern oder beenden können, finden Sie im Abschnitt „Synchronisieren der Einstellungen“. Weitere Informationen zu den Daten, die von Microsoft-Apps gesammelt werden, die ein Microsoft-Konto für die Authentifizierung verwenden, finden Sie in den entsprechenden Datenschutzbestimmungen. Die Datenschutzbestimmungen für Windows Live-Apps (Mail, Kalender, Fotos, Kontakte, Nachrichten, OneDrive) finden Sie unter go.microsoft.com/fwlink/?LinkId=257483, und die Datenschutzbestimmungen für Microsoft Office unter go.microsoft.com/fwlink/?LinkId=257484. Die Datenschutzbestimmungen für eine App können Sie auch über den Charm "Einstellungen" oder im Dialogfeld "Info" der App anzeigen.

Sie müssen sich nicht mit einem Microsoft-Konto bei Windows anmelden. Sie können ein lokales Konto oder ein Microsoft-Konto verwenden, wenn Sie beim Einrichten des PCs oder in den PC-Einstellungen unter **Benutzer** einen Benutzer hinzufügen Der Wechsel zwischen einem lokalen Konto und einem Microsoft-Konto ist in den PC-Einstellungen unter **Benutzer** jederzeit möglich. Wenn Sie sich mit einem Domänenkonto bei Windows anmelden, können Sie die Verbindung mit Ihrem Microsoft-Konto in den PC-Einstellungen unter **Benutzer** jederzeit herstellen oder trennen.

Beim InPrivate-Browsen in Internet Explorer werden Sie nicht automatisch bei anderen Webseiten angemeldet, die Microsoft-Konten verwenden.

Seitenanfang

Synchronisieren der Einstellungen

Funktionsweise dieses Features

Wenn Sie sich bei Windows mit einem Microsoft-Konto anmelden, werden die Einstellungen und Informationen von Windows mit Microsoft-Servern synchronisiert. Dadurch ist es ganz einfach, mehrere PCs zu personalisieren. Nach der Anmeldung an mindestens einem PC mit einem Microsoft-Konto,

werden von Windows beim ersten Anmelden an einem anderen PC mit demselben Microsoft-Konto die Einstellungen und Informationen heruntergeladen und angewendet, die Sie mit Ihren anderen PCs synchronisieren möchten. Für die Synchronisierung ausgewählte Einstellungen werden auf den Microsoft-Servern und Ihren anderen PCs bei ihrer Verwendung automatisch aktualisiert.

Gesammelte, verarbeitete und übertragene Informationen

Wenn Sie sich mit einem Microsoft-Konto bei Windows anmelden, synchronisiert Windows bestimmte Einstellungen mit Microsoft-Servern. Folgende Einstellungen werden synchronisiert:

- Spracheinstellungen
- Einstellungen für das Center für erleichterte Bedienung
- Personalisierungseinstellungen, z. B. das Profilbild, das Sperrbildschirmbild, der Hintergrund und Mauseinstellungen
- Einstellungen für Windows Store-Apps
- Wörterbücher für die Rechtschreibprüfung und den IME
- Webbrowserverlauf und -favoriten
- Gespeicherte App-, Webseite- und Netzwerkkennwörter

Aus Datenschutzgründen werden alle synchronisierten Einstellungen durch SSL verschlüsselt und gesendet. Einige dieser Einstellungen werden erst mit Ihrem PC synchronisiert, wenn Sie ihn Ihrem Microsoft-Konto als vertrauenswürdigen PC hinzufügen.

Wenn Sie sich bei Windows mit einem Domänenkonto anmelden, das mit einem Microsoft-Konto verbunden ist, werden die ausgewählten Einstellungen und Informationen mit dem Domänenkonto synchronisiert. Kennwörter, die Sie speichern, während Sie mit dem mit einem Microsoft-Konto verbundenen

Domänenkonto bei Windows angemeldet sind, werden nie synchronisiert. Da Domänenadministratoren auf alle Informationen auf Ihrem PC zugreifen können, besitzen sie auch Zugriff auf alle Einstellungen und Informationen einschließlich des Browserverlaufs, für die Sie die Synchronisierung mit anderen PCs über Ihr Microsoft-Konto ausgewählt haben.

Verwendung von Informationen

Windows 8 verwendet diese Einstellungen und Informationen, um den Synchronisierungsdienst bereitzustellen. Microsoft verwendet Ihre synchronisierten Einstellungen und Informationen nicht dazu, Sie zu identifizieren, Kontakt zu Ihnen aufzunehmen oder gezielte Werbung zu schalten.

Auswahl und Steuerung

Wenn Sie sich mit einem Microsoft-Konto bei Windows anmelden, wird „Einstellungen synchronisieren" aktiviert. In den PC-Einstellungen unter **Synchronisieren der Einstellungen** können Sie das Synchronisieren der Einstellungen festlegen und steuern, welche Elemente synchronisiert werden sollen. Wenn Sie sich mit einem Domänenkonto bei Windows anmelden und dann die Verbindung mit einem Microsoft-Konto herstellen möchten, werden Sie von Windows gefragt, welche Einstellungen synchronisiert werden sollen. Anschließend wird die Verbindung mit dem Microsoft-Konto hergestellt.

Seitenanfang

Teredo-Technologie

Funktionsweise dieses Features

Teredo-Technologie (Teredo) ermöglicht PCs und Netzwerken die Kommunikation über mehrere Netzwerkprotokolle.

Gesammelte, verarbeitete und übertragene Informationen

Bei jedem Start des PC versucht Teredo, einen öffentlichen IPv6-Dienst (Internetprotokoll, Version 6) im Internet zu finden. Diese Suche erfolgt automatisch, wenn Ihr PC mit einem öffentlichen

oder privaten Netzwerk verbunden ist. Bei verwalteten Netzwerken wie Unternehmensdomänen findet sie nicht statt. Wenn Sie eine App verwenden, die Teredo für IPv6-Konnektivität erfordert, oder Ihre Firewall so konfigurieren, dass IPv6-Konnektivität immer aktiviert ist, stellt Teredo regelmäßig über das Internet eine Verbindung mit dem Microsoft Teredo-Dienst her. Die einzigen Informationen, die an Microsoft gesendet werden, sind standardmäßige PC-Informationen und der Name des angeforderten Diensts (z. B. „teredo.ipv6.microsoft.com").

Verwendung von Informationen

Mit den Informationen, die Teredo von Ihrem PC sendet, wird überprüft, ob Ihr PC mit dem Internet verbunden ist und einen öffentlichen IPv6-Dienst finden kann. Nachdem der Dienst gefunden wurde, werden Informationen gesendet, um eine Verbindung mit dem IPv6-Dienst aufrechtzuerhalten.

Auswahl und Steuerung

Mit dem netsh-Befehlszeilentool können Sie die Abfrage ändern, die der Dienst über das Internet sendet, um stattdessen nicht von Microsoft stammende Server zu verwenden. Sie können den Dienst auch deaktivieren. Ausführliche Anweisungen finden Sie im Abschnitt zu Internetprotokoll, Version 6, Teredo und verwandten Technologien des technischen Whitepapers.

Seitenanfang

Trusted Platform Module (TPM)-Dienste

Funktionsweise dieses Features

Das Trusted Platform Module (TPM) ist eine auf manchen PCs verfügbare integrierte Sicherheitshardware, die es dem PC (sofern sie vorhanden und bereitgestellt ist) ermöglicht, erweiterte Sicherheitsfeatures zu nutzen. Zu den Windows-Features, die das TPM verwenden, zählen BitLocker-Laufwerkverschlüsselung, virtuelle Smartcard, sicheres Starten, Windows Defender und TPM-basierter Zertifikatspeicher.

Gesammelte, verarbeitete und übertragene Informationen

Standardmäßig übernimmt Windows den Besitz am TPM und speichert die vollständigen TPM-Besitzerautorisierungsinformationen, sodass diese nur für die Windows-Administratoren verfügbar sind. Zum Ausführen typischer administrativer Aktionen und standardmäßiger Benutzeraktionen werden eingeschränkte Autorisierungswerte von Windows erstellt und verwaltet.

Mithilfe der TPM-Verwaltungskonsole können Sie das TPM interaktiv bereitstellen und anschließend den TPM-Besitzerautorisierungswert auf externen Medien speichern, z. B. einem USB-Speicherstick. Eine gespeicherte Datei enthält die TPM-Besitzerautorisierungsinformationen für das TPM. Außerdem enthält die Datei den PC-Namen, die Betriebssystemversion, den Benutzer, von dem die Datei erstellt wurde, und das Erstellungsdatum, damit Sie die Datei leichter erkennen können.

In einer Domänenumgebung kann das vollständige TPM-Besitzerkennwort vom Domänenadministrator so konfiguriert werden, dass es bei der Bereitstellung des TPM in Active Directory unter einem TPM-Objekt gespeichert wird.

Jedes TPM verfügt über einen eindeutigen kryptografischen Endorsement Key, mit dem es seine Authentizität nachweist. Der Endorsement Key kann vom Hersteller des PC erstellt und im TPM gespeichert werden. Bei älteren PCs muss Windows die Erstellung des Endorsement Key möglicherweise im TPM auslösen. Der private Teil des Endorsement Key wird niemals außerhalb des TPM verfügbar gemacht und kann nach seiner Erstellung in der Regel nicht mehr zurückgesetzt werden. Ein Endorsement Key-Zertifikat wird im TPM der meisten Computer unter Windows 8 gespeichert. Das Endorsement Key-Zertifikat gibt an, dass der Endorsement Key in einem Hardware-TPM vorhanden ist. Mit dem Zertifikat können Remoteüberprüfungen feststellen, ob das TPM den TPM-Spezifikationen entspricht. Das Endorsement Key-Zertifikat ist normalerweise vom TPM- oder Plattformhersteller signiert.

Verwendung von Informationen

Nach der Initialisierung des TPM können Apps das TPM

verwenden, um zusätzliche eindeutige kryptografische Schlüssel zu erstellen und zu schützen. Die BitLocker-Laufwerkverschlüsselung verwendet das TPM z. B., um den zum Verschlüsseln des Laufwerks verwendeten Schlüssel zu schützen.

Wenn Sie das TPM-Besitzerkennwort in einer Datei speichern, können Sie mithilfe der zusätzlichen PC- und Benutzerinformationen, die in dieser Datei gespeichert werden, die passende Kombination von PC und TPM identifizieren. Der TPM-Endorsement Key wird während der TPM-Initialisierung von Windows verwendet, um Ihren TPM-Besitzerautorisierungswert zu verschlüsseln, bevor er an das TPM gesendet wird. Windows überträgt kryptografische Schlüssel nicht außerhalb Ihres PC. Windows stellt für Drittanbieter-Apps wie Antischadsoftware eine Schnittstelle bereit, über die der Endorsement Key für bestimmte TPM-Szenarien verwendet werden kann, z. B. für einen kontrollierten Start mit Nachweis. Antischadsoftware kann mithilfe des Endorsement Key und Endorsement Key-Zertifikats überprüfen, ob das TPM eines bestimmten Herstellers Startmessungen bietet. Standardmäßig können nur Administratoren oder Apps mit Administratorrechten den TPM-Endorsement Key verwenden.

Auswahl und Steuerung

Benutzer oder Administratoren aktivieren die Verwendung des TPM, indem sie ein Windows-Feature aktivieren oder eine App ausführen, das bzw. die das TPM verwendet.

Sie können das TPM bei Bedarf löschen und auf die Herstellerstandards zurücksetzen. Wenn Sie das TPM löschen werden die Besitzerinformationen und mit Ausnahme des Endorsement Key alle TPM-basierten Schlüssel oder kryptografischen Informationen gelöscht, die bei der Verwendung des TPM von Apps erstellt wurden.

Seitenanfang

Aktualisierung von Stammzertifikaten

Funktionsweise dieses Features

Zertifikate dienen in erster Linie zum Bestätigen der Identität einer Person oder eines Geräts, Authentifizieren eines Diensts oder Verschlüsseln von Dateien. Vertrauenswürdige Stammzertifizierungsstellen sind die Organisationen, die Zertifikate ausstellen. Die Aktualisierung von Stammzertifikaten stellt eine Verbindung mit dem Windows Update-Onlinedienst her, um zu überprüfen, ob Microsoft der Liste vertrauenswürdiger Zertifizierungsstellen eine Zertifizierungsstelle hinzugefügt hat. Diese Überprüfung erfolgt aber nur, wenn ein Zertifikat von einer nicht direkt vertrauenswürdigen Zertifizierungsstelle (ein Zertifikat, das nicht in einer Liste vertrauenswürdiger Zertifikate auf Ihrem PC gespeichert ist) an eine App übergeben wird. Wenn die Zertifizierungsstelle der Microsoft-Liste von vertrauenswürdigen Zertifizierungsstellen hinzugefügt wurde, wird das Zertifikat automatisch der Liste vertrauenswürdiger Zertifikate auf Ihrem PC hinzugefügt.

