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 8.1 und Windows Server 2012 R2

Letzte Aktualisierung: April 2014

In diesen wichtigsten Punkten der vollständigen Datenschutzbestimmungen für Windows 8.1 und Windows Server 2012 R2 („Windows-Datenschutzbestimmungen") werden einige der Datenerfassungs- und Datennutzungsverfahren von Windows 8.1 und Windows Server 2012 R2 („Windows") in zusammengefasster Form erläutert. Diese Erläuterungen konzentrieren sich auf Onlinefeatures und erheben keinen Anspruch auf Vollständigkeit. Sie gelten nicht für andere Online- oder Offlineinhalte von Microsoft-Websites, -Produkten oder -Diensten.

Diese Datenschutzbestimmungen umfassen folgende Abschnitte:

- **Schwerpunkte** (diese Seite)
- Bestimmungen, die die vollständigen Windows 8.1-Datenschutzbestimmungen darstellen und Links zu Datenschutzbestimmungen für Windows-Features enthalten, für die eigene Datenschutzbestimmungen vorhanden sind.

- Features – Ergänzung: Hier werden die Features beschrieben, die sich auf den Datenschutz in Windows 8.1 und Windows Server 2012 R2 auswirken.

- Apps – Ergänzung: Hier werden die Apps beschrieben, die sich auf den Datenschutz in Windows 8.1 auswirken.

- Server – Ergänzung: Hier werden die zusätzlichen Features beschrieben, die sich auf den Datenschutz in Windows Server 2012 R2 auswirken.

Weitere Informationen dazu, wie Sie Ihren PC, Ihre persönlichen Informationen und Ihre Familie online schützen können, finden Sie im Safety & Security Center.

Ihre Informationen

- Bei bestimmten Features von Windows werden Sie um Ihre Zustimmung zur Erfassung und Verwendung von Informationen auf Ihrem PC gebeten. Hierzu zählen auch persönliche Informationen. Diese Informationen werden von Windows gemäß den Erläuterungen in den vollständigen Windows 8.1-Datenschutzbestimmungenund unter Features – Ergänzung, Apps – Ergänzung und Server – Ergänzungverwendet.

- Einige Features von Windows ermöglichen Ihnen, mit Ihrer Zustimmung, persönliche Informationen über das Internet freizugeben.

- Bei der Registrierung Ihrer Software werden Sie um die Angabe bestimmter persönlicher Informationen gebeten.

- Die Aktivierung von Windows ist erforderlich, um Softwarepiraterie zu verringern und sicherzustellen, dass unsere Kunden die Softwarequalität erhalten, die sie erwarten. Bei der Aktivierung werden einige Informationen über Ihren PC an Microsoft gesendet.

- Wenn Sie sich bei Windows mit einem Microsoft-Konto anmelden, werden Ihre Einstellungen von Windows automatisch geräteübergreifend synchronisiert, und Sie werden bei

bestimmten Apps und Websites automatisch angemeldet. Unter Windows ist zum Zugreifen auf die E-Mail-Dienste oder sozialen Netzwerke von Drittanbietern nicht die Anmeldung mit einem Microsoft-Konto erforderlich. Falls der Drittanbieter jedoch eine App über den Store anbietet, müssen Sie sich beim Store mit einem Microsoft-Konto anmelden, um die App installieren zu können. Bei der Erstellung eines Microsoft-Kontos werden Sie gebeten, einige persönliche Informationen (wie etwa Ihre geografische Region und Ihr Geburtsdatum) anzugeben.

- Zusätzliche Details

Seitenanfang

Ihre Wahlmöglichkeiten

- In Windows haben Sie verschiedene Möglichkeiten, um zu steuern, wie Windows-Features Informationen über das Internet übertragen. Weitere Informationen zum Steuern dieser Features finden Sie unter Features – Ergänzung, Apps – Ergänzung und Server – Ergänzungverwendet.

- Zur Verbesserung der Benutzerfreundlichkeit sind einige Features, die eine Verbindung mit dem Internet herstellen, standardmäßig aktiviert.

- Zusätzliche Details

Seitenanfang

Verwendung der Informationen

- Microsoft nutzt die erfassten Informationen, um die von Ihnen verwendeten Features zu aktivieren und die von Ihnen angeforderten Dienste bereitzustellen. Zudem werden die Informationen verwendet, um Produkte und Dienste von Microsoft zu verbessern. Zur Bereitstellung unserer Dienste geben wir gelegentlich Informationen an andere Firmen weiter, die in unserem Auftrag arbeiten. Zugang zu den Informationen erhalten nur Firmen, die ein geschäftsbedingtes Interesse an der Verwendung der Informationen haben. Diese Firmen sind

verpflichtet, die Informationen vertraulich zu behandeln und zu keinem anderen Zweck zu nutzen.

- Zusätzliche Details

Seitenanfang

So erreichen Sie uns

Weitere Informationen zu unseren Datenschutzrichtlinien finden Sie in den vollständigen Windows 8.1-Datenschutzbestimmungen. Oder schreiben Sie uns über unser Webformularverwendet.

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 8.1 und Windows Server 2012 R2

Auf dieser Seite

Letzte Aktualisierung: April 2014

Diese Datenschutzbestimmungen gelten für Windows 8.1 und Windows Server 2012 R2 ("Windows"). Für bestimmte Komponenten von Windows gelten eigene Datenschutzbestimmungen. Diese finden Sie auch auf dieser Seite. Datenschutzbestimmungen für Software und Dienste in Verbindung mit Windows sowie für ältere Versionen sind ebenfalls hier aufgeführt.

Informationen zu bestimmten Features finden Sie unter Features – Ergänzung, Apps – Ergänzungund unter Server – Ergänzung. Informationen zu Windows Embedded Industry Pro und Windows Embedded Industry Enterprise finden Sie in diesen Datenschutzbestimmungen.

Dies sind Bestimmungen, die sich auf die Features konzentrieren, die mit dem Internet kommunizieren, und die nicht als vollständige Liste zu betrachten sind.

Sammlung und Verwendung Ihrer persönlichen Daten

Die erfassten persönlichen Informationen werden von Microsoft sowie deren Partnern und Tochtergesellschaften zur Aktivierung der Features, zur Bereitstellung der Dienste oder zur Durchführung der Transaktionen verwendet, die Sie angefordert oder in Auftrag gegeben haben. Die Informationen können auch zur Analyse und zur Verbesserung von Microsoft-Produkten und -Diensten verwendet werden.

Mit Ausnahme der in diesen Datenschutzbestimmungen erläuterten Fälle werden die von Ihnen angegebenen persönlichen Informationen nicht ohne Ihre Zustimmung an Dritte weitergeleitet. Microsoft beauftragt von Zeit zu Zeit andere Unternehmen mit bestimmten Dienstleistungen, wie beispielsweise der Durchführung statistischer Analysen seiner Dienste. Diese Unternehmen erhalten von Microsoft ausschließlich diejenigen persönlichen Informationen, die sie für die Erbringung der betreffenden Dienstleistung benötigen, und es ist ihnen strikt untersagt, diese Informationen zu anderen Zwecken zu verwenden.

Microsoft kann auf persönliche Informationen zugreifen oder solche Informationen bereitstellen (einschließlich der Inhalte Ihrer Mitteilungen), um (a) gesetzlichen Bestimmungen oder rechtlichen Forderungen zu genügen oder laufenden Verfahren zu dienen; (b) die Rechte oder das Eigentum von Microsoft oder von Microsoft-Kunden zu schützen, einschließlich der Durchsetzung von Verträgen oder Richtlinien, die Ihre Verwendung der Dienste regeln; oder (c) in der begründeten Annahme zu handeln, dass ein derartiger Zugriff oder eine derartige Offenlegung zum Schutz der persönlichen Sicherheit von Mitarbeitern oder Kunden von Microsoft oder der Öffentlichkeit erforderlich ist.

Informationen, die von Microsoft gesammelt oder von Windows 8.1 an Microsoft gesendet werden, werden möglicherweise in den USA oder anderen Ländern, in denen sich Niederlassungen von Microsoft, deren Partnern, Tochtergesellschaften oder Dienstanbietern befinden,

gespeichert und verarbeitet. Microsoft hält sich an die vom US-Handelsministerium dargelegten Safe-Harbor-Regeln bezüglich der Sammlung, Nutzung und Speicherung von Daten aus der Europäischen Union, dem Europäischen Wirtschaftsraum und der Schweiz.

Seitenanfang

Erfassung und Verwendung von Informationen über Ihren Computer

Wenn Sie Software mit internetfähigen Features verwenden, werden Informationen zu Ihrem Computer ("Standardcomputerinformationen") an von Ihnen besuchte Websites und von Ihnen verwendete Onlinedienste gesendet. Zu den Standardcomputerinformationen gehören im Allgemeinen Informationen wie die IP-Adresse, Betriebssystemversion, Browserversion sowie Regions- und Spracheinstellungen. In einigen Fällen können die Computerinformationen außerdem eine Hardware-ID beinhalten, die den Gerätehersteller, den Gerätenamen und die Geräteversion angibt. Wenn ein bestimmtes Feature oder ein Dienst Informationen an Microsoft sendet, werden auch Standardcomputerinformationen gesendet.

Informationen dazu, welche weiteren Informationen erfasst und wie diese verwendet werden, finden Sie in den Datenschutzdetails des jeweiligen Windows-Features unter "Features – Ergänzung", unter "Server – Ergänzung" sowie unter den anderen aufgeführten Features auf dieser Seite.

Administratoren können mithilfe von Gruppenrichtlinien zahlreiche Einstellungen für die hier beschriebenen Features ändern. Weitere Informationen finden Sie in diesem Whitepaper für Administratoren.

Seitenanfang

Sicherheit Ihrer Informationen

Microsoft tritt für den bestmöglichen Schutz der Sicherheit Ihrer Daten ein. Microsoft setzt eine Vielzahl an

Sicherheitstechnologien und -verfahren ein, um Ihre persönlichen Informationen vor unbefugtem Zugriff, unzulässiger Nutzung oder Offenlegung zu schützen. Zum Beispiel werden Ihre Daten auf Computersystemen an kontrollierten Standorten gespeichert, für die nur wenige Personen Zugriffsberechtigung besitzen. Streng vertrauliche Informationen (wie Kreditkartennummern oder Kennwörter), die über das Internet übertragen werden, schützt Microsoft darüber hinaus durch Verschlüsselung, z. B. mit dem Secure-Socket-Layer-Protokoll (SSL-Protokoll).

Seitenanfang

Änderungen an diesen Datenschutzbestimmungen

Diese Datenschutzbestimmungen werden von Zeit zu Zeit aktualisiert, um Änderungen an Produkten und Diensten sowie Feedback von Kunden zu berücksichtigen. In diesem Fall wird das Datum der letzten Aktualisierung am Anfang dieser Seite geändert. Bei grundlegenden Änderungen oder bei Änderungen in Bezug auf die Verwendung Ihrer persönlichen Informationen durch Microsoft wird entweder vor der Implementierung dieser Änderungen an hervorgehobener Stelle ein Hinweis angezeigt, oder Sie erhalten von Microsoft eine direkte Benachrichtigung. Sie sollten daher diese Datenschutzbestimmungen regelmäßig überprüfen, damit Sie im Hinblick auf den Schutz Ihrer persönlichen Daten durch Microsoft stets auf dem neusten Stand sind.

Seitenanfang

Weitere Informationen

Microsoft legt großen Wert auf Kommentare Ihrerseits bezüglich dieser Datenschutzbestimmungen. Wenn Sie Fragen zu diesen Datenschutzbestimmungen haben oder der Meinung sind, dass dagegen verstoßen wurde, können Sie uns über unser Webformular.

Microsoft Privacy
Microsoft Corporation

One Microsoft Way
Redmond, Washington 98052
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 8.1 und Windows Server 2012 R2

Auf dieser Seite

Letzte Aktualisierung: April 2014

Diese Seite ist eine Ergänzung der Datenschutzbestimmungen für Windows 8.1 und Windows Server 2012 R2 ("Windows-Datenschutzbestimmungen") und umfasst folgende Abschnitte:

- Schwerpunkte
- Die Bestimmungen: Diese enthalten die vollständigen Windows 8.1-Datenschutzbestimmungen sowie Links zu Datenschutzbestimmungen für Windows-Features, für die eigene Datenschutzbestimmungen vorhanden sind.
- **Features – Ergänzung** (diese Seite): Hier werden die Features beschrieben, die Auswirkungen auf den Datenschutz in Windows 8.1 und Windows Server 2012 R2 haben.
- Apps – Ergänzung: Hier werden die Apps beschrieben,

DirectAccess

Center für erleichterte Bedienung

Ereignisanzeige

Family Safety

Fax

Handschriftanpassung – Automatisches Lernen

Heimnetzgruppe

Eingabemethoden-Editor (Input Method Editor, IME)

Gemeinsame Nutzung der Internetverbindung

Internetdrucken

Spracheinstellungen

Positionsdienste

Verwalten von Anmeldeinformationen

Name und Profilbild

Netzwerkinformationen

Benachrichtigungen, Sperrbildschirm-Apps und Kachelupdates

Abzüge bestellen

Vorabruf und Vorabstart

Programmkompatibilitäts-Assistent

Eigenschaften

die sich auf den Datenschutz in Windows 8.1 auswirken.

- Server – Ergänzung: Hier werden die zusätzlichen Features beschrieben, die sich auf den Datenschutz in Windows Server 2012 R2 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

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 der Hardware oder der Software des PCs muss Windows möglicherweise erneut aktiviert werden. Bei der Aktivierung können Aktivierungsexploits (Software, die die Microsoft-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

Im Zuge der Aktivierung werden folgende Informationen an Microsoft gesendet:

- Der Microsoft-Produktcode (ein fünfstelliger Code zur Identifizierung des Windows-Produkts, das Sie aktivieren).

Näherung

RAS-Verbindungen

RemoteApp- und Desktopverbindungen

Remotedesktopverbindung

Anmelden mit einem Microsoft-Konto

OneDrive-Cloudspeicher

Synchronisierungseinstellungen

Teredo-Technologie

Trusted Platform Module (TPM)-Dienste

Aktualisierung von Stammzertifikaten

Update Services

Virtuelles privates Netzwerk

Windows-Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP)

Windows Defender

Windows-Fehlerberichterstattung

Windows-Dateizuordnung

Windows-Hilfe

Remoteunterstützung

Windows Search

Windows Setup

Windows-Freigabe

Windows SmartScreen

- Eine Kanal-ID oder ein Standortcode, der angibt, wie Sie das Windows-Produkt ursprünglich erhalten haben. Die 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 Informationen zu eventuellen Aktivierungsexploits und Schadsoftware oder nicht autorisierter 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.

Windows-Spracherkennung

Windows Store

Windows-Zeitdienst

Windows-Problembehandlung

Arbeitsordner

Arbeitsplatz

- 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. Außerdem werden PC-Standardinformationen gesendet.

- Wenn Sie eine Windows-Version mit Volumenlizenzierung verwenden, für die ein Aktivierungsserver genutzt wird, wird die IP-Adresse dieses Servers möglicherweise an Microsoft. gesendet.

Verwendung der 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. Mithilfe von Lizenzserverinformationen wird sichergestellt, dass von Lizenzservern die Bestimmungen des Lizenzvertrags eingehalten werden.

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

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 der 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

Werbungs-ID

Funktionsweise

Windows gewährt Apps Zugriff auf einen eindeutigen Bezeichner für jeden Benutzer eines Geräts, um relevantere Werbung bereitzustellen. Sie können diesen Bezeichner jederzeit zurücksetzen oder den Zugriff deaktivieren.

