Aktualne informacje o praktykach przetwarzania danych stosowanych przez Microsoft zawiera Oświadczenie o ochronie prywatności w firmie Microsoft. Tam również możesz się dowiedzieć o najnowszych udostępnianych przez nas narzędziach służących uzyskiwaniu dostępu i kontrolowaniu danych oraz o metodach kontaktowania się z nami w razie pytań dotyczących prywatności.

Oświadczenie o ochronie prywatności w systemach Windows 8.1 i Windows Server 2012 R2

Na tej stronie

Dane użytkownika

Opcje wybierane przez użytkownika

Używanie informacji

Kontakt z nami

Ostatnia aktualizacja: kwiecień 2014

W tych wyróżnionych zagadnieniach pełnych zasad zachowania poufności informacji dotyczących systemów Windows 8.1 i Windows Server 2012 R2 („zasad zachowania poufności informacji dotyczących systemu Windows”) wyjaśniono ogólnie wybrane metody zbierania i używania danych związane z systemami Windows 8.1 i Windows Server 2012 R2 („Windows”). Skupiono się w nich na funkcjach online i nie stanowią one pełnego opisu. Nie dotyczą innych witryn, produktów ani usług firmy Microsoft działających w trybie online czy offline.

Niniejsze zasady zachowania poufności informacji składają się z następujących sekcji:

- **Najważniejsze informacje** (ta strona)

- Instrukcja, czyli pełny tekst zasad zachowania poufności informacji w systemie Windows 8.1 z uwzględnieniem linków do zasad zachowania poufności informacji dotyczących funkcji systemu Windows, które nie mają własnych zasad w tym zakresie

- Uzupełnienie dotyczące funkcjizawierające opis funkcji mających wpływ na ochronę prywatności w systemach Windows 8.1 i Windows Server 2012 R2

- Uzupełnienie dotyczące aplikacjizawierające opis aplikacji mających wpływ na ochronę prywatności w systemie Windows 8.1

- Uzupełnienie dotyczące wersji serwerowejzawierające opis dodatkowych funkcji mających wpływ na ochronę prywatności w systemie Windows Server 2012 R2

Aby uzyskać więcej informacji o tym, jak chronić komputer osobisty, dane osobowe i rodzinę w trybie online, odwiedź centrum bezpieczeństwa i zabezpieczeń.

Dane użytkownika

- Niektóre funkcje systemu Windows pytają użytkownika o pozwolenie na zbieranie i używanie informacji znajdujących się na jego komputerze (w tym danych osobowych). System Windows używa tych informacji zgodnie z opisami w pełnych zasadach zachowania poufności informacji w systemieWindows 8.1, a także w Uzupełnienie dotyczące funkcji, Uzupełnienie dotyczące aplikacji i Uzupełnienie dotyczące wersji serwerowej.

- Niektóre funkcje systemu Windows umożliwiają użytkownikowi (za jego zgodą) udostępnianie danych osobowych przez Internet.

- Jeśli użytkownik zdecyduje się zarejestrować oprogramowanie, zostanie poproszony o podanie danych osobowych.

- W celu zwalczania piractwa komputerowego i zagwarantowania klientom firmy Microsoft dostępu do oprogramowania o

oczekiwanej jakości wymagana jest aktywacja systemu Windows. Podczas aktywacji do firmy Microsoft są wysyłane niektóre informacje dotyczące komputera.

- W systemie Windows można logować się za pomocą konta Microsoft, które umożliwia automatyczne synchronizowanie ustawień systemu Windows i automatyczne logowanie się w aplikacjach i na stronach sieci Web. System Windows nie wymaga logowania się za pomocą konta Microsoft do korzystania z usług e-mail lub sieci społecznościowych innych firm. Jeśli jednak dana firma udostępnia aplikację w Sklepie, trzeba zalogować się w Sklepie za pomocą konta Microsoft, aby można było zainstalować daną aplikację. Po utworzeniu konta Microsoft należy podać określone informacje osobiste, takie jak region geograficzny czy data urodzenia.

- Dodatkowe szczegóły

Góra strony

Opcje wybierane przez użytkownika

- System Windows udostępnia wiele sposobów sterowania tym, jak funkcje systemu Windows przesyłają informacje przez Internet. Aby uzyskać więcej informacji o tym, jak sterować tymi funkcjami, zobacz Uzupełnienie dotyczące funkcji, Uzupełnienie dotyczące aplikacji i Uzupełnienie dotyczące wersji serwerowej.

- Aby pomóc w zwiększeniu komfortu działania, niektóre funkcje korzystające z Internetu są domyślnie włączone.

- Dodatkowe szczegóły

Góra strony

Używanie informacji

- Firma Microsoft używa zbieranych informacji do udostępniania funkcji, z których korzysta użytkownik, i do świadczenia usług, o które się zwraca. Firma Microsoft używa ich też do udoskonalania swoich produktów i usług. Niekiedy firma Microsoft udostępnia

informacje działającym w jej imieniu podwykonawcom, którzy pomagają jej w świadczeniu usług. Dostęp do tych informacji mają tylko firmy, które muszą z nich korzystać w celach służbowych. Te firmy są zobowiązane do zachowania poufności tych informacji i nie mogą korzystać z nich w żadnym innym celu.

- Dodatkowe szczegóły

Góra strony

Kontakt z nami

Aby uzyskać więcej informacji dotyczących metod ochrony prywatności stosowanych przez firmę Microsoft, zobacz pełne zasady zachowania poufności informacji w systemie Windows 8.1. Ewentualnie skontaktuj się z nami, wypełniając ten formularz sieci Web.

Góra strony

Aktualne informacje o praktykach przetwarzania danych stosowanych przez Microsoft zawiera Oświadczenie o ochronie prywatności w firmie Microsoft. Tam również możesz się dowiedzieć o najnowszych udostępnianych przez nas narzędziach służących uzyskiwaniu dostępu i kontrolowaniu danych oraz o metodach kontaktowania się z nami w razie pytań dotyczących prywatności.

Oświadczenie o ochronie prywatności w systemach Windows 8.1 i Windows Server 2012 R2

Na tej stronie

Zbieranie i używanie informacji dotyczących użytkownika

Zbieranie i używanie informacji o komputerze użytkownika

Bezpieczeństwo informacji

Zmiany w niniejszych zasadach

Ostatnia aktualizacja: kwiecień 2014

Te zasady dotyczą systemów Windows 8.1 i Windows Server 2012 R2 („Windows”). Określone składniki systemu Windows mają własne zasady zachowania poufności informacji, które także znajdują się na tej stronie. Wymieniono tu także zasady zachowania poufności informacji dotyczące oprogramowania i usług powiązanych z systemem Windows oraz wcześniejszych wersji.

Aby uzyskać informacje o konkretnych funkcjach, zobacz Uzupełnienie dotyczące funkcji, Uzupełnienie dotyczące aplikacjii Uzupełnienie dotyczące wersji serwerowej. Informacje o systemach Windows Embedded Industry Pro i Windows Embedded Industry Enterprise można znaleźć w tych zasadach.

W tych zasadach skupiono się na funkcjach komunikujących się z

zachowania poufności informacji

Źródła dodatkowych informacji

Internetem. Ta wersja nie zawiera pełnej listy zasad.

Zbieranie i używanie informacji dotyczących użytkownika

Informacje osobiste zebrane od użytkownika są wykorzystywane przez firmę Microsoft oraz jej przedstawicielstwa i podmioty stowarzyszone na potrzeby udostępniania mu używanych przez niego funkcji oraz dostarczenia usług lub wykonania transakcji, które zamówił bądź autoryzował. Informacje te mogą być również używane do analizowania i usprawniania produktów oraz usług firmy Microsoft.

Poza sytuacjami opisanymi w tych zasadach dane osobowe podane przez użytkownika nie będą przekazywane innym podmiotom bez jego zgody. Niekiedy firma Microsoft zleca innym podmiotom świadczenie w jej imieniu ograniczonych usług, takich jak przeprowadzenie analizy statystycznej jej usług. Tacy usługodawcy mogą uzyskać tylko te dane osobowe, które są potrzebne do świadczenia danej usługi. Ponadto obowiązuje ich zakaz używania tych informacji do jakichkolwiek innych celów.

Firma Microsoft może uzyskać dostęp do informacji o użytkowniku, w tym treści jego komunikacji, i ujawnić je w celu (a) zachowania zgodności z przepisami prawa lub w odpowiedzi na zgodne z prawem żądanie bądź procedurę prawną; (b) ochrony praw lub własności firmy Microsoft lub jej klientów, w tym egzekwowania postanowień umów lub zasad korzystania z oprogramowania przez użytkownika; lub (c) działania w dobrej wierze, że taki dostęp lub ujawnienie jest wymagane w celu ochrony bezpieczeństwa osobistego pracowników firmy Microsoft, jej klientów lub osób trzecich.

Informacje zbierane przez firmę Microsoft lub wysyłane do niej przez system Windows 8.1 mogą być przechowywane i przetwarzane w Stanach Zjednoczonych albo w dowolnym innym kraju, w którym mieści się siedziba firmy Microsoft albo jej podmioty stowarzyszone, przedstawicielstwa lub dostawcy usług. Firma Microsoft przestrzega zasad Safe Harbor, zgodnie z wytycznymi Departamentu Handlu Stanów Zjednoczonych dotyczącymi zbierania, używania i przechowywania danych pochodzących z Unii Europejskiej, Europejskiego Obszaru Gospodarczego i Szwajcarii.

Góra strony

Zbieranie i używanie informacji o komputerze użytkownika

Podczas używania programów udostępniających funkcje internetowe do odwiedzanych witryn sieci Web i używanych usług online są wysyłane informacje o komputerze użytkownika („standardowe informacje o komputerze”). Standardowe informacje o komputerze to zwykle dane, takie jak adres IP, wersja systemu operacyjnego, wersja przeglądarki oraz ustawienia regionalne i językowe. W niektórych przypadkach mogą one również zawierać identyfikator sprzętu wskazujący producenta urządzenia, nazwę urządzenia i jego wersję. Informacje wysyłane przez daną funkcję lub usługę do firmy Microsoft obejmują również standardowe informacje o komputerze.

W szczegółowych informacjach o ochronie prywatności dotyczących poszczególnych funkcji systemu Windows w uzupełnieniu dotyczącym funkcji, uzupełnieniu dotyczącym aplikacji i uzupełnieniu dotyczącym wersji serwerowej oraz w informacjach dotyczących funkcji wymienionych w innym miejscu tej strony wyjaśniono, jakie dodatkowe informacje są zbierane i jak są używane.

Korzystając z zasad grupy, administratorzy mogą modyfikować wiele ustawień opisanych tutaj funkcji. Aby uzyskać więcej informacji, zobacz ten oficjalny dokument techniczny dla administratorów.

Góra strony

Bezpieczeństwo informacji

Firma Microsoft przywiązuje dużą wagę do zapewnienia bezpieczeństwa informacji użytkowników. Informacje są chronione przy użyciu odpowiednich technologii i procedur zabezpieczeń przed nieupoważnionym dostępem, użyciem lub ujawnieniem. Na przykład przechowujemy informacje dostarczane przez użytkowników na komputerach o ograniczonym dostępie, które znajdują się w kontrolowanych pomieszczeniach. Poufne informacje (takie jak numer karty kredytowej lub hasło) przesyłane za pośrednictwem Internetu są szyfrowane, na przykład za pomocą protokołu SSL (Secure Socket Layer).

Góra strony

Zmiany w niniejszych zasadach zachowania poufności informacji

Firma Microsoft co jakiś czas aktualizuje niniejsze zasady zachowania poufności informacji w celu uwzględnienia zmian w oferowanych produktach i usługach oraz opinii klientów. Wraz z ogłoszeniem zmian zostanie poprawiona data ostatniej aktualizacji, która znajduje się u góry tego dokumentu. W razie dokonania istotnych zmian w niniejszych zasadach lub w sposobie wykorzystywania informacji osobistych przez firmę Microsoft użytkownik zostanie powiadomiony o takich zmianach przed ich wprowadzeniem bezpośrednio lub za pośrednictwem ogłoszenia o zmianach. Firma Microsoft zachęca do okresowego przeglądania niniejszych zasad w celu zapoznania się ze stosowanymi przez nią sposobami ochrony danych użytkowników.

Góra strony

Źródła dodatkowych informacji

Firma Microsoft zachęca do przesyłania uwag dotyczących niniejszych zasad zachowania poufności informacji. W przypadku pytań związanych z niniejszymi zasadami lub wątpliwości dotyczących przestrzegania tych zasad przez firmę Microsoft można skontaktować się z firmą Microsoft za pomocą tego formularz sieci Web.

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

Góra strony

Aktualne informacje o praktykach przetwarzania danych stosowanych przez Microsoft zawiera Oświadczenie o ochronie prywatności w firmie Microsoft. Tam również możesz się dowiedzieć o najnowszych udostępnianych przez nas narzędziach służących uzyskiwaniu dostępu i kontrolowaniu danych oraz o metodach kontaktowania się z nami w razie pytań dotyczących prywatności.

Oświadczenie o ochronie prywatności w systemach Windows 8.1 i Windows Server 2012 R2

Na tej stronie

Aktywacja

Klient usług zarządzania prawami dostępu w usłudze Active Directory (AD RMS)

Identyfikator treści reklamowych

Inspekcja

Biometria

Szyfrowanie dysków

Ostatnia aktualizacja: kwiecień 2014

Ta strona stanowi uzupełnienie zasad zachowania poufności informacji w systemach Windows 8.1 i Windows Server 2012 R2 („zasad zachowania poufności informacji w systemie Windows”), które składają się z następujących sekcji:

- Najważniejsze informacje
- Instrukcja, czyli pełny tekst zasad zachowania poufności informacji w systemie Windows 8.1 z uwzględnieniem linków do zasad zachowania poufności informacji dotyczących funkcji systemu Windows, które nie mają własnych zasad w tym zakresie
- **Uzupełnienie dotyczące funkcji** (ta strona) zawierające opis funkcji mających wpływ na ochronę prywatności w systemach

funkcją BitLocker
Kontakty
Odnajdowanie i instalowanie urządzeń
Szyfrowania urządzeń
Funkcja DirectAccess
Centrum ułatwień dostępu
Podgląd zdarzeń
Filtr rodzinny
Faks
Personalizacja pisma ręcznego — automatyczna nauka
Grupa domowa
Edytor IME (Input Method Editor)
Udostępnianie połączenia internetowego
Drukowanie internetowe
Preferencje językowe
Usługi lokalizacyjne
Zarządzanie poświadczeniami
Nazwa i awatar
Rozpoznawanie sieci
Powiadomienia, aplikacje na ekranie

Windows 8.1 i Windows Server 2012 R2

- Uzupełnienie dotyczące aplikacjizawierające opis aplikacji mających wpływ na ochronę prywatności w systemie Windows 8.1
- Uzupełnienie dotyczące wersji serwerowejzawierające opis dodatkowych funkcji mających wpływ na ochronę prywatności w systemie Windows Server 2012 R2

Aby zapoznać się z działaniami w zakresie zbierania i używania danych dotyczącymi określonej funkcji lub usługi systemu Windows, należy przeczytać pełny tekst zasad zachowania poufności informacji i odpowiednie uzupełnienia lub autonomiczne zasady zachowania poufności informacji.

Aktywacja

Opis funkcji

Aktywacja pomaga ograniczyć rozpowszechnianie fałszywego oprogramowania, zapewniając klientom firmy Microsoft dostęp do oprogramowania o spodziewanej jakości. Aktywacja oprogramowania powoduje skojarzenie określonego klucza produktu z komputerem (sprzętem), na którym jest zainstalowane oprogramowanie. To skojarzenie zapobiega użyciu klucza produktu do aktywacji tej samej kopii oprogramowania na wielu komputerach. Niektóre zmiany składników sprzętowych lub oprogramowania komputera mogą wymagać ponownej aktywacji systemu Windows. W procesie aktywacji mogą zostać wykryte i wyłączone programy wykorzystujące luki w aktywacji (oprogramowanie omijające aktywację oprogramowania firmy Microsoft). Jeśli na komputerze jest obecny program wykorzystujący luki w procesie aktywacji, może to oznaczać, że dostawca oprogramowania lub sprzętu zmodyfikował oryginalne oprogramowanie firmy Microsoft w celu utworzenia nielegalnych kopii oprogramowania. Programy wykorzystujące luki w procesie aktywacji mogą zakłócać normalne działanie systemu.

Informacje zbierane, przetwarzane lub przesyłane

Podczas aktywacji do firmy Microsoft są wysyłane następujące

blokady i aktualizacje kafelków

Zamawianie odbitek

Pobieranie z wyprzedzeniem i wstępne uruchamianie

Asystent zgodności programów

Właściwości

Usługi zbliżeniowe

Połączenia dostępu zdalnego

Połączenia programów RemoteApp i pulpitu

Podłączanie pulpitu zdalnego

Logowanie się za pomocą konta Microsoft

Magazyn w chmurze usługi OneDrive

Synchronizacja ustawień

Technologia Teredo

Usługi modułu TPM (Trusted Platform Module)

Aktualizowanie certyfikatów głównych

Usługi aktualizacji

Wirtualne sieci

informacje:

- Kod produktu firmy Microsoft (pięciocyfrowy kod identyfikujący produkt Windows aktywowany przez użytkownika).
- Identyfikator partnera handlowego lub kod miejsca, który określa, gdzie produkt Windows został pierwotnie kupiony. Na przykład identyfikuje, czy produkt został kupiony w punkcie sprzedaży detalicznej, jest kopią ewaluacyjną, podlega programowi licencjonowania zbiorowego, czy też został wstępnie zainstalowany przez producenta komputera.
- Data przeprowadzenia instalacji i informacje o tym, czy instalacja przebiegła pomyślnie.
- Informacje pomocne w potwierdzeniu, czy klucz produktu systemu Windows nie został zmieniony.
- Marka i model komputera.
- Informacje o wersji systemu operacyjnego i oprogramowania.
- Ustawienia regionalne i językowe.
- Przypisany do komputera unikatowy numer nazywany unikatowym identyfikatorem globalnym (GUID).
- Klucz produktu (skrót) i identyfikator produktu.
- Nazwa, numer wersji i data wersji systemu BIOS.
- Numer seryjny woluminu dysku twardego (skrót).
- Wynik testu aktywacji. Zawiera kody błędów i informacje o znalezionych i wyłączonych programach wykorzystujących luki w procesie aktywacji oraz podobnym złośliwym lub nieautoryzowanym oprogramowaniu:
    - Identyfikator programu wykorzystującego luki w procesie aktywacji.
    - Obecny stan programu wykorzystującego luki w procesie aktywacji (wyczyszczony, poddany kwarantannie itp.).

prywatne

Program poprawy jakości obsługi klienta systemu Windows

Windows Defender

Raportowanie błędów systemu Windows

Kojarzenie plików systemu Windows

Pomoc systemu Windows

Pomoc zdalna

Windows Search

Instalator systemu Windows

Udostępnianie w systemie Windows

Windows SmartScreen

Rozpoznawanie mowy w systemie Windows

Sklep Windows

Usługa Czas systemu Windows

Rozwiązywanie problemów z systemem Windows

Foldery robocze

Miejsce pracy

Identyfikator producenta komputera.

- Nazwa pliku i skrót programu wykorzystującego luki w procesie aktywacji oraz skrót pokrewnych składników oprogramowania, które mogą wskazywać na obecność programu wykorzystującego luki w procesie aktywacji.

- Nazwa i skrót zawartości pliku instrukcji uruchamiania komputera. Jeśli licencja na system Windows jest udzielona na zasadach subskrypcji, zostaną wysłane również dane dotyczące sposobu działania subskrypcji. Oprócz tego są wysyłane standardowe informacje o komputerze.