Gesammelte, verarbeitete und übertragene Informationen

Die Aktualisierung von Stammzertifikaten fordert vom Windows Update-Onlinedienst die aktuelle Liste von Stammzertifizierungsstellen im Microsoft-Programm für Stammzertifikate an. Wenn das nicht vertrauenswürdige Zertifikat in der Liste enthalten ist, ruft die Aktualisierung von Stammzertifikaten das Zertifikat von Windows Update ab und speichert es im Speicher vertrauenswürdiger Zertifikate auf Ihrem PC. Die übertragenen Informationen beinhalten die Namen und kryptografischen Hashes von Stammzertifikaten.

Weitere Informationen zu Windows Update und dem Schutz Ihrer persönlichen Informationen finden Sie in den Datenschutzbestimmungen zu Update Servicesauf den Schlüssel zugreifen oder ihn löschen.

Verwendung von Informationen

Die Informationen werden von Microsoft dazu verwendet, die Liste vertrauenswürdiger Zertifikat auf Ihrem PC zu aktualisieren. Microsoft verwendet die Informationen nicht dazu, Sie zu

identifizieren, Kontakt mit Ihnen aufzunehmen oder gezielte Werbung zu schalten.

Auswahl und Steuerung

Die Aktualisierung von Stammzertifikaten ist standardmäßig aktiviert. Administratoren können die Gruppenrichtlinie konfigurieren, um die Aktualisierung von Stammzertifikaten auf einem PC zu deaktivieren.

Seitenanfang

Update Services

Funktionsweise dieses Features

Zu den Update Services für Windows zählen Windows Update und Microsoft Update:

- **Windows Update** ist ein Dienst, der Ihnen Softwareupdates für die Windows-Software und andere unterstützende Software (z. B. von Geräteherstellern zur Verfügung gestellte Treiber) bereitstellt.
- **Microsoft Update** ist ein Dienst, der Ihnen Softwareupdates für die Windows-Software und andere Microsoft-Software (z. B. Microsoft Office) bereitstellt.

Gesammelte, verarbeitete und übertragene Informationen

Wenn Sie den automatischen Download wichtiger Softwareupdates für Ihren PC aktivieren, kann das Windows-Tool zum Entfernen bösartiger Software (MSRT) in diesen Updates enthalten sein. MSRT überprüft, ob auf PCs Infektionen durch bestimmte, verbreitete Schadsoftware vorliegen, und unterstützt Sie beim Entfernen der gefundenen Infektionen. Bei ihrer Ausführung entfernt die Software die auf der Microsoft Support-Webseite aufgelistete Schadsoftware . Während der Überprüfung auf Schadsoftware wird ein Bericht mit spezifischen Informationen zu erkannter Schadsoftware, Fehlern und anderen Informationen zu Ihrem PC an Microsoft gesendet. Weitere Informationen finden Sie in den

Datenschutzbestimmungen für das Windows-Tool zum Entfernen von Schadsoftware auf den Schlüssel zugreifen oder ihn löschen.

Informationen zu weiteren von Update Services gesammelten Informationen finden Sie in den Datenschutzbestimmungen zu Update Servicesauf den Schlüssel zugreifen oder ihn löschen.

Verwendung von Informationen

Die MSRT-Informationen werden dazu verwendet, unsere Antischadsoftware sowie andere Sicherheitsprodukte und -dienste zu verbessern. Die Informationen in den MSRT-Berichten werden nicht dazu verwendet, Sie zu identifizieren oder Kontakt mit Ihnen aufzunehmen.

Informationen dazu, wie andere Informationen von Update Services verwendet werden, finden Sie in den Datenschutzbestimmungen zu Update Servicesauf den Schlüssel zugreifen oder ihn löschen.

Auswahl und Steuerung

Wenn Sie während der Installation von Windows die Option "Express-Einstellungen" auswählen, werden Update Services aktiviert, und Windows Update wird zum automatischen Installieren von Updates eingerichtet. Wenn Sie sich für das Anpassen der Einstellungen entscheiden, können Sie die Verwendung von Update Services in **Windows Update** unter **PC schützen und aktualisieren**steuern. Nach der Installation von Windows können Sie die Einstellungen für Update Services in der Systemsteuerung ändern. Weitere Informationen finden Sie in den Datenschutzbestimmungen zu Update Services.

Wenn Sie die Suche nach wichtigen Updates und deren Installation aktiviert haben und MSRT zusammen mit den Updates für Ihren PC erhalten, können Sie die Berichterstattungsfunktion der Software anhand dieser Anweisungen auf der Microsoft Support-Webseite deaktivieren.

Seitenanfang

Windows-Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP)

Funktionsweise dieses Features

Das Windows-Programm zur Verbesserung der Benutzerfreundlichkeit kann Informationen dazu sammeln, wie Sie Ihre Apps, PCs, verbundenen Geräte und Windows verwenden. Vom Programm können darüber hinaus Informationen zu möglichen Problemen mit der Leistung und der Zuverlässigkeit erfasst werden. Wenn Sie sich für die Teilnahme am Windows-Programm zur Verbesserung der Benutzerfreundlichkeit entscheiden, werden diese Daten von Windows an Microsoft gesendet. Außerdem wird regelmäßig eine Datei heruntergeladen, mit der weitere relevante Informationen zur Verwendung von Windows und Apps gesammelt werden. Die CEIP-Berichte werden an Microsoft gesendet und dort verwendet, um die von unseren Kunden am meisten verwendeten Features zu verbessern und Lösungen für häufige Probleme zu entwickeln.

Gesammelte, verarbeitete und übertragene Informationen

CEIP-Berichte können z. B. die folgenden Informationen enthalten:

- Konfigurationsinformationen. Hierzu zählen Informationen wie die Anzahl von Prozessoren im PC, die Anzahl verwendeter Netzwerkverbindungen, die Bildschirmauflösungen für Anzeigegeräte und die ausgeführte Windows-Version.

- Informationen zur Leistung und Zuverlässigkeit. Hierzu zählen z. B. die Geschwindigkeit, mit der eine App reagiert, wenn Sie auf eine Schaltfläche klicken, die Anzahl von Problemen, die bei Ihnen mit einer App oder einem Gerät aufgetreten sind, und die Geschwindigkeit, mit der Informationen über eine Netzwerkverbindung gesendet oder empfangen werden.

- App-Verwendung. Hierbei handelt es sich um Informationen zu den Features, die Sie am häufigsten verwenden, z. B. wie oft Sie Apps öffnen, wie oft Sie

Windows-Hilfe und Support verwenden und wie viele Ordner Sie normalerweise auf Ihrem Desktop erstellen.

CEIP-Berichte enthalten auch Informationen über Ereignisse (Ereignisprotokolldaten), die bis zu sieben Tage vor der Teilnahme am CEIP auf Ihrem PC aufgetreten sind. Da die meisten Benutzer sich innerhalb von einigen Tagen nach der Einrichtung vonWindows für die Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) entscheiden, verwendet Microsoft diese Informationen zur Analyse und Verbesserung der Windows-Setupumgebung.

Diese Informationen werden an Microsoft gesendet, wenn Sie eine Verbindung mit dem Internet herstellen. CEIP-Berichte enthalten nicht absichtlich Kontaktinformationen wie Name, Adresse oder Telefonnummer. Einige Berichte können aber unbeabsichtigt individuelle IDs enthalten, z. B. die Seriennummer eines an Ihren PC angeschlossenen Geräts. Mithilfe von Filtern versucht Microsoft, die möglicherweise enthaltenen individuellen IDs aus den CEIP-Berichten zu entfernen.

Das CEIP generiert eine als GUID (Globally Unique Identifier) bezeichnete Zufallsnummer, die zusammen mit jedem CEIP-Bericht an Microsoft gesendet wird. Anhand der GUID kann Microsoft erkennen, welche Daten im Laufe der Zeit von einem bestimmten Computer übermittelt werden. Von den vorinstallierten Microsoft-Apps, die mit Windows lizenziert wurden, werden möglicherweise eigene eindeutige Bezeichner für die Verwendung mit dem CEIP erstellt, die auf Informationen aus dem Microsoft-Konto basieren können.

Vom Programm zur Verbesserung der Benutzerfreundlichkeit wird außerdem regelmäßig eine Datei heruntergeladen, mit der weitere relevante Informationen zur Verwendung von Windows und Apps gesammelt werden. Mithilfe dieser Datei können von Windows zusätzliche Informationen gesammelt werden, die Microsoft dabei unterstützen, Lösungen für allgemeine Probleme zu entwickeln und die Verwendungsmuster von Windows und Apps nachzuvollziehen.

Verwendung von Informationen

Microsoft verwendet CEIP-Informationen , um seine Produkte und Dienste sowie Drittanbietersoftware und -hardware, die für die Verwendung mit diesen Produkten und Diensten entwickelt wurde, zu verbessern. Möglicherweise werden die Informationen des Programms zur Verbesserung der Benutzerfreundlichkeit auch an Microsoft-Partner weitergegeben, damit diese ihre Produkte und Dienste verbessern können. Die freigegebenen Informationen liegen in aggregierter Form vor und können nicht dazu verwendet werden, Sie zu identifizieren, Kontakt mit Ihnen aufzunehmen oder gezielte Werbung zu schalten.

Mithilfe der GUID können wir feststellen, wie breitgefächert das Feedback ist, das wir erhalten, und wie es priorisiert werden sollte. Mit der GUID kann Microsoft beispielsweise unterscheiden, ob ein Problem hundert Mal bei einem Kunden oder ob das gleiche Problem bei hundert Kunden jeweils einmal aufgetreten ist. Microsoft verwendet die über das Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) gesammelten Informationen nicht dazu, Sie zu identifizieren oder mit Ihnen in Kontakt zu treten.

Auswahl und Steuerung

Wenn Sie beim Einrichten von Windows die Expresseinstellungen auswählen, wird das Windows-Programm zur Verbesserung der Benutzerfreundlichkeit aktiviert: Von Windows und den Microsoft-Apps, die mit Windows lizenziert wurden, können CEIP-Berichte für alle Benutzer des PCs gesendet werden. Wenn Sie sich für das Anpassen der Einstellungen entscheiden, können Sie das Programm zur Verbesserung der Benutzerfreundlichkeit steuern, indem Sie unter **Ich möchte Informationen an Microsoft übermitteln, um die Optimierung von Windows und Apps zu ermöglichen** unter **Senden Sie uns (Microsoft) Infos, damit wir Windows und Apps verbessern können**auswählen. Administratoren können diese Einstellung nach der Einrichtung von Windows in der Systemsteuerung im Wartungscenter ändern.

Weitere Informationen finden Sie online in den häufig gestellten

Fragen zum Programm zur Verbesserung der Benutzerfreundlichkeit .

Seitenanfang

Windows Defender

Windows Defender sucht nach Schadsoftware und anderer potenziell unerwünschter Software auf Ihrem PC. Er enthält die Features Microsoft Active Protection Service und Verlauf.

Microsoft Active Protection Service

Funktionsweise dieses Features

Die Microsoft Active Protection Service (MAPS)-Antischadsoftware-Community ist eine weltweite Community auf freiwilliger Basis, der Benutzer von Windows Defender angehören. Über MAPS können Benutzer Informationen zu Schadsoftware und möglicherweise unerwünschter Software an Microsoft senden. MAPS trägt durch automatisches Herunterladen von neuen Signaturen für neu erkannte Schadsoftware zum Schutz Ihres PCs bei.

Gesammelte, verarbeitete und übertragene Informationen

MAPS-Berichte enthalten Informationen zu Dateien potenzieller Schadsoftware, z. B. Dateinamen, kryptografischer Hash, Softwarehersteller, Größe und Datumsstempel. Außerdem kann MAPS vollständige URLs sammeln, um den Ursprung der Datei zu bestimmen. Diese URLs können mitunter persönliche Informationen wie Suchbegriffe oder in Formularen eingegebene Daten enthalten. Die Berichte können außerdem die Aktionen enthalten, die Sie vorgenommen haben, als Sie von Windows Defender über erkannte Software benachrichtigt wurden. MAPS nimmt diese Informationen auf, damit Microsoft beurteilen kann, wie effektiv Windows Defender Schadsoftware und potenziell unerwünschte Software erkennen und entfernen kann. Außerdem soll mit diesen Informationen neue Schadsoftware identifiziert werden.