Gesammelte, verarbeitete und übertragene Informationen

Wenn Sie Apps Zugriff auf die Werbungs-ID gewähren, stellt Windows diese allen Apps zur Verfügung, die sie anfordern. Die entsprechenden Informationen werden von Apps möglicherweise gespeichert oder übertragen.

Verwendung der Informationen

Der Werbungs-ID wird von App-Entwicklern und Werbenetzwerken verwendet, um relevantere Werbung bereitzustellen. Hierzu wird ermittelt, welche Apps Sie verwenden bzw. wie Sie diese verwenden. Sie kann von den App-Entwicklern auch zur Verbesserung der Servicequalität verwendet werden, da sie mit ihrer Hilfe die Häufigkeit und Wirksamkeit der Werbung beurteilen sowie Betrugsversuche und Sicherheitsprobleme erkennen können.

Wenn Sie Apps Zugriff auf die Werbungs-ID gewähren, unterliegt die jegliche Verwendung der ID den Datenschutzpraktiken der jeweiligen App.

Auswahl und Steuerung

Wenn Sie beim Einrichten von Windows die Express-Einstellungen auswählen, gewährt Windows Apps Zugriff auf Ihre Werbungs-ID. Wenn Sie sich für das Anpassen der Einstellungen entscheiden, können Sie den Zugriff auf Ihre Werbungs-ID unter **Infos mit Microsoft und anderen Diensten teilen** mithilfe der Option **Apps die Verwendung**

der Werbungs-ID für App-übergreifende Erlebnisse erlauben steuern. Nach dem Einrichten von Windows können Sie diese Einstellung in den PC-Einstellungen unter **Datenschutz** ändern. Wenn Sie diese Einstellung deaktivieren, wird die Werbungs-ID nicht an Apps gesendet, die diese anfordern. Wenn Sie die Einstellung wieder aktivieren, wird eine neue ID erstellt.

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 können bestimmen, welche Informationen erfasst, wie lange sie gespeichert und ob sie an Dritte weitergegeben 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 der Informationen

Administratoren bestimmen auch, 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

Biometrie

Funktionsweise

Wenn Ihr PC über einen Fingerabdruckleser verfügt, können Sie sich per Fingerabdruck an Windows anmelden und sich bei Apps identifizieren, die dieses Feature unterstützen.

Gesammelte, verarbeitete und übertragene Informationen

Wenn Sie einen neuen Fingerabdruck einrichten, werden die Ablesungen Ihres Fingerabdrucks lokal auf dem PC gespeichert. Es werden keine Informationen an Microsoft gesendet. Wenn Sie Ihren Fingerabdruck zum Identifizieren bei einer App verwenden, wird der Fingerabdruck von Windows mit den auf dem PC gespeicherten Fingerabdrücken verglichen. Der App wird dann mitgeteilt, ob der gescannte Fingerabdruck mit einem Fingerabdruck übereinstimmt, der Ihrem Konto zugeordnet ist. Die Daten des gescannten Fingerabdrucks werden von Windows nicht für die App bereitgestellt.

Verwendung der Informationen

Von Windows werden die Fingerabdruckinformationen, die Sie auf dem PC speichern, zum Anmelden an Windows per Fingerabdruck verwendet.

Auswahl und Steuerung

Sie können Fingerabdrücke in den PC-Einstellungen unter **Konten** mithilfe der Option **Anmeldeoptionen** hinzufügen oder entfernen.

Seitenanfang

BitLocker-Laufwerkverschlüsselung

Funktionsweise

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 MicrosoftOneDrive 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 der 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.

Sie können die in Ihrem OneDrive-Konto gesicherten Wiederherstellungsschlüssel anzeigen und verwalten.

Seitenanfang

Kontakte

Funktionsweise

Wenn Sie zum Verwalten Ihrer Kontakte die Kontakte-App oder eine unterstützte Drittanbieter-App verwenden, können Sie festlegen, dass bestimmte Kontakte für andere Apps auf dem PC freigegeben werden, Kontaktinformationen auf einer Visitenkarte anzeigen oder bestimmte Kontaktinformationen für andere Apps auf dem PC zum Ausführen einer Aktion, z. B. Tätigen eines Anrufs oder Zuordnen einer Adresse, freigeben.

Gesammelte, verarbeitete, gespeicherte und übertragene Informationen

Wenn von einer App Kontaktinformationen angefordert werden, ermöglicht Windows das Auswählen bestimmter Kontakte zur Freigabe für die App. Die Kontakte können aus der Kontakte-App oder einer unterstützten Drittanbieter-App stammen. Windows gibt nicht die gesamte Liste Ihrer Kontakte für die anfordernde App frei.

Hat eine App Zugriff auf eine bestimmte Information eines Kontakts, z. B. die Telefonnummer oder E-Mail-Adresse, kann von Windows eine Visitenkarte mit den zusätzlichen Informationen aus der Kontakte-App für diesen Kontakt angezeigt werden. Von Windows werden die zusätzlichen Kontaktinformationen nicht für die App freigegeben, die die Visitenkarte anzeigt.

Wenn Sie auf der Visitenkarte auf einen Befehl wie **Anrufen**, **E-Mail** oder **Zuordnen** tippen oder klicken, wird von Windows die entsprechende App zum Ausführen der Aktion geöffnet. Außerdem werden der App die zum Ausführen der Aktion notwendigen Kontaktdetails (z. B. die Telefonnummer für einen Anruf) zur Verfügung gestellt.

Verwendung der Informationen

Von Windows werden die Kontaktinformationen aus Ihrer Kontakte-App verwendet, um bestimmte ausgewählte Kontakte freizugeben, Visitenkarten anzuzeigen, Apps zu öffnen und auf den Visitenkarten aufgeführte Kontaktinformationen zum Ausführen von Aktionen freizugeben sowie Ihre Kontakte in Windows Search anzuzeigen. Die Verwendung der Informationen zu Ihren Kontakten durch die Kontakte-App wird in den Datenschutzbestimmungen der Kommunikations-Apps beschrieben.

Bei der Freigabe von Kontaktinformationen für Drittanbieter-Apps unterliegt die Verwendung der Informationen den Datenschutzpraktiken des Drittanbieters. Wenn Sie Kontaktinformationen für eine Microsoft-App freigeben, werden die Datenschutzpraktiken der App in den zugehörigen Datenschutzbestimmungen erläutert.

Auswahl und Steuerung

Von Windows werden Kontaktinformationen nur angezeigt und freigegeben, wenn Sie festlegen, dass bestimmte Kontakte für eine App freigegeben oder Visitenkarten angezeigt werden sollen, oder eine Aktion auf der Visitenkarte auswählen.

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

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 eine App, die eine optimale Nutzung der Funktionen des Geräts und eine höhere Benutzerfreundlichkeit ermöglicht. 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 wird von Windows eine Onlineverbindung mit dem Windows Update-Dienst hergestellt, um Gerätetreiber zu suchen und herunterzuladen, falls auf dem PC nicht bereits ein geeigneter Treiber verfügbar ist. Weitere Informationen zu den von Windows Update gesammelten Informationen und ihrer Verwendung finden Sie in den Update Services-Datenschutzbestimmungen.

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 eine App für das Gerät verfügbar ist, wird diese von Windows automatisch aus dem Windows Store heruntergeladen und installiert. Die App steht in Ihrem Windows Store-Konto in der Liste der Ihnen gehörenden Apps zur Verfügung.

Verwendung der 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 gesendeten Informationen nicht dazu, Sie zu identifizieren oder Kontakt mit Ihnen aufzunehmen.

Auswahl und Steuerung

Wenn Sie beim Einrichten von Windows die Express-Einstellungen auswählen, aktivieren Sie dadurch das automatische Herunterladen und Installieren von Gerätetreibern, Geräteinformationen und Geräte-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 **PC schützen und aktualisieren** 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** auswählen.

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

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 der 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

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 der 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

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 den Bluetooth-Einstellungen die Option **Bluetooth-Geräte können diesen Computer ermitteln** aktivieren, überträgt Windows den Namen Ihres PC per Bluetooth, damit Bluetooth-fähige Geräte Ihren PC finden und identifizieren können.

Wenn Sie in den PC-Einstellungen unter "Geräte" die Option **Gerät hinzufügen** aktivieren, überträgt Windows den Namen Ihres PCs über WLAN, damit Wi-Fi Direct-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 der Informationen

Windows überträgt den Namen Ihres PCs, 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 PCs beim Hinzufügen von Geräten nicht per WLAN übertragen soll, können Sie das WLAN vor dem Hinzufügen eines Geräts in den PC-Einstellungen unter "Drahtlos" vorübergehend deaktivieren.

Seitenanfang

Geräteverschlüsselung

Funktionsweise

Die Geräteverschlüsselung schützt Ihre Daten durch Verschlüsselung mithilfe der BitLocker-Laufwerkverschlüsselungstechnologie und kann so Offlinesoftwareangriffe verhindern. Bei aktivierter Geräteverschlüsselung werden die Daten von Windows auf dem Laufwerk, auf dem Windows installiert ist, verschlüsselt.

Gesammelte, verarbeitete und übertragene

Informationen

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

Windows verwendet auf Ihrem PC das Trusted Platform Module (TPM) zum Speichern und Verwalten der kryptografischen Schlüssel für die Verschlüsselung Ihres Laufwerks. Bei aktivierter Geräteverschlüsselung verschlüsselt Windows automatisch das Laufwerk, auf dem Windows installiert ist, und generiert einen Wiederherstellungsschlüssel. Der Wiederherstellungsschlüssel kann Ihnen im Fall von bestimmten Hardwarefehlern oder anderen Problemen den Zugriff auf Ihre geschützten Daten ermöglichen.

Der BitLocker-Wiederherstellungsschlüssel für Ihren PC wird automatisch online im MicrosoftOneDrive-Konto der einzelnen Administratorkonten gesichert, die mit einem Microsoft-Konto verbunden sind. Im gleichen OneDrive-Konto werden auch Ihr Computername und ein Bezeichner für den Wiederherstellungsschlüssel gesichert. Aus Datenschutzgründen werden die gesendeten Informationen durch SSL verschlüsselt.

Verwendung der Informationen

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

Ihre Wiederherstellungsinformationen werden von Microsoft in Ihrem OneDrive-Konto gesichert, damit Sie jederzeit online

darauf zugreifen können. Die Informationen zum Wiederherstellungsschlüssel werden von uns nicht verwendet oder an einem anderen Ort als Ihrem OneDrive-Konto gespeichert. Aggregierte Daten zu den Wiederherstellungsschlüsseln können von uns zum Analysieren von Trends sowie zum Verbessern unserer Produkte und Dienste verwendet werden. Beispielsweise verwenden wir diese Informationen möglicherweise, um die Anzahl der PCs mit aktivierter Geräteverschlüsselung zu ermitteln.

Auswahl und Steuerung

Wenn Sie sich bei der Einrichtung Ihres PCs für die Verwendung eines Microsoft-Kontos entscheiden, wird die Geräteverschlüsselung aktiviert, falls sie von Ihrem PC unterstützt wird, und Ihr Wiederherstellungsschlüssel wird in Ihrem OneDrive-Konto gesichert. Entscheiden Sie sich bei der Einrichtung Ihres PCs für ein lokales Konto, wird die Geräteverschlüsselung nicht aktiviert.

Wenn Sie später ein Microsoft-Konto mit einem Administratorkonto auf Ihrem PC verbinden:

- Ist die Geräteverschlüsselung noch nicht aktiviert, wird sie von Windows automatisch aktiviert, und die Wiederherstellungsinformationen werden im OneDrive-Konto des jeweiligen Benutzers gesichert.
- Ist die Geräteverschlüsselung bereits aktiviert, werden die Wiederherstellungsinformationen für Ihren PC im OneDrive-Konto des jeweiligen Benutzers gesichert.

Sie können die in Ihrem OneDrive-Konto gesicherten Wiederherstellungsschlüssel hier anzeigen und verwalten.

Seitenanfang

DirectAccess

Funktionsweise

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 Websites, die Sie besuchen, wenn Sie sich nicht am Arbeitsplatz befinden.

DirectAccess sendet keine Informationen an Microsoft.

Verwendung der 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

Center für erleichterte Bedienung

Funktionsweise

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:

- Auf dem Fernsehgerät kann ich Bilder oder Text häufig nicht deutlich 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 der 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 PCs für niemanden zugänglich.

Auswahl und Steuerung

Sie können die gewünschten Aussagen in der Systemsteuerung unter "Erleichterte Bedienung" auswählen. Sie können die Auswahl jederzeit ändern. Außerdem können Sie die Empfehlungen auswählen, die Sie auf Ihrem PC konfigurieren möchten.

Seitenanfang

Ereignisanzeige

Funktionsweise

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 der 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 des Ereignisprotokolls" um Ihre Zustimmung gebeten, dass die angezeigten Informationen über das Internet gesendet werden. Ohne Ihre Zustimmung werden keine Ereignisprotokollinformationen über das Internet gesendet. Administratoren können die Website, an die Ereignisinformationen gesendet werden, mithilfe der Gruppenrichtlinie auswählen oder ändern.

Seitenanfang

Family Safety

Funktionsweise

Family Safety ermöglicht es Eltern, ihre Kinder bei der Nutzung eines PCs zu schützen. Eltern können festlegen, welche Apps, Spiele und Websites 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-Website 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 Websites (auch zu Versuchen, geblockte Websites 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-Website ändern. Eltern können anderen Personen erlauben, Aktivitätsberichte anzuzeigen und Einstellungen zu ändern, indem sie diese Personen auf der Microsoft Family Safety-Website 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 der Informationen

Die gesammelten Informationen werden von Windows und der Microsoft Family Safety-Website 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-Website hinzugefügt oder entfernt werden. Ein Benutzer, der auf der Website 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

Das Faxfeature ermöglicht Ihnen das Erstellen und Speichern von Faxdeckblättern sowie das Senden und Empfangen von Faxnachrichten 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 der 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 gesendeten und empfangenen Faxdokumente anzeigen und die Faxeinstellungen konfigurieren, beispielsweise wer berechtigt ist, Faxe anzuzeigen oder zu verwalten, sowie die Absender-ID und die Empfänger-ID.

Seitenanfang

Handschriftanpassung – Automatisches Lernen

Funktionsweise

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 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 Bildschirmtastaturen.
- Alternative Zeichen, die Sie zur Korrektur von erkanntem Text auswählen.

Verwendung der 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 Handschrifterkennung für jeden Benutzer eines PCs 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

Unter Windows können Sie PCs in Ihrem Heimnetzwerk mühelos verbinden, um Bilder, Musik, Videos, Dokumente und Dienste freizugeben. 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 der 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 **Netzwerk** die Option **Heimnetzgruppe** wählen,

um eine Heimnetzgruppe zu erstellen und ihre Einstellungen zu verwalten.

Seitenanfang

Eingabemethoden-Editor (Input Method Editor, IME)

Eingabemethoden-Editoren (IMEs) von Microsoft 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.

Cloud-IME-Kandidaten

Funktionsweise

Bei der Eingabe von Zeichen für vereinfachtes Chinesisch mit dem Microsoft Pinyin-IME kann der IME unter Verwendung eines Onlinediensts Kandidatenideogramme für die typisierte Eingabe nachschlagen, die nicht in einem lokalen Wörterbuch auf Ihrem PC vorhanden ist.