- W przypadku używania kopii systemu Windows z licencją zbiorczą, na potrzeby której jest używany serwer aktywacji, do firmy Microsoft może zostać wysłany adres IP tego serwera.

Używanie informacji

Firma Microsoft używa tych informacji do potwierdzenia, że użytkownik korzysta z licencjonowanej kopii oprogramowania. Firma Microsoft nie używa tych informacji do kontaktowania się z poszczególnymi użytkownikami. Informacje o serwerze licencyjnym używane do zapewnienia, że jest on zgodny z umową licencyjną.

Wybór i kontrola

Aktywacja jest wymagana i odbywa się automatycznie podczas instalacji systemu Windows. Jeśli użytkownik nie ma ważnej licencji oprogramowania, nie może aktywować systemu Windows.

Góra strony

Klient usług zarządzania prawami dostępu w usłudze Active Directory (AD RMS)

Opis funkcji

Klient usług zarządzania prawami dostępu w usłudze Active Directory (AD RMS) to technologia przeznaczona do ochrony danych współdziałająca z aplikacjami obsługującymi usługi AD RMS w celu zabezpieczenia informacji cyfrowych przed nieautoryzowanym dostępem. Właściciele informacji cyfrowych mogą zdefiniować sposób

używania przez odbiorców informacji zawartych w danym pliku (na przykład można określić, kto może otwierać, modyfikować, drukować i wykonywać inne działania na pliku). Aby można było utworzyć lub wyświetlić plik z ograniczonymi uprawnieniami, na komputerze musi być uruchomiona aplikacja obsługująca usługi AD RMS i trzeba mieć dostęp do serwera usług AD RMS.

Informacje zbierane, przetwarzane lub przesyłane

Adres e-mail użytkownika służy w usługach AD RMS do identyfikowania użytkownika na serwerze usług AD RMS. W wyniku tego adres e-mail użytkownika jest przechowywany na serwerze i na jego komputerze wraz z licencjami i certyfikatami tożsamości utworzonymi przez serwer. Certyfikaty tożsamości i licencje są przekazywane na serwery usług AD RMS i z tych serwerów, kiedy użytkownik próbuje otworzyć, wydrukować lub wykonać inne działania na dokumencie chronionym za pomocą zarządzania prawami dostępu. Jeśli dany komputer jest połączony z siecią przedsiębiorstwa, serwer usług AD RMS zwykle też jest obsługiwany w ramach przedsiębiorstwa. W przypadku korzystania z usług AD RMS w ramach usługi Windows Live serwer jest obsługiwany przez firmę Microsoft. W celu ochrony prywatności użytkownika informacje wysyłane na serwery usług AD RMS firmy Microsoft są szyfrowane.

Używanie informacji

Licencja umożliwia korzystanie z plików chronionych. Certyfikaty tożsamości służą do identyfikowania użytkowników na serwerze usług AD RMS i umożliwiają ochronę plików oraz korzystanie z plików chronionych.

Wybór i kontrola

Funkcje usług AD RMS należy włączyć za pomocą aplikacji obsługującej usługi AD RMS. Domyślnie są one wyłączone. Można zdecydować, aby ich nie włączać i nie używać. Jeśli jednak nie zostaną włączone, nie będzie można korzystać z plików chronionych.

Góra strony

Identyfikator treści reklamowych

Opis funkcji

Aby dostarczać trafniejsze reklamy, system Windows pozwala aplikacjom na uzyskiwanie dostępu do unikatowego identyfikatora każdego użytkownika urządzenia. W dowolnym momencie można zresetować ten identyfikator lub wyłączyć do niego dostęp.

Informacje zbierane, przetwarzane lub przesyłane

Jeśli użytkownik umożliwił aplikacjom uzyskiwanie dostępu do identyfikatora treści reklamowych, system Windows udostępnia go aplikacjom na żądanie. Aplikacje mogą przechowywać lub przesyłać te informacje.

Używanie informacji

Identyfikator treści reklamowych jest używany przez deweloperów aplikacji i sieci reklamowe w celu dostarczania użytkownikowi trafniejszych reklam dzięki analizowaniu używanych aplikacji oraz sposobu korzystania z nich przez użytkownika. Może on również zostać użyty przez deweloperów aplikacji do zwiększenia jakości usług przez umożliwienie określenia częstotliwości i skuteczności reklam oraz wykrywanie oszustw i problemów z bezpieczeństwem.

W przypadku zezwolenia aplikacjom na korzystanie z identyfikatora treści reklamowych, sposób używania go przez poszczególne aplikacje podlega zasadom zachowania poufności informacji danej aplikacji.

Wybór i kontrola

Wybranie ustawień ekspresowych podczas konfigurowania systemu Windows powoduje, że system Windows udostępnia aplikacjom identyfikator treści reklamowych użytkownika. Jeśli użytkownik zdecyduje się dostosować ustawienia, może kontrolować dostęp do swojego identyfikatora treści reklamowych, wybierając pozycję **Zezwalaj aplikacjom na używanie mojego identyfikatora treści reklamowych w różnych aplikacjach** w obszarze **Udostępniaj informacje firmie Microsoft i innym usługom**. Po ukończeniu konfiguracji systemu Windows można zmienić to ustawienie, korzystając z opcji **Prywatność** w ustawieniach komputera. Jeśli to ustawienie zostanie wyłączone, identyfikator treści reklamowych nie jest wysyłany do żądających go aplikacji. Po ponownym włączeniu tego ustawienia zostaje wygenerowany nowy identyfikator.

Góra strony

Inspekcja

Dzięki inspekcji administrator może skonfigurować system Windows do rejestrowania działań wykonywanych w systemie operacyjnym. Działania są rejestrowane w dzienniku zabezpieczeń, który można otworzyć w Podglądzie zdarzeń i innych aplikacjach. Dziennik ułatwia administratorowi wykrycie nieautoryzowanego dostępu do komputera i zasobów na komputerze. Dzięki dziennikowi administratorzy mogą na przykład szybciej rozwiązywać problemy i sprawdzać, czy ktoś zalogował się na komputerze, utworzył nowe konto użytkownika, zmienił zasady zabezpieczeń lub otworzył dokument.

Informacje zbierane, przetwarzane lub przesyłane

Administratorzy określają, jakie informacje są zbierane, jak długo są przechowywane i czy są przekazywane stronom trzecim. Wśród tych informacji mogą się znaleźć informacje osobiste, takie jak nazwy użytkownika czy nazwy plików. Aby uzyskać więcej informacji, należy skontaktować się z administratorem. Żadne informacje nie są wysyłane do firmy Microsoft.

Używanie informacji

Administratorzy określają również sposób wykorzystania informacji uzyskanych w ramach inspekcji. Zwykle dziennik zabezpieczeń służy audytorom i administratorom do śledzenia działań na komputerze lub identyfikowania nieautoryzowanego dostępu do komputera i jego zasobów.

Wybór i kontrola

Administratorzy określają, czy ta funkcja jest włączona i w jaki sposób są powiadamiani użytkownicy. O ile nie zezwoli na to administrator, inni użytkownicy nie mogą wyświetlać dziennika zabezpieczeń. Inspekcję można skonfigurować na komputerze, otwierając aplet Zasady zabezpieczeń lokalnych dostępny z poziomu okna Narzędzia administracyjne.

Góra strony

Biometria

Opis funkcji

Jeśli komputer jest wyposażony w skaner linii papilarnych, możesz przy użyciu linii papilarnych logować się w systemie Windows oraz w aplikacjach, które obsługują tę metodę.

Informacje zbierane, przetwarzane lub przesyłane

Kiedy użytkownik konfiguruje nowe linie papilarne, odczyty linii papilarnych są przechowywane lokalnie na komputerze. Żadne informacje nie są wysyłane do firmy Microsoft. W przypadku identyfikacji użytkownika w aplikacji za pomocą linii papilarnych system Windows porównuje jego linie papilarne z danymi zapisanymi na komputerze i informuje aplikację, czy zeskanowane linie papilarne są zgodne ze skojarzonymi z kontem. System Windows nie przekazuje aplikacji danych dotyczących zeskanowanych linii papilarnych.

Używanie informacji

System Windows korzysta z informacji dotyczących linii papilarnych przechowywanych przez użytkownika na komputerze do logowania go w systemie Windows za pomocą linii papilarnych.

Wybór i kontrola

Linie papilarne można dodawać lub usuwać, korzystając z pozycji **Opcje logowania** w obszarze **Konta** w ustawieniach komputera.

Góra strony

Szyfrowanie dysków funkcją BitLocker

Opis funkcji

Szyfrowanie dysków funkcją BitLocker umożliwia ochronę danych przez ich szyfrowanie, co pomaga w uniemożliwianiu dostępu do danych nieautoryzowanym osobom. Jeśli funkcja BitLocker jest włączona na obsługiwanym dysku, system Windows szyfruje dane na tym dysku.

Informacje zbierane, przetwarzane lub przesyłane

Jeśli funkcja BitLocker jest włączona przy użyciu szyfrowania programowego, klucze kryptograficzne nieustannie szyfrują i

odszyfrowują dane podczas odczytywania ich z chronionego dysku lub zapisywania ich na nim. Jeśli funkcja BitLocker jest włączona za pomocą szyfrowania sprzętowego, dysk wykonuje szyfrowanie i odszyfrowywanie danych.

Podczas konfigurowania funkcji BitLocker można zdecydować, czy klucz odzyskiwania ma zostać wydrukowany, czy raczej zapisany w lokalizacji sieciowej. Jeśli funkcja BitLocker jest zainstalowana na dysku niewymiennym, klucz odzyskiwania można także zapisać na dysku flash USB.

Jeśli komputer nie jest przyłączony do domeny, można utworzyć kopię zapasową klucza odzyskiwania funkcji BitLocker, identyfikatora klucza odzyskiwania i nazwy komputera w usłudze Microsoft OneDrive. W celu ochrony prywatności użytkownika informacje są wysyłane w szyfrowanej postaci za pomocą protokołu SSL.

Funkcję BitLocker można skonfigurować do szyfrowania danych za pomocą certyfikatu przechowywanego na karcie inteligentnej. Jeśli dysk danych jest chroniony za pomocą karty inteligentnej, klucz publiczny i unikatowy identyfikator karty inteligentnej są przechowywane na dysku w postaci niezaszyfrowanej. Te informacje mogą służyć do zlokalizowania certyfikatu użytego pierwotnie do wygenerowania certyfikatu szyfrowania karty inteligentnej.

Jeśli zabezpieczenia sprzętowe na komputerze korzystają z modułu TPM (Trusted Platform Module) w wersji co najmniej 1.2, funkcja BitLocker używa modułu TPM do sprzętowego zabezpieczenia danych na dysku, na którym jest zainstalowany system Windows. Więcej informacji można znaleźć w sekcji Usługi modułu TPM (Trusted Platform Module). Na komputerach z modułem TPM można także skonfigurować numer PIN (osobisty numer identyfikacyjny) w celu dodatkowego zabezpieczenia szyfrowanych danych. Funkcja BitLocker przechowuje taki numer PIN oparty na module TPM w postaci zaszyfrowanej i jako wartość skrótu na dysku.

Informacje zbierane przez funkcję BitLocker nie są wysyłane do firmy Microsoft, o ile użytkownik nie zdecyduje, że chce utworzyć kopię zapasową klucza odzyskiwania w usłudze OneDrive.

Używanie informacji

Klucze kryptograficzne i unikatowe identyfikatory globalne (GUID) są przechowywane w pamięci komputera, aby zapewnić obsługę funkcji BitLocker. Informacje dotyczące odzyskiwania funkcji BitLocker umożliwiają dostęp do chronionych danych w razie awarii sprzętu i innych problemów. Dzięki informacjom odzyskiwania funkcja BitLocker odróżnia użytkowników autoryzowanych od nieautoryzowanych.

Firma Microsoft nie używa kluczy odzyskiwania poszczególnych użytkowników do żadnych celów. Jeśli klucze odzyskiwania są wysyłane do usługi OneDrive, firma Microsoft może używać zagregowanych danych na ich temat do analizowania trendów i udoskonalania swoich produktów i usług.

Wybór i kontrola

Domyślnie funkcja BitLocker jest wyłączona. W przypadku dysku wymiennego dowolny użytkownik może włączyć lub wyłączyć funkcję BitLocker, otwierając aplet Szyfrowanie dysków funkcją BitLocker w Panelu sterowania. Administrator może włączyć lub wyłączyć funkcję BitLocker dla wszystkich dysków.

Klucze odzyskiwania przechowywane na koncie usługi OneDrive można wyświetlić oraz zarządzać nimi.

Góra strony

Kontakty

Opis funkcji

Jeśli zarządzasz kontaktami za pomocą aplikacji Kontakty lub obsługiwanej aplikacji innej firmy, możesz zdecydować się na udostępnianie określonych kontaktów innym aplikacjom na komputerze, wyświetlanie informacji o kontakcie na wizytówce lub udostępnianie określonych informacji o kontaktach innym aplikacjom na komputerze w celu wykonania określonego działania, takiego jak nawiązanie połączenia lub zamapowanie adresu.

Zbierane, przetwarzane, przechowywane i przesyłane informacje

Kiedy aplikacja żąda informacji dotyczących kontaktu, system Windows umożliwia wybranie określonych kontaktów, które mają zostać

udostępnione aplikacji. Kontakty mogą pochodzić z aplikacji Kontakty lub z obsługiwanej aplikacji innej firmy przeznaczonej do zarządzania kontaktami. System Windows nie udostępnia aplikacji całej listy kontaktów.

Jeśli aplikacja ma dostęp do informacji dotyczących jednego z kontaktów (np. do numeru telefonu lub adresu e-mail), system Windows może pokazać wizytówkę z dodatkowymi informacjami na temat tego kontaktu pochodzącymi z aplikacji kontaktów. System Windows nie udostępnia aplikacji, która wyświetla wizytówkę, dodatkowych informacji o kontakcie.

Jeśli naciśniesz lub klikniesz na wizytówce polecenie, takie jak **Zadzwoń**, **E-mail**lub **Wskaż na mapie** , system Windows otworzy odpowiednią aplikację umożliwiającą ukończenie danego działania i udostępni tej aplikacji szczegóły dotyczące kontaktu niezbędne do ukończenia akcji (np. numer telefonu konieczny do nawiązania połączenia telefonicznego).

Używanie informacji

System Windows używa informacji o kontaktach pochodzących z aplikacji do obsługi kontaktów w celu udostępniania wybranych kontaktów, wyświetlania wizytówek, otwierania aplikacji, udostępniania danych kontaktów umożliwiających ukończenie akcji wymienionych na wizytówkach oraz pokazywania kontaktów w usłudze Windows Search. Sposób wykorzystania informacji dotyczących kontaktów w aplikacji Kontakty jest opisany w zasadach zachowania poufności informacji aplikacji komunikacyjnychmożna wyświetlić oraz zarządzać nimi.

W przypadku udostępniania danych dotyczących kontaktów aplikacjom innych firm sposób wykorzystania tych informacji przez daną aplikację zależy od zasad zachowania poufności informacji obowiązujących w danej firmie. W razie udostępnienia informacji dotyczących kontaktów aplikacji firmy Microsoft informacje dotyczące prywatności obowiązujące dla tej aplikacji można znaleźć w jej zasadach zachowania poufności informacji.

Wybór i kontrola

System Windows wyświetla i udostępnia informacje kontaktowe tylko wtedy, gdy użytkownik zdecyduje się na udostępnianie określonych

kontaktów aplikacji, wyświetli wizytówkę lub wybierze akcję dostępną na wizytówce.

Góra strony

Odnajdowanie i instalowanie urządzeń

W systemie Windows jest kilka funkcji umożliwiających wykrywanie i konfigurowanie urządzeń na komputerze, takich jak Instalacja urządzenia, Instalacja urządzenia korzystającego z komórkowego połączenia szerokopasmowego, Odnajdowanie sieci i Bezprzewodowe parowanie urządzeń.

Instalacja urządzenia

Opis funkcji

Kiedy na komputerze jest instalowane nowe urządzenie, system Windows może automatycznie wyszukać, pobrać i zainstalować oprogramowanie sterownika urządzenia. System Windows może także pobrać informacje dotyczące urządzenia, takie jak opis, zdjęcie i logo producenta. Niektóre urządzenia, takie jak określone drukarki, kamery internetowe, urządzenia korzystające z komórkowego połączenia szerokopasmowego i urządzenia przenośne, które można zsynchronizować z systemem Windows, mają aplikację umożliwiającą włączenie wszystkich funkcji i udostępnienie całego środowiska użytkownika urządzenia. Jeśli producent urządzenia dostarczył aplikację dla danego urządzenia, system Windows może automatycznie pobrać i zainstalować tę aplikację ze Sklepu Windows, o ile użytkownik jest w nim zalogowany.

Informacje zbierane, przetwarzane lub przesyłane

Kiedy system Windows szuka sterowników, kontaktuje się z usługą Windows Update w trybie online w celu znalezienia i pobrania sterowników urządzeń, o ile odpowiedni sterownik nie znajduje się jeszcze na komputerze użytkownika. Aby dowiedzieć się więcej na temat informacji zbieranych przez usługę Windows Update oraz o sposobie wykorzystywania tych informacji, zobacz Zasady zachowania poufności informacji dotyczące usług aktualizacjimożna wyświetlić oraz zarządzać nimi.

Aby pobrać informacje dotyczące urządzenia i określić, czy jest dla

niego dostępna aplikacja, system Windows wysyła do firmy Microsoft dane na temat urządzenia obejmujące identyfikator urządzenia (na przykład identyfikator sprzętu lub modelu), region i język użytkownika, a także datę ostatniej aktualizacji informacji dotyczących urządzenia. Jeśli aplikacja dla urządzenia jest dostępna, system Windows automatycznie pobiera ją ze Sklepu Windows i instaluje. Aplikacja będzie dostępna na liście posiadanych aplikacji na koncie użytkownika w Sklepie Windows.

Używanie informacji

Informacje wysyłane do firmy Microsoft są używane do określania i pobierania odpowiedniego sterownika urządzenia, a także informacji oraz aplikacji dotyczących urządzenia. Firma Microsoft nie używa wysłanych informacji do ustalenia tożsamości użytkownika ani do kontaktowania się z nim.

Wybór i kontrola

Wybranie ustawień ekspresowych podczas konfiguracji systemu Windows powoduje włączenie automatycznego pobierania i instalowania sterowników urządzeń, a także informacji i aplikacji dotyczących urządzeń. Jeśli użytkownik zdecyduje się dostosować ustawienia, może kontrolować automatyczne pobieranie i instalowanie sterowników urządzeń, aplikacji i informacji, wybierając pozycję **Automatycznie pobierz sterowniki, aplikacje i informacje dla nowych urządzeń** w obszarze **Pomóż chronić i aktualizować komputer**. Po ukończeniu konfigurowania systemu Windows można zmienić te ustawienia w Panelu sterowania, wybierając pozycję Zmień ustawienia instalacyjne urządzenia, a następnie wybierając pozycję **Nie, pozwól mi wybrać, co zrobić**można wyświetlić oraz zarządzać nimi.

Aplikację urządzenia można odinstalować w dowolnym momencie bez konieczności odinstalowywania samego urządzenia. Aplikacja może jednak wymagać dostępu do określonych funkcji urządzenia, Po odinstalowaniu aplikacji urządzenia można ją ponownie zainstalować. Wystarczy przejść do listy posiadanych aplikacji w Sklepie Windows.