In folgenden Fällen werden automatisch Berichte an Microsoft

gesendet:

- Windows Defender erkennt Software, deren Risiken noch nicht analysiert wurden.
- Windows Defender erkennt Änderungen am PC, die von Software vorgenommen wurden, deren Risiken noch nicht analysiert wurden.
- Wenn Schadsoftware erkannt wird, wendet Windows Defender (im Rahmen der automatischen Wiederherstellung) Aktionen an.
- Windows Defender führt eine geplante Überprüfung aus, bei der auf erkannte Software automatisch Aktionen gemäß Ihren Einstellungen angewendet werden.

Für die Teilnahme an MAPS sind eine einfache und eine erweiterte Mitgliedschaft verfügbar. Wenn Sie MAPS beim Einrichten von Windows aktivieren, treten Sie mit einer einfachen Mitgliedschaft bei. Berichte einfacher Mitglieder enthalten die in diesem Abschnitt beschriebenen Informationen. Berichte erweiterter Mitglieder sind umfangreicher und können mitunter persönliche Informationen enthalten, z. B. Dateipfade und Teilspeicherabbilder. Diese Berichte und die Berichte anderer Windows Defender-Benutzer, die an MAPS teilnehmen, helfen unseren Entwicklern, neue Bedrohungen schneller zu erkennen. Dann werden für Apps, die den Analysekriterien entsprechen, Schadsoftwaredefinitionen erstellt, und diese aktualisierten Definitionen werden anschließend über Windows Update allen Benutzern zur Verfügung gestellt.

Bei der einfachen oder erweiterten Teilnahme an MAPS:

- Microsoft fordert ggf. einen Beispielübermittlungsbericht an. Dieser Bericht enthält spezifische Dateien von Ihrem PC, von denen Microsoft vermutet, dass es sich um potenziell unerwünschte Software handelt. Der Beispielbericht wird zur weiteren Analyse verwendet. Sie werden jedes Mal gefragt, ob Sie den Beispielübermittlungsbericht an Microsoft. senden möchten.

- Falls von Windows Update über längere Zeit keine aktualisierten Signaturen für Windows Defender abgerufen werden konnten, versucht Windows Defender, Signaturen mithilfe von MAPS aus einem anderen Downloadspeicherort herunterzuladen.

Aus Datenschutzgründen werden alle an MAPS gesendeten Informationen durch SSL verschlüsselt.

Verwendung von Informationen

An MAPS gesendete Berichte werden verwendet, um Microsoft-Software und -Dienste zu verbessern. Die Berichte können auch für statistische Zwecke oder andere Tests bzw. Analysen sowie zum Generieren von Definitionen verwendet werden. Persönliche Informationen werden nicht absichtlich von MAPS gesammelt. Falls MAPS unabsichtlich persönliche Informationen erfasst, werden sie von Microsoft nicht dazu verwendet, Sie zu identifizieren, Kontakt zu Ihnen aufzunehmen oder gezielte Werbung zu schalten.

Auswahl und Steuerung

Wenn Sie beim Einrichten von Windows die Expresseinstellungen auswählen, aktivieren Sie damit MAPS. Wenn Sie „Einstellungen anpassen" auswählen, können Sie MAPS mit der Option **Ich möchte Microsoft Active Protection Service (MAPS) beitreten, damit mein PC besser vor schädlichen Apps und Schadsoftware geschützt wird** unter **Senden Sie uns (Microsoft) Infos, damit wir Windows und Apps verbessern können**steuern und Microsoft unterstützen. Sie können Ihre Mitgliedschaft bei MAPS oder die MAPS-Einstellungen (einschließlich Deaktivieren von MAPS) nach dem Einrichten von Windows über das Menü „Extras" in Windows Defender ändern.

Verlaufsfeature

Funktionsweise dieses Features

Das Verlaufsfeature stellt eine Liste aller von Windows Defender auf Ihrem PC erkannten Apps und der beim Fund ausgeführten

Aktionen bereit.

Zudem können Sie eine Liste der Apps anzeigen, die bei ihrer Ausführung auf Ihrem PC nicht von Windows Defender überwacht werden (diese Apps werden als zugelassene Elemente bezeichnet). Sie können auch Apps anzeigen, deren Ausführung Windows Defender verhindert, bis Sie sie entfernen oder ihre Ausführung erneut zulassen (diese Apps werden als Elemente unter Quarantäne bezeichnet).

Gesammelte, verarbeitete und übertragene Informationen

Die Liste mit der von Windows Defender erkannten Software, den von Ihnen und anderen Benutzern ausgeführten Aktionen und den automatisch von Windows Defender ausgeführten Aktionen wird auf Ihrem PC gespeichert. Alle Benutzer können den Verlauf in Windows Defender anzeigen, um Schadsoftware und andere potenziell unerwünschte Software einzusehen, die versucht hat, sich selbst auf dem PC zu installieren oder auszuführen, oder deren Ausführung von einem anderen Benutzer zugelassen wurde. Wenn Sie z. B. von einer neuen Schadsoftware hören, können Sie im Verlauf überprüfen, ob Windows Defender eine entsprechende Infektion Ihres PC verhindert hat. Es werden keine Informationen an Microsoft gesendet.

Auswahl und Steuerung

Verlaufslisten können von Administratoren gelöscht werden.

Seitenanfang

Windows-Fehlerberichterstattung

Funktionsweise dieses Features

Mit der Windows-Fehlerberichterstattung können Microsoft und Microsoft-Partner Probleme in der von Ihnen verwendeten Software diagnostizieren und Lösungen bereitstellen. Es können nicht für alle Probleme Lösungen bereitgestellt werden. Wenn aber Lösungen verfügbar sind, werden sie als Schritte zum Beheben eines von Ihnen gemeldeten Problems oder als

installierbare Updates angeboten. Um Problemen vorzubeugen und die Zuverlässigkeit unserer Software zu verbessern, werden einige Lösungen auch in Service Packs und zukünftige Versionen der Software integriert.

Gesammelte, verarbeitete und übertragene Informationen

Viele Softwareprodukte sind zur Verwendung der Windows - Fehlerberichterstattung konzipiert. Wenn ein Problem in einem dieser Produkte auftritt, werden Sie möglicherweise gefragt, ob Sie das Problem melden möchten.

Die Windows-Fehlerberichterstattung sammelt Informationen, die für die Diagnose und Behandlung eines aufgetretenen Problems hilfreich sind, beispielsweise wo das Problem in der Software oder Hardware aufgetreten ist, der Typ oder Schweregrad des Problems, Dateien, die bei der Problembeschreibung nützlich sind, grundlegende Informationen zur Software und Hardware oder mögliche Problem in Bezug auf die Leistung oder Kompatibilität der Software. Wenn Sie mit Windows virtuelle Computer hosten, enthalten die an Microsoft gesendeten Berichte möglicherweise Informationen zu virtuellen Computern.

Von der Windows-Fehlerberichterstattung werden Informationen zu Apps, Treibern und Geräten gesammelt, um Microsoft dabei zu unterstützen, die App-und Gerätekompatibilität zu verstehen und zu verbessern. Zu den Informationen über eine App zählt u. a. der Name der ausführbaren Dateien einer App. Zu den Informationen über Geräte und Treiber gehören z. B. die Namen der am PC angeschlossenen Geräte und die zu den jeweiligen Gerätetreibern gehörigen ausführbaren Dateien. Möglicherweise werden Informationen zum Unternehmen, das eine App oder einen Treiber veröffentlicht hat, erfasst.

Wenn Sie beim Einrichten von Windows die automatische Berichterstattung aktivieren, sendet der Berichterstattungsdienst automatisch grundlegende Informationen zu den Stellen, an denen Probleme auftreten. Einige Fehlerberichte können unbeabsichtigt persönliche Informationen enthalten. Ein Bericht,

der eine Momentaufnahme des PC-Arbeitsspeichers umfasst, kann beispielsweise auch Ihren Namen, einen Teil des Dokuments, an dem Sie gearbeitet haben, oder vor kurzem an eine Webseite übermittelte Daten enthalten. Wenn ein Bericht möglicherweise diese Art von Informationen enthält, werden Sie von Windows gefragt, ob Sie diese Informationen senden möchten. Dies ist auch dann der Fall, wenn Sie die automatische Berichterstattung aktiviert haben. Berichte, die Dateien und Daten enthalten, werden ggf. auf dem PC gespeichert, bis sie gesendet oder gelöscht wurden.

Nachdem Sie ein Problem gemeldet haben, werden Sie möglicherweise aufgefordert, weitere Informationen zu dem aufgetretenen Fehler bereitzustellen. Wenn Sie in diesem Rahmen eine Telefonnummer oder E-Mail-Adresse angeben, kann der Fehlerbericht Ihnen persönlich zugeordnet werden. Microsoft nimmt möglicherweise Kontakt mit Ihnen auf, um zusätzliche Informationen einzuholen, die zum Lösen des gemeldeten Problems erforderlich sind.

Die Windows-Fehlerberichterstattung generiert eine GUID (Globally Unique Identifier), die mit dem Fehlerbericht an Microsoft gesendet wird. Die GUID ist eine zufällig generierte Zahl. Anhand der GUID kann Microsoft erkennen, welche Daten im Laufe der Zeit von einem bestimmten Computer übermittelt werden. Die GUID enthält keine persönlichen Informationen.

Aus Datenschutzgründen werden die gesendeten Informationen durch SSL verschlüsselt.

Verwendung von Informationen

Microsoft verwendet Informationen zu von Windows-Benutzern berichteten Fehlern und Problemen, um Microsoft-Produkte und -Dienste sowie Drittanbieterhardware und -software, die für die Verwendung mit diesen Produkten und Diensten entwickelt wurde, zu verbessern. Anhand der GUID kann Microsoft feststellen, wie weit verbreitet das empfangene Feedback ist und welche Priorität dem Feedback eingeräumt werden soll. Mit der GUID kann Microsoft beispielsweise unterscheiden, ob ein Problem hundert Mal bei einem Kunden oder ob das gleiche

Problem bei hundert Kunden jeweils einmal aufgetreten ist.

Mitarbeiter, Auftragnehmer, Partner und Lieferanten von Microsoft erhalten möglicherweise Zugriff auf relevante Teile der gesammelten Informationen. Sie können diese Informationen jedoch nur zum Reparieren oder Verbessern der Produkte und Dienste von Microsoft oder der für die Verwendung mit Microsoft entwickelten Software und Hardware von Drittanbietern verwenden. Wenn ein Fehlerbericht persönliche Informationen enthält, verwendet Microsoft diese Informationen nicht, um Sie zu identifizieren, Kontakt zu Ihnen aufzunehmen oder gezielte Werbung zu schalten. Wenn Sie jedoch Kontaktinformationen wie oben beschrieben angeben, werden wir uns ggf. an Sie wenden.

Auswahl und Steuerung

Wenn Sie beim Einrichten von Windows die Expresseinstellungen auswählen, sendet die Windows-Fehlerberichterstattung grundlegende Berichte und sucht automatisch online nach Lösungen für Probleme. Wenn Sie die Einstellungen anpassen möchten, können Sie die Windows-Fehlerberichterstattung steuern, indem Sie unter **Online nach Lösungen für Probleme suchen** unter **Problemlösungen mit der Windows-Fehlerberichterstattung suchen**auswählen. Sie können diese Einstellung nach der Einrichtung von Windows in der Systemsteuerung im Wartungscenter ändern.

Weitere Informationen finden Sie online in den Datenschutzbestimmungen für den Microsoft-Fehlerberichterstattungsdienst auf den Schlüssel zugreifen oder ihn löschen.

Seitenanfang

Windows-Dateizuordnung

Funktionsweise dieses Features

Mithilfe der Windows-Dateizuordnung können Benutzer Dateitypen bestimmten Apps zuordnen. Wenn Sie versuchen, einen Dateityp zu öffnen, für den keine App zugeordnet ist,

werden Sie von Windows gefragt, ob Sie mithilfe der Windows-Dateizuordnung eine App für die Datei suchen möchten. Dies schließt auch die Suche im Windows Store nach einer kompatiblen App ein. Als Ergebnis werden Apps angezeigt, die der Dateinamenerweiterung üblicherweise zugeordnet sind.

Gesammelte, verarbeitete und übertragene Informationen

Wenn Sie sich zur Verwendung der Windows-Dateizuordnung entscheiden, werden die Dateinamenerweiterung (z. B. DOCX oder PDF) und die Anzeigesprache des PCs an Microsoft gesendet. Der Rest des Dateinamens wird nicht an Microsoft gesendet. Wenn eine Dateinamenerweiterung einer bestimmten App zugeordnet wird, wird ein eindeutiger Bezeichner für die App gesendet, um die Standard-App für jeden Dateityp zu identifizieren.