Gesammelte, verarbeitete und übertragene Informationen

Bei der Eingabe von Zeichen für vereinfachtes Chinesisch mit dem Microsoft Pinyin-IME schlägt der IME Ideogramme vor, die Sie möglicherweise verwenden möchten. Findet der IME keinen geeigneten Vorschlag im lokalen Wörterbuch, sendet er die Tastatureingabe an Microsoft, um zu ermitteln, ob bessere Kandidatenideogramme für diese Eingabe vorhanden sind. Ist dies der Fall, werden sie in der Liste der Kandidaten angezeigt und bei ihrer Auswahl dem lokalen Wörterbuch hinzugefügt. Zusätzlich wird ein zufällig generierter eindeutiger Bezeichner gesendet, um eine Analyse der Verwendung dieses Features zu ermöglichen. Der Bezeichner ist nicht mit Ihrem Microsoft-Konto verknüpft und wird nicht dazu verwendet, Sie zu identifizieren, Kontakt mit Ihnen aufzunehmen oder gezielte Werbung zu schalten.

Verwendung der Informationen

Microsoft verwendet die erfassten Informationen dazu, Cloud-Ideogramme nachzuschlagen und seine 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

Cloud-IME-Kandidaten sind für den Microsoft Pinyin-IME für vereinfachtes Chinesisch standardmäßig deaktiviert. Öffnen Sie zum Anzeigen oder Ändern dieser Einstellung die PC-Einstellungen, und klicken Sie auf **Zeit und Sprache** und **Region und Sprache**. Wählen Sie Ihre Sprache aus, und klicken Sie dann auf **Optionen**.

IME – Automatische Abstimmung und Vorhersage

Funktionsweise

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 der 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

Die Features für automatisches Lernen und Wortvorschläge in den IMEs, von denen sie unterstützt werden, sind 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

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 der Informationen

Microsoft verwendet die Informationen, um seine 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

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 der Informationen

Microsoft verwendet die Informationen, um seine 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

Gemeinsame Nutzung der Internetverbindung

Funktionsweise

Mithilfe der gemeinsamen Nutzung der Internetverbindung können Sie Ihre mobile Breitband-Internetverbindung per WLAN für andere Geräte bereitstellen. Außerdem können Sie die gemeinsame Nutzung der Internetverbindung auf Ihrem Gerät mit mobiler Breitbandverbindung auch remote vom PC aus starten, wenn Sie sich jeweils mit demselben Microsoft-Konto angemeldet haben.

Gesammelte, verarbeitete und übertragene Informationen

Wenn Sie Ihre Internetverbindung zum ersten Mal für die gemeinsame Nutzung freigeben, wird von Windows automatisch ein Netzwerkname und ein Kennwort generiert und gespeichert. Sie können diese Angaben jederzeit ändern.

Wenn Ihr PC diese Funktion unterstützt und Sie den PC dem Microsoft-Konto als vertrauenswürdiges Gerät hinzugefügt haben, werden der Netzwerkname und das Kennwort von Windows mit Ihrem Microsoft-Konto synchronisiert. Außerdem werden von Windows weitere Informationen synchronisiert, damit Sie die gemeinsame Nutzung der Internetverbindung auch von Ihren anderen vertrauenswürdigen Geräten aus remote starten können. Zu diesen Informationen gehören auch die Hardwareadresse Ihres Bluetooth-Geräts und eine Zufallszahl zum Schützen der Verbindung.

Verwendung der Informationen

Diese Informationen werden zum Einrichten der gemeinsamen Nutzung der Internetverbindung verwendet. Microsoft verwendet die Informationen nicht dazu, Sie zu identifizieren, Kontakt mit Ihnen aufzunehmen oder gezielte Werbung zu schalten.

Auswahl und Steuerung

Wenn Sie sich an einem Gerät anmelden, von dem die gemeinsame Nutzung der Internetverbindung mit Ihrem Microsoft-Konto unterstützt wird, und Sie das Gerät als vertrauenswürdiges Gerät hinzufügen, werden die Informationen, die für den Remotestart der gemeinsamen Nutzung der Internetverbindung erforderlich sind, mit OneDrive synchronisiert. Sie können die Synchronisierung der Informationen beenden, indem Sie das Synchronisieren von Kennwörtern deaktivieren. Weitere Informationen finden Sie auf dieser Seite im Abschnitt "Synchronisierungseinstellungen".

Seitenanfang

Internetdrucken

Funktionsweise

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 der 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 die Option **Programme und Funktionen** öffnen und dann **Windows-Features aktivieren oder deaktivieren** auswählen.

Seitenanfang

Spracheinstellungen

Funktionsweise dieses Features

Sie können die bevorzugten Sprachen der Sprachenliste in Windows 8.1 hinzufügen. Apps und Websites werden in der ersten Sprache angezeigt, die in dieser Liste verfügbar ist.

Gesammelte, verarbeitete und übertragene Informationen

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

Verwendung der Informationen

Ihre Liste der bevorzugten Sprachen wird von Microsoft-Websites 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 Drittanbieterwebsites und Apps gesendeten oder verwendeten Sprachinformationen unterliegen den Datenschutzbestimmungen der

Drittanbieterwebsite oder des App-Herausgebers.

Auswahl und Steuerung

Ihre Liste der bevorzugten Sprachen steht den Apps, die Sie installieren, und den Websites, 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 Websites gesendet.

Seitenanfang

Positionsdienste

Bei den Windows-Positionsdiensten können Sie angeben, welche Apps, Websites und Windows-Features zum Bestimmen des Standorts Ihres PCs verwendet werden dürfen. Die Windows-Positionsdienste bestehen aus zwei Komponenten. Die Windows-Positionssuche stellt eine Verbindung mit einem Microsoft-Onlinedienst her, um Ihren Standort zu bestimmen. Von der Plattform für Windows-Position wird der Standort des PCs mithilfe von Hardware (z. B. einem GPS-Sensor) oder von Software (z. B. der Windows-Positionssuche) ermittelt.

Plattform für Windows-Position

Funktionsweise

Wenn Sie die Plattform für Windows-Position aktivieren, werden Sie möglicherweise von aus dem Windows Store installierten Apps und einigen Windows-Features gefragt, ob Sie die Ermittlung der Position Ihres PCs zulassen. Falls Sie die Nutzung Ihrer Position für eine App zulassen, kann Ihre Position während der Nutzung der App angegeben werden. Außerdem kann von der Plattform für Windows-Position eine Information an die App gesendet werden, wenn Sie sich mit Ihrem PC in einen von der App definierten geografischen Bereich bewegen (bzw. den Bereich verlassen). Beispielsweise

können Sie in einer App möglicherweise eine Erinnerung einrichten, die Sie an das Einkaufen von Lebensmitteln nach der Arbeit erinnert. Abhängig von der Systemkonfiguration kann die Position des PCs von der Plattform für Windows-Position mithilfe von Hardware (z. B. einem GPS-Sensor) oder von Software (z. B. der Windows-Positionssuche) ermittelt werden.

Die Plattform für Windows-Position verhindert nicht, dass Apps die Position Ihres PCs auf andere Weise ermitteln. Sie können z. B. Geräte installieren (z. B. einen GPS-Empfänger), die Positionsinformationen direkt an eine App senden und die Plattform 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 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 diese von der Plattform für Windows-Position zum Ermitteln der PC-Position aufgefordert werden. Apps, Websites und Features, die die Position Ihres PCs mithilfe der Plattform ermitteln dürfen, können diese Informationen auch übertragen oder speichern. Wenn von einer App ein überwachter geografischer Bereich eingerichtet wird, werden die Daten des Bereichs in verschlüsselter Form auf Ihrem PC gespeichert. Diese Daten enthalten einen Namen, eine Position und die Angabe, ob sich der PC bei der letzten Ermittlung der Position innerhalb oder außerhalb des Bereichs befunden hat. Von Apps, von denen geografische Bereiche eingerichtet werden, werden diese Informationen möglicherweise übertragen oder gespeichert.

Verwendung der Informationen

Wenn Sie die Plattform für Windows-Position aktivieren, können autorisierte Apps, Websites und Windows-Features auf

die Position Ihres PCs zugreifen und diese verwenden, um personalisierte Inhalte für Sie anzuzeigen. 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 sich für das Anpassen der Einstellungen entscheiden, können Sie die Plattform für Windows-Position steuern. Wählen Sie unter "Infos mit Microsoft und anderen Diensten teilen" die Option "Windows und Apps das Anfordern meines Standorts von der Plattform für Windows-Position erlauben". Wenn eine Store-App zum ersten Mal die Position Ihres PCs anfordert, werden Sie von Windows gefragt, ob Sie die Nutzung Ihrer Position durch die App zulassen möchten. Sie können diese Einstellung für jede Store-App über den Charm "Einstellungen" unter "Berechtigungen" anzeigen und ändern.

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 Apps in den PC-Einstellungen unter **Datenschutz** steuern. Administratoren können außerdem die Plattform in der Systemsteuerung unter **Standorteinstellungen** für alle Benutzer deaktivieren. Um zu verhindern, dass Apps beim Durchqueren der von ihnen definierten geografischen Bereiche informiert werden, kann ein Benutzer mit Administratorrechten in der Systemsteuerung den Windows-Positionsdienst deaktivieren.

Windows-Positionssuche

Funktionsweise

Die Windows-Positionssuche stellt eine Verbindung mit dem online verfügbaren Microsoft-Positionsdienst her. Damit kann der ungefähre Standort Ihres PCs anhand von Informationen zu WLANs in der Nähe des PCs sowie anhand der IP-Adresse Ihres 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) dazu, die aktuelle Position Ihres PCs zu ermitteln. Von der Windows-Positionssuche wird zuerst überprüft, ob eine Liste mit in der Nähe befindlichen WLAN-Zugriffspunkten vorhanden ist, die bei einer vorherigen Anforderung durch eine App mit Positionserkennung gespeichert wurde. Falls die Windows-Positionssuche noch nicht über eine Liste mit in der Nähe befindlichen WLAN-Zugriffspunkten verfügt oder die Liste veraltet ist, werden vom Anbieter Informationen zu WLAN-Zugriffspunkten in der Nähe sowie gegebenenfalls GPS-Informationen an den Microsoft-Positionsdienst gesendet. Der Dienst gibt die ungefähre Position Ihres PCs an die Positionssuche zurück. Diese gibt die Position an die Plattform für Windows-Position weiter, sodass sie für die anfordernde App verfügbar gemacht werden kann. Von der Windows-Positionssuche wird gegebenenfalls auch die gespeicherte Liste mit den WLAN-Zugriffspunkten aktualisiert. 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 WLAN-Zugriffspunkte zählen die BSSID (MAC-Adresse des WLAN-Zugriffspunkts) 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 WLAN-Besitzern zu gewährleisten, werden von Windows keine Informationen zu SSIDs (Namen von WLAN-Zugriffspunkten) oder ausgeblendeten WLANs gesendet. Aus Datenschutz- und Sicherheitsgründen werden über WLAN gesendete Informationen per SSL verschlüsselt.

Wenn Sie sich dafür entscheiden, zur Verbesserung des Microsoft-Positionsdiensts beizutragen, werden von Windows möglicherweise erneut Informationen zu in der Nähe befindlichen WLAN-Zugriffspunkten an Microsoft gesendet, nachdem von einer App der Standort Ihres PCs angefordert wurde. Wenn Sie eine getaktete Internetverbindung verwenden, wird von Windows die Häufigkeit begrenzt, mit der diese Informationen gesendet werden, um die Nutzung Ihrer Internetverbindung möglichst gering zu halten.

Verwendung der Informationen

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

Wenn Sie sich dafür entscheiden, zur Verbesserung des Microsoft-Positionsdiensts beizutragen, werden die an Microsoft gesendeten WLAN- 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 mit 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 zwischengespeicherte Liste mit in der Nähe befindlichen WLAN-Zugriffspunkten, die von der Windows-Positionssuche verschlüsselt und gespeichert werden, 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 sich für das Anpassen der Einstellungen entscheiden, können Sie steuern, ob Sie bei der Verbesserung des Microsoft-Positionsdiensts mithelfen möchten. Wählen Sie dazu unter **Verbesserung der Produkte und Dienste von Microsoft unterstützen** die Option **Bestimmte Positionsdaten an Microsoft senden, wenn standortbezogene Apps verwendet werden** aus. 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.

Die Windows-Positionssuche kann in der Systemsteuerung unter **Windows-Funktionen aktivieren oder deaktivieren** aktiviert und deaktiviert werden. Wenn Sie die Windows-Positionssuche deaktivieren, können Sie weiterhin andere Positionssuchdienste (z. B. GPS) mit der Plattform für Windows-Position verwenden.

Seitenanfang

Verwalten von Anmeldeinformationen

Funktionsweise

Unter Windows können Sie Windows Store-Apps mit Konten

verbinden, die Sie für Websites verwenden. Wenn Sie in Internet Explorer bereits ein Kennwort für eine Website gespeichert haben, kann das gespeicherte Kennwort von Windows beim Verbinden einer App mit dieser Website verwendet werden.

Gesammelte, verarbeitete und übertragene Informationen

Wenn eine App Anmeldeinformationen zum Anmelden an einer Website anfordert, können Sie angeben, ob die Anmeldeinformationen gespeichert werden sollen. Wenn Sie sich bereits in Internet Explorer an der Website angemeldet haben und das Speichern der Anmeldeinformationen zugelassen haben, werden die gespeicherten Anmeldeinformationen von Windows automatisch eingefügt. Die Anmeldeinformationen werden in verschlüsselter Form auf dem PC gespeichert. Weitere Informationen dazu, wie diese und andere Anmeldeinformationen mit OneDrive synchronisiert werden können, finden Sie auf dieser Seite im Abschnitt "Synchronisierungseinstellungen".

Verwendung der Informationen

Von Windows werden die gespeicherten Anmeldeinformationen nur genutzt, um Ihnen die Anmeldung bei den ausgewählten Websites zu erleichtern. Wenn Sie beim Verbinden einer App mit einer Website das Speichern von Anmeldeinformationen zulassen, werden die gespeicherten Anmeldeinformationen in Internet Explorer oder anderen Apps nicht verwendet.

Auswahl und Steuerung

Gespeicherte Anmeldeinformationen können in der Systemsteuerung unter "Anmeldeinformationsverwaltung" verwaltet werden. Weitere Informationen dazu, wie diese und andere Anmeldeinformationen mit OneDrive synchronisiert werden können, finden Sie auf dieser Seite im Abschnitt "Synchronisierungseinstellungen".

Seitenanfang

Name und Profilbild

Funktionsweise

Um personalisierte Inhalte bereitzustellen, können Apps Ihren Namen und Ihr Profilbild von Windows anfordern. Ihr Name und Profilbild werden in den PC-Einstellungen unter **Konten** > **Ihr Konto** angezeigt. Wenn Sie sich mit einem Microsoft-Konto bei Windows anmelden, werden von Windows der Name und das Profilbild dieses Kontos 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. Die entsprechenden Informationen werden von Apps möglicherweise gespeichert oder übertragen.

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 der 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 den Apps Zugriff auf Ihren Namen und Ihr Profilbild. Wenn Sie sich für das Anpassen der Einstellungen entscheiden, können Sie den Zugriff auf Ihren Namen und Ihr Profilbild unter **Infos mit Microsoft und anderen Diensten teilen** mit der Option **Apps die Verwendung meines Namen und meines Profilbilds gestatten** 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 **Konten** ändern. Außerdem können Sie bestimmten Apps das Ändern des Profilbilds erlauben.

Seitenanfang

Netzwerkinformationen

Funktionsweise

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 der 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

Windows Store-Apps können regelmäßig oder in Echtzeit Informationen an Sie übermitteln, die als Benachrichtigungen kurz in der Ecke des 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 der 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 **Suche & Apps** mit der Option **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

Einige Windows Store-Apps können bei gesperrtem PC Statusinformationen und Benachrichtigungen auf dem Bildschirm anzeigen. Von Sperrbildschirm-Apps können auch bei gesperrtem PC Aufgaben wie etwa das Synchronisieren von E-Mails im Hintergrund oder das Ermöglichen der Annahme von eingehenden Telefonanrufen ausgeführt werden. Außerdem können Sie über den Sperrbildschirm auch direkt auf die Kamera des PCs zugreifen.