Instalacja urządzenia korzystającego z komórkowego połączenia szerokopasmowego

Opis funkcji

Jeśli w komputerze znajduje się urządzenie korzystające z komórkowego połączenia szerokopasmowego udostępniane przez niektórych operatorów sieci komórkowych, system Windows może automatycznie pobrać i zainstalować aplikację umożliwiającą zarządzanie kontem i planem taryfowym u operatora, który dostarczył dane urządzenie. Pobierane są także dodatkowe informacje o urządzeniu pomocne w wyświetlaniu komórkowego połączenia szerokopasmowego na liście sieci.

Informacje zbierane, przetwarzane lub przesyłane

Aby określić informacje o urządzeniu oraz aplikacje, które mają zostać pobrane, system Windows wysyła część identyfikatorów sprzętu urządzenia korzystającego z komórkowego połączenia szerokopasmowego umożliwiającą zidentyfikowanie operatora sieci komórkowej. Aby pomóc w ochronie prywatności użytkownika, system Windows nie wysyła do firmy Microsoft pełnych identyfikatorów sprzętu urządzenia korzystającego z komórkowego połączenia szerokopasmowego.

Jeśli dany operator dostarczył firmie Microsoft aplikację, system Windows pobiera ją ze Sklepu Windows, a następnie instaluje. Kiedy użytkownik otworzy zainstalowaną aplikację, będzie ona miała dostęp do urządzenia korzystającego z komórkowego połączenia szerokopasmowego, w tym także do unikatowych identyfikatorów sprzętu za pomocą których operator sieci komórkowej może zidentyfikować konto użytkownika.

Używanie informacji

Korzystając z części identyfikatora urządzenia korzystającego z komórkowego połączenia szerokopasmowego wysłanego przez system Windows, firma Microsoft może określić operatora, którego aplikację należy zainstalować na danym komputerze. Po zainstalowaniu aplikacja może używać identyfikatorów urządzenia korzystającego z komórkowego połączenia szerokopasmowego. Na przykład aplikacja operatora może za pomocą tych identyfikatorów sprawdzać informacje dotyczące konta i planu taryfowego w trybie online. Wykorzystanie tych danych przez aplikację podlega zasadom zachowania poufności informacji danego operatora.

Wybór i kontrola

Wybranie ustawień ekspresowych podczas konfigurowania systemu Windows po raz pierwszy powoduje, że system Windows automatycznie sprawdza dostępność aplikacji operatora i je pobiera. Tę funkcję można włączyć lub wyłączyć w Panelu sterowania. Więcej informacji można znaleźć w powyższej sekcji Instalacja urządzenia.

Aplikację operatora można odinstalować w dowolnym czasie. Nie wymaga to odinstalowywania samego urządzenia korzystającego z komórkowego połączenia szerokopasmowego.

Odnajdowanie sieci

Opis funkcji

Jeśli komputer zostanie połączony z małą siecią prywatną (na przykład domową), system Windows może automatycznie odnaleźć inne komputery i urządzenia udostępnione w sieci oraz sprawić, że dany komputer będzie widoczny dla innych użytkowników korzystających z tej sieci. Po znalezieniu urządzeń udostępnionych system Windows może automatycznie połączyć się z nimi i je zainstalować. Takimi urządzeniami udostępnionymi mogą być drukarki i urządzenia Media Extender, ale nie urządzenia do użytku osobistego, takie jak aparaty fotograficzne czy telefony komórkowe.

Informacje zbierane, przetwarzane lub przesyłane

Jeśli udostępnianie urządzeń i łączenie się z nimi zostanie włączone, informacje na temat danego komputera (na przykład jego nazwa i adres sieciowy) mogą być przekazywane w sieci lokalnej, aby umożliwić innym komputerom odnajdowanie tego komputera i łączenie się z nim.

Niektóre informacje o sieci są zbierane i wysyłane do firmy Microsoft, aby umożliwić określenie, czy urządzenia połączone z daną siecią mają być instalowane automatycznie. Te informacje to między innymi liczba urządzeń w sieci, typ sieci (na przykład sieć prywatna) i typy oraz nazwy modeli urządzeń w sieci. Nie są zbierane żadne informacje osobiste, takie jak nazwa sieci czy hasło.

W zależności od ustawień instalacji urządzenia podczas instalowania urządzeń udostępnionych w systemie Windows określone informacje mogą być wysyłane przez system Windows do firmy Microsoft, po

czym oprogramowanie urządzenia jest instalowane na komputerze. Więcej informacji można znaleźć w sekcji Instalacja urządzenia.

Używanie informacji

Informacje dotyczące sieci wysyłane do firmy Microsoft służą do określenia urządzeń w sieci, które mają być instalowane automatycznie. Firma Microsoft nie używa zebranych informacji do ustalania tożsamości użytkownika, kontaktowania się z nim ani do kierowania do niego reklam.

Wybór i kontrola

Jeśli podczas łączenia się z siecią użytkownik włączył udostępnianie urządzeń i łączenie się z nimi, odnajdowanie jest w tej sieci włączone. Można zmienić to ustawienie dla bieżącej sieci, klikając typ sieci wymieniony pod nazwą sieci w Centrum sieci i udostępniania.

Wybierając pozycję **Zmień zaawansowane ustawienia udostępniania** w Centrum sieci i udostępniania, można zdecydować, czy ma być włączone odnajdowanie urządzeń w sieci i automatyczne instalowanie urządzeń połączonych z siecią.

Bezprzewodowe parowanie urządzeń

Opis funkcji

System Windows umożliwia parowanie komputera z urządzeniami bezprzewodowymi korzystającymi z technologii Bluetooth lub Wi–Fi Direct. Wi–Fi Direct to technologia bezprzewodowa umożliwiająca bezpośrednią komunikację urządzeń bez konieczności łączenia się z siecią Wi–Fi.

Informacje zbierane, przetwarzane lub przesyłane

Jeśli użytkownik wybrał pozycję **Zezwalaj urządzeniom Bluetooth na odnajdywanie tego komputera** w oknie Ustawienia Bluetooth, system Windows rozgłasza nazwę komputera przy użyciu technologii Bluetooth, dzięki czemu urządzenia obsługujące technologię Bluetooth mogą wykryć i zidentyfikować dany komputer.

Jeśli użytkownik wybrał pozycję **Dodaj urządzenie** w obszarze urządzeń w ustawieniach komputera, system Windows rozgłasza nazwę komputera przy użyciu technologii Wi–Fi, dzięki czemu urządzenia obsługujące technologię Wi–Fi Direct mogą wykryć i

zidentyfikować ten komputer. Jeśli okno **Dodaj urządzenie**zostanie zamknięte, system Windows przestanie rozgłaszać nazwę komputera w sieci Wi–Fi.

W zależności od ustawień instalacji urządzenia podczas parowania urządzenia bezprzewodowego z systemem Windows określone informacje mogą być wysyłane przez system Windows do firmy Microsoft, po czym oprogramowanie urządzenia jest instalowane na komputerze. Więcej informacji można znaleźć w powyższej sekcji Instalacja urządzenia.

Używanie informacji

System Windows rozgłasza nazwę komputera, aby umożliwić innym urządzeniom zidentyfikowanie go i połączenie się z nim. Nazwa komputera nie jest wysyłana do firmy Microsoft.

Wybór i kontrola

Aby zmienić ustawienie rozgłaszania nazwy komputera przy użyciu połączenia Bluetooth przez system Windows, należy nacisnąć i przytrzymać lub kliknąć prawym przyciskiem myszy nazwę swojego komputera w aplecie Urządzenia i drukarki w Panelu sterowania, wybrać polecenie **Ustawienia Bluetooth**, a następnie wybrać pozycję **Zezwalaj urządzeniom Bluetooth na odnajdywanie tego komputera**. Aby system Windows nie rozgłaszał nazwy komputera w sieci Wi–Fi podczas dodawania urządzeń, przed dodaniem urządzenia należy tymczasowo wyłączyć sieć Wi–Fi w obszarze połączeń bezprzewodowych w ustawieniach komputera.

Góra strony

Szyfrowania urządzeń

Opis funkcji

Szyfrowanie urządzeń umożliwia ochronę danych przez ich szyfrowanie za pomocą technologii szyfrowania dysków funkcją BitLocker, co pomaga w zapobieganiu atakom oprogramowania w trybie offline. Kiedy szyfrowanie urządzeń jest włączone, system Windows szyfruje dane na dysku, na którym jest zainstalowany system Windows.

Informacje zbierane, przetwarzane lub przesyłane

Jeśli jest włączone szyfrowanie programowe, klucze kryptograficzne nieustannie szyfrują i odszyfrowują dane podczas odczytywania ich z chronionego dysku lub zapisywania ich na nim. Jeśli jest włączone szyfrowanie sprzętowe, szyfrowanie i odszyfrowywanie danych wykonuje dysk.

Do przechowywania kluczy kryptograficznych służących do szyfrowania dysku system Windows używa modułu TPM (Trusted Platform Module) na komputerze użytkownika. Jeśli szyfrowanie urządzeń jest włączone, system Windows automatycznie szyfruje dysk, na którym jest zainstalowany system Windows, i generuje klucz odzyskiwania. Klucz odzyskiwania może ułatwić użytkownikowi dostęp do chronionych danych w razie określonych awarii sprzętu i innych problemów.

Kopia zapasowa klucza odzyskiwania funkcji BitLocker dla danego komputera jest tworzona automatycznie w trybie online w ramach konta usługi Microsoft OneDrive przypisanego do każdego konta administratora połączonego z danym kontem Microsoft. Na tym samym koncie usługi OneDrive jest tworzona kopia zapasowa nazwy komputera i identyfikatora klucza odzyskiwania. W celu ochrony prywatności użytkownika informacje są wysyłane w szyfrowanej postaci za pomocą protokołu SSL.

Używanie informacji

Klucze kryptograficzne i unikatowe identyfikatory globalne (GUID) są przechowywane w pamięci komputera, aby zapewnić obsługę operacji funkcji BitLocker. Informacje dotyczące odzyskiwania umożliwiają dostęp do chronionych danych w razie określonych awarii sprzętu i innych problemów i pozwalają funkcji BitLocker na rozróżnienie użytkowników autoryzowanych i nieautoryzowanych.

Firma Microsoft tworzy kopię zapasową informacji odzyskiwania na koncie usługi OneDrive użytkownika, dzięki czemu są one dostępne w trybie online. Nie używamy informacji dotyczących klucza odzyskiwania ani nie przechowujemy ich w miejscu innym niż konto usługi OneDrive. Możemy jedynie używać zagregowanych danych na temat kluczy odzyskiwania do analizowania trendów i udoskonalania naszych produktów i usług. Informacje te mogą na przykład służyć do określenia odsetka komputerów, na których jest włączone szyfrowanie urządzeń.

Wybór i kontrola

Jeśli podczas konfigurowania komputera użytkownik zdecydował się na korzystanie z konta Microsoft, szyfrowanie urządzeń jest włączone, a kopia zapasowa klucza odzyskiwania zostaje utworzona na koncie usługi OneDrive użytkownika. Jeśli podczas konfigurowania komputera użytkownik zdecydował się na używanie konta lokalnego, szyfrowanie urządzeń nie jest włączone.

Jeśli użytkownik połączy później konto Microsoft z kontem administratora na swoim komputerze:

- Jeśli szyfrowanie urządzeń nie jest jeszcze włączone, system Windows włączy je automatycznie i utworzy kopię zapasową informacji odzyskiwania na koncie usługi OneDrive danego użytkownika.
- Jeśli szyfrowanie urządzeń jest już włączone, kopia zapasowa informacji odzyskiwania danego komputera zostanie utworzona na koncie usługi OneDrive użytkownika.

Klucze odzyskiwania przechowywane na koncie usługi OneDrive można wyświetlić oraz zarządzać nimi tutajmożna wyświetlić oraz zarządzać nimi.

Góra strony

Funkcja DirectAccess

Opis funkcji

Funkcja DirectAccess umożliwia łatwe połączenie zdalne komputera z siecią w miejscu pracy za każdym razem, gdy komputer połączy się z Internetem bez względu na lokalizację.

Informacje zbierane, przetwarzane lub przesyłane

Po każdym uruchomieniu komputera przez użytkownika funkcja DirectAccess próbuje się połączyć z siecią w miejscu pracy bez względu na to, czy użytkownik fizycznie znajduje się w tym miejscu. Po nawiązaniu połączenia na komputer zostaną pobrane zasady obowiązujące w miejscu pracy, dzięki czemu będzie można uzyskać dostęp do skonfigurowanych zasobów w sieci firmowej. Za pomocą

połączenia DirectAccess administrator miejsca pracy może zdalnie zarządzać danym komputerem i monitorować go (na przykład odwiedzane witryny sieci Web) nawet wtedy, gdy użytkownik nie jest fizycznie obecny w miejscu pracy.

Funkcja DirectAccess nie wysyła żadnych informacji do firmy Microsoft.

Używanie informacji

Sposób wykorzystania informacji zbieranych przez administratora miejsca pracy definiują zasady obowiązujące w danej firmie.

Wybór i kontrola

Funkcja DirectAccess musi zostać skonfigurowana przez administratora miejsca pracy za pomocą zasad grupy. Wprawdzie administrator może pozwolić użytkownikowi na tymczasowe dezaktywowanie niektórych elementów funkcji DirectAccess, ale tylko administrator miejsca pracy może skonfigurować system Windows, aby nie próbował łączyć się z miejscem pracy na potrzeby zarządzania. Jeśli użytkownik lub administrator miejsca pracy usunie dany komputer z domeny miejsca pracy, funkcja DirectAccess nie będzie mogła nawiązać połączenia z siecią w miejscu pracy.

Góra strony

Centrum ułatwień dostępu

Opis funkcji

Centrum ułatwień dostępu umożliwia włączenie opcji ułatwień dostępu umożliwiających ułatwienie interakcji z komputerem.

Informacje zbierane, przetwarzane lub przesyłane

W przypadku korzystania z tej funkcji trzeba wybrać odpowiednie stwierdzenia.

Są to następujące stwierdzenia:

- Nie widzę dobrze obrazu i tekstu w telewizorze.
- Warunki oświetlenia utrudniają oglądanie obrazów na monitorze.
- Nie korzystam z klawiatury.

- Jestem osobą niewidomą.
- Jestem osobą niesłyszącą.
- Mam wadę wymowy.

Te informacje są zapisywane w postaci nieczytelnej dla człowieka i przechowywane lokalnie na komputerze użytkownika.

Używanie informacji

Na podstawie wybranych stwierdzeń zostanie utworzony zestaw zaleceń dotyczących konfiguracji. Te informacje nie są wysyłane do firmy Microsoft i nie są dostępne dla użytkowników innych niż bieżący użytkownik i administratorzy komputera.

Wybór i kontrola

Korzystając z apletu Ułatwienia dostępu w Panelu sterowania, można zdecydować, które stwierdzenia mają być dostępne do wybrania. Wybrane opcje można zmienić w dowolnym momencie. Można także wybrać, które zalecenia mają zostać skonfigurowane na komputerze.

Góra strony

Podgląd zdarzeń

Opis funkcji

Korzystając z Podglądu zdarzeń, użytkownicy komputerów (głównie administratorzy) mogą wyświetlać dzienniki zdarzeń i zarządzać nimi. Dzienniki zdarzeń zawierają informacje na temat zdarzeń dotyczących sprzętu, oprogramowania oraz zabezpieczeń na komputerze. Klikając pozycję Pomoc online dziennika zdarzeń, informacje na temat zdarzeń z dzienników zdarzeń można także uzyskać od firmy Microsoft.

Informacje zbierane, przetwarzane lub przesyłane

Dzienniki zdarzeń zawierają informacje na temat zdarzeń wygenerowane przez wszystkich użytkowników i aplikacje na danym komputerze. Domyślnie wpisy w dzienniku zdarzeń są dostępne dla wszystkich użytkowników, ale administratorzy mogą ograniczyć dostęp do dzienników zdarzeń. Dostęp do dzienników zdarzeń swojego komputera można uzyskać, otwierając Podgląd zdarzeń. Informacje o

sposobie otwierania Podglądu zdarzeń można uzyskać w Pomocy i obsłudze technicznej systemu Windows.

W przypadku korzystania z pomocy online dziennika zdarzeń do uzyskiwania dodatkowych informacji na temat określonych zdarzeń, informacje o tych zdarzeniach są wysyłane do firmy Microsoft.

Używanie informacji

Kiedy użytkownik uzyskuje informacje o zdarzeniu w pomocy online dziennika zdarzeń, dane dotyczące zdarzenia wysyłane z komputera użytkownika służą do zlokalizowania i dostarczenia użytkownikowi dodatkowych informacji o zdarzeniu. W przypadku zdarzeń dotyczących produktów firmy Microsoft szczegóły zdarzeń zostaną wysłane do firmy Microsoft. Firma Microsoft nie używa tych informacji do ustalania tożsamości użytkownika, kontaktowania się z nim ani do kierowania do niego reklam. W przypadku zdarzeń dotyczących aplikacji innych firm informacje zostaną wysłane do miejsca określonego przez odpowiedniego wydawcę lub producenta. Informacje dotyczące zdarzeń wysyłane do innych wydawców i producentów są używane zgodnie z zasadami zachowania poufności informacji obowiązującymi w danej firmie.

Wybór i kontrola

Administratorzy mogą ograniczyć dostęp do dzienników Podglądu zdarzeń. Użytkownicy mający pełny dostęp do dzienników Podglądu zdarzeń mogą czyścić te dzienniki. O ile wcześniej użytkownik nie wyraził zgody na automatyczne wysyłanie informacji o zdarzeniach, kliknięcie łącza Pomoc online dziennika zdarzeń spowoduje wyświetlenie monitu o zaakceptowanie wysłania przedstawionych informacji przez Internet. Informacje z dziennika zdarzeń zostaną wysłane przez Internet tylko po wyrażeniu na to zgody przez użytkownika. Korzystając z zasad grupy, administratorzy mogą wybrać lub zmienić witrynę, do której są wysyłane informacje o zdarzeniach.

Góra strony

Filtr rodzinny

Opis funkcji

Funkcja Bezpieczeństwo rodzinne pomaga rodzicom w umożliwieniu

dzieciom bezpiecznego korzystania z komputera. Rodzice mogą decydować o tym, z jakich aplikacji, gier i witryn sieci Web mogą korzystać ich dzieci. Rodzice mogą także określać ograniczenia i otrzymywać pocztą e-mail regularne raporty aktywności. Rodzice mogą zarządzać ograniczeniami i wyświetlać raporty aktywności lokalnie na komputerze lub w trybie online za pośrednictwem witryny sieci Web Bezpieczeństwo rodzinne firmy Microsoft.

Informacje zbierane, przetwarzane lub przesyłane

Ustawienia bezpieczeństwa rodzinnego i raporty aktywności dzieci są przechowywane na komputerze użytkownika. Raporty aktywności mogą zawierać dane dotyczące czasu korzystania z komputera, czasu korzystania z poszczególnych aplikacji i gier oraz odwiedzonych witryn sieci Web (w tym prób uzyskania dostępu do zablokowanych witryn). Administratorzy komputera mogą zmieniać ustawienia i wyświetlać raport aktywności.

Jeśli konto dziecka jest objęte zarządzaniem w trybie online, rodzice mogą wyświetlać raport aktywności dziecka i zmieniać ustawienia w witrynie sieci Web Bezpieczeństwo rodzinne firmy Microsoft. Rodzic może także umożliwić innym osobom wyświetlanie raportów aktywności i zmienianie ustawień, dodając te osoby jako rodziców w witrynie sieci Web Bezpieczeństwo rodzinne firmy Microsoft. Jeśli rodzic konfigurujący funkcję bezpieczeństwa rodzinnego jest zalogowany w systemie Windows za pomocą konta Microsoft, zarządzanie w trybie online jest automatycznie włączone.