Verwendung von Informationen

Nach dem Senden einer Dateinamenerweiterung gibt der Dienst eine Liste aller Microsoftbekannten Apps zurück, mit denen sich Dateien mit dieser Erweiterung öffnen lassen. Sofern Sie sich nicht zum Herunterladen und Installieren einer App entscheiden, werden keine Dateitypzuordnungen verändert.

Auswahl und Steuerung

Wenn Sie einen Dateityp ohne zugeordnete App öffnen, können Sie auswählen, ob die Windows-Dateizuordnung verwendet werden soll. Solange Sie den Dienst nicht verwenden, werden keine Dateizuordnungsinformationen an Microsoft gesendet.

Seitenanfang

Windows-Hilfe

Windows-Onlinehilfe und -support

Funktionsweise dieses Features

Wenn Windows-Onlinehilfe und -support aktiviert ist, können Sie bei aktiver Internetverbindung online nach Hilfeinhalten suchen und finden so die neuesten verfügbaren Inhalte.

Gesammelte, verarbeitete und übertragene Informationen

Wenn Sie Windows-Onlinehilfe und -support verwenden, werden Ihre Suchabfragen sowie Ihre Anforderungen zum Aufrufen von Hilfeinhalt durch Klicken auf einen Link an Microsoft gesendet. Windows sendet für die Suche nach weiteren relevanten Hilfeinhalten einige Informationen zur Konfiguration Ihres PCs. Windows-Onlinehilfe und -support verwendet außerdem übliche Webtechnologien wie Cookies.

Verwendung von Informationen

Microsoft verwendet diese Informationen, um Hilfethemen zu Ihren Suchabfragen anzuzeigen, die bestmöglichen Ergebnisse zurückzugeben, neue Inhalte zu entwickeln und vorhandene Inhalte zu verbessern. Die Informationen zur Konfiguration Ihres PCs werden dazu verwendet, Hilfeinhalte für diese Konfiguration anzuzeigen. Mithilfe von Cookies und anderen Webtechnologien wird die Navigation in Hilfeinhalten erleichtert. Zudem tragen diese dazu bei, dass Microsoft besser versteht, wie Benutzer die Windows-Onlinehilfe nutzen.

Auswahl und Steuerung

Onlinehilfe und -support ist standardmäßig aktiviert. Sie können diese Einstellung ändern, indem Sie oben im Hilfe- und Supportfenster auf das Symbol **Einstellungen** tippen oder klicken und dann **Onlinehilfe abrufen**aktivieren oder deaktivieren. Sie können die von der Windows-Hilfe verwendeten Cookies löschen. Öffnen Sie hierzu in der Systemsteuerung die Internetoptionen, klicken oder tippen Sie unter **Browserverlauf** auf die Schaltfläche **Löschen**, wählen Sie **Cookies und Webseitedaten**aus, und klicken oder tippen Sie auf **Browserverlauf**. Wenn Sie in den Internetoptionen im Abschnitt zum Datenschutz alle Cookies blocken, werden von der Windows-Hilfe keine Cookies festgelegt.

Programm zur Verbesserung der Hilfebenutzerfreundlichkeit

Funktionsweise dieses Features

Das Programm zur Verbesserung der Hilfebenutzerfreundlichkeit hilft Microsoft beim Erkennen von Trends bei der Verwendung von Windows-Onlinehilfe und -support, um auf diese Weise die Suchergebnisse und die Relevanz der Inhalte zu verbessern.

Gesammelte, verarbeitete und übertragene Informationen

Das Programm zur Verbesserung der Hilfebenutzerfreundlichkeit (HEIP) sendet Microsoft Informationen zur der auf Ihrem PC ausgeführten Version von Windows und darüber, wie Sie Windows-Hilfe und -Support nutzen. Dies beinhaltet auch Abfragen, die Sie bei der Suche in Windows-Hilfe und -Support eingeben, sowie Bewertungen oder Feedback zu den von Ihnen aufgerufenen Hilfethemen. Wenn Sie die angezeigten Hilfethemen durchsuchen bzw. Bewertungen oder Feedback zu den Hilfethemen bereitstellen, werden diese Informationen an Microsoft gesendet.

Vom Programm zur Verbesserung der Hilfebenutzerfreundlichkeit wird eine Zahl generiert, die so genannte GUID (Globally Unique Identifier, global eindeutiger Bezeichner), die mit jedem Bericht des Programms an Microsoft gesendet wird. Anhand der GUID kann Microsoft ermitteln, welche Daten im Lauf der Zeit von einem bestimmten Computer gesendet wurden. Die GUID enthält keine persönlichen Informationen. Die GUID ist unabhängig von den GUIDs, die von der Windows-Fehlerberichterstattung und vom Windows-Programm zur Verbesserung der Benutzerfreundlichkeit verwendet werden.

Verwendung von Informationen

Die erfassten Daten dienen dazu, Trends und Nutzungsmuster zu ermitteln, damit Microsoft die Qualität der angebotenen Inhalte und die Relevanz der Suchergebnisse verbessern kann. Anhand der GUID wird ermittelt, wie verbreitet die gemeldeten Probleme sind und welche Priorität ihnen beigemessen werden sollte. Anhand der GUID kann Microsoft beispielsweise unterscheiden, ob ein Problem hundert Mal bei einem Kunden oder ob das gleiche Problem bei hundert Kunden jeweils einmal aufgetreten ist.

Vom Programm zur Verbesserung der Hilfebenutzerfreundlichkeit werden nicht beabsichtigt Informationen gesammelt, die verwendet werden können, um Sie persönlich zu identifizieren. Wenn Sie solche Informationen in die Such- oder Feedbackfelder eingeben, werden diese oder andere gesammelte Informationen zwar gesendet, aber von Microsoft nicht dazu verwendet, Sie zu identifizieren, Kontakt mit Ihnen aufzunehmen oder gezielte Werbung zu schalten.

Auswahl und Steuerung

Wenn Sie beim Einrichten von Windows die Expresseinstellungen auswählen, nehmen Sie damit am Programm zur Verbesserung der Hilfebenutzerfreundlichkeit teil. Wenn Sie sich für das Anpassen der Einstellungen entscheiden, können Sie das Programm zur Verbesserung der Hilfebenutzerfreundlichkeit steuern, indem Sie unter **Ich möchte Informationen an Microsoft übermitteln, um die Optimierung von Windows und Apps zu ermöglichen** unter **Senden Sie uns (Microsoft) Infos, damit wir Windows und Apps verbessern können**auswählen. Nach dem Einrichten von Windows können Sie diese Einstellung in Windows-Hilfe und Support ändern.

Seitenanfang

Remoteunterstützung

Funktionsweise dieses Features

Mithilfe der Remoteunterstützung können Sie eine Person einladen, eine Verbindung mit Ihrem PC herzustellen, um Ihnen bei einem PC-Problem zu helfen, und zwar auch dann, wenn diese Person nicht in der Nähe ist. Sobald die Verbindung hergestellt ist, kann die andere Person Ihren PC sehen. Mit Ihrer Erlaubnis kann die andere Person mithilfe von Maus und Tastatur die Steuerung über Ihren Computer übernehmen und Ihnen zeigen, wie ein Problem behoben werden kann.

Gesammelte, verarbeitete und übertragene Informationen

Remoteunterstützung stellt über das Internet oder das lokale Netzwerk eine verschlüsselte Verbindung zwischen den beiden PCs her. Stellt eine Person über die Remoteunterstützung eine Verbindung mit Ihrem PC her, kann diese Person Ihren Desktop, alle geöffneten Dokumente und sämtliche sichtbaren privaten Informationen sehen. Wenn Sie der anderen Person erlauben, Ihren PC mit der eigenen Maus zu steuern, kann diese Person zudem Aktionen auf dem PC ausführen, beispielsweise Dateien löschen oder Einstellungen ändern. Nach der Verbindungsherstellung tauscht Remoteunterstützung Kontaktinformationen aus, z. B. Benutzername, PC-Name und Profilbild. In einer Sitzungsprotokolldatei werden alle Remoteunterstützungsverbindungen festgehalten.

Verwendung von Informationen

Die Informationen werden dazu verwendet, um eine verschlüsselte Verbindung herzustellen und der anderen Person Zugriff auf Ihren Desktop zu gewähren. Es werden keine Informationen an Microsoft gesendet.

Auswahl und Steuerung

Bevor Sie einer anderen Person erlauben, eine Verbindung mit Ihrem PC herzustellen, sollten Sie alle geöffneten Apps oder Dokumente schließen, die für die andere Person nicht einsehbar sein sollen. Wenn Sie zu irgendeinem Zeitpunkt Bedenken hinsichtlich dessen haben sollten, was die Person auf Ihrem PC sieht oder welche Aktionen die Person durchführt, können Sie die Sitzung durch Drücken der ESC-TASTE beenden. Sie können die Sitzungsprotokollierung und den Austausch von Kontaktinformationen deaktivieren, indem Sie die entsprechenden Optionen in den Einstellungen von Remoteunterstützung deaktivieren.

Seitenanfang

Windows Search

Funktionsweise dieses Features

Windows Search bietet Ihnen einen schnellen und konsistenten

Einstiegspunkt für die Suche nach Apps, Einstellungen, Dateien oder Inhalten in Apps.

Gesammelte, verarbeitete und übertragene Informationen

Wenn Sie Windows Search verwenden, werden die in das Suchfeld eingegebenen Zeichen (schon während der Eingabe) sowie die endgültig übermittelte Suchabfrage nur an Windows und alle durchsuchten Apps übermittelt, damit von Windows oder von den Apps Suchvorschläge bereitgestellt und Suchergebnisse angezeigt werden können. In Windows werden Suchabfragen und Daten über die Häufigkeit der Suche in Apps gespeichert.

Verwendung von Informationen

Die gespeicherten vorherigen Suchvorgänge werden von Windows verwendet, um im Suchbereich Suchvorschläge bereitzustellen. Die Informationen darüber, wie häufig Sie in Apps suchen, werden verwendet, um die Liste der durchsuchbaren Apps im Suchbereich in der Reihenfolge der Suchhäufigkeit zu sortieren. Wenn Sie in einer Drittanbieter-App suchen, unterliegt die Nutzung der gesammelten Informationen den Datenschutzpraktiken des Drittanbieters. Wenn Sie in einer Microsoft-App suchen, werden die Datenschutzpraktiken der App in den dazugehörigen Datenschutzbestimmungen erläutert.

Auswahl und Steuerung

Diese Informationen werden standardmäßig in Windows gespeichert. Sie können mithilfe der Einstellungen unter „Auf PC suchen" die Speicherung dieser Informationen deaktivieren oder alle zuvor gespeicherten Suchen löschen.

Seitenanfang

Windows-Freigabe

Funktionsweise dieses Features

Mit der Windows-Freigabe können Sie Inhalte zwischen Windows Store-Apps freigeben, die die Freigabe unterstützen. Sie können

auch Inhalte für Ihre Freunde freigeben.

Gesammelte, verarbeitete und übertragene Informationen

Bei der Freigabe von Inhalt übergibt die Quell-App den Inhalt nur an die Ziel-App, nachdem Sie das Ziel im Freigabebereich ausgewählt haben. Wenn in der Ziel-App die Freigabe nicht implementiert ist, haben Sie dennoch die Möglichkeit, ein Bild des jeweiligen Bildschirminhalts freizugeben. Für einen leichteren Zugriff werden die Ziel-Apps und Personen, für die Sie häufig Inhalte freigeben, im Freigabebereich in einer Liste angezeigt. Es werden keine Informationen an Microsoft gesendet.

Verwendung von Informationen

Die gespeicherten Informationen darüber, wie häufig Sie Inhalte für Ziel-Apps oder Personen freigeben, werden verwendet, um die Liste im Freigabebereich in der Reihenfolge der Freigabehäufigkeit zu sortieren. Wenn Sie Informationen mit einer Drittanbieter-App freigeben, unterliegt die Nutzung der gesammelten Informationen den Datenschutzpraktiken des Drittanbieters. Wenn Sie Inhalt mit einer Microsoft-App freigeben, wird die Datenschutzpraktiken der App in den zugehörigen Datenschutzbestimmungen erläutert.

Auswahl und Steuerung

Informationen zu Ihrer Verwendung von Windows-Freigabe werden von Windows standardmäßig gespeichert. Sie können mithilfe der Einstellungen unter „Auf PC freigeben" die Speicherung dieser Informationen deaktivieren oder alle gespeicherten Ziele löschen.