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 der 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 Skype-Apps automatisch als Sperrbildschirm-Apps festgelegt. Sie können diese und andere Apps dem

Sperrbildschirm hinzufügen oder davon entfernen sowie die Nutzung der Kamera deaktivieren. Verwenden Sie hierzu in den PC-Einstellungen unter **PC & Geräte** die Option **Sperrbildschirm**. 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 **Suche & Apps** mithilfe der Option **Benachrichtigungen** festlegen, ob Sperrbildschirm-Apps Benachrichtigungen auf dem Sperrbildschirm anzeigen können.

Kachelupdates

Funktionsweise

Windows Store-Apps können regelmäßig oder in Echtzeit Informationen an Sie übermitteln, die im Menü "Start" 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 der 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 Bildschirmrand 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

Mit "Abzüge bestellen" können Sie auf Ihrem PC oder einem Netzlaufwerk gespeicherte digitale Bilder an einen Onlinefotodruckdienst 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 Onlinefotodruckdienst 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 dem 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 Website des Diensts umgeleitet. Alle Informationen, die Sie auf der Website des Onlinefotodruckdiensts eingeben, werden an den Dienst übermittelt.

Verwendung der Informationen

Die von der Kamera in Digitalfotodateien gespeicherten Informationen können vom Onlinefotodruckdienst beim Druck der Fotos verwendet werden, z. B. um Farbe oder Bildschärfe vor dem Druck zu optimieren. Von Verwaltungs-Apps für digitale Bilder gespeicherte Informationen können vom Onlinefotodruckdienst 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 Websites 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. Oder Sie können die Eigenschaften der Datei bearbeiten und die gespeicherten persönlichen Informationen entfernen.

Seitenanfang

Vorabruf und Vorabstart

Funktionsweise

Windows ermöglicht das schnellere Starten von Apps und Windows-Features. Hierzu wird überwacht, wann und wie oft diese Apps und Features verwendet und welche Systemdateien jeweils geladen werden.

Gesammelte, verarbeitete und übertragene Informationen

Bei Verwendung einer App oder eines Windows-Features werden von Windows auf dem PC Informationen zu den verwendeten Systemdateien sowie zu Verwendungszeitpunkt und -häufigkeit der App oder des Features gespeichert.

Verwendung der Informationen

Diese Informationen zur Verwendung von Apps und Features werden von Windows dazu genutzt, den Start von Apps und Features zu beschleunigen. In bestimmten Fällen werden Apps ggf. automatisch im angehaltenen Zustand gestartet.

Auswahl und Steuerung

Apps, die automatisch gestartet und angehalten wurden, werden im Task-Manager angezeigt und können beendet werden. Im angehaltenen Zustand können diese Apps nicht auf Ihre Webcam oder auf Ihr Mikrofon zugreifen. Dies ist erst möglich, nachdem Sie sie gestartet haben, und gilt auch, wenn Sie diese Funktion zuvor aktiviert haben.

Seitenanfang

Programmkompatibilitäts-Assistent

Funktionsweise

Wird ein Kompatibilitätsproblem mit einer auszuführenden Desktop-App festgestellt, 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 der Informationen

Fehlerberichte werden dazu verwendet, Antworten für Probleme bereitzustellen, die Sie für Ihre Apps melden. Antworten enthalten (sofern verfügbar) Links zur Website 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

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 der 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 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

Wenn Ihr PC mit Nahfeldkommunikations-Hardware (NFC-Hardware) ausgestattet ist, können Sie ihn physisch an ein anderes Gerät oder Zubehörteil 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 WLAN, WiFi Direct oder Bluetooth eine kurz- oder langfristige Verbindung zwischen Geräten herstellen. Bei "Tippen und halten" ist die Verbindung aktiv, solange 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-Kopplungsinformationen, WLAN-Netzwerkadressen sowie den Namen Ihres PCs 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 der 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.

Koppeln und senden

Funktionsweise

Mit dem Windows-Feature "Koppeln 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 der 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 "Koppeln und senden" aktiviert. Weitere Informationen finden Sie im Abschnitt "Nahfeldnäherungsdienst".

Seitenanfang

RAS-Verbindungen

Funktionsweise

RAS-Verbindungen ermöglichen es Ihnen, über eine VPN (Virtuelles Privates Netzwerk)-Verbindung und den RAS (Remote Access Service)-Dienst 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 Benutzern die Verbindung mit einem privaten Netzwerk, beispielsweise einem Firmennetzwerk, über das Internet.

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 der 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 Wählhilfen mit Befehlszeilen wie "RasDial" können Sie das Kennwort nicht speichern.

Seitenanfang

RemoteApp- und Desktopverbindungen

Funktionsweise

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.

Wenn der PC oder die App, mit dem bzw. der Sie eine Verbindung herstellen, von Microsoft gehostet wird, werden möglicherweise zusätzliche Informationen zu Ihrer Verbindung zu Supportzwecken an Microsoft gesendet.

Verwendung der 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 nur dann Informationen an Microsoft gesendet, wenn die Remoteverbindung von Microsoft gehostet wird.

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 die Option **Auf RemoteApp und Desktops zugreifen** 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

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. Eine Liste wird in der Registrierung gespeichert. Diese Liste wird permanent gespeichert, sofern sie nicht von einem Administrator gelöscht wird. Es werden nur dann Informationen an Microsoft gesendet, wenn die Remoteverbindung von Microsoft gehostet wird.

Verwendung der 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

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

Sie können sich bei Windows mit einem Microsoft-Konto anmelden oder Ihr lokales Konto oder Domänenkonto mit einem Microsoft-Konto verknüpfen. Letzteres funktioniert allerdings nur bei Produkten, die dies unterstützen. 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 eine Website besuchen, auf der Sie zum Anmelden ein Microsoft-Konto verwenden, werden Sie von Windows auf dieser Website automatisch angemeldet.

Gesammelte, verarbeitete und übertragene Informationen

Wenn Sie eine E-Mail-Adresse eingeben, die beim Einrichten des PCs oder in den PC-Einstellungen unter **Konten** 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). Damit können wir überprüfen, ob das Konto tatsächlich Ihnen gehört. Wenn Sie kein Microsoft-Konto besitzen, können Sie mit einer beliebigen E-Mail-Adresse ein Konto erstellen.

Bei der Anmeldung mit einem Microsoft-Konto sendet Windows außerdem Standardcomputerinformationen an Microsoft, einschließlich des Geräteherstellers, des Modellnamens und der Version.

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 Ihrem Microsoft-Konto anmelden. Weitere Informationen zu den synchronisierten Einstellungen und deren Steuerung finden Sie auf dieser Seite im Abschnitt "Synchronisierungseinstellungen".

- Microsoft-Apps, die zur Authentifizierung ein Microsoft-Konto verwenden (wie Mail, Kalender, Kontakte, 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 Websites ausführen, bei denen Sie sich mit Ihrem Microsoft-Konto anmelden. Wenn Sie z. B. "Bing.com" besuchen, werden Sie automatisch angemeldet, ohne das Kennwort für Ihr Microsoft-Konto 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 Websites angemeldet. Da Domänenadministratoren auf alle Informationen auf Ihrem PC zugreifen können, haben 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 Name, Profilbild und Browserverlauf. Weitere Informationen zu den synchronisierten Einstellungen und deren Steuerung finden Sie auf dieser Seite im Abschnitt "Synchronisierungseinstellungen".

Verwendung der 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 Websites anzumelden. Weitere Informationen zu den Auswirkungen, die sich bei der Verwendung eines Microsoft-Kontos ergeben, erhalten Sie, wenn Sie die Datenschutzbestimmungen zum Microsoft-Konto lesen. Details dazu, wie einzelne Microsoft-Apps mit dem Microsoft-Konto zusammenhängende Informationen verwenden, finden Sie in den Datenschutzbestimmungen der jeweiligen App. Die Datenschutzbestimmungen für eine Microsoft-App können Sie über die Einstellungen einer App oder im Dialogfeld "Info" anzeigen.

Anhand der Standardgeräteinformationen können an Sie gerichtete Mitteilungen personalisiert werden (beispielsweise E-Mails, die Sie bei den ersten Schritten mit Ihrem Gerät unterstützen).

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 auf dieser Seite im Abschnitt "Synchronisierungseinstellungen". 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.

Bei Produkten, die dies unterstützen, können Sie jederzeit in den PC-Einstellungen unter **Konten** ein lokales Konto oder ein Microsoft-Konto erstellen. Wenn Sie sich mit einem Domänenkonto bei Windows anmelden, können Sie die Verbindung mit Ihrem Microsoft-Konto in den PC-Einstellungen unter **Konten** jederzeit herstellen oder trennen.

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

Seitenanfang

OneDrive-Cloudspeicher

Funktionsweise

Wenn Sie sich mit einem Microsoft-Konto an Ihrem Gerät anmelden, können Sie bestimmte Inhalte und Einstellungen automatisch auf Microsoft-Servern speichern, sodass Sie über eine Sicherungskopie verfügen.

Gesammelte, verarbeitete und übertragene Informationen

Wenn Sie beim Einrichten die Verwendung von OneDrive als Cloud-Speicher auswählen, sendet Windows automatisch Inhalte an Microsoft-Server. Hierzu zählt u. a. Folgendes:

- Im Ordner **Eigene Aufnahmen** gespeicherte Fotos und Videos auf dem Gerät.
- Einstellungen des Geräts, die nur auf dem Gerät vorhanden sind und nicht von mehreren Geräten gemeinsam genutzt werden.
- Beschreibende Informationen zum Gerät, z. B. Gerätename und -typ.

Darüber hinaus können Sie festlegen, dass Inhalte auf Microsoft-Servern gespeichert werden sollen, und auch Apps können Microsoft-Server als Standardspeicherort für Ihre Dateien verwenden.

Verwendung der Informationen

Von Windows werden diese Inhalte zum Bereitstellen des Cloud-Speicherdiensts verwendet. Microsoft verwendet die Inhalte bzw. die Informationen nicht dazu, Sie zu identifizieren, Kontakt zu Ihnen aufzunehmen oder gezielte Werbung zu schalten.

Auswahl und Steuerung

Wenn Sie beim Einrichten des PCs die Option "OneDrive

verwenden" auswählen, werden von Windows die in diesem Abschnitt beschriebenen Inhalte auf OneDrive gespeichert. Sie können diese Einstellungen jederzeit in den PC-Einstellungen im Abschnitt OneDrive ändern.

Seitenanfang

Synchronisierungseinstellungen

Funktionsweise

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

- Layout Ihrer Startseite
- Aus dem Windows Store installierte Apps
- 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 der Rechtschreibprüfung, IME-Wörterbücher und persönliche Wörterbücher
- Webbrowserverlauf, Favoriten und geöffnete Websites
- Gespeicherte App-, Website- und Netzwerkkennwörter
- Adressen freigegebener Netzwerkdrucker, zu denen eine Verbindung eingerichtet wurde

Aus Datenschutzgründen werden alle synchronisierten Einstellungen per 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 verknüpft 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, haben sie auch Zugriff auf alle Einstellungen und Informationen, für die Sie die Synchronisierung mit anderen PCs über Ihr Microsoft-Konto ausgewählt haben.

Verwendung der Informationen

Windows 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 bei Windows mit einem Microsoft-Konto anmelden, werden Ihre Einstellungen standardmäßig synchronisiert. In den PC-Einstellungen im Abschnitt OneDrive

können Sie unter **Synchronisierungseinstellungen** 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

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 der 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

Das TPM (Trusted Platform Module) 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 Geräteverschlüsselung, 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 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 der Informationen

Nach der Initialisierung des TPM können Apps das TPM verwenden, um zusätzliche eindeutige kryptografische Schlüssel zu erstellen und zu schützen. Die Geräteverschlüsselung 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

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.

Verwendung der 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

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

Von Update Services werden Informationen auf dem PC gesammelt, mit denen Microsoft die Dienste betreiben und verbessern kann, z. B.:

- Microsoft-Software und andere unterstützende Software (z. B. von Geräteherstellen bereitgestellte Treiber und Firmware), die auf dem PC installiert ist und für die Updates verfügbar sind. Dadurch können wir ermitteln, welche Updates für Sie geeignet sind.

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

- Informationen zu erfolgreichen oder gescheiterten Updates oder zu Fehlern, die beim Zugreifen und Verwenden von Update Services aufgetreten sind.

- Plug & Play-IDs von Hardwaregeräten – ein vom Gerätehersteller zugewiesener Code, der das Gerät identifiziert (z. B. einen bestimmten Tastaturtyp).

- 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, Anbieter 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.

- Hersteller, Modell, Plattformrolle und SKU-Nummer – Informationen zum PC, mit denen die diagnostische Untersuchung von Treiberinstallationen ermöglicht wird.

Rufen Sie die Updatedienste in der Systemsteuerung unter Windows Update auf, und suchen Sie nach Updates. Oder ändern Sie die Einstellungen, um die automatische Installation von Updates durch Windows zuzulassen, sobald diese verfügbar werden (empfohlen). Unter Windows Update können Sie auswählen, ob Sie Microsoft Update verwenden möchten.

Wenn Sie den automatischen Download wichtiger Softwareupdates für Ihren PC aktivieren, ist in diesen Updates unter Umständen das Windows-Tool zum Entfernen bösartiger Software (MSRT) enthalten. 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-Website aufgelistete Schadsoftware. Während der Überprüfung auf Schadsoftware wird ein Bericht mit spezifischen Informationen zu erkannter Schadsoftware, zu Fehlern und zu anderen Informationen über Ihren PC an Microsoft gesendet. Weitere Informationen finden Sie in den Datenschutzbestimmungen zum Windows-Tool zum Entfernen von Schadsoftware.

Verwendung der Informationen

Die an Microsoft gesendeten Daten werden zum Betreiben und Warten von Update Services verwendet. Mit ihnen werden außerdem aggregierte Statistiken erstellt, mit deren Hilfe wir Trends analysieren sowie Produkte und Dienste wie etwa Update Services verbessern können.

Bei der Generierung aggregierter Statistiken wird von den Updatediensten die GUID herangezogen, die von

Update Services erfasst wurde, um die Anzahl der einzelnen Computer, auf denen Update Services verwendet wird, sowie Informationen zu erfolgreichen oder gescheiterten Downloads und Installationen von bestimmten Updates nachzuverfolgen und zu erfassen. Von Update Services werden die GUID des Computers, auf dem der Download und die Installation ausgeführt wurden, die ID des angeforderten Elements, Informationen zur Verfügbarkeit von Updates sowie Standardcomputerinformationen erfasst.

Die oben beschriebenen 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.

Erforderliche Updates

Wenn Sie Update Services aktivieren, müssen für den einwandfreien Betrieb einige Softwarekomponenten Ihres Systems, die Update Services bilden oder direkt mit Update Services in Zusammenhang stehen, regelmäßig aktualisiert werden. Diese Updates müssen ausgeführt werden, bevor vom Dienst andere Updates gesucht, heruntergeladen oder installiert werden können. Durch diese erforderlichen Updates werden Fehler behoben, aktuelle Verbesserungen bereitgestellt und die Kompatibilität mit den Microsoft-Servern gewährleistet, die den Dienst unterstützen.

Ist Update Services deaktiviert, erhalten Sie diese Updates nicht.