Jeśli funkcja bezpieczeństwa rodzinnego jest skonfigurowana dla konta dziecka objętego zarządzaniem w trybie online, tygodniowe raporty aktywności dziecka są wysyłane do rodzica automatycznie.

Używanie informacji

Zebrane informacje są używane w systemie Windows i witrynie Bezpieczeństwo rodzinne firmy Microsoft w celu zapewnienia prawidłowego działania funkcji Bezpieczeństwo rodzinne. Firma Microsoft może analizować informacje z dziennika w postaci zbiorczej, aby zapewnić wysoką jakość danych, ale nie używa tych informacji do ustalania tożsamości użytkownika, kontaktowania się z nim ani do kierowania do niego reklam.

Wybór i kontrola

Funkcja Bezpieczeństwo rodzinne jest domyślnie wyłączona. Funkcję Bezpieczeństwo rodzinne można otworzyć, korzystając z apletu Bezpieczeństwo rodzinne w Panelu sterowania. Tylko administratorzy mogą otwierać funkcję Bezpieczeństwo rodzinne, a monitorowanie i określanie ograniczeń może obejmować tylko użytkowników bez uprawnień administracyjnych. Dzieci widzą swoje ustawienia, ale nie mogą ich zmieniać. Jeśli funkcja Bezpieczeństwo rodzinne jest włączona, podczas każdego logowania się w systemie Windows dziecko otrzyma powiadomienie, że jego konto jest monitorowane za pomocą tej funkcji. Jeśli podczas tworzenia konta zostanie ono zdefiniowane jako konto dziecka, można zdecydować o włączeniu funkcji Bezpieczeństwo rodzinne dla tego konta.

Jeśli administrator konfigurujący konto dziecka jest zalogowany w systemie Windows za pomocą konta Microsoft, zarządzanie w trybie online jest automatycznie włączone, a raporty aktywności dziecka będą wysyłane raz w tygodniu. Konta rodziców można dodawać i usuwać w witrynie Bezpieczeństwo rodzinne firmy Microsoft. Każda osoba dodana jako rodzic na stronie sieci Web może wyświetlać raport aktywności dziecka i zmieniać ustawienia funkcji Bezpieczeństwo rodzinne dotyczące danego dziecka, nawet jeśli rodzic nie jest administratorem komputera, z którego korzysta dziecko.

Aby zapewnić prawidłowe działanie funkcji Bezpieczeństwo rodzinne, tylko rodzice powinni być administratorami komputera, a dzieciom nie należy przyznawać uprawnień administracyjnych. Należy pamiętać, że monitorowanie innych użytkowników (na przykład dorosłych) za pomocą tej funkcji może stanowić naruszenie obowiązującego prawa.

Góra strony

Faks

Opis funkcji

Funkcja faksu umożliwia tworzenie i zapisywanie stron tytułowych faksu oraz wysyłanie i odbieranie faksów za pomocą komputera i zewnętrznego lub wbudowanego faks-modemu albo serwera faksów.

Informacje zbierane, przetwarzane lub przesyłane

Zbierane informacje obejmują wszelkie informacje osobiste wprowadzone na stronie tytułowej faksu, a także identyfikatory zawarte w standardowych protokołach obsługi faksów, takie jak identyfikator subskrybenta nadającego (Transmitting Subscriber ID — TSID) i identyfikator wywołanego subskrybenta (Call Subscriber ID — CSID). Domyślnie wartością każdego identyfikatora w systemie Windows jest „Faks”.

Używanie informacji

Informacje wprowadzone w oknie dialogowym nadawcy są przedstawione na stronie tytułowej faksu. Identyfikatory, takie jak TSID i CSID, mogą zawierać dowolny tekst i zwykle służą do identyfikacji nadawcy za pomocą faksu lub komputera odbiorcy. Żadne informacje nie są wysyłane do firmy Microsoft.

Wybór i kontrola

Dostęp do faksu jest określony przez uprawnienia konta użytkownika na komputerze. Jeśli administrator faksu nie zmieni ustawień dostępu, wszyscy użytkownicy mogą wysyłać i odbierać faksy. Domyślnie wszyscy użytkownicy mogą wyświetlać dokumenty, które wysyłają, i wszystkie faksy odebrane na danym komputerze. Administratorzy mogą wyświetlać wszystkie dokumenty wysłane i odebrane faksem, a także konfigurować ustawienia faksu, takie jak uprawnienia użytkowników do wyświetlania faksów i zarządzania nimi oraz wartości identyfikatorów TSID i CSID.

Góra strony

Personalizacja pisma ręcznego — automatyczna nauka

Opis funkcji

Automatyczna nauka to narzędzie personalizacji rozpoznawania pisma ręcznego dostępne na komputerach wyposażonych w płytkę dotykową lub pióro cyfrowe. Ta funkcja zbiera dane dotyczące słów używanych przez użytkownika i sposobu ich pisania. To ułatwia oprogramowaniu do rozpoznawania pisma ręcznego interpretację charakteru pisma oraz słownictwa stosowanego przez użytkownika, a także poprawia skuteczność autokorekty i sugestii tekstowych w przypadku języków bez edytorów IME.

Informacje zbierane, przetwarzane lub przesyłane

Informacje zbierane przez funkcję automatycznej nauki są przechowywane w profilu każdego użytkownika komputera. Dane są przechowywane w formacie zastrzeżonym, którego nie można odczytać przy użyciu aplikacji do wyświetlania tekstu (takiej jak Notatnik czy WordPad), i nie są dostępne dla innych użytkowników poza administratorami komputera.

Zbierane informacje obejmują:

- Tekst wiadomości pisanych i wpisów tworzonych w kalendarzu za pomocą aplikacji do obsługi poczty e-mail (takiej jak Office Outlook lub Poczta systemu Windows Live) — w tym także wiadomości, które już zostały wysłane.
- Pismo odręczne w Panelu wprowadzania.
- Tekst rozpoznany z pisma odręcznego w Panelu wprowadzania lub wpisywany za pomocą klawiatury dotykowej.
- Znaki zamienne wybrane w celu skorygowania tekstu.

Używanie informacji

Zbierane informacje służą do usprawnienia rozpoznawania pisma ręcznego dzięki utworzeniu wersji oprogramowania do rozpoznawania pisma spersonalizowanej z uwzględnieniem charakteru pisma i słownictwa używanego przez danego użytkownika, a także do umożliwienia autokorekty i sugestii tekstowych wyświetlanych podczas wpisywania tekstu za pomocą klawiatury dotykowej.

Próbki tekstu służą do utworzenia słownika rozszerzonego. Próbki pisma odręcznego umożliwiają usprawnienie rozpoznawania charakteru pisma poszczególnych użytkowników na komputerze. Żadne informacje nie są wysyłane do firmy Microsoft.

Wybór i kontrola

Automatyczna nauka jest domyślnie włączona. Automatyczną naukę można włączyć lub wyłączyć w dowolnej chwili, korzystając z pozycji **Ustawienia zaawansowane** w obszarze **Języki** w Panelu sterowania. Po wyłączeniu automatycznej nauki wszystkie dane

zebrane i przechowywane przez tę funkcję zostaną usunięte.

Góra strony

Grupa domowa

Opis funkcji

System Windows umożliwia łatwe połączenie komputerów w sieci domowej w celu udostępniania obrazów, muzyki, filmów, dokumentów i urządzeń. Umożliwia także przesyłanie strumieniowe multimediów z komputerów do urządzeń w sieci domowej (na przykład do urządzeń Media Extender). Te komputery i urządzenia to grupa domowa użytkownika. Grupa domowa może być chroniona hasłem. Udostępniane elementy można dowolnie wybrać.

Informacje zbierane, przetwarzane lub przesyłane

Użytkownik może uzyskać dostęp do własnych plików, takich jak obrazy, filmy, utwory muzyczne i dokumenty, za pomocą dowolnego komputera w grupie domowej. Kiedy użytkownik przyłącza się do grupy domowej, informacje dotyczące wszystkich kont Microsoft (w tym adres e-mail, nazwa wyświetlana i awatar) na danym komputerze zostaną udostępnione innym użytkownikom w grupie domowej, aby umożliwić udostępnianie elementów tym użytkownikom.

Używanie informacji

Dzięki zbieranym informacjom wiadomo, jaka zawartość na których komputerach w grupie domowej powinna być udostępniana określonym użytkownikom i w jakiej postaci ma być prezentowana. Żadne informacje nie są wysyłane do firmy Microsoft.

Wybór i kontrola

Użytkownik może dodawać komputery do grupy domowej i je z niej usuwać, a także decydować, jakie elementy chce udostępnić innym użytkownikom w grupie domowej. Grupę domową można utworzyć i zarządzać jej ustawieniami, przechodząc do pozycji **Grupa domowa** w obszarze **Sieć** w ustawieniach komputera.

Góra strony

Edytor IME (Input Method Editor)

Edytory IME firmy Microsoft w przypadku języków wschodnioazjatyckich służą do konwertowania danych wprowadzanych za pomocą klawiatury na ideogramy. Ta sekcja dotyczy kilku funkcji, takich jak automatyczne dostosowywanie i przewidywanie edytora IME, raportowanie błędów konwersji IME i rejestrowanie słów w edytorze IME.

Kandydaci z edytora IME w chmurze

Opis funkcji

W przypadku wprowadzania znaków w języku chińskim uproszczonym za pomocą edytora IME Pinyin firmy Microsoft, edytor IME może korzystać z usługi online do szukania potencjalnych ideogramów odpowiadających wpisanym danym, których nie ma w lokalnym słowniku na komputerze.

Informacje zbierane, przetwarzane lub przesyłane

Podczas pisania znaków w języku chińskim uproszczonym za pomocą edytora IME Pinyin firmy Microsoft edytor IME podpowiada ideogramy, które mogą się przydać. Jeśli edytor IME nie znajduje dobrej propozycji w słowniku lokalnym, wysyła dane wprowadzone za pomocą klawiatury do firmy Microsoft w celu sprawdzenia, czy są lepsi kandydaci na ideogramy odpowiadający tym danym. Jeśli są takie propozycje, zostaną wyświetlone na liście kandydatów, a po wybraniu — dodane do słownika lokalnego. Wysyłany jest także losowo generowany unikatowy identyfikator, aby pomóc nam w analizie wykorzystania tej funkcji. Identyfikator nie jest skojarzony z kontem Microsoft i nie jest używany do ustalania tożsamości użytkownika, kontaktowania się z nim ani kierowania do niego reklam.

Używanie informacji

Firma Microsoft korzysta z zebranych informacji do szukania ideogramów w chmurze oraz do usprawnienia oferowanych produktów i usług. Nie używamy tych informacji do ustalania tożsamości użytkownika, kontaktowania się z nim ani do kierowania do niego reklam.

Wybór i kontrola

Funkcja kandydatów z edytora IME w chmurze jest domyślnie wyłączona w edytorze IME Pinyin firmy Microsoft dla języka chińskiego uproszczonego. Aby wyświetlić lub zmienić to ustawienie, należy otworzyć ustawienia komputera, kliknąć pozycję **Czas i język**, kliknąć pozycję **Region i język**, wybrać język, a następnie kliknąć pozycję **Opcje**można wyświetlić oraz zarządzać nimi.

Funkcje automatycznego dostosowywania i przewidywania edytora IME

Opis funkcji

W zależności od używanego edytora IME i od wybranych ustawień funkcje automatycznego dostosowywania i sugestii tekstowych edytora IME mogą rejestrować słowa lub sekwencje słów, aby usprawnić wybieranie wyświetlanych ideogramów.

Informacje zbierane, przetwarzane lub przesyłane

Funkcje automatycznego dostosowywania (automatycznego uczenia) i sugestii tekstowych edytora IME rejestrują słowa i sekwencje słów oraz częstotliwość ich używania. Informacje z zakresu automatycznego dostosowywania (z wyjątkiem sekwencji cyfr/symboli) są przechowywane na komputerze w plikach odpowiadających poszczególnym użytkownikom.

Używanie informacji

Dane automatycznego dostosowywania i sugestii tekstowych są używane przez edytor IME na komputerze, aby usprawnić wybieranie ideogramów wyświetlanych podczas korzystania z edytora IME. Jeśli użytkownik zdecydował się wysyłać te dane do firmy Microsoft, służą one do udoskonalania edytora IME i pokrewnych produktów oraz usług.

Wybór i kontrola

Funkcje automatycznej nauki i sugestii tekstowych są domyślnie włączone w tych edytorach IME, które je obsługują. Zbierane dane nie są automatycznie wysyłane do firmy Microsoft. Korzystając z apletu Język w Panelu sterowania, można zdecydować, czy te dane mają być zbierane i wysyłane.

Raportowanie błędów konwersji IME

Opis funkcji

Jeśli podczas prezentowania ideogramów lub konwertowania danych wprowadzonych za pomocą klawiatury na ideogramy wystąpią błędy, ta funkcja umożliwia zebranie informacji na temat błędów. Dane te pomogą firmie Microsoft udoskonalić oferowane produkty i usługi.

Informacje zbierane, przetwarzane lub przesyłane

Funkcja raportowania błędów konwersji IME zbiera informacje na temat błędów konwersji IME, takie jak wpisane dane, wynik pierwszej konwersji lub przewidywania, wybrany ciąg zamienny, informacje o używanym edytorze IME i o sposobie jego używania. Oprócz tego w przypadku japońskiego edytora IME można zdecydować się także na uwzględnienie w raportach o błędach konwersji informacji na temat automatycznego uczenia.

Używanie informacji

Firma Microsoft korzysta z tych informacji w celu udoskonalania swoich produktów i usług. Firma Microsoft nie używa zebranych informacji do ustalania tożsamości użytkownika, kontaktowania się z nim ani do kierowania do niego reklam.

Wybór i kontrola

Po zgromadzeniu określonej liczby błędów konwersji w narzędziu do raportowania błędów konwersji zostanie wyświetlone pytanie, czy użytkownik chce wysłać raport dotyczący błędów konwersji. Raport na temat błędów konwersji można także wysłać z narzędzia do raportowania błędów konwersji IME w dowolnym momencie. Przed podjęciem decyzji dotyczącej wysłania można wyświetlić informacje zawarte w poszczególnych raportach. Korzystając z ustawień edytora IME, można także włączyć automatyczne wysyłanie raportów o błędach konwersji.

Rejestrowanie słów w edytorze IME

Opis funkcji

W niektórych edytorach IME można korzystać z rejestracji słów do zgłaszania nieobsługiwanych słów (słów, które mogłyby zostać nieprawidłowo przekonwertowane z danych wprowadzonych za pomocą klawiatury na ideogramy).

Informacje zbierane, przetwarzane lub przesyłane

Raporty rejestracyjne mogą zawierać informacje na temat zgłaszanych słów wprowadzone w oknie dialogowym dodawania słowa, a także numer wersji oprogramowania edytora IME. Raporty mogą zawierać także informacje osobiste, jeśli za pomocą funkcji rejestrowania słów są dodawane imiona i nazwiska. Przed podjęciem decyzji dotyczącej wysłania można wyświetlić dane zawarte w poszczególnych raportach.

Używanie informacji

Te informacje pomagają firmie Microsoft w udoskonalaniu jej produktów i usług. Firma Microsoft nie używa zebranych informacji do ustalania tożsamości użytkownika, kontaktowania się z nim ani do kierowania do niego reklam.

Wybór i kontrola

Po utworzeniu każdego raportu rejestracyjnego słowa użytkownik decyduje, czy chce wysłać ten raport do firmy Microsoft. Przed podjęciem decyzji dotyczącej wysłania można wyświetlić informacje zawarte w raporcie.

Góra strony

Udostępnianie połączenia internetowego

Opis funkcji

Udostępnianie połączenia internetowego umożliwia udostępnianie komórkowego połączenia szerokopasmowego z Internetem innym urządzeniom przez sieć Wi-Fi. Udostępnianie połączenia internetowego na urządzeniu korzystającym z komórkowego połączenia szerokopasmowego można także rozpocząć z poziomu komputera, o ile na obu urządzeniach zalogowano się za pomocą tego samego konta Microsoft.

Informacje zbierane, przetwarzane lub przesyłane

Po pierwszym udostępnieniu połączenia internetowego system Windows automatycznie generuje i zapisuje nazwę sieci oraz hasło. Można je zmienić w dowolnym momencie.

Jeśli dany komputer obsługuje takie działanie i został dodany do konta

Microsoft jako urządzenie zaufane, system Windows synchronizuje nazwę sieci i hasło z kontem Microsoft użytkownika. System Windows synchronizuje także inne informacje, dzięki czemu można zdalnie rozpocząć udostępniania połączenia internetowego z innych zaufanych urządzeń. Te informacje obejmują adres sprzętowy radia korzystającego z technologii Bluetooth oraz losowy numer pomagający zabezpieczyć połączenie.

Używanie informacji

Te informacje służą do konfigurowania udostępniania połączenia internetowego. Firma Microsoft nie używa zebranych informacji do ustalania tożsamości użytkownika, kontaktowania się z nim ani do kierowania do niego reklam.

Wybór i kontrola

Jeśli użytkownik zaloguje się za pomocą konta Microsoft na urządzeniu obsługującym udostępnianie połączenia internetowego i doda to urządzenie jako urządzenie zaufane, informacje potrzebne do zdalnego rozpoczęcia udostępniania połączenia internetowego zostaną zsynchronizowane z usługą OneDrive. Aby zatrzymać synchronizowanie informacji, wystarczy anulować synchronizowanie haseł. Aby uzyskać więcej informacji, zobacz sekcję „Synchronizacja ustawień” na tej stronie.

Góra strony

Drukowanie internetowe

Opis funkcji

Drukowanie internetowe umożliwia drukowanie przez Internet.

Informacje zbierane, przetwarzane lub przesyłane

Podczas drukowania za pomocą tej funkcji należy najpierw połączyć się z serwerem drukowania internetowego i uwierzytelnić się na nim. Informacje, które trzeba przesłać do serwera wydruku zależą od poziomu zabezpieczeń obsługiwanego przez serwer wydruku (na przykład może być konieczne podanie nazwy użytkownika i hasła). Po nawiązaniu połączenia zostaje wyświetlona lista zgodnych drukarek. Jeśli na danym komputerze nie ma sterownika wybranej drukarki,

można pobrać sterownik z serwera wydruku. Zadania drukowania nie są szyfrowane, w związku z czym inne osoby mogą zobaczyć ich zawartość podczas przesyłania.

Używanie informacji

Zbierane informacje umożliwiają użytkownikom drukowanie na drukarkach zdalnych. W przypadku wybrania serwera wydruku hostowanego przez firmę Microsoft firma ta nie używa przekazanych informacji do ustalania tożsamości użytkownika, do kontaktowania się z nim ani do kierowania do niego reklam. Informacje wysyłane do serwera wydruku innej firmy są używane zgodnie z zasadami zachowania poufności informacji obowiązującymi w danej firmie.

Wybór i kontrola

Drukowanie internetowe można włączyć lub wyłączyć, otwierając aplet **Programy i funkcje** w Panelu sterowania, a następnie wybierając pozycję **Włącz lub wyłącz funkcje systemu Windows**można wyświetlić oraz zarządzać nimi.

Góra strony

Preferencje językowe

Opis funkcji

Preferowane języki można dodać do listy języków w systemie Windows 8.1. Aplikacje i witryny sieci Web są wyświetlane w pierwszym języku dostępnym na liście.

Informacje zbierane, przetwarzane lub przesyłane

Kiedy użytkownik odwiedza witryny sieci Web i instaluje aplikacje na komputerze, lista preferowanych języków jest wysyłana do odwiedzanych witryn sieci Web i zostaje udostępniona w używanych aplikacjach, dzięki czemu mogą one wyświetlać zawartość w odpowiednich językach.