Seitenanfang

Windows SmartScreen

Funktionsweise dieses Features

Windows SmartScreen trägt zur Sicherheit Ihres PCs bei, indem Dateien und Apps vor dem Öffnen und Ausführen durch Senden von Informationen an Microsoft geprüft werden, um Sie vor

potenziell unsicheren Dateien und Apps zu schützen. Sie werden von Windows gefragt, wie vorgegangen werden soll, bevor eine unbekannte oder potenziell unsichere Datei oder App geöffnet wird.

Gesammelte, verarbeitete und übertragene Informationen

Wenn Sie sich zur Verwendung dieses Features entscheiden, werden Informationen zu einigen verwendeten Apps und zu einigen aus dem Internet heruntergeladenen Apps an Microsoft gesendet. Neben den Standardcomputerinformationen und der Versionsnummer des Windows SmartScreen-Filters können diese Informationen auch einen Dateinamen, eine Dateikennung ("Hash") und digitale Zertifikatinformationen enthalten. Zum Schutz Ihrer Daten werden die an Microsoft übermittelten Informationen durch SSL verschlüsselt.

Von Windows SmartScreen wird eine GUID (Globally Unique Identifier) generiert, die mit Ihren SmartScreen-Nutzungsdaten an Microsoft gesendet wird. Die GUID ist eine zufällig generierte Zahl. Anhand der GUID kann Microsoft ermitteln, welche Daten im Lauf der Zeit von einem bestimmten PC gesendet wurden. Die GUID enthält keine persönlichen Informationen.

Verwendung von Informationen

Microsoft verwendet die oben beschriebenen Informationen, um Sie vor potenziell unsicheren Dateien und Apps zu warnen. Zudem dienen die Informationen dazu, die Leistung des Features zu analysieren und die Qualität der Produkte und Dienste von Microsoft zu verbessern. Anhand der GUID kann Microsoft feststellen, wie weit verbreitet das empfangene Feedback ist und welche Priorität dem Feedback eingeräumt werden soll. Mit der GUID kann Microsoft beispielsweise unterscheiden, ob ein Problem hundert Mal bei einem Kunden oder ob das gleiche Problem bei hundert Kunden jeweils einmal aufgetreten ist. Microsoft verwendet die Informationen nicht dazu, Sie zu identifizieren, Kontakt mit Ihnen aufzunehmen oder gezielte Werbung zu schalten.

Auswahl und Steuerung

Wenn Sie beim Einrichten von Windows die Expresseinstellungen auswählen, aktivieren Sie Windows SmartScreen. Wenn Sie sich für das Anpassen der Einstellungen entscheiden, können Sie Windows SmartScreen steuern, indem Sie unter **Ihre Privatsphäre und den PC schützen** unter **Windows SmartScreen-Filter verwenden, um Dateien und Apps durch Microsoft zu überprüfen**auswählen. Sie können diese Einstellung nach der Einrichtung von Windows in der Systemsteuerung im Wartungscenter ändern.

Seitenanfang

Windows-Spracherkennung

Funktionsweise dieses Features

Die Windows-Spracherkennung stellt in Windows und für alle Apps, in denen dieses Feature verwendet wird, Spracherkennungsfunktionen bereit. Die Windows-Spracherkennung wird kontinuierlich verbessert, indem sie Ihre Sprachnutzung erlernt. Dazu gehören auch die Sprachlaute und Wörter, die Sie bevorzugt verwenden.

Gesammelte, verarbeitete und übertragene Informationen

Von der Windows-Spracherkennung wird auf dem PC eine Liste von Wörtern und deren Aussprache gespeichert. Wörter und Aussprache werden dieser Liste über das Sprachwörterbuch sowie über das Verwenden der Windows-Spracherkennung zum Diktieren und Korrigieren von Wörtern hinzugefügt.

Wenn das Windows-Spracherkennungsfeature zur Überprüfung von Dokumenten aktiviert ist, werden Texte aus Microsoft Office Word-Dokumenten (mit der Dateinamenerweiterung DOC oder DOCX) und E-Mail-Nachrichten (aus E-Mail-Ordnern außer "Gelöschte Elemente" oder "Junk-E-Mail"), die sich auf Ihrem PC oder auf verbundenen Dateifreigaben in Ihren Windows-Suchindexpfaden befinden, erfasst und in Fragmenten gespeichert, die aus einem, zwei oder drei Wörtern bestehen. Ein-Wort-Fragmente enthalten nur Wörter, die Sie

benutzerdefinierten Wörterbüchern hinzugefügt haben, und Zwei- oder Drei-Wort-Fragmente enthalten nur Wörter, die in Standardwörterbüchern zu finden sind.

Alle gesammelten Informationen werden in Ihrem persönlichem Sprachprofil auf dem PC gespeichert. Sprachprofile werden für jeden getrennt Benutzer gespeichert, und die Benutzer eines PCs können nicht auf die Profile anderer zugreifen. Administratoren haben dagegen Zugriff auf alle Profile auf dem jeweiligen Computer. Die Profilinformationen werden nur dann Microsoft gesendet, wenn Sie bei Aufforderung durch die Windows-Spracherkennung auswählen, dass die Informationen gesendet werden sollen. Sie können die Daten vor dem Senden prüfen. Wenn Sie auswählen, dass die Daten gesendet werden sollen, werden auch die Daten der akustischen Adaption gesendet, mit denen Ihre Audiomerkmale adaptiert wurden.

Wenn Sie eine Sprachtrainingssitzung beenden möchten, werden Sie von derWindows-Spracherkennung gefragt, ob Ihre Sprachprofildaten an Microsoft gesendet werden sollen. Sie können die Informationen vor dem Senden prüfen. Diese Daten können aus den Aufzeichnungen Ihrer Stimme aus der Trainingssitzung und den anderen Daten aus Ihrem persönlichen Sprachprofil (siehe weiter oben) bestehen.

Verwendung von Informationen

Die Windows-Spracherkennung wandelt mithilfe der Wörter aus dem Sprachprofil Ihre Sprache in Text um. Microsoft verwendet die Daten des persönlichen Sprachprofils dazu, die Microsoft-Produkte und -Dienste zu verbessern. Microsoft verwendet die Informationen nicht dazu, Sie zu identifizieren, Kontakt mit Ihnen aufzunehmen oder gezielte Werbung zu schalten.

Auswahl und Steuerung

Sie können entscheiden, ob die Windows-Spracherkennung ausgeführt wird. Bei Ausführung der Windows-Spracherkennung ist das Feature zur Dokumentüberprüfung standardmäßig aktiviert. Wenn Sie die Windows-Spracherkennung das erste Mal ausführen, haben Sie die Möglichkeit, die Einstellungen für die Überprüfung von Dokumenten zu ändern. Sie können Ihre

Einstellungen für die Überprüfung von Dokumenten ändern oder persönliche Sprachprofile (und die meisten Daten für die Überprüfung von Dokumenten) löschen, indem Sie in der Systemsteuerung "Spracherkennung" öffnen und auf **Erweiterte Sprachoptionen**klicken. Außerdem können Sie Wörter, die Sie zum Sprachprofil hinzugefügt haben, über die Option "Vorhandene Wörter ändern" im Wörterbuch wieder löschen. Wenn Sie Ihr persönliches Sprachprofil löschen, werden jedoch keine über das Sprachwörterbuch hinzugefügten Wörter gelöscht.

Sie können steuern, an welchen Orten bei der Überprüfung von Dokumenten Wortfragmente gesammelt werden, indem Sie die Orte im Windows-Suchindex ändern. Öffnen Sie "Indizierungsoptionen" in der Systemsteuerung, um die Orte, die in den Windows-Suchindex einbezogen werden, anzuzeigen oder zu ändern.

Am Ende der Trainingssitzung können Sie entscheiden, ob Ihre Trainingsinformationen und Ihre anderen Profilinformationen an Microsoft gesendet werden. Außerdem können Sie Informationen senden, wenn die Windows-Spracherkennung gestartet wird. Klicken Sie dazu mit der rechten Maustaste auf **Mikrofon**, und klicken Sie dann auf **Beitrag zur Verbesserung der Spracherkennung leisten**. In beiden Fällen können Sie alle Datendateien vor dem Senden anzeigen, und dann entscheiden, ob die Informationen gesendet werden.

Seitenanfang

Windows Store

Der Windows Store dient zum Suchen, Verwalten und Installieren von Apps. In den folgenden Abschnitten wird beschrieben, wie sich die Windows Store-Features und die Apps, die Sie über den Store herunterladen, auf den Schutz Ihrer Daten auswirken und was Sie dagegen unternehmen können.

Store-App und -Dienst

Funktionsweise dieses Features

Im Store können Sie nach Apps für Ihren PC suchen und diese installieren. Im Store wird auch nachverfolgt, welche Store-Apps Sie installiert haben, damit Sie Updates für die Apps erhalten und die Apps auf mehreren PCs installieren können.

Gesammelte, verarbeitete und übertragene Informationen

Zum Suchen und Installieren von Apps müssen Sie sich mit einem Microsoft-Konto beim Store anmelden. Auf diese Weise kann der Store auf Informationen in Ihrem Microsoft-Kontoprofil zugreifen, beispielsweise Name, E-Mail-Adresse und Profilbild. Der Store sammelt folgende zusätzliche Informationen und verknüpft sie mit Ihrem Store-Konto:

- Zahlungen an den Store. Informationen darüber, was Sie gekauft haben, welchen Betrag Sie gezahlt haben und wie Sie für Apps oder In-App-Käufe mit Ihrem Store-Konto bezahlt haben.

- Installierte Apps. Die Liste der installierten Apps, die Lizenzrichtlinie für jede App (permanente Lizenz oder zeitlich begrenzte Testversion) und eine Liste der Einkäufe, die Sie mit Ihrem Store-Konto in den einzelnen Apps getätigt haben. Neben der Onlinespeicherung dieser Informationen in Ihrem Store-Konto werden die Lizenzinformationen für jede installierte App auch auf Ihrem PC gespeichert. Anhand dieser Informationen können Sie als Besitzer der Lizenz identifiziert werden.

- PCs, auf denen die Apps installiert sind. Das Fabrikat, Modell und der Computername jedes PCs, auf den Apps installiert sind, zusammen mit einer Zahl, die den PC eindeutig identifiziert. Diese Zahl wird basierend auf der Hardwarekonfiguration des PCs generiert und enthält keine Informationen zu Ihrer Person.

- Bewertungen, Rezensionen und Problemberichte. Sobald Sie eine App installiert haben, können Sie eine Rezension schreiben oder im Store eine Bewertung für die App abgeben. Ihr Microsoft-Konto wird mit diesen Bewertungen

verknüpft. Wenn Sie eine Rezension schreiben, werden Name und Bild aus Ihrem Microsoft-Konto zusammen mit Ihrer Rezension veröffentlicht.

- Store-Einstellungen. Einstellungen, die Sie für die Anzeige von Apps im Store festlegen, wie z. B., ob nur Apps angezeigt werden sollen, die in Ihrer Muttersprache verfügbar sind.

Sie können auch festlegen, dass in Ihrem Store-Konto Zahlungsinformationen gespeichert werden, beispielsweise eine Kreditkartennummer. Aus Sicherheitsgründen werden diese Informationen über SSL übermittelt, und die Kreditkartennummer wird (bis auf die letzten vier Ziffern) verschlüsselt gespeichert.

Im Store werden einige Informationen zu Ihrer Kopie von Windows gespeichert, um festzustellen, ob sie im Einzelhandel gekauft wurde, vom PC-Hersteller auf dem PC vorinstalliert wurde oder ob es sich um eine Evaluierungskopie handelt, die dem Volumenlizenzprogramm unterliegt. Wenn Sie zum ersten Mal eine Verbindung mit dem Store herstellen, wird eine Liste aller auf Ihrem PC vorinstallierter Apps an den Store gesendet. Dort werden Ihrem Store-Konto Lizenzen für diese Apps zugeordnet.

Der Store prüft automatisch, ob für Ihre Apps Updates vorhanden sind. Sie können benachrichtigt werden, wenn neue Updates verfügbar sind. Zum Bereitstellen von Updates sendet der Store die folgenden Informationen an Microsoft:

- Eine Liste der Apps, die von allen Benutzern des PCs über den Store installiert wurden.

- Die Lizenzierungsinformationen für jede App, einschließlich Besitzer jeder Lizenz.

- Ihre Windows Update- und/oder Microsoft Update-Konfigurationseinstellungen, wie z. B., ob Updates automatisch heruntergeladen oder installiert werden.