Zum Installieren oder Aktualisieren von Windows Store-Apps erforderliche Softwareupdates werden automatisch heruntergeladen und installiert. Diese Updates müssen ausgeführt werden, damit Apps einwandfrei funktionieren.

Cookies und Token

Ein Token ähnelt einem Cookie. Es speichert Informationen in einer kleinen Datei, die vom Update Services-Server auf der

Festplatte abgelegt wird. Das Token wird verwendet, wenn der Computer eine Verbindung mit dem Update Services-Server herstellt, um eine gültige Verbindung aufrechtzuerhalten. Es wird nur auf dem Computer und nicht auf dem Server gespeichert. Das Cookie oder Token enthält Informationen (z. B. die Uhrzeit der letzten Überprüfung), damit die neuesten verfügbaren Updates gesucht werden. Es enthält Informationen dazu, welche Inhalte auf den Computer heruntergeladen werden sollen und zu welchem Zeitpunkt der Download stattfinden soll. Darüber hinaus enthält es eine GUID zur Identifikation Ihres Computers auf dem Server.

Im Inhalt des Cookies oder Tokens enthaltene Informationen werden vom Server verschlüsselt. Von der Verschlüsselung ausgenommen ist die Ablaufzeit des Cookies oder Tokens. Bei diesem Cookie oder Token handelt es sich nicht um ein Browsercookie, daher können Sie es nicht über die Browsereinstellungen steuern. Das Cookie oder Token kann nicht entfernt werden. Wenn Sie Update Services jedoch nicht verwenden, wird auch das Cookie oder Token nicht verwendet.

Auswahl und Steuerung

Wenn Sie beim Einrichten von Windows die Express-Einstellungen auswählen, wird der Windows Update-Dienst aktiviert und so festgelegt, dass Updates automatisch installiert werden.

Wenn Sie Update Services aktivieren, werden unabhängig von der ausgewählten Einstellung erforderliche Updates für einige Komponenten des Diensts heruntergeladen und installiert, ohne dass Sie darüber informiert werden. Falls Sie keine erforderlichen Updates erhalten möchten, deaktivieren Sie Update Services.

Sie können auch auswählen, ob wichtige und empfohlene Updates für den Computer oder nur wichtige Updates gesucht und automatisch installiert werden sollen. Optionale Updates werden nie automatisch installiert. Sie können die Windows Update-Einstellungen nach der Einrichtung von

Windows in der Systemsteuerung oder in den PC-Einstellungen ändern.

Wenn Sie ausgewählt haben, dass wichtige Updates automatisch gesucht und installiert werden sollen und dass Sie MSRT im Rahmen dieser Updates für den Computer erhalten möchten, können Sie die Berichterstattungsfunktionalität der Software deaktivieren.

Seitenanfang

Virtuelles privates Netzwerk

Funktionsweise

Per VPN (virtuelles privates Netzwerk) können Sie über das Internet eine Verbindung mit einem privaten Netzwerk, z. B. einem Firmennetzwerk, herstellen. Eine VPN-Verbindung kann über den VPN-Client von Windows oder eine VPN-App eines Drittanbieters bereitgestellt werden.

Gesammelte, verarbeitete und übertragene Informationen

Wenn Sie eine VPN-Verbindung herstellen, werden die Anmeldeinformationen, die Sie im VPN-Client angeben, an das Remotenetzwerk gesendet. Möglicherweise können Sie diese Anmeldeinformationen auf Ihrem PC speichern. Nach der Verbindungsherstellung werden je nach Konfiguration des VPN einige oder alle Netzwerkaktivitäten über das Remotenetzwerk weitergeleitet. Administratoren können bestimmte Apps so konfigurieren, dass deren Datenverkehr immer über das VPN weitergeleitet wird und dass die Verbindung zum VPN automatisch hergestellt wird, wenn diese Apps gestartet werden. Es werden keine Informationen an Microsoft gesendet.

Von VPN-Software von Drittanbietern werden möglicherweise weitere Informationen erfasst. Die Erfassung und Nutzung dieser Informationen unterliegt den Datenschutzpraktiken des Drittanbieters.

Verwendung der Informationen

Von VPN-Clients werden die von Ihnen angegebenen Anmeldeinformationen zum Authentifizieren beim Remotenetzwerk und zum Weiterleiten von Netzwerkdatenverkehr in das und aus dem Remotenetzwerk verwendet. Falls von einem VPN-Client eines Drittanbieters weitere Informationen erfasst werden, unterliegt die Nutzung dieser Informationen den Datenschutzpraktiken des Drittanbieters.

Auswahl und Steuerung

Sie können eine VPN-Verbindung hinzufügen oder entfernen und den Status der bestehenden Verbindungen anzeigen, indem Sie in den PC-Einstellungen auf die Option **Netzwerk** zugreifen. Nach dem Einrichten einer VPN-Verbindung können Sie diese Verbindung manuell herstellen oder trennen, indem Sie in den Einstellungen in der Liste das Netzwerk auswählen.

Seitenanfang

Windows-Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP)

Funktionsweise

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 auf Ihrem PC befindliche Windows-Version.

- Informationen zu 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 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 dazu, wie oft Sie Apps öffnen, wie oft Sie Windows-Hilfe und Support verwenden, mit welchen Diensten Sie sich bei Apps anmelden und wie viele Ordner Sie normalerweise auf Ihrem Desktop erstellen.

CEIP-Berichte können auch Informationen über Ereignisse (Ereignisprotokolldaten) enthalten, die bis zu sieben Tage vor Beginn Ihrer Teilnahme am CEIP auf Ihrem PC aufgetreten sind. Da die meisten Benutzer sich innerhalb von einigen Tagen nach der Einrichtung von Windows 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. Sollten trotzdem individuelle IDs an Microsoft übermittelt werden, werden diese nicht verwendet, um Sie zu identifizieren oder Kontakt mit Ihnen aufzunehmen.

Das CEIP generiert eine als GUID (Globally Unique Identifier) bezeichnete Zufallsnummer, die zusammen mit jedem CEIP-Bericht an Microsoft gesendet wird. Anhand der GUID können wir feststellen, welche Daten im Laufe der Zeit von einem bestimmten Computer gesendet werden. Einige CEIP-Berichte können außerdem von Ihrem Microsoft-Konto abgeleitete GUIDs enthalten.

Vom Programm zur Verbesserung der Benutzerfreundlichkeit wird außerdem ggf. von Zeit zu Zeit 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 der 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. Ggf. werden die aggregierten Informationen des Programms zur Verbesserung der Benutzerfreundlichkeit auch an Microsoft-Partner weitergegeben, damit diese ihre Produkte und Dienste verbessern können. Die Informationen können jedoch nicht verwendet werden, um Sie zu identifizieren, Kontakt mit Ihnen 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. 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 Express-Einstellungen auswählen, wird das Windows-Programm zur Verbesserung der Benutzerfreundlichkeit aktiviert: Von Windows und den Microsoft-Apps aus dem Windows Store können CEIP-Berichte für alle Benutzer des PCs gesendet werden. Wenn Sie sich für das Anpassen der Einstellungen entscheiden, können Sie Ihre Teilnahme am CEIP steuern. Wählen Sie dazu unter **Verbesserung der Produkte und Dienste von Microsoft unterstützen** die Option **Im Rahmen des Programms zur Verbesserung der Benutzerfreundlichkeit Informationen zu meiner Verwendung des PCs an Microsoft senden** aus. Administratoren können diese Einstellung nach der Einrichtung von Windows in der Systemsteuerung im **Wartungscenter** ändern.

Weitere Informationen finden Sie in den häufig gestellten Fragen zum CEIP.

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

Wenn Sie Windows Defender verwenden, kann der Microsoft Active Protection Service (MAPS) zur Verbesserung des Schutzes Ihres PCs beitragen, indem neue Signaturen für neu erkannte Schadsoftware automatisch heruntergeladen werden

und der Sicherheitsstatus Ihres PCs überwacht wird. Von MAPS werden Informationen zu Schadsoftware und anderer möglicherweise unerwünschter Software an Microsoft gesendet. Außerdem werden gegebenenfalls Dateien gesendet, die möglicherweise Schadsoftware enthalten. Wenn von MAPS erkannt wird, dass Ihr PC mit bestimmten Arten von Schadsoftware infiziert ist, werden Sie von MAPS gegebenenfalls automatisch über Ihr Microsoft-Konto kontaktiert, um die Lösung des Problems einzuleiten.

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 Dateien zu bestimmen, sowie die IP-Adressen, zu denen Dateien mit potenzieller Schadsoftware Verbindungen herstellen. 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.
- Windows Defender scannt ein ActiveX-Steuerelement in Internet Explorer.

Wenn Sie MAPS beim Einrichten von Windows beitreten, tun Sie dies mit einer einfachen Mitgliedschaft. 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 über Windows Update allen Benutzern zur Verfügung gestellt.

Wenn Sie MAPS beitreten, werden von Windows Defender ggf. bestimmte Dateien oder Webinhalte von Ihrem PC gesendet, die von Microsoft als potenziell unerwünschte Software eingestuft werden. Der Musterbericht wird zur weiteren Analyse verwendet. Falls eine Datei möglicherweise persönliche Informationen enthält, wird Ihnen vor dem Senden eine entsprechende Meldung angezeigt. 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 per SSL verschlüsselt.

Um zur Erkennung und Beseitigung bestimmter Arten von Infektionen durch Schadsoftware beizutragen, werden von

Windows Defender regelmäßig Informationen zum Sicherheitsstatus Ihres PCs an MAPS gesendet. Darin sind Informationen zu den Sicherheitseinstellungen Ihres PCs und Protokolldateien enthalten, in denen die Treiber und andere Software beschrieben sind, die beim Starten des PCs geladen werden. Außerdem wird eine Zahl gesendet, mit der Ihr PC eindeutig identifiziert wird.

Verwendung der 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.

Mit den Informationen zum Sicherheitsstatus Ihres PCs, die von MAPS erfasst werden, wird ermittelt, ob der PC mit bestimmten Arten von Schadsoftware infiziert ist. In diesem Fall werden die Kontaktinformationen in Ihrem Microsoft-Konto von Microsoft verwendet, um Ihnen Details zum Problem und zu dessen Beseitigung zukommen zu lassen.

Auswahl und Steuerung

Wenn Sie beim Einrichten von Windows die Express-Einstellungen auswählen, aktivieren Sie damit MAPS. Wenn Sie sich für das Anpassen der Einstellungen entscheiden, können Sie MAPS steuern. Wählen Sie dazu unter **Infos mit Microsoft und anderen Diensten teilen** die Option **Informationen an den Microsoft Active Protection Service senden, wenn Windows Defender aktiviert ist, um den Schutz vor Schadsoftware zu verbessern** aus. Sie können Ihre Mitgliedschaft bei MAPS oder die MAPS-Einstellungen nach dem Einrichten von Windows über das Menü **Einstellungen** in Windows Defender ändern. Dazu zählt auch das Deaktivieren von MAPS.

Wenn Sie das Tool zum Entfernen bösartiger Software über Windows Update erhalten, werden möglicherweise auch dann ähnliche Informationen an MAPS gesendet, wenn Windows Defender deaktiviert ist. Weitere Informationen finden Sie unter Windows-Tool zum Entfernen von Schadsoftware.

Verlaufsfeature

Funktionsweise

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

Mit der Windows-Fehlerberichterstattung können Microsoft und Microsoft-Partner Probleme in der von Ihnen verwendeten Software diagnostizieren und Lösungen bereitstellen. Nicht für alle Probleme können Lösungen bereitgestellt werden. Falls jedoch Lösungen verfügbar sind, werden sie in Form von schrittweisen Anleitungen zur Lösung des gemeldeten Problems oder in Form von zu installierenden Updates bereitgestellt. 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 zugehörigen ausführbaren Dateien. 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. In einigen Fällen sendet der Berichterstellungsdienst automatisch zusätzliche Informationen, die bei der Diagnose des Problems hilfreich sein können, z. B. eine Teilmomentaufnahme des PC-Speichers. 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 Website übermittelte Daten enthalten.

Zum Diagnostizieren bestimmter Problemtypen kann die Windows-Fehlerberichterstattung einen Bericht mit zusätzlichen Informationen wie Protokolldateien erstellen. Bevor ein Bericht mit solchen zusätzlichen Informationen gesendet wird, werden Sie von Windows gefragt, ob Sie den Bericht senden möchten. Diese Bestätigung wird auch dann eingeholt, wenn Sie die automatische Berichterstellung aktiviert haben.

Nachdem Sie ein Problem gemeldet haben, werden Sie möglicherweise aufgefordert, weitere Informationen zum 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 können wir feststellen, welche Daten im Laufe der Zeit von einem bestimmten Computer gesendet werden. Die GUID enthält keine persönlichen Informationen.

Aus Datenschutzgründen werden die gesendeten Informationen durch SSL verschlüsselt.

Verwendung der 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 Express-

Einstellungen 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 suchen** die Option **Mit der Windows-Fehlerberichterstattung online nach Problemlösungen suchen** auswählen. Sie können diese Einstellung nach der Einrichtung von Windows in der Systemsteuerung im Wartungscenter ändern.

Weitere Informationen finden Sie in den Datenschutzbestimmungen für den Microsoft-Fehlerberichterstattungsdienst.

Seitenanfang

Windows-Dateizuordnung

Funktionsweise

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 der 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

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 der 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 Websitedaten** aus, und klicken oder tippen Sie auf **Löschen**. 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

Das Programm zur Verbesserung der Hilfebenutzerfreundlichkeit (Help Experience Improvement Program, HEIP) 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 PC 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 der 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.

Das Programm zur Verbesserung der Hilfebenutzerfreundlichkeit sammelt nicht absichtlich Informationen, die zum Feststellen Ihrer Identität verwendet werden können. Wenn Sie solche Informationen in die Such- oder Feedbackfelder eingeben, werden sie zwar gesendet, aber nicht von Microsoft verwendet, um Sie zu identifizieren, Kontakt mit Ihnen aufzunehmen oder gezielte Werbung zu schalten.

Auswahl und Steuerung

Wenn Sie beim Einrichten von Windows die Express-Einstellungen auswählen, nehmen Sie damit am Programm zur Verbesserung der Hilfebenutzerfreundlichkeit teil. Wenn Sie sich für das Anpassen der Einstellungen entscheiden, können Sie die Einstellungen des Programms zur Verbesserung der Hilfebenutzerfreundlichkeit steuern. Wählen Sie dazu unter **Verbesserung der Produkte und Dienste von Microsoft unterstützen** die Option **Im Rahmen des Programms zur Verbesserung der Hilfebenutzerfreundlichkeit Informationen zu meiner Verwendung der Hilfe an Microsoft senden** aus. Nach dem Einrichten von Windows können Sie diese Einstellung in "Windows-Hilfe und Support" ändern.

Seitenanfang

Remoteunterstützung

Funktionsweise

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

Die 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 die Remoteunterstützung Kontaktinformationen aus, z. B. Benutzername, PC-Name und Profilbild. In einer Sitzungsprotokolldatei werden alle Remoteunterstützungsverbindungen festgehalten.

Verwendung der Informationen

Die Informationen werden dazu verwendet, 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 der Remoteunterstützung deaktivieren.

Seitenanfang

Windows Search

Funktionsweise

Windows Search ermöglicht es Ihnen, gleichzeitig sowohl Ihr Gerät als auch das Web zu durchsuchen. Um bessere Suchergebnisse zu liefern, kann Windows Search Bing und die Plattform für Windows-Position verwenden. Beachten Sie, dass auf Ihrem Gerät noch andere Suchfunktionen von Microsoft zur Verfügung stehen – beispielsweise die Suche im Windows Store, in Internet Explorer sowie in anderen Microsoft-Produkten.