Używanie informacji

Lista preferowanych języków umożliwia wyświetlanie zawartości w witrynach sieci Web i aplikacjach firmy Microsoft w preferowanym języku użytkownika. Firma Microsoft nie używa informacji dotyczących

języków do ustalenia tożsamości użytkownika ani do kontaktowania się z nim. Informacje dotyczące języków wysyłane do witryn sieci Web oraz aplikacji innych firm i przez nie używane podlegają zasadom zachowania poufności informacji obowiązującym u danego wydawcy witryny sieci Web lub aplikacji.

Wybór i kontrola

Lista preferowanych języków jest dostępna dla instalowanych aplikacji i odwiedzanych witryn sieci Web. Języki na tej liście można dodawać lub usuwać, korzystając z ustawień preferencji językowych w Panelu sterowania. Jeśli na liście nie ma żadnych języków, do odwiedzanych witryn sieci Web będzie wysyłany język wybrany na karcie Formaty w aplecie Region w Panelu sterowania.

Góra strony

Usługi lokalizacyjne

Usługi lokalizacyjne systemu Windows pozwalają wybrać, które aplikacje, witryny i funkcje systemu Windows mogą określać lokalizację komputera. Usługi lokalizacyjne systemu Windows obejmują dwa składniki. Dostawca lokalizacji systemu Windows łączy się z usługami online firmy Microsoft w celu określenia lokalizacji. Platforma lokalizacji systemu Windows może określić lokalizację komputera, korzystając z rozwiązań sprzętowych (takich jak czujnik GPS) lub programowych (takich jak dostawca lokalizacji systemu Windows).

Platforma lokalizacji systemu Windows

Opis funkcji

W przypadku włączenia Platformy lokalizacji systemu Windows aplikacje instalowane ze Sklepu Windows oraz niektóre funkcje systemu Windows będą mogły prosić o pozwolenie na dostęp do danych dotyczących lokalizacji komputera. W przypadku wyrażenia zgody na korzystanie z informacji o lokalizacji przez aplikację oprócz dostarczania informacji o lokalizacji Platforma lokalizacji systemu Windows może też informować aplikację, gdy komputer znajdzie się wewnątrz obszaru geograficznego zdefiniowanego przez aplikację lub poza takim obszarem. Na przykład aplikacja może pozwalać ustawiać przypomnienie o zrobieniu zakupów, gdy użytkownik wychodzi z pracy.

W zależności od konfiguracji systemu Platforma lokalizacji systemu Windows może określić lokalizację komputera, korzystając z rozwiązań sprzętowych (takich jak czujnik GPS) lub programowych (takich jak dostawca lokalizacji systemu Windows).

Platforma lokalizacji systemu Windows nie uniemożliwia aplikacjom dostępu do danych dotyczących lokalizacji komputera uzyskanych przy użyciu innych metod. Można na przykład zainstalować urządzenia (takie jak odbiornik GPS), które mogą wysyłać informacje o lokalizacji bezpośrednio do aplikacji, pomijając platformę. Bez względu na ustawienia Platformy lokalizacji systemu Windows usługi w trybie online mogą za pomocą adresu IP komputera określać jego przybliżoną lokalizację (zwykle miasto, w którym użytkownik korzysta z komputera).

Informacje zbierane, przetwarzane lub przesyłane

Sama Platforma lokalizacji systemu Windows nie wysyła żadnych informacji z komputera użytkownika, ale mogą to robić poszczególni dostawcy lokalizacji (na przykład Dostawca lokalizacji systemu Windows), kiedy Platforma lokalizacji systemu Windows zażąda określenia lokalizacji komputera. Aplikacje, witryny i funkcje autoryzowane do określania lokalizacji użytkownika za pomocą platformy również mogą przesyłać lub przechowywać takie informacje. Jeśli w aplikacji są zapisane obszary geograficzne do monitorowania, są one przechowywane na komputerze w postaci zaszyfrowanej. Zapisane informacje o takich obszarach obejmują nazwę, lokalizację oraz informację o tym, czy komputer był w obszarze czy poza nim, gdy ostatnio określano lokalizację. Aplikacje, które pozwalają ustawiać obszary geograficzne, mogą przesyłać lub zapisywać takie informacje.

Używanie informacji

Jeśli Platforma lokalizacji systemu Windows zostanie włączona, autoryzowane aplikacje, witryny i funkcje systemu Windows będą mogły korzystać z danych dotyczących lokalizacji w celu dostarczenia użytkownikowi spersonalizowanej zawartości. W przypadku korzystania z aplikacji innej firmy lub innego dostawcy lokalizacji używanie informacji dotyczących lokalizacji komputera zależy od zasad zachowania poufności informacji obowiązujących w danej firmie. Przed pobraniem aplikacji ze Sklepu Windows można sprawdzić w jej opisie,

czy obsługuje ona usługi lokalizacji.

Wybór i kontrola

Wybranie ustawień ekspresowych podczas konfiguracji systemu Windows powoduje włączenie platformy lokalizacji systemu Windows. Jeśli użytkownik zdecyduje się dostosować ustawienia, może kontrolować Platformę lokalizacji systemu Windows przez wybranie opcji Zezwalaj systemowi Windows i aplikacjom na żądanie informacji o mojej lokalizacji z platformy lokalizacji systemu Windows w obszarze Udostępniaj informacje firmie Microsoft i innym usługom. Kiedy dana aplikacja kupiona w Sklepie po raz pierwszy zażąda lokalizacji komputera, system Windows wyświetli pytanie o zezwolenie na udostępnienie danych dotyczących lokalizacji komputera. Ustawienia każdej aplikacji ze Sklepu można wyświetlić i zmienić w obszarze Uprawnienia w ustawieniach aplikacji.

Jeśli jest używana aplikacja klasyczna, która korzysta z platformy lokalizacji systemu Windows, powinna wyświetlić monit o zgodę użytkownika na korzystanie z danych dotyczących lokalizacji komputera. Kiedy aplikacja uzyskuje dostęp do danych dotyczących lokalizacji komputera, w obszarze powiadomień jest wyświetlana ikona informująca użytkownika o korzystaniu z tych danych. Każdy użytkownik może sterować własnymi ustawieniami lokalizacji dla wszystkich aplikacji w sekcji **Prywatność** w ustawieniach komputera. Ponadto za pomocą opcji **Ustawienia lokalizacji** w Panelu sterowania administrator może wyłączyć Platformę lokalizacji systemu Windows dla wszystkich użytkowników. Aby uniemożliwić powiadamianie aplikacji o przekroczeniu obszarów geograficznych zdefiniowanych przez aplikacje, administrator może wyłączyć Usługę struktury lokalizacji systemu Windows w Panelu sterowania.

Dostawca lokalizacji systemu Windows

Opis funkcji

Dostawca lokalizacji systemu Windows nawiązuje połączenie z usługą lokalizacyjną firmy Microsoft w trybie online, co ułatwia określenie przybliżonej lokalizacji komputera na podstawie informacji dotyczących sieci Wi-Fi w pobliżu komputera oraz adresu IP komputera.

Informacje zbierane, przetwarzane lub przesyłane

Kiedy aplikacja autoryzowana przez użytkownika do korzystania z danych dotyczących lokalizacji chce uzyskać takie dane, platforma lokalizacji systemu Windows próbuje określić bieżącą lokalizację, korzystając z informacji dostarczonych przez wszystkich zainstalowanych dostawców lokalizacji (w tym przez dostawcę lokalizacji systemu Windows). Dostawca lokalizacji systemu Windows sprawdza najpierw, czy istnieje zapisana lista pobliskich punktów dostępu Wi-Fi utworzona w wyniku poprzedniego żądania ze strony aplikacji obsługującej usługi lokalizacji. Jeśli nie ma jeszcze listy pobliskich punktów dostępu Wi-Fi lub jeśli ta lista jest nieaktualna, wówczas dostawca wysyła informacje dotyczące pobliskich punktów dostępu Wi-Fi oraz dane GPS (jeśli są dostępne) do usługi lokalizacyjnej firmy Microsoft. Usługa zwraca dane o przybliżonej lokalizacji komputera, a dostawca przekazuje je do platformy lokalizacji systemu Windows w celu udostępnienia ich aplikacjom, które wysłały odpowiednie żądanie. Dostawca lokalizacji systemu Windows może również zaktualizować swoją listę punktów dostępu Wi-Fi. Dostawca lokalizacji systemu Windows zachowuje tę listę, aby określić przybliżoną lokalizację komputera bez konieczności każdorazowego łączenia się z Internetem. Jeśli lista punktów dostępu jest przechowywana na dysku, wówczas jest szyfrowana, aby aplikacje nie mogły uzyskać do niej bezpośredniego dostępu.

Informacje dotyczące pobliskich punktów dostępu Wi-Fi zawierają między innymi identyfikator BSSID (adres MAC punktu dostępu Wi-Fi) i dane dotyczące siły sygnału. Dane GPS to między innymi szerokość i długość geograficzna, prędkość i wysokość. Aby chronić prywatność użytkowników, dostawca lokalizacji systemu Windows nie wysyła żadnych informacji, które umożliwiałyby jednoznaczną identyfikację komputera, a jedynie standardowe informacje o komputerze, które są wysyłane w ramach każdego połączenia z Internetem. Aby zapewnić ochronę prywatności właścicieli sieci Wi-Fi, system Windows nie wysyła identyfikatorów SSID (nazw punktów dostępu Wi-Fi) ani informacji o ukrytych sieciach Wi-Fi. W celu zapewnienia ochrony prywatności i bezpieczeństwa informacje o sieciach Wi-Fi są wysyłane w postaci szyfrowanej przez protokół SSL.

Jeśli użytkownik zadeklarował chęć pomocy w ulepszaniu usługi lokalizacyjnej, system Windows firmy Microsoft może ponownie wysłać do firmy Microsoft informacje o pobliskich punktach dostępu do sieci

Wi-Fi po wysłaniu przez aplikację żądania dotyczącego lokalizacji komputera. Jeśli użytkownik korzysta z taryfowego połączenia z Internetem, system Windows zmniejszy dzienną częstotliwość wysyłania informacji, aby ograniczyć użycie połączenia z Internetem.

Używanie informacji

Informacje są używane przez dostawcę lokalizacji systemu Windows w celu przekazywania platformie lokalizacji systemu Windows przybliżonej lokalizacji komputera, kiedy autoryzowana aplikacja wyśle odpowiednie żądanie.

Jeśli użytkownik zdecydował się pomagać w udoskonalaniu usługi lokalizacji firmy Microsoft, informacje dotyczące sieci Wi-Fi oraz danych GPS wysyłane do firmy Microsoft służą do udoskonalania usług lokalizacyjnych firmy Microsoft, co przyczynia się do poprawy usług tego typu używanych przez aplikacje użytkownika. Firma Microsoft nie przechowuje żadnych danych zebranych za pomocą tej usługi, które mogłyby posłużyć do ustalenia tożsamości użytkownika, kontaktowania się z nim ani kierowania do niego reklam czy też śledzenie danego komputera lub utworzenie historii jego lokalizacji.

Wybór i kontrola

Dostawca lokalizacji systemu Windows jest używany, tylko jeśli autoryzowana aplikacja żąda danych dotyczących lokalizacji komputera. Więcej informacji na temat umożliwiania aplikacjom żądania danych dotyczących lokalizacji komputera użytkownika można znaleźć w sekcji Platforma lokalizacji systemu Windows. Jeśli aplikacje mają pozwolenie użytkownika na żądanie danych dotyczących lokalizacji komputera, buforowana lista lokalizacji pobliskich punktów dostępu Wi-Fi zaszyfrowanych i przechowywanych przez dostawcę lokalizacji systemu Windows będzie okresowo usuwana i zamieniana.

Wybranie ustawień ekspresowych podczas konfiguracji systemu Windows jest równoznaczne z zadeklarowaniem chęci pomocy w udoskonalaniu usługi lokalizacyjnej firmy Microsoft. Jeśli użytkownik zdecyduje się dostosować ustawienia, może kontrolować, czy pomagać w ulepszaniu usługi lokalizacyjnej firmy Microsoft, przez wybranie opcji **Wysyłaj do firmy Microsoft pewne dane o lokalizacji podczas używania aplikacji uwzględniających lokalizację** w obszarze **Pomóż w ulepszaniu produktów i usług firmy Microsoft**. Po

ukończeniu konfiguracji systemu Windows można zmienić to ustawienie, korzystając z ustawień lokalizacji w Panelu sterowania. Użytkownik może określać przybliżoną lokalizację komputera za pomocą dostawcy lokalizacji systemu Windows, nawet jeśli zdecydował się nie pomagać w udoskonalaniu tej usługi.

Dostawcę lokalizacji systemu Windows można włączyć lub wyłączyć, otwierając ustawienia **Włącz lub wyłącz funkcje systemu Windows** w Panelu sterowania. Nawet jeśli dostawca lokalizacji systemu Windows zostanie wyłączony, w ramach platformy lokalizacji systemu Windows wciąż można używać innych dostawców lokalizacji (na przykład systemów GPS).

Góra strony

Zarządzanie poświadczeniami

Opis funkcji

System Windows umożliwia łączenie aplikacji ze Sklepu Windows z kontami używanymi w witrynach sieci Web. Jeśli użytkownik zapisał wcześniej w programie Internet Explorer hasło do witryny sieci Web, system Windows może użyć tego hasła, kiedy użytkownik łączy aplikację z daną witryną.

Informacje zbierane, przetwarzane lub przesyłane

Jeśli aplikacja wyświetla monit o podanie poświadczeń umożliwiających zalogowanie się w witrynie sieci Web, można zdecydować się na ich zapisanie. Jeśli użytkownik wcześniej logował się w danej witrynie sieci Web za pomocą programu Internet Explorer i wybrał opcję zapisania poświadczeń, system Windows automatycznie wprowadza zapisane poświadczenia. Poświadczenia są przechowywane na komputerze w postaci zaszyfrowanej. Więcej informacji na temat synchronizowania tych i innych poświadczeń z usługą OneDrive można znaleźć w sekcji „Synchronizacja ustawień” na tej stronie.

Używanie informacji

System Windows korzysta z zapisanych poświadczeń tylko do ułatwienia użytkownikom logowania się w wybranych witrynach sieci Web. Jeśli poświadczenia zostały zapisane podczas łączenia aplikacji z witryną sieci Web, zapisane poświadczenia nie będą używane w

programie Internet Explorer ani w innych aplikacjach.

Wybór i kontrola

Zapisanymi poświadczeniami można zarządzać za pomocą Menedżera poświadczeń dostępnego w Panelu sterowania. Więcej informacji na temat synchronizowania tych i innych poświadczeń z usługą OneDrive można znaleźć w sekcji „Synchronizacja ustawień” na tej stronie.

Góra strony

Nazwa i awatar

Opis funkcji

W celu dostarczenia spersonalizowanej zawartości niektóre aplikacje mogą żądać nazwy i awatara użytkownika z systemu Windows. Nazwa i awatar użytkownika są wyświetlone w obszarze **Twoje konto** w obszarze **Konta** w ustawieniach komputera. Jeśli użytkownik zaloguje się w systemie Windows za pomocą konta Microsoft, system Windows użyje nazwy i awatara użytkownika skojarzonych z tym kontem. Jeśli użytkownik nie wybrał awatara, będzie nim domyślny awatar systemu Windows.

Informacje zbierane, przetwarzane lub przesyłane

Jeśli użytkownik umożliwił aplikacjom używanie swojej nazwy i awatara, system Windows udostępnia aplikacjom na żądanie nazwę i awatara użytkownika. Aplikacje mogą przechowywać lub przesyłać te informacje.

Jeśli użytkownik zaloguje się w systemie Windows za pomocą konta domeny i umożliwi aplikacjom używanie swojej nazwy i awatara, aplikacje, które mogą korzystać z poświadczeń użytkownika w systemie Windows, będą miały dostęp do określonych innych typów informacji dotyczących konta domeny. Wśród tych informacji jest na przykład główna nazwa użytkownika (np. jacek@contoso.com) i nazwa DNS domeny (np. firma.contoso.com\jacek).

Jeśli użytkownik zaloguje się w systemie Windows za pomocą konta Microsoft lub jeśli zaloguje się w systemie Windows za pomocą konta domeny połączonego z kontem Microsoft, system Windows może automatycznie zsynchronizować awatara na komputerze z awatarem

konta Microsoft.

Używanie informacji

W przypadku korzystania z aplikacji innych firm używanie nazwy i awatara przez daną aplikację zależy od zasad zachowania poufności informacji obowiązujących w danej firmie. Jeśli użytkownik korzysta z aplikacji firmy Microsoft, odpowiednie informacje można znaleźć w zasadach zachowania poufności informacji danej aplikacji.

Wybór i kontrola

Wybranie ustawień ekspresowych podczas konfiguracji systemu Windows powoduje, że system Windows udostępnia aplikacjom nazwę i awatara użytkownika. Jeśli użytkownik zdecyduje się dostosować ustawienia, może kontrolować dostęp do swojej nazwy i awatara, wybierając pozycję **Zezwalaj aplikacjom na użycie mojej nazwy i awatara** w obszarze **Udostępniaj informacje firmie Microsoft i innym usługom**. Po ukończeniu konfiguracji systemu Windows można zmienić to ustawienie, korzystając z opcji **Prywatność** w ustawieniach komputera. Awatara można zmienić, korzystając z opcji **Konta** w ustawieniach komputera. Można także zdecydować, że określone aplikacje mogą zmienić awatara.

Góra strony

Rozpoznawanie sieci

Opis funkcji

Jeśli użytkownik korzysta z planu taryfowego obejmującego dostęp do sieci (na przykład przez komórkowe połączenie szerokopasmowe), ta funkcja udostępnia informacje o planie taryfowym aplikacjom i funkcjom systemu Windows na komputerze. Funkcje systemu Windows i aplikacje mogą korzystać z tych informacji do zoptymalizowania działania. Jeśli na przykład użytkownik korzysta z planu taryfowego z naliczaniem, usługa Windows Update poczeka z pobieraniem na komputer aktualizacji o niższym priorytecie, aż użytkownik połączy się z innym typem sieci. Ta funkcja udostępnia także informacje na temat połączenia sieciowego, takie jak siła sygnału i czy komputer jest połączony z Internetem.

Informacje zbierane, przetwarzane lub przesyłane

Ta funkcja zbiera informacje dotyczące łączności z Internetem i siecią intranet, takie jak sufiks DNS (Domain Name Service) komputera, nazwa sieci i adres bramy sieci, z którymi łączy się komputer. Funkcja otrzymuje także informacje na temat planu taryfowego, takie jak ilość danych pozostałych w ramach planu.

Profile łączności sieciowej mogą zawierać historię wszystkich odwiedzonych sieci oraz datę i godzinę ostatniego połączenia. Ta funkcja może próbować połączyć się z serwerem firmy Microsoft w celu sprawdzenia, czy użytkownik jest połączony z Internetem. Jedyne dane wysyłane do firmy Microsoft podczas testów łączności sieciowej to standardowe informacje o komputerze.

Używanie informacji

Jeśli dane są wysyłane do firmy Microsoft, służą wyłącznie do ustalenia stanu łączności sieciowej. Stan łączności sieciowej jest udostępniany aplikacjom i funkcjom na komputerze wymagającym podania takich danych. Jeśli użytkownik korzysta z aplikacji strony trzeciej, używanie informacji podlega zasadom zachowania poufności informacji danej firmy.

Wybór i kontrola

Funkcja rozpoznawania sieci jest domyślnie włączona. Administrator może ją wyłączyć, korzystając z opcji usług w aplecie Narzędzie administracyjne w Panelu sterowania. Nie zaleca się wyłączania tej funkcji, ponieważ spowoduje to nieprawidłowe działanie niektórych funkcji systemu Windows.