- Informationen zu erfolgreichen oder gescheiterten Updates

oder zu Fehlern, die beim Aktualisieren der Apps aus dem Store aufgetreten sind.

- Globally Unique Identifier (GUID) – eine zufällig generierte Zahl, die keine persönlichen Informationen enthält. Anhand von GUIDs werden einzelne PCs identifiziert, ohne die Identität des Benutzers zu offenbaren.

- BIOS-Name, Revisionsnummer und Revisionsdatum – Informationen zum Satz wichtiger Softwareroutinen, die dazu dienen, die Hardware zu testen, das Betriebssystem auf dem PC zu starten und Daten zwischen den an den PC angeschlossenen Hardwaregeräten zu übertragen.

Wenn Sie im Store navigieren und Apps aus dem Store verwenden, sammelt Microsoft einige Informationen, um die Verwendungsmuster und Trends zu analysieren, so wie auf vielen Webseiten auch die Browsingdaten der Besucher analysiert werden. Beachten Sie, dass diese Aktivitätsdaten nicht verwendet werden, um Sie zu identifizieren oder Kontakt mit Ihnen aufzunehmen.

Verwendung von Informationen

Microsoft verwendet die Kontaktinformationen, um Ihnen E-Mails zu senden, die zum Bereitstellen der Store-Dienste erforderlich sind, z. B. Quittungen für gekaufte Apps. Ihre Zahlungsinformationen werden für die Zahlungsabwicklung der Einkäufe verwendet. Wenn Sie sich entscheiden, diese Informationen zu speichern, ersparen Sie sich die wiederholte Eingabe dieser Informationen. Microsoft verwendet die Informationen zu Ihren Einkäufen, um den Store zu betreiben und Kundensupport bereitzustellen.

Im Store werden alle installierten Apps nachverfolgt. Sie können den Store verwenden, um die Liste der Geräte zu verwalten, auf denen die Apps installiert sind. Auch der Kundensupport kann Ihnen beim Verwalten dieser Informationen helfen. Sobald Sie eine App installiert haben, wird sie immer im Store-Einkaufsverlauf angezeigt, auch wenn Sie die App wieder deinstalliert haben. Im Store dient diese Liste auch dazu, die

maximale Anzahl von PCs, auf denen Apps installiert werden können, zu erzwingen, so wie in den Windows Store-Nutzungsbedingungen beschrieben. Wenn Sie eine Rezension für eine App schreiben, werden Name und Profilbild, die Ihrem Windows-Konto zugeordnet sind, neben der Rezension im Store veröffentlicht. Wird ein Problem mit einer App gemeldet, wird der Problembericht den Store-Mitarbeitern zur Verfügung gestellt, um das Problem einzuschätzen und entsprechende Maßnahmen zu ergreifen. Wenn die Mitarbeiter den Bericht prüfen, können diese Sie bei Bedarf über die Ihrem Store-Konto zugeordnete E-Mail-Adresse zu kontaktieren.

Sind zu den von Ihnen installierten Apps Updates verfügbar, wird im Store eine Benachrichtigung angezeigt, und auf der Kachel der Store-App wird die Anzahl der verfügbaren Updates angezeigt. Sie können dann die Liste der verfügbaren Updates anzeigen und die zu installierenden Updates auswählen. In den aktualisierten Apps stehen ggf. andere Windows-Funktionen als in den vorherigen Versionen zur Verfügung, sodass die Apps möglicherweise auf andere Ressourcen auf dem PC zugreifen können. Sie können die aktualisierten Listen der Funktionen auf den App-Beschreibungsseiten sehen, auf die über einen Link von der Seite mit den verfügbaren Updates aus zugegriffen werden kann.

Der Store verwendet die Informationen, die über Ihre Kopie von Windows gesammelt werden, um zu ermitteln, wie Windows auf Ihrem PC installiert wurde (beispielsweise, ob die Kopie vom PC-Hersteller auf dem PC vorinstalliert wurde). Anhand dieser Informationen gewährt der Store Ihnen Zugriff auf die Apps, die ausschließlich von diesem Hersteller für seine Kunden bereitgestellt werden. Zudem dienen diese Informationen dazu, um Microsoft (und in einigen Fällen auch in zusammengefasster Form dem Hersteller) Angaben über die Windows-Nutzungsmuster bereitzustellen.

Microsoft verwendet einigen Daten zum App-Einkauf und zur App-Nutzung in zusammengefasster Form, um zu erfahren, wie Benutzer den Store verwenden (wie z. B. Benutzer die Apps finden, die sie installieren). Microsoft kann einen Teil dieser

gesammelten Statistikdaten für App-Entwickler freigeben. Microsoft gibt keine persönlichen Informationen an App-Entwickler weiter. Microsoft nutzt die vom Store gesammelten Browser- und Nutzungsdaten, um besser zu verstehen, wie Benutzer den Store verwenden, und um die Store-Features und -Dienste zu verbessern.

Auswahl und Steuerung

Wenn Sie den Store verwenden, werden die in diesem Abschnitt beschriebenen Informationen in der oben beschriebenen Art an Microsoft gesendet.

Sie können eine von Ihnen veröffentlichte Rezension zu einer App entfernen, indem Sie zur App-Beschreibung im Store wechseln, die Rezension bearbeiten und den gesamten Text löschen.

Berechtigung für Store-Apps

Funktionsweise dieses Features

Viele Apps, die Sie aus dem Windows Store installieren, sind so konzipiert, dass sie bestimmte Hardware- und Softwarefeatures des PCs nutzen. Eine Foto-App muss ggf. Ihre Webcam verwenden, und ein Restaurantführer muss Ihren Standort kennen, um Empfehlungen für Restaurants in Ihrer Nähe zu geben.

Gesammelte, verarbeitete und übertragene Informationen

Im Folgenden sind die Features aufgelistet, deren Verwendung durch die App offen gelegt werden muss:

- Ihre Internetverbindung. Erlaubt der App, eine Internetverbindung herzustellen.
- Über eine Firewall eingehende Verbindungen. Erlaubt der App, über eine Firewall Informationen an oder von Ihrem PC zu senden.
- Ein Heim- oder Unternehmensnetzwerk. Erlaubt der App, Informationen zwischen Ihrem PC und anderen PCs im

gleichen Netzwerk zu senden.

- Ihre Bild-, Video-, Musik- oder Dokumentbibliotheken. Erlauben der App, auf Dateien in den Bibliotheken zuzugreifen und zu ändern oder zu löschen. Dies beinhaltet den Zugriff auf zusätzliche Daten, die in diesen Dateien eingebettet sind, beispielsweise Standortinformationen in Fotos.

- Wechselmedien. Erlaubt der App, Dateien auf einer externen Festplatte, einem USB-Speicherstick oder einem tragbaren Gerät hinzuzufügen, zu ändern, zu löschen oder darauf zuzugreifen.

- Ihre Windows-Anmeldeinformationen. Erlaubt der App, sich mit Ihren Anmeldeinformationen bei einem Unternehmensnetzwerk zu authentifizieren, um darauf zugreifen zu können.

- Auf dem PC oder einer Smartcard gespeicherte Zertifikate. Erlaubt der App, Zertifikate zu verwenden, um eine sichere Verbindung mit Organisationen zu ermöglichen, beispielsweise Banken, Behörden oder Ihrem Arbeitgeber.

- Das Textnachrichtenfeature des PCs. Erlaubt der App, Textnachrichten (SMS) zu senden und zu empfangen.

- Webcam und Mikrofon. Erlaubt der App, Fotos aufzunehmen und Audio- und Videoaufzeichnungen zu erstellen.

- Ihr Standort. Erlaubt der App, basierend auf einem GPS-Sensor oder anhand von Netzwerkinformationen Ihren ungefähren Standort zu ermitteln.

- Das PC-Feature zur Nahfeldkommunikation. Erlaubt der App, eine Verbindung mit anderen Geräten in der Nähe herzustellen, auf denen dieselbe App ausgeführt wird.

- Ihre tragbaren Geräte. Erlaubt der App die Kommunikation mit Geräten, beispielsweise einem Mobiltelefon, einem tragbaren Musikplayer oder einer Digitalkamera.

- Ihre Informationen auf einem tragbaren Gerät. Erlaubt der App, auf Kontakte, Kalender, Aufgaben, Notizen, Statusinformationen oder Klingeltöne auf Ihrem tragbaren Gerät zuzugreifen bzw. diese hinzuzufügen, zu ändern oder zu löschen.

- Ihr mobiles Breitbandkonto. Erlaubt der App, Ihr mobiles Breitbandkonto zu verwalten.

Die von einer App verwendeten Features werden auf der Seite mit der App-Beschreibung aufgelistet. Wenn Sie eine App installieren, wird der App die Verwendung dieser Features (außer der besonders sensiblen Features für Standortinformationen, Textnachrichten sowie Webcam und Mikrofon) von Windows erlaubt. Wenn eine App zum ersten Mal Zugriff auf diese sensiblen Features anfordert, werden Sie von Windows gefragt, ob Sie der App die Nutzung erlauben möchten. Sie können die Nutzungsberechtigung für die App jederzeit ändern.

Verwendung von Informationen

Alle Apps, die diese Features verwenden, unterliegen den Datenschutzpraktiken der jeweiligen Entwickler. Wenn eine App eines der weiter oben beschriebenen sensiblen Features verwendet, steht im Store auf der Seite „App-Beschreibung" ein Link zu den Datenschutzbestimmungen des App-Herausgebers zur Verfügung.

Auswahl und Steuerung

Bevor Sie eine App installieren, können Sie im Store prüfen, welche Features die App benötigt. Sie werden von Windows gefragt, ob Sie der App den Zugriff auf die sensibelsten dieser Features – Standortinformationen, Textnachrichten, Webcam und Mikrofon – erlauben oder verweigern möchten, bevor die App die Features zum ersten Mal verwendet.

Wenn Sie sich im Windows die Seite "App-Beschreibung" einer App ansehen, wird unten in der linken Spalte eine gekürzte Liste der Features angezeigt. Die vollständige Liste wird auf der Detailseite der App-Beschreibung angezeigt. Nachdem Sie eine App installiert haben, können Sie jederzeit die vollständige Liste

der von der App verwendeten Features anzeigen und den Zugriff auf die besonders sensiblen Features steuern. Hierzu öffnen Sie die App, klicken oder tippen auf den Charm „Einstellungen" und wählen dann **Berechtigungen**auf den Schlüssel zugreifen oder ihn löschen.

Ich möchte URLs für von Apps verwendete Webinhalte übermitteln, um den Windows Store zu verbessern

Funktionsweise dieses Features

Einige Apps, die Sie im Store erhalten, sind mit Webseiten vergleichbar und können Ihren PC einem Sicherheitsrisiko durch möglicherweise unsichere Software, z. B. Schadsoftware, aussetzen. Wenn Sie dieses Feature aktivieren, werden Informationen zu dem von diesen Apps verwendeten Webinhalt gesammelt, um Microsoft bei der Diagnose eines eventuell unsicheren Verhaltens zu unterstützen. Microsoft kann diese Informationen beispielsweise verwenden, um eine App aus dem Store zu entfernen.

Gesammelte, verarbeitete und übertragene Informationen

Wenn Sie sich entscheiden, Informationen über den von Ihrem Apps verwendeten Webinhalt zu übermitteln, sammelt Microsoft Daten zu den URLs und den Arten des Inhalts, um zu ermitteln, auf welche Informationen diese Apps zugreifen, wenn Sie sie verwenden. Auf diese Weise kann Microsoft besser feststellen, welche dieser Apps Inhalte von schädlichen oder unsicheren Webseiten empfängt. Die an Microsoft gesendeten Berichte enthalten Informationen, z. B. Name oder Bezeichner der App, die vollständigen URLs der Webseiten, auf die die App zugreift, und die vollständigen URLs, die den Ort aller JavaScript-Elemente angeben, auf die die App zugreift. Von Windows wird eine GUID (Globally Unique Identifier) generiert, die in jedem an Microsoft gesendeten Bericht enthalten ist. Die GUID ist eine zufällig generierte Zahl. Anhand der GUID kann Microsoft erkennen, welche Daten im Laufe der Zeit von einem bestimmten Computer übermittelt werden. Die GUID enthält

keine persönlichen Informationen und wird nicht verwendet, um Ihre Identität festzustellen.