Gesammelte, verarbeitete und übertragene Informationen

Wenn Sie sich für die Verwendung von Websuchergebnissen entscheiden, sendet Windows Ihre Eingabe in Windows Search an Microsoft. Um die Suchergebnisse zu verbessern, sendet Windows Search auch Informationen dazu, wie Sie mit dem Feature interagieren, an Microsoft. Zudem sendet Windows Search einen Bezeichner, um basierend auf Ihrer Interaktion mit Bing und anderen Microsoft-Produkten und -Diensten personalisierte Suchergebnisse bereitzustellen. Wenn Sie sich mit einem Microsoft-Konto bei Windows anmelden, wird der Bezeichner mit Ihrem Microsoft-Konto verknüpft. Sie können festlegen, dass keine personalisierten Ergebnisse in Windows Search verwendet werden sollen. In diesem Fall wird der Bezeichner nicht gesendet.

Wenn Sie Windows Search die Verwendung Ihrer Position erlauben, wird mit jeder Suchanforderung der ungefähre Standort Ihres Geräts gemäß Angabe der Plattform für Windows-Position an Microsoft gesendet. Wir können alternativ auch versuchen, Ihren ungefähren Standort auf Basis Ihrer IP-Adresse zu ermitteln.

Wenn Sie Windows Search für die Suche innerhalb einer App verwenden, werden Ihre Suchbegriffe der App zur Verfügung gestellt.

Verwendung der Informationen

Wenn Sie sich für die Verwendung von Windows Search entscheiden, um Websuchergebnisse zu erhalten, werden der von Ihnen eingegebene Suchbegriff, Ihr lokaler Suchverlauf und Ihr Onlinesuchverlauf, mit Ihrem Microsoft-Konto verknüpfte Informationen sowie der ungefähre Standort Ihres Geräts verwendet, um relevante Suchvorschläge, personalisierte Suchergebnisse und personalisierte Umgebungen in anderen Microsoft-Produkten und -Diensten bereitzustellen. Weitere Informationen zur Verwendung Ihrer Daten finden Sie in den Bing-Datenschutzbestimmungen.

Wenn Sie Windows Search für die Suche in einer Drittanbieter-

App verwenden, 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

Wenn Sie beim Einrichten von Windows die Express-Einstellungen auswählen, gestatten Sie dadurch Windows Search das Abrufen von Suchvorschlägen und Suchergebnissen. Außerdem gestatten Sie Microsoft die Nutzung von Daten aus Windows Search (einschließlich Position), um Windows Search und andere Microsoft-Umgebungen zu personalisieren. Wenn Sie sich entscheiden, die Einstellungen anzupassen, können Sie entscheiden, ob Sie diese Einstellungen für Windows Search ändern möchten. Nach dem Einrichten von Windows können Sie diese Einstellung in den PC-Einstellungen unter **Suche** ändern.

Ihren lokalen Suchverlauf und Teile des Bing-Suchverlaufs, die zum Personalisieren der Ergebnisse von Windows Search verwendet werden, können Sie in den PC-Einstellungen im Abschnitt **Suche und Apps** unter **Suche** löschen. Durch Löschen des Suchverlaufs wird Microsoft angewiesen, Suchvorschläge oder die Reihenfolge der Suchergebnisse nicht auf der Grundlage eines zuvor erstellten Suchverlaufs zu personalisieren. Dabei werden allerdings weder Werbe- oder andere Personalisierungsinformationen (einschließlich von Ihrem Suchverlauf abgeleitete Informationen) noch Informationen gelöscht, die von Microsoft aggregiert werden, um die Suchergebnisse und andere Microsoft-Features zu verbessern. Diese Informationen werden aufbewahrt und anonymisiert. Eine Beschreibung hierzu finden Sie in den Bing-Datenschutzbestimmungen. Die Informationen für Werbung und andere Personalisierungen von Microsoft können online verwaltet werden.

Seitenanfang

Windows Setup

Dieser Abschnitt enthält Beschreibungen für die Features, die bei der Windows-Installation zur Verfügung stehen.

Dynamisches Update

Funktionsweise

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:

- **Installationsupdates.** Wichtige Softwareupdates für Installationsdateien, mit denen eine erfolgreiche Installation sichergestellt wird.
- **Updates für mitgelieferte Treiber.** Wichtige Treiberupdates für die installierte Windows-Version.

Darüber hinaus werden beim dynamischen Update bei der Installation von Windows aus dem Windows Store die aktuellen Updates für Windows sowie bestimmte vom PC benötigte Hardwaretreiber heruntergeladen und installiert.

Verwendung der Informationen

Beim dynamischen Update werden Informationen zur Hardware Ihres PC an Microsoft gesendet, damit die richtigen Treiber für Ihr System ermittelt werden können.

Auswahl und Steuerung

Bei der Installation von Windows aus dem Windows Store werden Updates von Setup automatisch heruntergeladen und installiert. Bei der Installation von Windows von physischen Medien werden Sie gefragt, ob Sie in den Onlinemodus wechseln möchten, um Updates zu installieren.

Programm zur Verbesserung der Installation

Funktionsweise

Dieses Feature sendet einmalig einen Bericht mit grundlegenden Informationen zum PC und zur Installation von Windows 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 können wir feststellen, welche Daten im Laufe der Zeit von einem bestimmten Computer gesendet werden. Die GUID enthält keine persönlichen Informationen und wird nicht dazu verwendet, Sie zu identifizieren.

Verwendung der Informationen

Microsoft und seine Partner verwenden den Bericht, um die eigenen 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 verwenden.

Auswahl und Steuerung

Sie können während der Installation von Windows entscheiden, ob Sie an diesem Programm teilnehmen möchten, indem Sie **Ich möchte zur Verbesserung der Installation von Windows beitragen** aktivieren bzw. nicht aktivieren.

Weitere Informationen finden Sie im Abschnitt zum Windows CEIP.

Installationskompatibilitätsprüfung

Funktionsweise

Bei der Installation von Windows können Sie mithilfe von Setup ermitteln, ob Ihr aktueller PC für ein Upgrade auf Windows 8.1 geeignet ist, und Sie erhalten Kompatibilitätsinformationen zu Ihren Programmen und Geräten.

Gesammelte, verarbeitete und übertragene Informationen

Beim Ermitteln der Kompatibilität werden bestimmte Informationen zu Ihren Updatemöglichkeiten erfasst, z. B. zur Leistungsfähigkeit der Computerhardware, zu den an den Computer angeschlossenen Geräten und den Programmen, die auf dem Computer installiert sind. Gelegentlich können die Daten des Programmherausgebers Informationen wie Namen oder E-Mail-Adresse des Herausgebers enthalten.

Verwendung der Informationen

Mit den erfassten Informationen werden die richtigen Treiber für Ihren PC und die Kompatibilität des PCs und der Programme und Geräte mit Windows 8.1 ermittelt. Zudem

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

Auswahl und Steuerung

Bei der Installation von Windows aus dem Windows Store oder von einem physischen Medium in einer vorhandenen Windows-Installation werden die in diesem Abschnitt beschriebenen Informationen an Microsoft gesendet. Beim Starten von einem physischen Installationsmedium zum Installieren von Windows wird von Setup nicht online nach Kompatibilitätsinformationen gesucht.

Seitenanfang

Windows-Freigabe

Funktionsweise

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 der 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 der Windows-Freigabe werden von Windows standardmäßig gespeichert. Sie können die Speicherung dieser Informationen beenden oder alle gespeicherten Ziele löschen, indem Sie in den PC-Einstellungen unter **Suche & Apps** die Option **Freigeben** verwenden.

Seitenanfang

Windows SmartScreen

Funktionsweise

Windows SmartScreen trägt zur Sicherheit Ihres PCs bei, indem heruntergeladene Dateien und Webinhalte in Apps überprüft werden, um Sie vor Schadsoftware und potenziell unsicheren Webinhalten zu schützen. Bevor eine unbekannte oder potenziell unsichere heruntergeladene Datei geöffnet wird, wird von Windows eine Warnung angezeigt. Falls von SmartScreen in einer App potenziell unsichere Webinhalte erkannt werden, wird von Windows anstelle der Inhalte eine Warnung angezeigt.

Gesammelte, verarbeitete und übertragene Informationen

Wenn Sie heruntergeladene Dateien von Windows SmartScreen überprüfen lassen, werden von Windows Information an den SmartScreen-Onlinedienst gesendet. Neben den Standardcomputerinformationen und der Versionsnummer des Windows SmartScreen-Filters können diese Informationen auch einen Dateinamen, eine

Dateikennung ("Hash") und Informationen zum digitalen Zertifikat enthalten. Zum Schutz Ihrer Daten werden die an Microsoft übermittelten Informationen per SSL verschlüsselt.

Wenn Sie potenziell unsichere Inhalte in Apps von Windows SmartScreen blockieren lassen, werden von Windows Informationen an den SmartScreen-Onlinedienst gesendet. Hierzu zählen unter anderem die Adressen und Inhaltsarten, auf die Windows Store-Apps bei ihrer Verwendung zugreifen. Im Gegenzug erfährt der PC, ob die Inhalte als unsicher oder verdächtig an Microsoft gemeldet wurden. Die an Microsoft gesendeten Berichte enthalten Informationen wie den Namen oder Bezeichner der App und die vollständigen Adressen der Webinhalte, auf die von der App zugegriffen wird.

Zum Schutz Ihrer Daten werden die an Microsoft übermittelten Informationen verschlüsselt. In der an Microsoft gesendeten Adresse können auch Informationen enthalten sein, die einer Webseite zugeordnet sind, auf die mit einer App zugegriffen wird, z. B. Suchbegriffe. Wenn Sie beispielsweise in einer Wörterbuch-App ein Wort nachschlagen, wird das gesuchte Wort möglicherweise als Teil der vollständigen Adresse, auf die von der App zugegriffen wird, an Microsoft gesendet. Microsoft filtert diese Adressen, um persönliche Informationen zu entfernen, sofern möglich.

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 können wir feststellen, welche Daten im Laufe der Zeit von einem bestimmten Computer gesendet werden. Die GUID enthält keine persönlichen Informationen.

Verwendung der Informationen

Microsoft verwendet die oben beschriebenen Informationen, um Sie vor potenziell unsicheren heruntergeladenen Dateien und Inhalten in Apps zu warnen. Wenn von SmartScreen beispielsweise eine potenzielle Bedrohung innerhalb einer App erkannt wird, die SmartScreen unterstützt, wird von Windows anstelle der Inhalte eine Warnung angezeigt. Zudem werden

die Informationen verwendet, um SmartScreen und andere Produkte und Dienste zu verbessern. Microsoft verwendet die Informationen nicht dazu, gezielte Werbung zu schalten.

Auswahl und Steuerung

Wenn Sie beim Einrichten von Windows die Expresseinstellungen auswählen, aktivieren Sie Windows SmartScreen. Wenn Sie die Einstellungen anpassen möchten, können Sie Windows SmartScreen steuern, indem Sie unter **PC und Privatsphäre schützen** die Option **SmartScreen-Onlinedienste verwenden, um den PC vor schädlichen Inhalten in Websites, die von Windows Store-Apps und Internet Explorer geladen werden, sowie vor schädlichen Downloads zu schützen** aus. Sie können diese Einstellung nach der Einrichtung von Windows in der Systemsteuerung im Wartungscenter ändern. Informationen zu Internet Explorer-SmartScreen finden Sie im Abschnitt "SmartScreen-Filter" der Datenschutzbestimmungen zu Internet Explorer.

Seitenanfang

Windows-Spracherkennung

Funktionsweise

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 der 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

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 über den Store 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.

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 Websites auch die Browsingdaten der Besucher analysiert werden.

Verwendung der 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 Store-Kachel 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, wodurch 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.

Automatische Updates für Apps

Funktionsweise

Dieses Feature sucht nach Updates für Windows Store-Apps, lädt sie herunter und installiert sie, um sicherzustellen, dass Sie über die aktuellen Versionen verfügen. Zu App-Updates können Sicherheitsupdates, Leistungsupdates und neue Funktionen oder Inhalte zählen. In den aktualisierten Apps stehen ggf. andere Windows-Funktionen als in den vorherigen Versionen zur Verfügung, wodurch die Apps möglicherweise auf andere Ressourcen auf dem PC zugreifen können. Informationen zu den Funktionsänderungen finden Sie auf der Produktbeschreibungsseite für die App im Windows Store.

Gesammelte, verarbeitete und übertragene Informationen

Zum Bereitstellen von automatischen App-Updates sendet der Store die folgenden Informationen an Microsoft:

- Liste der Apps, die von allen Benutzern des PCs über den Store installiert wurden
- Lizenzierungsinformationen für jede App
- 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
- BIOS-Name, -Versionsnummer und -Versionsdatum
- Grundlegende Informationen zum PC, z. B. Hersteller, Modell und verwendete Windows-Edition

Verwendung der Informationen

Diese Informationen werden verwendet, um den Updatedienst bereitzustellen. Anhand der Informationen werden außerdem aggregierte Statistiken erstellt, mit deren Hilfe Microsoft Trends analysieren sowie Produkte und Dienste verbessern kann. Sie 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 Express-Einstellungen auswählen, sucht der Windows Store automatisch nach Updates, lädt sie herunter und installiert sie (auch wenn Sie sich vom Windows Store abgemeldet haben). Wenn Sie automatische App-Updates deaktivieren, können Sie bei der Anmeldung beim Windows Store entscheiden, ob Sie ein App-Update installieren möchten.

So deaktivieren Sie automatische App-Updates

1. Öffnen Sie den Windows Store.
2. Wischen Sie vom rechten Bildschirmrand nach innen, und tippen Sie dann auf **Einstellungen**.

   Zeigen Sie bei Verwendung einer Maus auf die untere rechte Bildschirmecke, und klicken Sie dann auf **Einstellungen**.
3. Tippen oder klicken Sie auf **App-Updates**.
4. Tippen oder klicken Sie auf die Option **Meine Apps automatisch aktualisieren**, um automatische App-Updates zu deaktivieren.

Informationen zu den Funktionen der aktuellen App-Version und das letzte Aktualisierungsdatum einer App finden Sie auf der Produktbeschreibungsseite für die App im Windows Store.

Berechtigung für Store-Apps

Funktionsweise

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.

Wenn von einer App Informationen von einem Gerät angefordert werden, auf dem Daten zu Ihnen oder Ihrem Verhalten gespeichert sind, wird von Windows zusätzlich zu den obigen Berechtigungen abgefragt, ob Sie die Nutzung durch die App zulassen möchten. Wenn Sie beispielsweise ein Fitnessgerät anschließen, mit dem Ihre Position nachverfolgt wird, werden Sie von Windows gefragt, ob Sie den Zugriff darauf für die App zulassen möchten.

Verwendung der 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, öffnen **Einstellungen** und wählen dann **Berechtigungen**.

Empfehlungen zur personalisierten Store-Suche und zu Apps

Funktionsweise

Wenn Sie im Windows Store browsen oder nach Apps suchen, werden von Microsoft Empfehlungen und Suchergebnisse bereitgestellt, damit Sie die für Sie relevanten Apps schneller finden.

Gesammelte, verarbeitete und übertragene Informationen

Um die Suchergebnisse zu verbessern, werden vom Windows Store Informationen dazu an Microsoft gesendet, wie Sie damit interagieren, also wonach Sie suchen und welche Suchergebnisse Sie auswählen. Zudem sendet Windows Store einen mit Ihrem Microsoft-Konto verknüpften Bezeichner, um basierend auf Ihrer Interaktion mit Bing sowie anderen Produkten und Diensten von Microsoft personalisierte Suchergebnisse bereitzustellen. Sie können festlegen, dass keine personalisierten Ergebnisse verwendet werden sollen. In diesem Fall wird der Bezeichner nicht gesendet.