Góra strony

Powiadomienia, aplikacje na ekranie blokady i aktualizacje kafelków

Aplikacje ze Sklepu Windows mogą automatycznie otrzymywać zawartość i wyświetlać powiadomienia na kilka sposobów. Mogą na przykład prezentować powiadomienia wyświetlane przez chwilę w rogu ekranu lub na kafelkach aplikacji, które są przypięte do ekranu startowego. Te powiadomienia można także otrzymywać na ekranie blokady. Na ekranie blokady mogą być także wyświetlane szczegółowe lub ogólne informacje o stanie poszczególnych aplikacji. Wydawcy

aplikacji mogą wysyłać zawartość do aplikacji w Sklepie Windows za pośrednictwem usługi powiadamiania WNS (Windows Push Notification Service) uruchomionej na serwerach firmy Microsoft. Zamiast tego aplikacje mogą też pobierać informacje bezpośrednio z serwerów innych firm.

Powiadomienia

Opis funkcji

Aplikacje ze Sklepu Windows mogą udostępniać użytkownikom informacje w trybie okresowym lub w czasie rzeczywistym, wyświetlając je przez chwilę jako powiadomienia w rogu ekranu.

Informacje zbierane, przetwarzane lub przesyłane

Aplikacje mogą prezentować w powiadomieniach tekst, obrazy albo oba typy informacji. Zawartość powiadomień może być dostarczana lokalnie przez aplikację — na przykład alarm z aplikacji budzika. Powiadomienia mogą być także wysyłane z usługi aplikacji w trybie online za pośrednictwem usługi powiadamiania WNS (Windows Push Notification Service) — na przykład aktualizacja w sieci społecznościowej. Obrazy wyświetlane w powiadomieniach mogą być pobierane bezpośrednio z serwera określonego przez wydawcę aplikacji. W takiej sytuacji na dany serwer są wysyłane standardowe informacje o komputerze.

Używanie informacji

Firma Microsoft używa informacji dotyczących powiadomień wyłącznie do obsługi powiadomień wysyłanych z aplikacji do użytkownika. Przed dostarczeniem powiadomienia do użytkownika może być ono tymczasowo przechowywane w usłudze powiadamiania WNS (Windows Push Notification Service). Jeśli nie można natychmiast dostarczyć powiadomienia, będzie ono przechowywane tylko przez kilka minut, a potem zostanie usunięte.

Wybór i kontrola

Powiadomienia wysyłane przez wszystkie lub niektóre aplikacje można wyłączyć, korzystając z opcji **Powiadomienia** w obszarze **Wyszukiwanie i aplikacje** w ustawieniach komputera. Jeśli użytkownik wyłączy powiadomienia dla danej aplikacji lub ją

odinstaluje, dostawca aplikacji może nadal wysyłać aktualizacje do usługi powiadamiania WNS (Windows Push Notification Service), ale te powiadomienia nie zostaną przekazane do komputera użytkownika.

Aplikacje na ekranie blokady

Opis funkcji

Niektóre aplikacje ze Sklepu Windows mogą wyświetlać na ekranie informacje o stanie i powiadomienia, kiedy komputer jest zablokowany. Aplikacje na ekranie blokady mogą także wykonywać zadania, kiedy komputer jest zablokowany. Mogą na przykład synchronizować pocztę e-mail w tle lub umożliwiać odbieranie przychodzących połączeń telefonicznych. Z poziomu ekranu blokady można także obsługiwać aparat komputera.

Informacje zbierane, przetwarzane lub przesyłane

Aplikacje na ekranie blokady mogą otrzymywać aktualizacje stanu od wydawcy aplikacji za pośrednictwem usługi powiadamiania WNS (Windows Push Notification Service) lub bezpośrednio z serwerów wydawcy aplikacji (lub podobnej innej firmy). Aplikacje na ekranie blokady mogą także przesyłać lub przetwarzać inne informacje, które nie dotyczą powiadomień ani aktualizacji.

Używanie informacji

System Windows używa informacji dotyczących stanu i powiadomień dostarczanych przez aplikacje na ekranie blokady w celu aktualizowania tego ekranu.

Wybór i kontrola

Po skonfigurowaniu systemu Windows aplikacje Poczta, Kalendarz i Skype są automatycznie ustawiane jako aplikacje na ekranie blokady. Korzystając z pozycji **Ekran blokady** w obszarze **Komputer i urządzenia** w ustawieniach komputera, można dodać te i inne aplikacje na ekranie blokady lub je z niego usunąć, a także wyłączyć możliwość obsługi aparatu. Można także wybrać jedną aplikację, której szczegółowy stan ma być wyświetlany w trybie ciągłym na ekranie blokady (na przykład szczegóły kolejnego terminu w kalendarzu).

Za pomocą pozycji **Powiadomienia** w obszarze **Wyszukiwanie i aplikacje** w ustawieniach komputera.

Aktualizacje kafelków

Opis funkcji

Aplikacje ze Sklepu Windows mogą udostępniać użytkownikom informacje w trybie okresowym lub w czasie rzeczywistym, wyświetlając je jako aktualizacje kafelków aplikacji na ekranie startowym.

Informacje zbierane, przetwarzane lub przesyłane

Aplikacje ze Sklepu przypięte do ekranu startowego mogą aktualizować swoje kafelki za pomocą tekstu, obrazów lub tekstu i obrazów. Zawartość wyświetlana na kafelku aplikacji może być dostarczana lokalnie przez aplikację, pobierana okresowo z serwera określonego przez wydawcę aplikacji lub wysyłana przez usługi aplikacji w trybie online za pośrednictwem usługi powiadamiania WNS (Windows Push Notification Service). Jeśli zawartość kafelka jest pobierana bezpośrednio z serwera określonego przez wydawcę aplikacji, na dany serwer są wysyłane standardowe informacje o komputerze.

Używanie informacji

Firma Microsoft używa informacji dotyczących kafelków wyłącznie do obsługi aktualizacji kafelków wysyłanych z aplikacji do użytkownika. Przed dostarczeniem na komputer użytkownika te informacje mogą być tymczasowo przechowywane w usłudze powiadamiania WNS (Windows Push Notification Service). Jeśli nie można natychmiast dostarczyć aktualizacji kafelka, będzie ona przechowywana tylko przez kilka dni, a potem zostanie usunięta.

Wybór i kontrola

Jeśli aplikacja zaczęła otrzymywać aktualizacje kafelków, można je wyłączyć, zaznaczając kafelek aplikacji na ekranie startowym i wybierając pozycję **Wyłącz dynamiczny kafelek** spośród poleceń dostępnych dla aplikacji. Po odpięciu kafelka aplikacji z ekranu startowego aktualizacje jej kafelka nie będą już wyświetlane. Jeśli użytkownik odinstaluje aplikację, dostawca aplikacji może nadal wysyłać aktualizacje do usługi powiadamiania WNS (Windows Push Notification Service), ale nie zostaną one przekazane do komputera użytkownika.

Aby wyczyścić bieżące aktualizacje wyświetlone na kafelkach z ekranu

startowego, należy przesunąć szybko od prawej krawędzi do środka ekranu startowego lub wskazać jego prawy górny róg, nacisnąć lub kliknąć pozycję **Ustawienia**, a następnie nacisnąć lub kliknąć pozycję **Kafelki**. Następnie należy nacisnąć lub kliknąć przycisk **Wyczyść** w obszarze **Wyczyść informacje osobiste z kafelków**. Aktualizacje kafelków dostarczone po wyczyszczeniu bieżących aktualizacji nadal będą wyświetlane.

Góra strony

Zamawianie odbitek

Opis funkcji

Funkcja zamawiania odbitek umożliwia wysłanie zdjęć cyfrowych przechowywanych na komputerze lub dysku sieciowym do wybranego zakładu świadczącego usługi drukowania zdjęć w trybie online. W zależności od oferty zdjęcia mogą zostać wydrukowane i wysłane pocztą albo przygotowane do odbioru w miejscowym sklepie.

Informacje zbierane, przetwarzane lub przesyłane

Jeśli użytkownik zdecyduje się skorzystać z usługi drukowania zdjęć w trybie online, jego zdjęcia cyfrowe zostaną wysłane przez Internet do wybranego zakładu. Ścieżka do cyfrowych zdjęć wybranych przez użytkownika (która może zawierać nazwę użytkownika) może zostać wysłana do danej usługi, aby umożliwić wyświetlenie i przekazanie zdjęć. Pliki zdjęć cyfrowych mogą zawierać dane o obrazie przechowywane razem z plikiem w aparacie, takie jak data i godzina wykonania zdjęcia lub miejsce wykonania zdjęcia (jeśli aparat ma funkcje GPS). Pliki mogą też zawierać informacje osobiste (na przykład podpisy), które mogły zostać skojarzone z plikami za pomocą aplikacji do zarządzania zdjęciami cyfrowymi i Eksploratora plików. Więcej informacji można znaleźć w poniższej sekcji Właściwości.

Po wybraniu usługi drukowania zdjęć w trybie online za pomocą funkcji zamawiania odbitek użytkownik zostanie przekierowany w oknie dialogowym Zamawianie odbitek do witryny danej usługi w sieci Web. Informacje wprowadzone w witrynie usługi drukowania zdjęć w trybie online są przesyłane do danej usługi.

Używanie informacji

Informacje przechowywane przez aparat w plikach zdjęć cyfrowych mogą być używane w zakładzie świadczącym usługi drukowania zdjęć w trybie online podczas procesu drukowania — na przykład w celu dostosowania koloru lub ostrości obrazu przed wydrukowaniem. Informacje przechowywane przez aplikacje do zarządzania zdjęciami cyfrowymi mogą być używane w zakładzie świadczącym usługi drukowania zdjęć w trybie online jako podpisy drukowane z przodu lub z tyłu zdjęcia. Te i inne informacje przekazane do zakładu świadczącego usługi drukowania zdjęć w trybie online (na przykład dane wprowadzone w witrynie takiego zakładu w sieci Web) mogą być używane zgodnie z zasadami zachowania poufności informacji obowiązującymi w danym zakładzie.

Wybór i kontrola

Funkcja zamawiania odbitek umożliwia wybranie zdjęć do wysłania i usług, za pośrednictwem których mają zostać wydrukowane odbitki. Niektóre aplikacje do zarządzania zdjęciami cyfrowymi umożliwiają usunięcie zapisanych informacji osobistych przed wysłaniem zdjęć do druku. W celu usunięcia zapisanych informacji osobistych można także spróbować skorzystać z opcji edytowania właściwości pliku.

Góra strony

Pobieranie z wyprzedzeniem i wstępne uruchamianie

Opis funkcji

System Windows ułatwia szybsze uruchamianie aplikacji i funkcji systemu Windows, śledząc czas i częstotliwość używania tych aplikacji i funkcji oraz ładowane przez nie pliki systemowe.

Informacje zbierane, przetwarzane lub przesyłane

Kiedy użytkownik korzysta z aplikacji lub funkcji systemu Windows, system Windows zapisuje na komputerze niektóre informacje o używanych plikach systemowych oraz o czasie i częstotliwości używania danej aplikacji lub funkcji.

Używanie informacji

System Windows używa informacji o korzystaniu z aplikacji i funkcji, aby umożliwić szybsze uruchamianie aplikacji oraz funkcji. W

niektórych przypadkach aplikacje mogą być automatycznie uruchamiane w stanie wstrzymania.

Wybór i kontrola

Aplikacje, które automatycznie są uruchamiane i wstrzymywane, są wyświetlane w Menedżerze zadań. Można zakończyć ich działanie. W trybie wstrzymania te aplikacje nie mogą korzystać z kamery internetowej ani mikrofonu (do momentu ich uruchomienia), nawet jeśli wcześniej włączono taką możliwość.

Góra strony

Asystent zgodności programów

Opis funkcji

Jeśli uruchamiana aplikacja klasyczna spowoduje wystąpienie problemu ze zgodnością, Asystent zgodności programów spróbuje pomóc w jego rozwiązaniu.

Informacje zbierane, przetwarzane lub przesyłane

Jeśli uruchamiana aplikacja powoduje wystąpienie problemu ze zgodnością, zostaje wygenerowany raport zawierający informacje, takie jak nazwa i wersja aplikacji, wymagane ustawienia zgodności i dotychczasowe akcje dotyczące aplikacji. Problemy dotyczące niezgodnych aplikacji są zgłaszane do firmy Microsoft za pośrednictwem funkcji Raportowanie błędów systemu Windows lub Programu poprawy jakości obsługi klienta (CEIP) systemu Windows.

Używanie informacji

Raporty o błędach służą do udostępniania użytkownikom odpowiedzi dotyczących zgłoszonych przez nich problemów w zakresie aplikacji. Odpowiedzi zawierają linki (jeśli są dostępne) do witryny wydawcy aplikacji w sieci Web, w której można uzyskać więcej informacji na temat możliwych rozwiązań. Raporty o błędach utworzone na skutek błędów aplikacji umożliwiają łatwiejsze określenie ustawienia, które należy dostosować po napotkaniu problemów ze zgodnością aplikacji uruchomionych w tej wersji systemu Windows. Informacje zgłoszone za pośrednictwem Programu poprawy jakości obsługi klienta służą do zidentyfikowania problemów ze zgodnością aplikacji.

Firma Microsoft nie używa informacji zebranych za pomocą tej funkcji do ustalania tożsamości użytkownika, kontaktowania się z nim ani do kierowania do niego reklam.

Wybór i kontrola

W przypadku problemów zgłaszanych z pomocą funkcji Raportowanie błędów systemu Windows raport o błędzie jest tworzony tylko wtedy, gdy użytkownik wybrał opcję sprawdzania dostępności rozwiązania w trybie online. O ile użytkownik nie zgodził się wcześniej na automatyczne zgłaszanie problemów w celu sprawdzania dostępności rozwiązań, zostanie wyświetlony monit umożliwiający zdecydowanie, czy raport o błędach ma zostać wysłany. Więcej informacji można znaleźć w sekcji dotyczącej funkcji Raportowanie błędów systemu Windows.

Niektóre problemy będą automatycznie zgłaszane za pośrednictwem Programu poprawy jakości obsługi klienta systemu Windows, jeśli został on włączony. Więcej informacji można znaleźć w sekcji dotyczącej Programu poprawy jakości obsługi klienta systemu Windows.

Góra strony

Właściwości

Opis funkcji

Właściwości to informacje o pliku umożliwiające szybkie przeszukiwanie i organizowanie plików. Niektóre właściwości mają charakter wewnętrzny (na przykład rozmiar pliku), a inne mogą być charakterystyczne dla aplikacji lub urządzenia (na przykład ustawienia aparatu podczas robienia zdjęcia lub dane o lokalizacji zarejestrowane przez aparat dla zdjęcia).

Informacje zbierane, przetwarzane lub przesyłane

Rodzaj przechowywanych informacji zależy od typu pliku i aplikacji, które niego korzystają. Przykładowe właściwości to nazwa pliku, data modyfikacji, rozmiar pliku, autor, słowa kluczowe i komentarze. Właściwości są przechowywane w pliku i przenoszone z plikiem, jeśli jest on przenoszony lub kopiowany do innej lokalizacji, takiej jak udział

pliku, albo wysyłany jako załącznik do wiadomości e-mail.

Używanie informacji

Właściwości umożliwiają szybsze wyszukiwanie i organizowanie plików. Mogą także służyć aplikacjom do szybszego wykonywania określonych zadań. Żadne informacje nie są wysyłane do firmy Microsoft.

Wybór i kontrola

Określone właściwości pliku można wyedytować lub usunąć, zaznaczając dany plik w Eksploratorze plików i klikając pozycję **Właściwości**. W ten sposób nie można usuwać określonych właściwości wewnętrznych, takich jak data modyfikacji, rozmiar pliku, nazwa pliku, ani określonych właściwości charakterystyczne dla aplikacji. Właściwości charakterystyczne dla aplikacji można edytować i usuwać tylko wtedy, gdy aplikacja użyta do wygenerowania pliku obsługuje te funkcje.

Góra strony

Usługi zbliżeniowe

Usługa zbliżeniowej wymiany danych

Opis funkcji

Jeśli komputer jest wyposażony w urządzenie do komunikacji zbliżeniowej (NFC, near-field communication), wystarczy fizyczne zetknięcie go z innym urządzeniem lub akcesorium obsługującym technologię NFC, aby można było udostępniać linki, pliki i inne informacje. Istnieją dwa rodzaje połączeń zbliżeniowych: wykonanie przez zetknięcie oraz zetknięcie i przytrzymanie. Metoda „wykonanie przez zetknięcie” umożliwia tworzenie krótko– i długoterminowych połączeń między urządzeniami przy użyciu technologii Wi-Fi, Wi-Fi Direct lub Bluetooth. Metoda „zetknięcie i przytrzymanie” pozwala utworzyć połączenie, które jest aktywne, dopóki urządzenia są trzymane obok siebie.

Informacje zbierane, przetwarzane lub przesyłane

Po zetknięciu urządzeń obsługujących komunikację zbliżeniową następuje wymiana informacji między nimi w celu ustanowienia wzajemnego połączenia. W zależności od konfiguracji urządzeń dane

te mogą zawierać informacje dotyczące parowania w technologii Bluetooth, adresy sieciowe Wi-Fi oraz nazwę komputera.

Po nawiązaniu połączenia może nastąpić wymiana innych informacji między urządzeniami w zależności od używanej funkcji lub aplikacji do obsługi komunikacji zbliżeniowej. System Windows umożliwia przesyłanie plików, łączy i innych informacji między urządzeniami korzystającymi z połączenia zbliżeniowego. Aplikacje obsługujące komunikację zbliżeniową mogą wysyłać i odbierać wszelkie informacje, do których mają dostęp. Te informacje mogą być wysyłane przy użyciu połączenia sieciowego lub internetowego albo bezpośrednio przez połączenie bezprzewodowe między urządzeniami.

Używanie informacji

Informacje dotyczące sieci i komputera przesyłane w ramach połączenia zbliżeniowego służą do nawiązania połączenia sieciowego i identyfikacji urządzeń nawiązujących połączenie. Dane przesłane za pośrednictwem połączenia zbliżeniowego zainicjowanego z poziomu aplikacji mogą być używane przez tę aplikację w dowolny sposób. Żadne informacje nie są wysyłane do firmy Microsoft.

Wybór i kontrola

Usługa zbliżeniowej wymiany danych jest domyślnie włączona. Administrator może ją wyłączyć za pomocą opcji dostępnych w aplecie Urządzenia i drukarki w Panelu sterowania.

Funkcja Wyślij przez zetknięcie

Opis funkcji

Funkcja Wyślij przez zetknięcie systemu Windows ułatwia udostępnianie wybranych informacji osobie znajdującej się obok bieżącego użytkownika lub na innym jego urządzeniu (na przykład na telefonie komórkowym). Aby na przykład uruchomić w przeglądarce funkcję Wyślij przez zetknięcie, wystarczy skorzystać z okienka Urządzenia. Urządzenie, z którym nastąpi najbliższe zetknięcie, otrzyma link do aktualnie wyświetlonej strony sieci Web. Takie działanie ma także zastosowanie w przypadku aplikacji obsługujących udostępnianie informacji, takich jak obrazy, tekst czy pliki.

Informacje zbierane, przetwarzane lub przesyłane

Funkcja Wyślij przez zetknięcie korzysta z udostępnianych informacji oraz z informacji opisanych w powyższej sekcji Usługa zbliżeniowej wymiany danych.

Używanie informacji

Te informacje służą tylko do utworzenia połączenia między parą urządzeń. Funkcja Wyślij przez zetknięcie nie przechowuje udostępnionych informacji. Żadne informacje nie są wysyłane do firmy Microsoft.