Zum Schutz Ihrer Daten werden die an Microsoft übermittelten Informationen verschlüsselt. Dies kann auch Informationen zu einer Webseite beinhalten, auf die diese Apps zugreifen, beispielsweise Suchbegriffe oder Daten, die Sie in die Apps eingegeben haben. Wenn Sie beispielsweise in einer Wörterbuch-App ein Wort nachschlagen, ist das gesuchte Wort möglicherweise als Teil der vollständigen Adresse, auf die von der App zugegriffen wird, in den an Microsoft gesendeten Informationen enthalten. Microsoft filtert diese Adressen, um persönliche Informationen zu entfernen, sofern möglich.

Verwendung von Informationen

Microsoft überprüft die übermittelten Informationen regelmäßig, um Apps zu erkennen, die möglicherweise mit unsicherem Webinhalt interagieren, beispielsweise mit gefährlichen Webadressen oder schädlichen Skripts. Microsoft ergreift basierend auf diesen Informationen eventuell Maßnahmen gegen diese potenziell schädlichen Apps. Die Adressen von Webinhalten können unbeabsichtigt persönliche Informationen enthalten, aber diese Informationen werden nicht verwendet, um Sie zu identifizieren, mit Ihnen Kontakt aufzunehmen oder gezielte Werbung zu schalten. Anhand der GUID kann Microsoft feststellen, wie weit verbreitet das empfangene Feedback ist und welche Priorität dem Feedback eingeräumt werden soll. Anhand der GUID kann Microsoft beispielsweise zwischen einem potenziell unsicheren Verhalten, das hundertmal auf einem einzigen PC auftritt, und demselben Verhalten unterscheiden, dass einmal auf 100 PCs auftritt.

Auswahl und Steuerung

Wenn Sie beim Einrichten von Windows die Expresseinstellungen auswählen, werden von Windows keine Informationen zum Webinhalt gesendet, der von Ihren in JavaScript geschriebenen Apps aus dem Store verwendet wird. Wenn Sie die Einstellungen anpassen möchten, können Sie diese Einstellung steuern, indem Sie **Ich möchte URLs für von Apps verwendete**

Webinhalte übermitteln, um den Windows Store zu verbessern unter **Senden Sie uns (Microsoft) Infos, damit wir Windows und Apps verbessern können**. Nach der Installation können Sie diese Einstellung in den PC-Einstellungen unter „Datenschutz" ändern.

Seitenanfang

Windows-Zeitdienst

Funktionsweise dieses Features

Der Windows-Zeitdienst synchronisiert die PC-Zeit automatisch mit einem Zeitserver im Netzwerk.

Gesammelte, verarbeitete und übertragene Informationen

Der Dienst stellt über das Internet oder ein lokales Netzwerk mit dem Standardprotokoll NTP (Network Time-Protokoll) eine Verbindung mit einem Zeitserver her. Standardmäßig wird dieser Dienst einmal wöchentlich mit time.windows.com synchronisiert. An den Zeitserver werden ausschließlich PC-Standardinformationen gesendet.

Verwendung von Informationen

Der Windows-Zeitdienst synchronisiert mit diesen Informationen automatisch die Uhrzeit des lokalen PCs.

Auswahl und Steuerung

Der Windows-Zeitdienst ist standardmäßig aktiviert. Sie können dieses Feature deaktivieren oder Ihre bevorzugte Zeitquelle auswählen, indem Sie in der Systemsteuerung unter "Datum und Uhrzeit" die Registerkarte "Internetzeit" auswählen und auf **Einstellungen ändern**klicken. Das Deaktivieren des Windows-Zeitdiensts hat keinen direkten Einfluss auf Apps oder andere Dienste. Ohne zuverlässige Zeitquelle kann jedoch die Uhrzeit des lokalen Computers immer mehr von anderen Computern im Netzwerk oder Internet abweichen. Apps und Dienste, die von der genauen Zeit abhängen, können scheitern oder werden nicht mehr korrekt ausgeführt, wenn zwischen den PCs im Netzwerk

ein erheblicher Zeitunterschied besteht.

Seitenanfang

Windows-Problembehandlung

Funktionsweise dieses Features

Mit der Windows-Problembehandlung können Sie allgemeine Probleme auf dem PC diagnostizieren und beheben.

Gesammelte, verarbeitete und übertragene Informationen

Nach dem Ausführen des Problembehandlungspakets werden die Ergebnisse auf dem PC gespeichert. Diese Ergebnisse können persönliche Informationen enthalten, beispielsweise Ihren Benutzernamen oder den Namen eines Geräts. Die Windows-Problembehandlung kann Sie bei der Onlinesuche nach Problemlösungen in der Windows-Hilfe und in den Windows-Communitys unterstützen. Schlüsselwörter, die dem Problem zugeordnet sind, werden an Microsoft gesendet, um die Suche nach einer Lösung zu unterstützen. Wenn beispielsweise der Drucker nicht korrekt funktioniert und Sie nach Hilfe suchen, werden die Wörter "Drucker" und "drucken" an Microsoft gesendet.

Verwendung von Informationen

Microsoft verwendet die von der Windows-Problembehandlung gesammelten Informationen, um Benutzer bei der Behandlung von Problemen, die bei ihnen auftreten, zu unterstützen.

Auswahl und Steuerung

Wenn Sie beim Windows-Setup die Expresseinstellungen auswählen, wird von der Windows-Problembehandlung standardmäßig online nach Problembehandlungspaketen gesucht. Sie können diese Einstellungen in der Systemsteuerung unter „Problembehandlung“ ändern und Ergebnisse der Problembehandlung löschen. Klicken Sie auf **Verlauf anzeigen**, wählen Sie ein Ergebnis aus, und klicken Sie dann auf **Browserverlauf**auf den Schlüssel zugreifen oder ihn löschen.

Aktuelle Informationen über Methoden für die Verarbeitung der Daten von Microsoft, finden Sie in der Datenschutzerklärung von Microsoft. Hier erfahren Sie mehr über die neuesten Tools für den Zugriff auf und die Steuerung Ihrer Daten, und wie Sie uns kontaktieren, wenn Sie eine Abfrage zum Datenschutz haben.

Datenschutzbestimmungen für Windows 8 und Windows Server 2012

Auf dieser Seite finden Sie Folgendes:

Letzte Aktualisierung: **August 2012**

Diese Seite ist eine Ergänzung der Datenschutzbestimmungen für Windows 8 und Windows Server 2012 ("Windows-Datenschutzbestimmungen"). Die Datenschutzrichtlinie umfasst vier Abschnitte:

- Highlights
- Bestimmungen, die die vollständige Windows-DatenschutzbestimmungSie enthält Links für Windows-Features, für die eigene Bestimmungen vorliegen.
- Features – ErgänzungHier werden die Features beschrieben, die eine Auswirkungen auf den Datenschutz in Windows 8 und Windows Server 2012 haben.
- Server – Ergänzung (dieses Dokument) mit

Beschreibungen zu zusätzlichen Features, die Auswirkungen auf den Datenschutz in Windows Server 2012 haben

Zum besseren Verständnis der Datensammlung und Verwendungszwecke bestimmter Features oder Dienste von Windows lesen Sie die vollständigen Windows-Datenschutzbestimmungen und alle geltenden Ergänzungen. Darüber hinaus sollten Sie lesen dieses Whitepaper für Administratorenan.

Benutzerzugriffsprotokollierung

Dieses Feature hat folgende Funktion:

Benutzerzugriffsprotokollierung (UAL) sammelt und aggregiert Datensätze von Clientanforderungen der Serverrollen (sowohl Benutzer-als auch Geräteanforderungen) und installiert Produkte (sofern für UAL registriert) auf dem lokalen Server. Diese Daten – in Form von IP-Adressen, Benutzernamen und in einigen Fällen Hostnamen und/oder Identitäten virtueller Computer – werden in der lokalen Datenbank für Extensible Storage Engine (ESE) gespeichert und auf sie können nur von Administratoren zugreifen. UAL verfügt über einen WMIv2-Anbieter und zugehörige Windows PowerShell-Cmdlets zum Abrufen von Benutzerzugriffsdaten, die für die Offline-Kundenverwaltung von Berechtigungen (Client Access License, CAL) vorgesehen sind, bei denen tatsächliche Datensätze von eindeutigen Clientanforderungen wichtig sind.

Gesammelte, verarbeitete oder übertragene Informationen

IP-Adressen, Benutzernamen und in einigen Fällen Hostnamen (sofern DNS-Rolle installiert ist), und die Identitäten virtueller Computer (sofern Hyper-V-Rolle installiert ist) werden lokal auf dem Server gesammelt, wenn UAL aktiviert ist. Es werden keine gesammelten

Daten an Microsoft gesendet.

Verwendung der Informationen

UAL-Daten werden Administratoren über lokale ESE-Datenbanken, die WMI-Anbieter und die Windows PowerShell-Cmdlets zur Verfügung gestellt. Windows verwendet diese Daten nicht außerhalb des UAL-Features.

Auswahl und Kontrolle

Standardmäßig ist UAL aktiviert. Der UAL-Dienst kann beendet und gestartet werden, während der Server ausgeführt wird. Um UAL dauerhaft zu deaktivieren, öffnen Sie Windows PowerShell, geben Sie "Disable-UAL" ein, und starten Sie den Server neu. Ein Administrator kann alle gesammelten Verlaufsdaten löschen, indem er zunächst den Dienst beendet, UAL deaktiviert und dann alle Dateien im Ordner "%SystemRoot%\System32\LogFiles\SUM\" löscht.

Seitenanfang

Server-Manager

Dieses Feature hat folgende Funktion:

Server-Manager ist ein Verwaltungstool, mit dem ein Administrator einen oder mehrere Server überwachen und allgemeine oder rollenspezifische Status anzeigen kann, um Verwaltungsaufgaben auszuführen und auf andere Serververwaltungstools zuzugreifen.

Gesammelte, verarbeitete oder übertragene Informationen

Server-Manager erfasst die folgenden Arten von Informationen von einem Server, der vom Administrator verwaltet wird:

- **Allgemeine Serverinformationen:** NetBios-Name und vollqualifizierter Domänenname (FQDN), Anmeldeinformationen, die im die Feature "Verwalten als" eingegeben wurden, IPv4-Adresse,

IPv6-Adresse, Verwaltbarkeitsstatus, Beschreibung, Version des Betriebssystems, Typ, letztes Update, Prozessoren, Arbeitsspeicher, Clustername, Cluster-Objekttyp, Aktivierungsstatus, SKU, Architektur des Betriebssystems, Hersteller, Konfiguration des Programms zur Verbesserung der Benutzerfreundlichkeit (CEIP) und Konfiguration der Windows-Fehlerberichterstattung (WER).

- **Ereignisse:** ID, Schweregrad, Quelle, Protokoll, Datum und Uhrzeit für jedes Ereignis in Windows und andere Protokolle, die vom Administrator ausgewählt werden.
- **Alle Dienste:** Name, Status und Starttyp.
- **Informationen zur Serverrolle:** Best Practice Analyzer (BPA)-Ergebnisse für Rollen, die auf dem Server installiert sind.
- **Leistungsinformationen:** Beispiele für Leistungsindikatoren sowie Benachrichtigungen zu CPU-Auslastung und verfügbarem Arbeitsspeicher.

Verwendung der Informationen

Diese Informationen werden in Server-Manager gespeichert und nicht an Microsoft gesendet. Sie werden im Server-Manager anzeigt und unterstützen Administratoren in der Überwachung der Systeme.

Auswahl und Kontrolle

Ein Administrator kann das Sammeln von Daten von einem Server mit Ausnahme des lokalen Servers aktivieren oder deaktivieren, indem er den Server im Server-Manager hinzufügt oder entfernt. Ein Administrator kann explizit Anmeldeinformationen für die Verbindung zu einem Remoteserver bereitstellen. Server-Manager fordert den Administrator auf, ausdrücklich zuzustimmen, dass die Anmeldeinformationen in Server-Manager lokal gespeichert werden sollen, und der Administrator kann diese Anmeldeinformationen jederzeit

löschen.

Seitenanfang

Active Directory-Verbunddienste

Dieses Feature hat folgende Funktion:

Active Directory-Verbunddienste (AD FS) ist eine Verbund- und SSO-Lösung für lokale oder andere netzwerkbasierte Anwendungen in Unternehmen. Mit AD FS können Administratoren Benutzern die Zusammenarbeit in Organisationen und bequemen Zugriff auf lokale oder andere Netzwerken ermöglichen und gleichzeitig die Anwendungssicherheit gewährleisten. AD FS verwendet einen Sicherheitstokendienst, der Active Directory Domain Services (AD DS) verwendet, um Benutzer zu authentifizieren und ihnen Sicherheitstoken auszustellen. Dazu werden verschiedener Protokolle verwendet. Das Token ist digital signiert und enthält Ansprüche des Benutzers, die aus AD DS, Lightweight Directory Access Protocol (LDAP), SQL Server oder einem benutzerdefinierten Store oder einer Kombination daraus stammen.