Verwendung der Informationen

Vom Store wird der mit dem Microsoft-Konto verknüpfte Bezeichner verwendet, um basierend auf Ihrer Interaktion mit dem Store und anderen Produkten und Diensten von Microsoft, wie Bing und dem Windows Phone Store, personalisierte Suchergebnisse und Empfehlungen bereitzustellen. Dazu zählen auch Informationen wie von Ihnen erworbene Apps, im Microsoft-Konto angegebene Profilinformationen und Ihre Bewertungen und Rezensionen von Apps. Diese Informationen können auch zum Personalisieren von anderen Microsoft-Produkten und -Diensten verwendet werden.

Auswahl und Steuerung

Wenn Sie sich an Windows mit einem Microsoft-Konto angemeldet haben, sind die personalisierten Ergebnisse und Empfehlungen von Windows Store standardmäßig aktiviert. Sie können in den Store-Einstellungen unter **Einstellungen** auch angeben, dass Sie keine personalisierten Ergebnisse und Empfehlungen vom Store erhalten möchten.

Tragen Sie dazu bei, den Windows Store zu verbessern, indem Sie die URLs für den von der App verwendeten Webinhalt senden.

Funktionsweise

Einige Apps, die Sie im Store erhalten, sind mit Websites 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 Websites empfängt. Die an Microsoft gesendeten Berichte enthalten Informationen, z. B. Name oder Bezeichner der App, die vollständigen URLs der Websites, 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 können wir feststellen, welche Daten im Laufe der Zeit von einem bestimmten Computer gesendet werden. Die GUID enthält keine persönlichen Informationen und wird nicht dazu verwendet, Sie zu identifizieren.

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 der 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 sich für das Anpassen der Einstellungen entscheiden, können Sie diese Einstellung steuern. Wählen Sie dazu unter **Verbesserung der Produkte und Dienste von Microsoft unterstützen** die Option **SmartScreen-**

Onlinedienste verwenden, um den PC vor schädlichen Inhalten in Websites, die von Windows Store-Apps und Internet Explorer geladen werden, sowie vor schädlichen Downloads zu schützen aus. Nach der Installation können Sie diese Einstellung in den PC-Einstellungen unter **Datenschutz** ändern.

Seitenanfang

Windows-Zeitdienst

Funktionsweise

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 der Informationen

Der Windows-Zeitdienst synchronisiert anhand dieser Informationen automatisch die Uhrzeit des lokalen PCs.

Auswahl und Steuerung

Der Windows-Zeitdienst ist standardmäßig aktiviert. Dieses Feature kann in den PC-Einstellungen unter **Datum und Uhrzeit** deaktiviert werden. Die Deaktivierung des Windows-Zeitdiensts hat keinen direkten Einfluss auf Apps oder andere Dienste. Ohne zuverlässige Zeitquelle kann jedoch die Zeitangabe Ihres PCs von der Zeitangabe anderer PCs im Netzwerk oder Internet abweichen. Apps und Dienste, die auf eine genaue Zeitangabe angewiesen sind, werden unter Umständen nicht mehr korrekt ausgeführt, wenn zwischen den PCs im Netzwerk ein erheblicher Zeitunterschied besteht.

Seitenanfang

Windows-Problembehandlung

Funktionsweise

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 der 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

Sie können die Ergebnisse der Problembehandlung in der Systemsteuerung unter "Problembehandlung" löschen. Klicken Sie auf **Verlauf anzeigen**, wählen Sie ein Ergebnis aus, und klicken Sie dann auf **Löschen**.

Seitenanfang

Arbeitsordner

Funktionsweise

Arbeitsordner sind Ordner auf Ihrem PC, die automatisch mit dem Dateiserver an Ihrem Arbeitsplatz synchronisiert werden.

Gesammelte, verarbeitete, gespeicherte und übertragene Informationen

Wenn Sie eine Datei in einem Arbeitsordner speichern, wird diese Datei automatisch mit einem Dateiserver synchronisiert, der an Ihrem Arbeitsplatz verwaltet wird. Dateien, die von andere PCs aus in Ihrem Arbeitsordner gespeichert werden, werden mit Ihrem PC synchronisiert.

Verwendung der Informationen

Windows sendet und empfängt die Dateien in Ihren Arbeitsordnern, um die Synchronisierung der Ordner zu gewährleisten. Die Verwendung der Informationen, die auf den Servern an Ihrem Arbeitsplatz gespeichert sind, unterliegt den Datenschutzrichtlinien an Ihrem Arbeitsplatz.

Auswahl und Steuerung

Die Verbindung zwischen Ihrem PC und den Arbeitsordnern kann in den PC-Einstellungen unter **Arbeitsplatz** verwaltet werden.

Seitenanfang

Arbeitsplatz

Unter "Arbeitsplatz" können Sie eine Verbindung zwischen Ihrem Gerät und Windows (separates Abonnement von Microsoft erforderlich) oder einem anderen Verwaltungsdienst eines Drittanbieters herstellen. Wenn Sie dem Firmenadministrator die Verwaltung Ihres PCs über Arbeitsplatz erlauben, kann der Firmenadministrator u. a. folgende Aufgaben ausführen: Erzwingen von Sicherheitsrichtlinien auf dem PC, Installieren von Apps, Anzeigen bestimmter Konfigurationsinformationen und anderer Informationen auf dem PC sowie Ausführen weiterer Verwaltungsaufgaben. Weitere Informationen zur Verwendung dieses Features in Ihrem Unternehmen erhalten Sie vom

Datenschutzrichtlinien- oder Systemadministrator Ihres Unternehmens.

Gesammelte, verarbeitete und übertragene Informationen

Beim Einrichten und Verwenden des Arbeitsplatzes kommuniziert Ihr PC mit dem Geräteverwaltungsdienst, der von Ihrem Unternehmen genutzt wird und gegebenenfalls von Microsoft gehostet wird. Die Anmeldeinformationen, mit deren Hilfe Sie eine Verbindung mit dem Arbeitsplatz herstellen, werden an den Dienst gesendet.

Verwendung der Informationen

Die an den Geräteverwaltungsdienst gesendeten Informationen werden dazu verwendet, eine Verbindung zwischen dem Dienst und Ihrem PC herzustellen und Ihnen die Installation einer Self-Service-App aus dem Windows Store zu ermöglichen. Weitere Informationen zur Self-Service-App erhalten Sie vom Sicherheitsrichtlinien- oder Systemadministrator Ihres Unternehmens.

Auswahl und Steuerung

Wenn "Arbeitsplatz" von Ihrem Unternehmen verwendet wird, können Sie die Verbindung zum Arbeitsplatz in den PC-Einstellungen unter **Netzwerk** herstellen und trennen. Nachdem Sie eine Verbindung zwischen dem PC und dem Dienst hergestellt haben, können Sie Informationen zur Verbindung anzeigen oder die Verbindung jederzeit trennen.

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 8.1 und Windows Server 2012 R2

Diese Seite ist eine Ergänzung der Datenschutzbestimmungen für Windows 8.1 und Windows Server 2012 R2 ("Windows-Datenschutzbestimmungen") und umfasst folgende Abschnitte:

- Schwerpunkte
- Die Bestimmungen: Diese enthalten die vollständigen Windows 8.1-Datenschutzbestimmungen sowie Links zu Datenschutzbestimmungen für Windows-Features, für die eigene Datenschutzbestimmungen vorhanden sind.
- Features – Ergänzung: Hier werden die Features beschrieben, die sich auf den Datenschutz in Windows 8.1 und Windows Server 2012 R2 auswirken.
- **Apps – Ergänzung** (diese Seite): Hier werden die Apps beschrieben, die sich auf den Datenschutz in Windows 8.1 auswirken. Außerdem finden Sie hier Links zu den Datenschutzbestimmungen der einzelnen Apps.

- Server – Ergänzung: Hier werden die zusätzlichen Features beschrieben, die sich auf den Datenschutz in Windows Server 2012 R2 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.

Wenn Sie sich beim Einrichten des PCs für die Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) entscheiden, wird von diesen Apps ein Bericht mit Informationen zur App-Verwendung sowie zu Leistung und Zuverlässigkeit der jeweiligen App generiert. Microsoft nutzt die CEIP-Informationen, um seine Produkte und Dienste zu verbessern. Die Informationen werden nicht dazu verwendet, Sie zu identifizieren, Kontakt mit Ihnen aufzunehmen oder gezielte Werbung zu schalten. CEIP kann in den PC-Einstellungen deaktiviert werden. Weitere Informationen finden Sie in den CEIP-Datenschutzbestimmungen.

Über die folgenden Links gelangen Sie zu Datenschutzbestimmungen der jeweiligen App:

Wecker

Rechner

Kalender

Kamera

Finanzen

Ernährung

Spiele

Gesundheit

Hilfe + Tipps

Mail

Karten

Musik

Nachrichten

Kontakte

Reader

Leseliste

Scan

Skype

Audiorekorder

Sport

Reisen

Video

Wetter

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 8.1 und Windows Server 2012 R2

Auf dieser Seite

Diese Seite ist eine Ergänzung zu den Datenschutzbestimmungen für Windows 8.1 und Windows Server 2012 R2 („Windows-Datenschutzbestimmungen"). Die Datenschutzbestimmungen umfassen folgende Abschnitte:

- Highlights
- Bestimmungen, die die vollständigen Windows 8.1-Datenschutzbestimmungen darstellen und Links zu Datenschutzbestimmungen für Windows-Features enthalten, für die eigene Datenschutzbestimmungen vorhanden sind.
- Features – Ergänzung: Hier werden die Features beschrieben, die sich auf den Datenschutz in Windows 8.1 und Windows Server 2012 R2 auswirken.
- Apps – Ergänzung: Hier werden die Apps beschrieben, die sich auf den Datenschutz in Windows 8.1 auswirken.

- **Server – Ergänzung** (diese Seite): Hier werden die zusätzlichen Features beschrieben, die sich auf den Datenschutz in Windows Server 2012 R2 auswirken.

Sie sollten sich sowohl die vollständigen Windows-Datenschutzbestimmungen als auch alle geltenden Ergänzungen durchlesen, damit Sie die Datenerhebungs- und Nutzungspraktiken kennen, die für ein bestimmtes Feature oder einen Dienst von Windows relevant sind. Weitere Informationen finden Sie in diesem Whitepaper für Administratoren.

Informationen zu den datenschutzbezogenen Auswirkungen der Features in Windows Server 2012 R2 Essentials finden Sie in den Datenschutzbestimmungen für Windows Server 2012 R2 Essentials und Windows Server Essentials Experience.

Protokollierung des Benutzerzugriffs

Funktionsweise dieses Features

Die Benutzerzugriffsprotokollierung (User Access Logging, UAL) sammelt und aggregiert Datensätze von Clientanforderungen der Serverrollen (sowohl Benutzer- als auch Geräteanforderungen) und von installierten Produkten (sofern für UAL registriert) auf dem lokalen Server. Diese Daten, in Form von IP-Adressen, Benutzernamen und in manchen Fällen Hostnamen und/oder Identitäten virtueller Computer, werden in den lokalen ESE-Datenbanken (Extensible Storage Engine) gespeichert und sind nur für Administratoren zugänglich. UAL umfasst einen WMIv2-Anbieter und zugehörige Windows PowerShell-Cmdlets zum Abrufen von Benutzerzugriffsdaten, die für die Offlineverwaltung der CAL-Berechtigungen (Client Access License, Clientzugriffslizenz) von Kunden vorgesehen sind, bei der tatsächliche Datensätze von eindeutigen Clientanforderungen wichtig sind.

Gesammelte, verarbeitete und übertragene Informationen

IP-Adressen, Benutzernamen und in manchen Fällen Hostnamen (sofern die DNS-Rolle installiert ist) sowie Identitäten virtueller Computer (sofern die Hyper-V-Rolle installiert ist) werden lokal auf dem Server gesammelt, wenn UAL aktiviert ist. Es werden keine erfassten Daten an Microsoft gesendet.

Verwendung von Informationen

Die UAL-Daten werden den Administratoren über lokale ESE-Datenbanken, den WMI-Anbieter und Windows PowerShell-Cmdlets zur Verfügung gestellt. Diese Daten werden in Windows ausschließlich für das UAL-Feature verwendet.

Auswahl und Steuerung

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

Seitenanfang

Server-Manager

Funktionsweise dieses Features

Server-Manager ist ein Verwaltungstool, mit dem ein Administrator Server überwachen und den allgemeinen oder rollenspezifischen Status anzeigen kann, um Verwaltungsaufgaben auszuführen oder auf andere Serververwaltungstools zuzugreifen.

Gesammelte, verarbeitete und übertragene Informationen

Von Server-Manager werden von einem Server, der vom

Administrator verwaltet wird, die folgenden Arten von Informationen gesammelt:

- **Allgemeine Serverinformationen:** NetBios-Name und vollqualifizierter Domänenname (FQDN), die für das Feature „Verwalten als" eingegebenen Kontoanmeldeinformationen, IPv4-Adresse, IPv6-Adresse, Verwaltbarkeitsstatus, Beschreibung, Betriebssystemversion und -typ, letztes Update, Prozessoren, Arbeitsspeicher, Clustername, Clusterobjekttyp, Aktivierungsstatus, SKU, Betriebssystemarchitektur, 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 aus Windows und anderen vom Administrator ausgewählten Protokollen.

- **Alle Dienste:** Name, Status und Starttyp.

- **Serverrolleninformationen:** BPA-Ergebnisse (Best Practice Analyzer) für die auf dem Server installierten Rollen.

- **Leistungsinformationen:** Beispiele für Leistungsindikatoren sowie Benachrichtigungen für CPU-Auslastung und verfügbaren Arbeitsspeicher.

Verwendung von Informationen

Diese Informationen werden in Server-Manager gespeichert und nicht an Microsoft gesendet. Sie werden in Server-Manager angezeigt, um Administratoren bei der Überwachung der Systeme zu unterstützen.

Auswahl und Steuerung

Ein Administrator kann sich für oder gegen das Sammeln von Daten von einem beliebigen (außer dem lokalen) Server entscheiden, indem er den entsprechenden Server zu Server-

Manager hinzufügt bzw. daraus entfernt. Ein Administrator kann explizit Anmeldeinformationen für die Verbindung mit einen Remoteserver bereitstellen. Der Administrator wird aufgefordert, der lokalen Speicherung von Anmeldeinformationen in Server-Manager ausdrücklich zuzustimmen, und kann diese Anmeldeinformationen jederzeit löschen.

Seitenanfang

Active Directory-Verbunddienste

Funktionsweise dieses Features

Die Active Directory-Verbunddienste (AD FS) sind eine Unternehmenslösung für Verbund und einmaliges Anmelden (SSO) für lokale und andere netzwerkbasierte Apps. Mit AD FS können Administratoren Benutzern die Zusammenarbeit in Organisationen und den einfachen Zugriff auf Apps in lokalen oder anderen Netzwerken ermöglichen und dabei die Sicherheit der Apps wahren. Von AD FS wird ein Sicherheitstokendienst verwendet, der Active Directory-Domänendienste (Active Directory Domain Services, AD DS) nutzt, um mithilfe verschiedener Protokolle Benutzer zu authentifizieren und ihnen Sicherheitstoken auszustellen. Das Token ist digital signiert und enthält Ansprüche des Benutzers, die aus AD DS, LDAP (Lightweight Directory Access-Protokoll), SQL Server, einem benutzerdefinierten Speicher oder einer Kombination davon stammen.