Wybór i kontrola

Jeśli usługa zbliżeniowej wymiany danych jest włączona, funkcja Wyślij przez zetknięcie także jest włączona. Więcej informacji można znaleźć w sekcji Usługa zbliżeniowej wymiany danych.

Góra strony

Połączenia dostępu zdalnego

Opis funkcji

Połączenia dostępu zdalnego umożliwiają nawiązywanie połączenia z sieciami prywatnymi przy użyciu połączenia wirtualnej sieci prywatnej (VPN) i usługi dostępu zdalnego (RAS). Usługa RAS jest składnikiem, który łączy komputer kliencki (zazwyczaj komputer użytkownika) z komputerem-hostem (określanym również jako serwer dostępu zdalnego) przy użyciu standardowych protokołów komunikacyjnych. Technologie VPN umożliwiają użytkownikom nawiązywanie połączenia przez Internet z siecią prywatną, na przykład siecią firmową.

Składnikiem funkcji połączeń dostępu zdalnego jest program Dial-up Networking, który umożliwia dostęp do Internetu przy użyciu modemu telefonicznego i technologii szerokopasmowej, na przykład modemu kablowego i cyfrowej linii abonenckiej (DSL). Program Dial-up Networking zawiera składniki programu wybierającego numery telefoniczne (takie jak Klient RAS, Menedżer połączeń i Telefon RAS) oraz programy wybierające numery uruchamiane z wiersza polecenia (takie jak rasdial).

Informacje zbierane, przetwarzane lub przesyłane

Składniki programu wybierającego numery telefoniczne zbierają z

komputera takie informacje, jak nazwa użytkownika, hasło i nazwa domeny. Te informacje są wysyłane do systemu, z którym użytkownik próbuje nawiązać połączenie. Aby pomóc w ochronie danych użytkownika i zapewnić bezpieczeństwo komputera, informacje związane z zabezpieczeniami (m.in. nazwa użytkownika i hasło) są szyfrowane i przechowywane lokalnie na komputerze.

Używanie informacji

Informacje zebrane przez program wybierający numery telefoniczne pomagają komputerowi nawiązywać połączenia z Internetem. Serwer dostępu zdalnego może zachować informacje dotyczące nazwy użytkownika i adresu IP do obsługi rozliczeń i zapewnienia zgodności, ale żadne informacje nie są wysyłane do firmy Microsoft.

Wybór i kontrola

W przypadku programów wybierających, które nie są uruchamiane z wiersza polecenia, można wybrać zapisanie hasła, zaznaczając opcję **Zapisz tę nazwę użytkownika i hasło**. W dowolnym momencie można też wyczyścić tę opcję, aby usunąć wcześniej zapisane hasło z programu wybierającego. Ponieważ opcja ta jest domyślnie wyłączona, podczas łączenia z Internetem lub siecią może zostać wyświetlony monit o podanie hasła. W przypadku programów wybierających numery uruchamianych z wiersza polecenia, takich jak rasdial, opcja zapisania hasła nie jest dostępna.

Góra strony

Połączenia programów RemoteApp i pulpitu

Opis funkcji

Połączenia programów RemoteApp i pulpitu umożliwiają dostęp do aplikacji i pulpitów na komputerach zdalnych, które udostępniono w trybie online na użytek dostępu zdalnego.

Informacje zbierane, przetwarzane lub przesyłane

Po włączeniu połączenia na komputer są pobierane pliki konfiguracyjne z określonego zdalnego adresu URL. Te pliki konfiguracyjne umożliwiają połączenie aplikacji i pulpitów na komputerach zdalnych, dzięki czemu użytkownik może je uruchamiać na własnym komputerze.

Co pewien czas komputer automatycznie sprawdza, czy są dostępne aktualizacje tych plików konfiguracyjnych, i pobiera je. Te aplikacje działają na komputerach zdalnych, a informacje w nich wprowadzane są przesyłane przez sieć do komputerów zdalnych, z którymi łączy się użytkownik.

Jeśli firma Microsoft obsługuje komputer lub aplikację, z którą następuje połączenie, do firmy Microsoft mogą zostać wysłane dodatkowe informacje umożliwiające zapewnienie odpowiedniej obsługi.

Używanie informacji

Aktualizacje plików konfiguracyjnych mogą zawierać zmiany ustawień, w tym dostęp do nowych aplikacji. Nowe aplikacje zostaną uruchomione tylko wtedy, gdy użytkownik wyrazi na to zgodę. Ta funkcja wysyła także informacje do komputerów zdalnych, na których działają aplikacje zdalne. Wykorzystanie tych danych przez aplikacje zdalne podlega zasadom zachowania poufności informacji obowiązującym dostawców aplikacji i administratorów komputerów zdalnych. Jeśli firma Microsoft nie obsługuje danego połączenia zdalnego, żadne informacje nie są wysyłane do firmy Microsoft.

Wybór i kontrola

Użytkownik może sam zdecydować, czy chce korzystać z funkcji Połączenia programów RemoteApp i pulpitu. Połączenia programów RemoteApp i pulpitu można dodawać i usuwać, korzystając z apletu Połączenia programów RemoteApp i pulpitu w Panelu sterowania. Nowe połączenie można dodać, klikając pozycję **Uzyskaj dostęp do programów RemoteApp i pulpitów**i wprowadzając w oknie dialogowym adres URL połączenia. W celu pobrania adresu URL połączenia można także użyć swojego adresu e-mai. Połączenie i jego pliki można usunąć, klikając pozycję **Usuń** w oknie dialogowym opisu połączenia. Jeśli użytkownik zakończy połączenie bez zamykania wszystkich otwartych aplikacji, te aplikacje pozostaną otwarte na komputerze zdalnym. Funkcja Połączenia programów RemoteApp i pulpitu nie jest widoczna na liście Dodaj lub usuń programy w Panelu sterowania.

Góra strony

Podłączanie pulpitu zdalnego

Opis funkcji

Funkcja Podłączanie pulpitu zdalnego umożliwia nawiązanie połączenia zdalnego z komputerem-hostem, na którym uruchomiono usługi pulpitu zdalnego.

Informacje zbierane, przetwarzane lub przesyłane

Ustawienia funkcji Podłączanie pulpitu zdalnego są przechowywane w magazynie lokalnym aplikacji lub w pliku protokołu pulpitu zdalnego (RDP, Remote Desktop Protocol) na komputerze użytkownika. Te ustawienia obejmują nazwę domeny i ustawienia konfiguracyjne połączenia, takie jak nazwa komputera zdalnego, nazwa użytkownika, informacje wyświetlane, informacje o urządzeniu lokalnym, informacje dźwiękowe, schowek, ustawienia połączenia, nazwy aplikacji zdalnych oraz ikona lub miniatura sesji.

Poświadczenia dotyczące tych połączeń, poświadczenia bramy usług pulpitu zdalnego i lista nazw zaufanych serwerów bramy usług pulpitu zdalnego są przechowywane lokalnie na komputerze. Lista jest przechowywana w rejestrze. Ta lista jest przechowywana do momentu usunięcia przez administratora. Jeśli firma Microsoft nie obsługuje danego połączenia zdalnego, żadne informacje nie są wysyłane do firmy Microsoft.

Używanie informacji

Informacje zbierane przez funkcję Podłączanie pulpitu zdalnego umożliwiają łączenie się z hostami, na których działają usługi pulpitu zdalnego, przy użyciu preferowanych ustawień użytkownika. Dzięki zbieraniu informacji, takich jak nazwa użytkownika, hasło i dane dotyczące domeny, użytkownik może zapisać ustawienia połączenia, po czym wystarczy, że kliknie dwukrotnie plik RDP lub kliknie element dodany do ulubionych, aby uruchomić połączenie bez konieczności ponownego wprowadzania tych danych.

Wybór i kontrola

Użytkownik może sam zdecydować, czy chce korzystać z funkcji Podłączanie pulpitu zdalnego. Jeśli funkcja jest używana, pliki RDP użytkownika i jego elementy ulubione dotyczące funkcji Podłączanie

pulpitu zdalnego zawierają informacje wymagane do połączenia się z komputerem zdalnym (w tym opcje i ustawienia skonfigurowane podczas automatycznego zapisywania połączenia). Pliki RDP i elementy ulubione można dostosować. Dotyczy to także plików umożliwiających łączenie się z tym samym komputerem przy użyciu różnych ustawień. Aby zmodyfikować zapisane poświadczenia, należy otworzyć Menedżera poświadczeń w ustawieniach kont użytkownika w Panelu sterowania.

Góra strony

Logowanie się za pomocą konta Microsoft

Opis funkcji

Konto Microsoft (wcześniej znane jako konto Windows Live ID) to jeden adres e-mail i hasło, za pomocą których użytkownik może się logować do aplikacji, witryn i usług firmy Microsoft i wybranych partnerów firmy Microsoft. Konto Microsoft można utworzyć, korzystając z systemu Windows lub z witryn firmy Microsoft w sieci Web, które wymagają logowania się za pomocą konta Microsoft.

W systemie Windows można logować się za pomocą konta Microsoft lub (w przypadku produktów obsługujących tę funkcję) połączyć konto lokalne albo konto domeny z kontem Microsoft. Po połączeniu kont system Windows może ujednolicić wygląd komputerów i sposób korzystania z nich, automatycznie synchronizując ustawienia i informacje w systemie Windows i aplikacjach firmy Microsoft. W przypadku odwiedzenia witryny, w której do logowania jest używane konto Microsoft, system Windows automatycznie zaloguje użytkownika w witrynie.

Informacje zbierane, przetwarzane lub przesyłane

Jeśli użytkownik wprowadzi swój adres e-mail, który ma być używany do logowania na koncie Microsoft, konfigurując ustawienia komputera lub w obszarze **Konta** w ustawieniach komputera, system Windows wyśle ten adres do firmy Microsoft, aby sprawdzić, czy nie ma jeszcze skojarzonego z nim konta Microsoft. Jeśli dany adres jest już używany w ramach konta Microsoft, można zalogować się w systemie Windows za pomocą tego adresu i hasła do konta Microsoft. Jeśli użytkownik nie

ma jeszcze wystarczających informacji dotyczących zabezpieczeń konta Microsoft, możemy poprosić o podanie dodatkowych informacji, takich jak numer telefonu komórkowego, pozwalających zweryfikować właściciela danego konta. Jeśli użytkownik nie ma jeszcze konta Microsoft, może je utworzyć, korzystając z dowolnego adresu e-mail.

Gdy użytkownik zaloguje się za pomocą konta Microsoft, system Windows wyśle do firmy Microsoft także standardowe informacje o komputerze, m.in. nazwę jego producenta i modelu oraz wersję.

Za każdym razem, kiedy użytkownik loguje się w systemie Windows za pomocą konta Microsoft, a komputer jest połączony z Internetem, system Windows sprawdza adres e-mail i hasło użytkownika na serwerach firmy Microsoft. Jeśli użytkownik jest zalogowany w systemie Windows za pomocą konta Microsoft lub konta domeny połączonego z kontem Microsoft:

- Określone ustawienia systemu Windows zostaną zsynchronizowane na komputerach, na których użytkownik loguje się za pomocą konta Microsoft. Więcej informacji o synchronizowanych ustawieniach i sterowaniu nimi można znaleźć w sekcji „Synchronizacja ustawień” na tej stronie.

- Aplikacje firmy Microsoft przeprowadzające uwierzytelnianie za pomocą konta Microsoft (na przykład Poczta, Kalendarz, Kontakty, Microsoft Office i inne aplikacje) mogą automatycznie pobierać odpowiednie informacje (na przykład aplikacja Poczta może automatycznie pobierać wiadomości wysłane na adres w usłudze Outlook.com lub Hotmail.com, jeśli użytkownik taki posiada). W przeglądarkach sieci Web może następować automatyczne logowanie użytkownika w witrynach sieci Web, w których użytkownik loguje się za pomocą konta Microsoft (na przykład podczas wizyty w witrynie Bing.com może nastąpić logowanie automatyczne bez konieczności wprowadzania hasła do konta Microsoft).

System Windows wyświetli monit z pytaniem o zgodę użytkownika, zanim umożliwi aplikacjom innych firm używanie informacji z profilu użytkownika lub innych informacji osobistych skojarzonych z jego kontem Microsoft. Jeśli użytkownik zaloguje się w systemie Windows za pomocą konta domeny połączonego z kontem Microsoft, wybrane

przez niego ustawienia i informacje zostaną zsynchronizowane z kontem domeny, a użytkownik zostanie automatycznie zalogowany w aplikacjach i witrynach sieci Web, jak to opisano powyżej. Administrator domeny ma dostęp do wszelkich informacji na komputerze, a zatem może uzyskiwać dostęp do dowolnych ustawień i informacji, które użytkownik zdecydował się synchronizować z innymi komputerami za pośrednictwem konta Microsoft. Mogą to być ustawienia, takie jak nazwa, awatar i historia przeglądania. Więcej informacji o synchronizowanych ustawieniach i sterowaniu nimi można znaleźć w sekcji „Synchronizacja ustawień” na tej stronie.

Używanie informacji

Jeśli użytkownik tworzy nowe konto Microsoft w systemie Windows, używamy podanych przez niego informacji do utworzenia i zabezpieczenia konta. Informacje pomocne w zabezpieczeniu konta (takie jak numer telefonu lub dodatkowy adres e-mail) są na przykład używane w przypadku problemów z zalogowaniem się na koncie. Jeśli użytkownik zaloguje się w systemie Windows za pomocą konta Microsoft, system Windows automatycznie loguje go w aplikacjach i witrynach sieci Web, korzystając z danych konta Microsoft. Aby uzyskać więcej informacji o wpływie korzystania z konta Microsoft na prywatność, zobacz Zasady zachowania poufności informacji dotyczących konta Microsoft. Informacje na temat używania informacji skojarzonych z kontem Microsoft przez poszczególne aplikacje firmy Microsoft można znaleźć w zasadach zachowania poufności informacji poszczególnych aplikacji. Zasady zachowania poufności informacji aplikacji firmy Microsoft można znaleźć w obszarze Ustawienia aplikacji, w oknie dialogowym Informacje.

Standardowe informacje o urządzeniu mogą posłużyć do personalizacji pewnych powiadomień przeznaczonych dla użytkownika, np. wiadomości e-mail z podstawowymi instrukcjami ułatwiającymi rozpoczęcie pracy.

Wybór i kontrola

Jeśli użytkownik loguje się w systemie Windows za pomocą konta Microsoft, niektóre ustawienia są synchronizowane automatycznie. Informacje na temat sposobu zmieniania ustawień synchronizowanych i zatrzymywania synchronizacji w systemie Windows można znaleźć w

sekcji „Synchronizacja ustawień” na tej stronie. Więcej informacji na temat danych zbieranych przez aplikacje firmy Microsoft używające konta Microsoft do uwierzytelniania można znaleźć w ich zasadach zachowania poufności informacji.

W przypadku produktów obsługujących tę funkcję można w dowolnym momencie utworzyć konto lokalne lub konto Microsoft w obszarze **Konta** w ustawieniach komputera. Użytkownik, który zalogował się w systemie Windows za pomocą konta domeny, może w dowolnym momencie połączyć lub rozłączyć się z kontem Microsoft, korzystając z obszaru **Konta** w ustawieniach komputera.

W przypadku korzystania z przeglądania InPrivate w programie Internet Explorer nie następuje automatyczne logowanie w witrynach sieci Web korzystających z kont Microsoft.

Góra strony

Magazyn w chmurze usługi OneDrive

Opis funkcji

Jeśli włączysz odpowiednią opcję, po zalogowaniu się na urządzeniu za pomocą konta Microsoft wybrane treści i ustawienia mogą być automatycznie zapisywane na serwerach firmy Microsoft. Dzięki temu uzyskujesz kopię zapasową na wypadek utraty lub awarii urządzenia.

Informacje zbierane, przetwarzane lub przesyłane

Jeśli w trakcie konfiguracji zdecydujesz, że chcesz korzystać z usługi OneDrive jako przestrzeni dyskowej w chmurze, system Windows będzie automatycznie wysyłać na serwery firmy Microsoft dane, takie jak:

- Zdjęcia i filmy z urządzenia zapisane w folderze **Z aparatu** .
- Ustawienia, które nie są współużytkowane przez inne urządzenia użytkownika.
- Opisowe informacje na temat urządzenia (np. jego nazwa i typ).

Możesz także włączyć zapisywanie zawartości na serwerach firmy Microsoft lub ustawić serwery firmy Microsoft jako domyślną lokalizację zapisu plików dla aplikacji.

Używanie informacji

Przekazana zawartość jest używana przez system Windows tylko na potrzeby świadczenia usługi przechowywania danych w chmurze. Firma Microsoft nie używa jej do ustalania tożsamości użytkownika, kontaktowania się z nim ani do kierowania do niego reklam.

Wybór i kontrola

Jeśli podczas konfigurowania komputera zostanie wybrana pozycja „Używaj usługi OneDrive”, system Windows będzie zapisywać treści opisane w tej sekcji w usłudze OneDrive. W każdej chwili można zmienić te ustawienia w sekcji OneDrive na stronie Ustawienia komputera.

Góra strony

Synchronizacja ustawień

Opis funkcji

Jeśli użytkownik loguje się w systemie Windows za pomocą konta Microsoft, system Windows synchronizuje niektóre ustawienia i informacje użytkownika z serwerami firmy Microsoft, aby ułatwić spersonalizowane korzystanie z wielu komputerów. Jeśli użytkownik zaloguje się na jednym lub kilku komputerach za pomocą konta Microsoft, to po pierwszym zalogowaniu się na innym komputerze za pomocą tego samego konta Microsoft system Windows pobierze i zastosuje ustawienia i informacje, które mają być synchronizowane z innymi komputerami. Ustawienia wybrane przez użytkownika do synchronizowania zostaną automatycznie zaktualizowane na serwerach firmy Microsoft i na innych komputerach, z których będzie korzystał użytkownik.

Informacje zbierane, przetwarzane lub przesyłane

Jeśli użytkownik zaloguje się w systemie Windows za pomocą konta Microsoft, system Windows zsynchronizuje określone ustawienia z serwerami firmy Microsoft. Oto niektóre z tych ustawień:

- Układ ekranu startowego
- Aplikacje zainstalowane ze Sklepu Windows

- Preferencje językowe
- Preferencje dotyczące łatwego dostępu
- Ustawienia personalizacji, takie jak awatar, obraz ekranu blokady, tło i ustawienia myszy
- Ustawienia aplikacji ze Sklepu Windows
- Słowniki pisowni, słowniki edytora IME i słowniki osobiste
- Historia przeglądarki sieci Web, ulubione i otwierane witryny sieci Web
- Zapisane hasła do aplikacji i witryn sieci Web oraz hasła sieciowe
- Adresy udostępnianych drukarek sieciowych, z którymi nawiązywano połączenia

W celu ochrony prywatności użytkownika wszystkie synchronizowane ustawienia są wysyłane w szyfrowanej postaci za pomocą protokołu SSL. Część tych ustawień nie zostanie zsynchronizowana na danym komputerze, jeśli nie zostanie on dodany do konta Microsoft jako zaufany komputer.

Jeśli użytkownik zaloguje się w systemie Windows za pomocą konta domeny połączonego z kontem Microsoft, wybrane przez niego ustawienia i informacje zostaną zsynchronizowane z kontem domeny. Hasła zapisane w czasie, kiedy użytkownik jest zalogowany w systemie Windows za pomocą konta domeny połączonego z kontem Microsoft, nie są synchronizowane. Administrator domeny ma dostęp do wszelkich informacji na komputerze, a zatem może uzyskiwać dostęp do dowolnych ustawień i informacji, które użytkownik zdecydował się synchronizować z innymi komputerami za pośrednictwem konta Microsoft.