Gesammelte, verarbeitete oder übertragene Informationen

Die Anmeldeinformationen eines Benutzers werden gesammelt, wenn der Benutzer bei AD FS authentifiziert ist. Die Anmeldeinformationen werden sofort zur Authentifizierung an Active Directory Domain Services gesendet und nicht lokal in AD FS gespeichert. Die Benutzerattribute in den Active Directory Domain Services können verwendet werden, um abhängig von den Anspruchsregeln ausgehende Ansprüche zu generieren, die ein AD FS-Administrator konfiguriert hat. Ausgehende Ansprüche werden an vertrauenswürdige Partner gesendet werden, für die ein AD FS-Administrator eine Vertrauensstellung eingerichtet hat. Es werden keine Informationen an Microsoft gesendet.

Verwendung der Informationen

Microsoft greift nicht auf diese Informationen zu. Diese Informationen sind nur für die Verwendung durch den Kunden bestimmt.

Auswahl und Kontrolle

Verwenden Sie AD FS, wenn Sie AD FS Daten sammeln oder an vertrauenswürdige Partner senden soll.

Seitenanfang

IP-Adressverwaltung

Dieses Feature hat folgende Funktion:

Mit IP-Adressverwaltung (IPAM) können Serveradministratoren die IP-Adresse, den Hostname und die Client-ID (z. B. die MAC-Adresse in IPv4 und DUID in IPv6) von Computern und Geräten in einem Netzwerk mit Benutzeranmeldeinformationen nachverfolgen.

Gesammelte, verarbeitete oder übertragene Informationen

Der IPAM-Server sammelt Überwachungsprotokolle und Ereignisse von DHCP-Servern, Domänencontrollern und Netzwerkrichtlinienservern und speichert dann die die IP-Adresse, den Hostnamen, den Clientbezeichner und den Benutzernamen des angemeldeten Benutzers lokal. Ein Serveradministrator kann die gesammelten Protokolle anhand der IP-Adresse, der Client-ID, des Hostnames und des Namens des Benutzers mit der IPAM-Konsole suchen. Diese Informationen werden nicht an Microsoft gesendet.

Verwendung der Informationen

Microsoft greift nicht auf diese Informationen zu. Diese Informationen sind nur für die Verwendung durch den Kunden bestimmt.

Auswahl und Kontrolle

IPAM wird nicht standardmäßig installiert und muss vom Serveradministrator installiert werden. Nachdem IPAM

installiert wurde, wird die IP-Adressenüberwachung automatisch aktiviert. Starten Sie zum Deaktivieren der IP-Adressenüberwachung auf einem Server, auf dem IPAM installiert ist, die Aufgabenplanung auf dem IPAM-Server, suchen Sie "Überwachungsaufgabe" unter Microsoft\Windows\IPAM, und deaktivieren Sie die Aufgabe.

Seitenanfang

Einheitlicher Remotezugriff

Dieses Feature hat folgende Funktion:

Mit einheitlichem Remotezugriff können Remotebenutzer über das Internet eine Verbindung mit einem privaten Netzwerk, z. B. einem Firmennetzwerk, herstellen. Einheitlicher Remotezugriff verwendet DirectAccess, um Remoteclientcomputern unter Windows 8 mit ununterbrochenen und transparenten Verbindungen mit Firmennetzwerken zu versorgen. Die Funktion bietet auch Remote Access Service (RAS), einen herkömmlichen VPN-Dienst mit Verbindung zu lokalen oder anderen Netzwerken.

Gesammelte, verarbeitete oder übertragene Informationen

Zur Benutzerüberwachung beim einheitlichen Remotezugriff speichert der DirectAccess-Server die Details der Remotebenutzer, die eine Verbindung mit dem privaten Netzwerk herstellen. Hierzu gehören Informationen wie der Hostname des Remotebenutzers, der Name des Active Directory-Benutzers und die öffentliche IP-Adresse des Remoteclients (wenn sich der Client hinter einer Netzwerkadressübersetzung (NAT) befindet, wird die öffentliche IP-Adresse gespeichert). Diese Daten können auch auf den internen Windows-Datenbank (WID)-/RADIUS-Servern gespeichert werden, aber nur mit Administratorzustimmung. Nur ein DirectAccess-Administrator (ein Domänenbenutzer mit

einem lokalen Administratorkonto), der auf einen Server zugreift, kann diese Informationen anzeigen.

Verwendung der Informationen

Diese Informationen werden vom Administrator zur Behandlung von Problemen mit der Clientverbindung sowie zur Überwachung und Compliance verwendet werden. Es werden keine Informationen an Microsoft gesendet.

Auswahl und Kontrolle

Die Remoteclientüberwachung ist standardmäßig aktiviert und kann nicht deaktiviert werden. Die Überwachungsdaten werden nur auf den WID/RADIUS-Servern gespeichert, wenn ein Administrator die Kontoführung zur Verwendung dieser Optionen konfiguriert hat. Wenn ein Administrator keine Kontoführung konfiguriert hat, wird keine dieser Informationen gespeichert. Der Administrator kann auch Kontoführung auf einem RAS-Server konfigurieren, damit der Benutzername und die IP-Adresse nicht gespeichert werden.

Seitenanfang

Remotedesktopdienste

Dieses Feature hat folgende Funktion:

Remotedesktopdienste (RDS) bietet eine Plattform, mit der Unternehmen eine zentralisierte Desktopstrategie implementieren, Desktops und Anwendungen verwalten sowie die Flexibilität und Einhaltung verbessern und gleichzeitig die Datensicherheit verbessern kann.

Gesammelte, verarbeitete oder übertragene Informationen

Für die RDS-Benutzerüberwachung speichert der Remotedesktop-Sitzungshostserver Informationen zu Remotebenutzern, die eine Verbindung mit RDS-Ressourcen herstellen. Hierzu gehören Informationen wie

der Hostname des Remotebenutzers, der Name des Active Directory-Benutzers und die öffentliche IP-Adresse des Remoteclients (wenn sich der Client hinter einer Netzwerkadressübersetzung (NAT) befindet, wird die öffentliche IP-Adresse gespeichert). Diese Daten werden automatisch auf den internen Windows-Datenbank (WID)-/SQL-Servern gespeichert, sobald der Benutzer die Verbindung herstellt. Es werden keine Informationen an Microsoft gesendet. Nur Domänenbenutzer mit einem lokalen Administratorkonto können auf diese Informationen zugreifen und sie anzeigen.

Verwendung der Informationen

Diese Informationen werden vom Administrator zur Behandlung von Problemen mit der Clientverbindung sowie zur internen Überwachung und Compliance verwendet werden. Es werden keine Informationen an Microsoft gesendet.

Auswahl und Kontrolle

Die Clientüberwachung ist standardmäßig aktiviert und kann nicht deaktiviert werden. Die Überwachungsinformationen werden auf dem WID/SQL Server gespeichert.

Seitenanfang

Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) und Windows-Fehlerberichterstattung (WER)

Dieses Feature hat folgende Funktion:

Weitere Informationen zu diesen Features finden Sie unter . Features – Ergänzung Registerkarte oder dieses Whitepaper für Administratorenan.

Gesammelte, verarbeitete oder übertragene Informationen

Weitere Informationen zu den Informationen, die von diesem Feature gesammelt, verarbeitet und übertragen von diesen Features finden Sie im CEIP und WER auf der Registerkarte Features – Ergänzung .

Verwendung der Informationen

Informationen darüber, wie wir Informationen verwenden, die von diesem Features gesammelt werden, finden Sie unter CEIP und WER auf der Registerkarte Features – Ergänzung .

Auswahl und Kontrolle

CEIP ist standardmäßig deaktiviert, und WER ist standardmäßig so eingestellt ist, dass Sie vor dem Senden von Absturzberichten an Microsoft eine Aufforderung erhalten. Sie können CEIP über Server-Manager und die Systemsteuerung sowie mit den Steuermethoden der Befehlszeile aktivieren und deaktivieren. WER kann nur über die Befehlszeile gesteuert werden.

Um CEIP über die Systemsteuerung zu aktivieren oder deaktivieren, klicken Sie auf**System und Wartung**. Klicken Sie auf **Problemberichte und -lösungen**. Klicken Sie dann im linken Bereich unter "Siehe auch" auf **Einstellungen zur Verbesserung der Benutzerfreundlichkeit** , um CEIP zu aktivieren oder zu deaktivieren.

Server-Manager-Steuerelemente

Lokaler Server

- CEIP aktivieren
  Öffnen Sie den Server-Manager, und wählen Sie**Lokaler Server**. Klicken Sie auf den Link "Programm zur Verbesserung der Benutzerfreundlichkeit", wählen Sie **Ja, ich möchte am Programm zur Verbesserung der Benutzerfreundlichkeit teilnehmen**im Dialogfeld aus, und klicken Sie auf**„OK“.**

- CEIP deaktivieren
  Öffnen Sie den Server-Manager, und wählen Sie**Lokaler Server**. Klicken Sie auf den Link "Programm zur Verbesserung der

Benutzerfreundlichkeit", und wählen Sie **Nein, ich möchte nicht teilnehmen**im Dialogfeld aus, und klicken Sie auf**„OK".**

- WER aktivieren
  Öffnen Sie den Server-Manager, und wählen Sie**Lokaler Server**. Klicken Sie auf den Link "Windows-Fehlerberichterstattung", wählen Sie **Ja, automatisch Zusammenfassungsberichte senden**, und klicken Sie dann auf **„OK"**an.

- WER deaktivieren
  Öffnen Sie den Server-Manager, und wählen Sie**Lokaler Server**. Klicken Sie auf den Link "Windows-Fehlerberichterstattung", wählen Sie **Ich möchte nicht teilnehmen und auch nicht mehr zur Teilnahme aufgefordert werden**, und klicken Sie dann auf **„OK"**an.

Mehrere Computer

- CEIP aktivieren
  Öffnen Sie den Server-Manager, und wählen Sie**Alle Server**. Wählen Sie in der Kachel "Server" alle Server (STRG+A) aus, klicken Sie mit der rechten Maustaste, und wählen Sie **Automatisches Windows-Feedback konfigurieren** . Wählen Sie auf der Registerkarte "Programm zur Verbesserung der Benutzerfreundlichkeit" **Ja, ich möchte teilnehmen (empfohlen)**. Wenden Sie diese Einstellung auf alle Server an, indem Sie das Kontrollkästchen neben dem Servernamen im Steuerelement "Server auswählen" aktivieren. Klicken Sie dann auf **„OK"**an.

- CEIP deaktivieren
  Öffnen Sie Server-Manager, und wählen Sie "Alle Server". Wählen Sie in der Kachel "Server" alle Server (STRG+A) aus, klicken Sie mit der rechten Maustaste, und wählen Sie **Automatisches**

Windows-Feedback konfigurieren . Wählen Sie auf der Registerkarte "Programm zur Verbesserung der Benutzerfreundlichkeit" **Nein, ich möchte nicht teilnehmen**. Wenden Sie diese Einstellung auf alle Server an, indem Sie das Kontrollkästchen neben dem Servernamen im Steuerelement "Server auswählen" aktivieren. Klicken Sie dann auf **„OK".**

- WER aktivieren
  Öffnen Sie den Server-Manager, und wählen Sie**Alle Server**. Wählen Sie in der Kachel "Server" alle Server (STRG+A) aus, klicken Sie mit der rechten Maustaste, und wählen Sie **Automatisches Windows-Feedback konfigurieren** . Wählen Sie auf der Registerkarte "Windows-Fehlerberichterstattung" **Ja, automatisch Zusammenfassungsberichte senden (empfohlen)**. Wenden Sie diese Einstellung auf alle Server an, indem Sie das Kontrollkästchen neben dem Servernamen im Steuerelement "Server auswählen" aktivieren. Klicken Sie dann auf **„OK"**an.

- WER deaktivieren
  Öffnen Sie den Server-Manager, und wählen Sie**Alle Server**. Wählen Sie in der Kachel "Server" alle Server (STRG+A) aus, klicken Sie mit der rechten Maustaste, und wählen Sie **Automatisches Windows-Feedback konfigurieren** . Wählen Sie auf der Registerkarte "Windows-Fehlerberichterstattung" **Nein, ich möchte nicht teilnehmen**. Wenden Sie diese Einstellung auf alle Server an, indem Sie das Kontrollkästchen neben dem Servernamen im Steuerelement "Server auswählen" aktivieren. Klicken Sie dann auf **„OK"**an.

Seitenanfang