Gesammelte, verarbeitete und übertragene Informationen

Die Anmeldeinformationen eines Benutzers werden erfasst, wenn sich der Benutzer bei AD FS authentifiziert. Die Anmeldeinformationen werden sofort zur Authentifizierung an Active Directory-Domänendienste gesendet und von AD FS nicht lokal gespeichert. Die Benutzerattribute in Active Directory-Domänendienste können verwendet werden, um ausgehende Ansprüche zu generieren. Dies hängt von den Anspruchsregeln ab, die ein AD FS-Administrator konfiguriert

hat. Ausgehende Ansprüche werden an vertrauenswürdige Partner gesendet, für die ein AD FS-Administrator eine Vertrauensstellung eingerichtet hat. Es werden keine Informationen an Microsoft gesendet.

Verwendung von Informationen

Microsoft hat keinen Zugriff auf diese Informationen. Sie sind ausschließlich für die Verwendung durch den Kunden bestimmt.

Auswahl und Steuerung

Verwenden Sie AD FS, wenn Sie möchten, dass von AD FS Daten gesammelt und an vertrauenswürdige Partner gesendet werden.

Seitenanfang

IP-Adressverwaltung

Funktionsweise dieses Features

Mithilfe der IP-Adressverwaltung (IP Address Management, IPAM) können Serveradministratoren die IP-Adresse, den Hostnamen und die Clientbezeichner (z. B. die MAC-Adresse in IPv4 und DUID in IPv6) von Computern und Geräten in einem Netzwerk mit Benutzeranmeldeinformationen nachverfolgen.

Gesammelte, verarbeitete und übertragene Informationen

Der IPAM-Server sammelt Überwachungsprotokolle und Ereignisse von DHCP-Servern, Domänencontrollern und Netzwerkrichtlinienservern und speichert dann die IP-Adresse sowie den Hostnamen, Clientbezeichner und Benutzernamen des angemeldeten Benutzers lokal. Ein Serveradministrator kann die gesammelten Protokolle mit der IPAM-Konsole basierend auf der IP-Adresse und dem Hostnamen, Clientbezeichner und Benutzernamen durchsuchen. Keine dieser Informationen wird an Microsoft gesendet.

Verwendung von Informationen

Microsoft hat keinen Zugriff auf diese Informationen. Sie sind ausschließlich für die Verwendung durch den Kunden bestimmt.

Auswahl und Steuerung

IPAM wird nicht standardmäßig installiert und muss vom Serveradministrator installiert werden. Nach der IPAM-Installation ist die IP-Adressenüberwachung automatisch aktiviert. Sie können die IP-Adressenüberwachung auf einem Server, auf dem IPAM installiert ist, wie folgt deaktivieren: Starten Sie auf dem IPAM-Server die Aufgabenplanung, navigieren Sie unter „Microsoft\Windows\IPAM" zu „Überwachungsaufgabe" und deaktivieren Sie dann die Aufgabe.

Seitenanfang

Einheitlicher Remotezugriff

Funktionsweise dieses Features

Mit dem Feature für einheitlichen Remotezugriff können Remotebenutzer über das Internet eine Verbindung mit einem privaten Netzwerk, z. B. einem Firmennetzwerk, herstellen. Das Feature für einheitlichen Remotezugriff verwendet DirectAccess, um Remoteclientcomputern mit Windows 8 eine unterbrechungsfreie und transparente Verbindung mit Firmennetzwerken zu ermöglichen. Das Feature für einheitlichen Remotezugriff umfasst zudem eine RAS-Funktion (Remote Access Service), die herkömmliche VPN-Dienste bereitstellt, einschließlich Standort-zu-Standort-Verbindungen mit lokalen oder anderen Netzwerken.

Gesammelte, verarbeitete und übertragene Informationen

Zur Benutzerüberwachung beim einheitlichen Remotezugriff speichert der DirectAccess-Server Details zu den Remotebenutzern, die eine Verbindung mit dem privaten Netzwerk herstellen. Hierzu gehören Informationen wie

Hostname des Remotebenutzers, Active Directory-Benutzername und öffentliche IP-Adresse des Remoteclients (wenn sich der Client hinter einer Netzwerkadressübersetzung (NAT) befindet, ist es die öffentliche IP-Adresse). Diese Daten können mit Zustimmung des Administrators auch in der internen Windows-Datenbank (WID) oder auf RADIUS-Servern gespeichert werden. Nur ein DirectAccess-Administrator (ein Domänenbenutzer mit einem lokalen Administratorkonto), der auf einen Server zugreift, kann diese Informationen anzeigen.

Verwendung von Informationen

Diese Informationen werden vom Administrator zum Beheben von Problemen mit Clientverbindungen, zu Überwachungszwecken oder zum Prüfen der Richtlinieneinhaltung verwendet. Es werden keine Informationen an Microsoft gesendet.

Auswahl und Steuerung

Die Remoteclientüberwachung ist standardmäßig aktiviert und kann nicht deaktiviert werden. Die Überwachungsdaten werden nur in der internen Windows-Datenbank (WID) oder auf RADIUS-Servern gespeichert, wenn ein Administrator die Kontoführung für die Verwendung dieser Optionen konfiguriert hat. Wurde die Kontoführung nicht entsprechend von einem Administrator konfiguriert, werden keine dieser Informationen gespeichert. Ein Administrator kann auch die Kontoführung auf einem RAS-Server so konfigurieren, dass Benutzername und IP-Adresse nicht gespeichert werden.

Seitenanfang

Remotedesktopdienste

Funktionsweise dieses Features

Die Remotedesktopdienste (RDS) stellen eine Plattform bereit, um Unternehmen bei der Umsetzung einer zentralisierten Desktopstrategie und der Verwaltung von Desktops und Apps zu unterstützen und die Flexibilität und

Einhaltung von Richtlinien zu verbessern, während gleichzeitig die Datensicherheit erhöht wird.

Gesammelte, verarbeitete und übertragene Informationen

Zur RDS-Benutzerüberwachung speichert der Remotedesktop-Sitzungshostserver Informationen zu Remotebenutzern, die eine Verbindung mit RDS-Ressourcen herstellen. Hierzu gehören Informationen wie Hostname des Remotebenutzers, Active Directory-Benutzername und öffentliche IP-Adresse des Remoteclients (wenn sich der Client hinter einer Netzwerkadressübersetzung (NAT) befindet, ist es die öffentliche IP-Adresse). Diese Daten werden automatisch in der internen Windows-Datenbank (WID) oder auf Servern mit SQL Server gespeichert, wenn Benutzer eine Verbindung herstellen. Es werden keine Informationen an Microsoft gesendet. Nur Domänenbenutzer mit einem lokalen Administratorkonto können auf diese Informationen zugreifen und sie anzeigen.

Verwendung von Informationen

Diese Informationen werden vom Administrator zur Behandlung von Problemen mit Clientverbindungen, zu internen Überwachungszwecken oder zum Prüfen der Richtlinieneinhaltung verwendet. Es werden keine Informationen an Microsoft gesendet.

Auswahl und Steuerung

Die Clientüberwachung ist standardmäßig aktiviert und kann nicht deaktiviert werden. Die Überwachungsinformationen werden in der internen Windows-Datenbank (WID) oder auf Servern mit SQL Server gespeichert.

Seitenanfang

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

Funktionsweise dieses Features

Weitere Informationen zu diesen Features finden Sie auf der Registerkarte Features – Ergänzung oder in diesem Whitepaper für Administratoren.

Gesammelte, verarbeitete und übertragene Informationen

Mehr über die Informationen, die von diesen Features erfasst, verarbeitet und übertragen werden, erfahren Sie im Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) und in der Windows-Fehlerberichterstattung (WER) auf der Registerkarte Features – Ergänzung .

Verwendung von Informationen

Weitere Informationen zur Verwendung der von diesen Features erfassten Informationen finden Sie im Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) und in der Windows-Fehlerberichterstattung (WER) auf der Registerkarte Features – Ergänzung .

Auswahl und Steuerung

CEIP ist standardmäßig deaktiviert, während WER standardmäßig so eingerichtet ist, dass Sie vor dem Senden von Absturzberichten an Microsoft benachrichtigt werden. Sie können CEIP sowohl über den Server-Manager und die Systemsteuerung als auch über die Befehlszeile aktivieren und deaktivieren. WER kann ausschließlich über die Befehlszeile gesteuert werden.

Zum Aktivieren bzw. Deaktivieren von CEIP über die Systemsteuerung klicken Sie auf **System und Wartung**und dann auf **Problemberichte und -lösungen**. Klicken Sie dann unter **Siehe auch**auf **Einstellungen für das Programm zur Verbesserung der Benutzerfreundlichkeit** , um CEIP zu aktivieren oder zu deaktivieren.

Server-Manager-Steuerelemente

Lokaler Server

- Programm zur Verbesserung der Benutzerfreundlichkeit

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

- Programm zur Verbesserung der Benutzerfreundlichkeit deaktivieren
  Öffnen Sie den Server-Manager und wählen Sie **Lokaler Server**aus. Klicken Sie auf den Link für das Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP), wählen Sie im Dialogfeld **Nein, ich möchte nicht teilnehmen** aus und klicken Sie dann auf **OK**.

- Windows-Fehlerberichterstattung aktivieren
  Öffnen Sie den Server-Manager und wählen Sie **Lokaler Server**aus. Klicken Sie auf den Link für die Windows-Fehlerberichterstattung (WER), wählen Sie **Ja, automatisch Zusammenfassungsberichte senden**aus und klicken Sie dann auf **OK**.

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

Mehrere Computer

- Programm zur Verbesserung der Benutzerfreundlichkeit aktivieren
  Öffnen Sie den Server-Manager und wählen Sie **Alle Server**aus. Wählen Sie auf der Kachel „Server" alle Server aus (STRG+A), klicken Sie mit der rechten Maustaste und wählen Sie **Automatisches Feedback für Windows konfigurieren** aus. Wählen Sie auf der

Registerkarte „Programm zur Verbesserung der Benutzerfreundlichkeit“ die Option **Ja, ich möchte teilnehmen (empfohlen)**aus. Wenden Sie diese Einstellung auf alle Server an, indem Sie das Kontrollkästchen neben dem Servernamen im Steuerelement "Server auswählen" aktivieren und dann auf **OK**.

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

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

- Windows-Fehlerberichterstattung deaktivieren
  Öffnen Sie den Server-Manager und wählen Sie **Alle Server**aus. Wählen Sie auf der Kachel „Server“ alle Server aus (STRG+A), klicken Sie mit der rechten

Maustaste und wählen Sie **Automatisches Feedback für Windows konfigurieren** aus. Aktivieren Sie auf der Registerkarte „Windows-Fehlerberichterstattung“ die Option **Nein, ich möchte nicht teilnehmen**aus. Wenden Sie diese Einstellung auf alle Server an, indem Sie das Kontrollkästchen neben dem Servernamen im Steuerelement "Server auswählen" aktivieren und dann auf **OK**.

Seitenanfang

Softwareinventurprotokollierung

Funktionsweise dieses Features

Die Softwareinventurprotokollierung (Software Inventory Logging, SIL) stellt einen neuen Satz von WMI-Klassen und PowerShell-Cmdlets zum Vereinfachen des grundlegenden Bestands des Windows Server-Betriebssystems, der auf dem Windows Server installierten Software sowie der Merkmale der auf dem Server ausgeführten Software bereit. Darüber hinaus kann SIL (nach der Aktivierung durch einen Administrator) stündlich Daten vom WMI-Anbieter erfassen und diese über das Netzwerk an einen Aggregationsserver übermitteln, wenn eine Einheit mithilfe des Cmdlets „Set-SilLogging - TargerUri“ spezifiziert ist.

Gesammelte, verarbeitete und übertragene Informationen

Daten können nach der Konfiguration durch den Administrator über das Netzwerk an einen Aggregationsserver übermittelt werden. Standardmäßig werden keine Daten erfasst, verarbeitet oder übertragen. Zu diesen Daten gehören:

- Name des Windows Server und Version des installierten Betriebssystems
- Eine Liste von Namen, Versionen und Herausgebern der auf dem Server installierten Software und Installationsdatum dieser Software

- Der vollqualifizierte Domänenname des Serversystems
- Anzahl, Typ und Hersteller der auf dem Serversystem installierten oder zugewiesenen Prozessoren, logischen Prozessoren und Kerne

Erfasste und verarbeitete, jedoch nicht standardmäßig übertragene Daten (auch bei aktivierten stündlichen Aufgaben und vom Administrator angegebenem Zielaggregator):

- Klasse „MsftSil_UalAccess" und Cmdlet „Get-SilUalAccess", verarbeitet zwei Tage vor der Abfrage mit dem Feature „Protokollierung des Benutzerzugriffs" (User Access Logging, UAL) die Anzahl der eindeutigen Benutzer insgesamt sowie die Geräte jeder einzelnen Rolle oder jedes registrierten Produkts. Hierbei handelt es sich um eine Zählung. Benutzer- oder Geräteinformationen werden weder ausgegeben noch übertragen. Die Verarbeitung der Benutzer- und Geräteinformationen von SIL aus den UAL-Klassen ist erforderlich, um die Anzahl selbst zu berechnen. Nur ein Administrator kann über einen lokalen Computer auf diese Daten zugreifen. Der für die UAL-APIs erforderliche Zugriff wird von SIL nicht geändert.

Es werden keine erfassten Daten an Microsoft gesendet.

Verwendung von Informationen

Die SIL WMI-Anbieter sammeln Daten von anderen APIs, die bereits im System vorhanden sind. Daten können nach der Konfiguration durch den Administrator über das Netzwerk an einen Server für eine weitere Aggregation übermittelt werden. Standardmäßig werden keine Daten erfasst, verarbeitet oder übertragen. Im Fall der Klasse „MsftSil_UalAccess" und des Cmdlets „Get-SilUalAccess" stellen verarbeitete Daten zwei Tage vor der Abfrage mit dem Feature „Protokollierung des Benutzerzugriffs" (User Access Logging, UAL) die Anzahl der eindeutigen Benutzer insgesamt

sowie die Geräte jeder einzelnen Rolle oder jedes registrierten Produkts, jedoch keine identifizierenden Benutzer- oder Gerätedaten bereit. Obwohl diese WMI-Klasse und das Cmdlet im System vorhanden sind, sind diese nicht Teil der erfassten und stündlich an einen Aggregator weitergeleiteten SIL-Datennutzlast, außer SIL wurde von einem Systemadministrator hierfür konfiguriert.

Auswahl und Steuerung

Die stündliche Aufgabe von SIL ist standardmäßig deaktiviert. Alle SIL-APIs sind für die Abfrage von Administratoren des lokalen Systems standardmäßig verfügbar. Die stündliche Aufgabe von SIL kann mithilfe der Cmdlets „Start-SilLogging" und „Stop-SilLogging" gestartet und angehalten werden, während der Server ausgeführt wird. Das Cmdlet „Set-SilLogging" ermöglicht den Serveradministratoren das Festlegen von Datum und Uhrzeit der stündlichen Aufgabe (Standardwert: 3 Uhr des lokalen Systems), des URI Uniform Resource Identifier (URI) eines Zielaggregationsservers und des erforderlichen Fingerabdrucks des Zertifikats, um eine vertrauenswürdige Übertragung der Daten zu gewährleisten.

Alle SIL-Konfigurationseinstellungen, einschließlich Start und Ende der stündlichen Aufgabe, können in der Registrierung geändert werden und sollen nur bei virtuellen Computern und nur vor dem ersten Systemstart erfolgen.

Seitenanfang