Używanie informacji

System Windows korzysta z tych ustawień i informacji do zapewnienia usługi synchronizacji. Firma Microsoft nie używa synchronizowanych ustawień ani informacji do ustalania tożsamości użytkownika, do kontaktowania się z nim ani do kierowania do niego reklam.

Wybór i kontrola

Jeśli użytkownik loguje się w systemie Windows za pomocą konta Microsoft, ustawienia są synchronizowane automatycznie. Korzystając z obszaru **Synchronizacja ustawień** w sekcji OneDrive w ustawieniach komputera, można włączyć synchronizowanie ustawień i wybrać poszczególne synchronizowane ustawienia. Jeśli użytkownik zaloguje się w systemie Windows za pomocą konta domeny i zdecyduje się połączyć je z kontem Microsoft, system Windows przed utworzeniem połączenia z kontem Microsoft wyświetli monit umożliwiający zdecydowanie, które ustawienia mają zostać zsynchronizowane.

Góra strony

Technologia Teredo

Opis funkcji

Technologia Teredo umożliwia komputerom i sieciom komunikację przy użyciu wielu protokołów sieciowych.

Informacje zbierane, przetwarzane lub przesyłane

Po każdym uruchomieniu komputera funkcja Teredo próbuje zlokalizować w Internecie usługę publicznego protokołu internetowego w wersji 6 (IPv6). Następuje to automatycznie, jeśli komputer jest połączony z siecią publiczną lub prywatną, ale nie w przypadku sieci zarządzanych, takich jak domeny przedsiębiorstwa. Jeśli użytkownik korzysta z aplikacji, która wymaga, aby funkcja Teredo używała łączności IPv6, lub jeśli skonfiguruje zaporę tak, aby zawsze włączała obsługę łączności IPv6, wówczas funkcja Teredo okresowo kontaktuje się z usługą Teredo firmy Microsoft przez Internet. Jedyne informacje wysyłane do firmy Microsoft to standardowe informacje o komputerze i nazwa żądanej usługi (na przykład teredo.ipv6.microsoft.com).

Używanie informacji

Informacje wysyłane z komputera przez funkcję Teredo służą do określenia, czy dany komputer jest połączony z Internetem i czy może zlokalizować publiczną usługę IPv6. Po zlokalizowaniu usługi wysyłane są informacje umożliwiające utrzymanie połączenia z usługą IPv6.

Wybór i kontrola

Korzystając z narzędzia wiersza polecenia netsh, można zmienić zapytanie, które usługa wysyła przez Internet, aby korzystało z serwerów innych niż serwery firmy Microsoft, lub zupełnie je wyłączyć. Szczegółowe instrukcje można znaleźć w sekcji dotyczącej protokołu internetowego w wersji 6, technologii Teredo i technologii pokrewnych w tym oficjalnym dokumencie technicznymmożna wyświetlić oraz zarządzać nimi.

Góra strony

Usługi modułu TPM (Trusted Platform Module)

Opis funkcji

Moduł TPM (Trusted Platform Module) to urządzenie zabezpieczające wbudowane w niektóre komputery które, jeśli jest obecne i obsługiwane, umożliwia pełne wykorzystanie zaawansowanych funkcji zabezpieczeń na komputerze. Funkcje systemu Windows korzystające z modułu TPM to między innymi szyfrowanie dysków, wirtualna karta inteligentna, bezpieczny rozruch, Windows Defender i magazyn certyfikatów oparty na module TPM.

Informacje zbierane, przetwarzane lub przesyłane

Domyślnie moduł TPM należy do systemu Windows, który przechowuje wszystkie informacje o autoryzacji właściciela modułu TPM, przez co te dane są dostępne tylko dla administratorów systemu Windows. Wartości autoryzacji ograniczonej są tworzone w celu wykonywania typowych zadań administracyjnych i standardowych działań użytkownika. Zarządza nimi system Windows.

Konsola zarządzania modułem TPM umożliwia interaktywną obsługę modułu TPM i zapisywanie wartości autoryzacji właściciela modułu TPM na nośniku zewnętrznym, takim jak dysk flash USB, po zainicjowaniu obsługi modułu TPM. Zapisany plik zawiera informacje o autoryzacji właściciela modułu TPM. Plik zawiera także nazwę komputera, wersję systemu operacyjnego, nazwę użytkownika, który utworzył plik, i datę utworzenia, dzięki czemu łatwiej jest rozpoznać plik.

W środowisku domeny administrator domeny może tak skonfigurować

pełne hasło właściciela modułu TPM, aby było przechowywane w usłudze Active Directory w obiekcie TPM po zainicjowaniu obsługi modułu TPM.

Każdy moduł TPM ma unikatowy kryptograficzny klucz poręczenia gwarantujący autentyczność modułu. Klucz poręczenia mógł zostać utworzony i zapisany w module TPM przez producenta komputera. Starsze komputery mogą wymagać uruchomienia przez system Windows operacji tworzenia klucza poręczenia w module TPM. Część prywatna klucza poręczenia nie jest uwidoczniana poza modułem TPM, a po jej utworzeniu zwykle nie można jej już zresetować. Certyfikat klucza poręczenia będzie przechowywany w module TPM większości komputerów z systemem Windows. Certyfikat klucza poręczenia wskazuje, że w sprzętowym module TPM istnieje klucz poręczenia. Certyfikat umożliwia weryfikatorom zdalnym potwierdzenie, że dany moduł TPM jest zgodny ze specyfikacją modułu TPM. Certyfikat klucza poręczenia jest zwykle podpisany przez producenta modułu TPM lub producenta platformy.

Używanie informacji

Kiedy moduł TPM zostanie zainicjowany, aplikacje mogą przy użyciu modułu TPM tworzyć dodatkowe unikatowe klucze kryptograficzne i pomagać w ich zabezpieczaniu. Na przykład w ramach szyfrowania dysków moduł TPM pomaga w ochronie klucza szyfrującego dysk.

Jeśli hasło właściciela modułu TPM zostanie zapisane w pliku, dodatkowe informacje o komputerze i użytkowniku zapisane w tym pliku pomogą w zidentyfikowaniu odpowiedniego komputera i modułu TPM. Klucz poręczenia modułu TPM jest używany w systemie Windows podczas inicjowania modułu TPM do szyfrowania wartości autoryzacji właściciela modułu TPM przed wysłaniem jej do modułu TPM. System Windows nie przesyła kluczy kryptograficznych poza komputer. System Windows nie zawiera interfejsu dla aplikacji innych firm, takich jak oprogramowanie chroniące przed złośliwym kodem, umożliwiającego korzystanie z klucza poręczenia w określonych scenariuszach z wykorzystaniem modułu TPM, takich jak mierzony rozruch z zaświadczeniem. W przypadku oprogramowania chroniącego przed złośliwym kodem klucz poręczenia i certyfikat klucza poręczenia umożliwiają także potwierdzenie, że moduł TPM określonego producenta zapewnia miary rozruchu. Domyślnie z klucza poręczenia

modułu TPM mogą korzystać tylko administratorzy lub aplikacje z prawami administracyjnymi.

Wybór i kontrola

Użytkownicy lub administratorzy używają modułu TPM, włączając funkcję systemu Windows lub uruchamiając aplikację korzystającą z modułu TPM.

Moduł TPM można wyczyścić, przywracając mu domyślne ustawienia fabryczne. Wyczyszczenie modułu TPM powoduje usunięcie informacji o właścicielu oraz wszystkich (z wyjątkiem klucza poręczenia) kluczy opartych na module TPM oraz danych kryptograficznych, które mogły zostać utworzone przez aplikacje podczas używania modułu TPM.

Góra strony

Aktualizowanie certyfikatów głównych

Opis funkcji

Certyfikaty służą przede wszystkim do weryfikowania tożsamości osoby lub urządzenia, uwierzytelniania usługi lub szyfrowania plików. Zaufane urzędy certyfikacji to organizacje wydające certyfikaty. Funkcja aktualizowania certyfikatów głównych kontaktuje się z usługą Windows Update w trybie online, aby sprawdzić czy firma Microsoft dodała urząd certyfikacji do swojej listy zaufanych urzędów, ale tylko wtedy, gdy aplikacji zostaje przedstawiony certyfikat wystawiony przez urząd certyfikacji, który nie jest bezpośrednio zaufany (certyfikat, który nie znajduje się na liście zaufanych certyfikatów na komputerze użytkownika). Jeśli urząd certyfikacji został dodany do listy firmy Microsoft zawierającej zaufane urzędy, dany certyfikat zostaje automatycznie dodany do listy zaufanych certyfikatów na komputerze.

Informacje zbierane, przetwarzane lub przesyłane

Funkcja aktualizowania certyfikatów głównych wysyła żądanie do usługi Windows Update w trybie online w celu uzyskania aktualnej listy głównych urzędów certyfikacji w programie certyfikatów głównych firmy Microsoft. Jeśli na liście znajduje się niezaufany certyfikat, usługa aktualizowania certyfikatów głównych uzyskuje certyfikat od usługi Windows Update i umieszcza go w magazynie zaufanych certyfikatów

na komputerze. Przesyłane informacje to między innymi nazwy i skróty kryptograficzne certyfikatów głównych.

Używanie informacji

Informacje służą firmie Microsoft do aktualizowania listy zaufanych certyfikatów na komputerze. Firma Microsoft nie używa tych informacji do ustalania tożsamości użytkownika, kontaktowania się z nim ani do kierowania do niego reklam.

Wybór i kontrola

Funkcja aktualizowania certyfikatów głównych jest domyślnie włączona. Administratorzy mogą wyłączyć funkcję aktualizowania certyfikatów głównych na komputerze, konfigurując zasady grupy.

Góra strony

Usługi aktualizacji

Opis funkcji

Usługi aktualizacji dla systemu Windows obejmują usługi Windows Update i Microsoft Update:

- **Windows Update** to usługa zapewniająca aktualizacje programowe dla systemu Windows oraz oprogramowania pomocniczego, takiego jak sterowniki dostarczane przez producentów urządzeń.
- **Microsoft Update** to usługa zapewniająca aktualizacje programowe dla systemu Windows oraz innego oprogramowania firmy Microsoft, takiego jak pakiet Microsoft Office.

Informacje zbierane, przetwarzane lub przesyłane

Usługi aktualizacji zbierają z komputera użytkownika informacje umożliwiające firmie Microsoft uruchamianie i usprawnianie usług. Są to na przykład następujące informacje:

- Zainstalowane na komputerze oprogramowanie firmy Microsoft i inne oprogramowanie pomocnicze (na przykład sterowniki i oprogramowanie układowe dostarczane przez producentów urządzeń), dla których są dostępne aktualizacje w usługach

aktualizacji. Pomaga to firmie Microsoft określić, które aktualizacje są odpowiednie dla danego użytkownika.

- Ustawienia konfiguracji usługi Windows Update i/lub Microsoft Update, takie jak informacja, czy aktualizacje mają być automatycznie pobierane lub instalowane.
- Informacje o powodzeniach, niepowodzeniach i błędach związanych z uzyskiwaniem dostępu do usług aktualizacji oraz korzystaniem z nich.
- Numery identyfikacyjne Plug and Play urządzeń sprzętowych — kod przypisany przez producenta urządzenia umożliwiający identyfikację urządzenia (np. określonego typu klawiatury).
- Identyfikator GUID — wygenerowany losowo numer, który nie zawiera żadnych informacji osobistych. Identyfikatory GUID służą do identyfikowania konkretnych komputerów bez identyfikowania użytkownika.
- Nazwa, numer wersji, dostawca i data wersji systemu BIOS — informacje o zestawie niezbędnych procedur oprogramowania testujących sprzęt, uruchamiających system operacyjny na komputerze oraz przesyłających dane między urządzeniami sprzętowymi podłączonymi do komputera.
- Producent, model, rola platformy i numer SKU — informacje o komputerze umożliwiające badanie diagnostyczne instalacji sterowników.

Aby użyć usług aktualizacji, należy otworzyć aplet Windows Update w Panelu sterowania i sprawdzić dostępność aktualizacji lub zmienić ustawienia tak, aby system Windows automatycznie instalował aktualizacje, gdy tylko staną się dostępne (zalecana opcja). Za pośrednictwem funkcji Windows Update można zdecydować, czy ma być używana usługa Microsoft Update.

W przypadku włączenia otrzymywania ważnych aktualizacji oprogramowania dla danego komputera w aktualizacjach może zostać uwzględnione Narzędzie Windows do usuwania złośliwego oprogramowania. Narzędzie Windows do usuwania złośliwego oprogramowania sprawdza występowanie infekcji na komputerze

spowodowanych przez konkretne, powszechnie występujące złośliwe oprogramowanie („złośliwe oprogramowanie”) i pomaga usuwać znalezione infekcje. Jeśli oprogramowanie jest uruchomione, usuwa złośliwe oprogramowanie wymienione w witrynie pomocy technicznej firmy Microsoft. W ramach procesu sprawdzania obecności złośliwego oprogramowania do firmy Microsoft zostanie wysłany raport zawierający określone informacje o wykrytym złośliwym oprogramowaniu, błędach i komputerze. Więcej informacji można znaleźć w zasadach zachowania poufności informacji Narzędzia Windows do usuwania złośliwego oprogramowania można wyświetlić oraz zarządzać nimi.

Używanie informacji

Dane wysyłane do firmy Microsoft służą do obsługi i utrzymywania usług aktualizacji. Są one również używane do generowania zbiorczych danych statystycznych, które pozwalają firmie Microsoft analizować tendencje oraz poprawiać produkty i usługi, w tym usługi aktualizacji.

Identyfikator GUID zebrany przez usługi aktualizacji jest przez nie używany do generowania zbiorczych danych statystycznych w celu śledzenia i rejestrowania liczby odrębnych komputerów, na których są używane usługi aktualizacji, oraz do rejestrowania informacji o powodzeniu lub niepowodzeniu pobierania i instalacji konkretnych aktualizacji. Usługi aktualizacji rejestrują identyfikator GUID komputera, który próbuje pobrać i zainstalować aktualizację, identyfikator żądanego elementu, informację o dostępności aktualizacji oraz standardowe informacje o komputerze.

Opisane powyżej informacje zbierane przez Narzędzie Windows do usuwania złośliwego oprogramowania służą do udoskonalania produktów i usług firmy Microsoft chroniących przed złośliwym oprogramowaniem i innymi zagrożeniami. Informacje zawarte w raportach Narzędzia Windows do usuwania złośliwego oprogramowania nie będą używane do identyfikowania użytkownika ani kontaktowania się z nim.

Aktualizacje wymagane

W przypadku włączenia usług aktualizacji ich poprawne działanie wymaga niekiedy zaktualizowania składników systemu operacyjnego, które tworzą usługi aktualizacji lub są bezpośrednio z nimi powiązane.

Aktualizacje te muszą zostać wykonane, aby usługa mogła sprawdzić dostępność, pobrać lub zainstalować inne aktualizacje. Te aktualizacje wymagane zawierają poprawki błędów, zapewniają udoskonalenia oraz utrzymują zgodność z serwerami firmy Microsoft, które obsługują usługę.

Jeśli usługi aktualizacji są wyłączone, użytkownik nie będzie otrzymywał tych aktualizacji.

Aktualizacje oprogramowania wymagane do zainstalowania lub zaktualizowania aplikacji ze Sklepu Windows będą pobierane automatycznie. Aby aplikacje działały prawidłowo, te aktualizacje muszą zostać zainstalowane.

Pliki cookie i tokeny

Token jest podobny do pliku cookie. Jest to mały plik z informacjami, który jest zapisywany na dysku twardym przez serwer usług aktualizacji i używany w celu zachowania poprawnego połączenia, gdy komputer łączy się z tym serwerem. Jest przechowywany tylko na komputerze użytkownika, nie na serwerze. Ten plik cookie lub token zawiera informacje (takie jak data ostatniego skanowania) umożliwiające znalezienie najnowszych dostępnych aktualizacji. Zawiera on informacje umożliwiające ustalenie, jaka zawartość powinna zostać pobrana na komputer i kiedy pobieranie powinno mieć miejsce. Ponadto zawiera identyfikator GUID, dzięki któremu serwer może zidentyfikować komputer użytkownika.

Informacje zawarte w pliku cookie lub tokenie są szyfrowane przez serwer (z wyjątkiem daty ważności pliku cookie lub tokenu). Plik cookie lub token nie jest plikiem cookie przeglądarki, więc nie można nim sterować przy użyciu ustawień przeglądarki. Pliku cookie lub tokenu nie można usunąć. Jeśli jednak użytkownik nie korzysta z usług aktualizacji, plik cookie lub token nie będzie używany.

Wybór i kontrola

Wybranie ustawień ekspresowych podczas konfiguracji systemu Windows powoduje włączenie usługi Windows Update i automatyczne instalowanie aktualizacji przez tę usługę.

Jeśli usługi aktualizacji zostaną włączone, to niezależnie od wybranego ustawienia, bez powiadomienia użytkownika będą pobierane i

instalowane wymagane aktualizacje niektórych składników usługi. Aby nie otrzymywać aktualizacji wymaganych, należy wyłączyć usługi aktualizacji.

Usługi można też skonfigurować do sprawdzania lub automatycznego instalowania ważnych i zalecanych bądź tylko ważnych aktualizacji. Opcjonalne aktualizacje nie są instalowane automatycznie. Po ukończeniu konfiguracji systemu Windows można zmienić ustawienia usługi Windows Update w Panelu sterowania lub w ustawieniach komputera.

Jeśli użytkownik zdecydował się sprawdzać dostępność ważnych aktualizacji i instalować je, a także otrzymać Narzędzie Windows do usuwania złośliwego oprogramowania w ramach tych aktualizacji dla komputera, może wyłączyć funkcję raportowania tego oprogramowaniamożna wyświetlić oraz zarządzać nimi.

Góra strony

Wirtualne sieci prywatne

Opis funkcji

Wirtualne sieci prywatne (sieci VPN) umożliwiają łączenie się przez Internet z siecią prywatną, na przykład z siecią firmową. Połączenie VPN może być udostępnione przez klienta VPN systemu Windows lub przez aplikację innej firmy przeznaczoną do obsługi sieci VPN.

Informacje zbierane, przetwarzane lub przesyłane

W momencie połączenia się z wirtualną siecią prywatną poświadczenia wprowadzone przez użytkownika w kliencie VPN zostają wysłane do sieci zdalnej. Czasami można przechowywać te poświadczenia na swoim komputerze. Po nawiązaniu połączenia i w zależności od konfiguracji wirtualnej sieci prywatnej część działań użytkownika wykonywanych w sieci (lub wszystkie takie działania) będzie kierowana przez sieć zdalną. Administratorzy mogą skonfigurować określone aplikacje, aby zawsze kierowały ruch za pośrednictwem wirtualnej sieci prywatnej i automatycznie łączyły się z wirtualną siecią prywatną po uruchomieniu. Żadne informacje nie są wysyłane do firmy Microsoft.

Oprogramowanie innych firm do obsługi wirtualnej sieci prywatnej może gromadzić dodatkowe informacje. Zbieranie i używanie tych

informacji podlega zasadom ochrony prywatności obowiązującym w danej firmie.

Używanie informacji

Klienci sieci VPN korzystają z dostarczonych przez użytkownika poświadczeń do obsługi uwierzytelniania w sieci zdalnej oraz kierowania ruchu sieciowego do sieci zdalnej i z tej sieci. Jeśli klient sieci VPN innej firmy gromadzi dodatkowe informacje, sposób korzystania z tych informacji przez daną firmę podlega zasadom ochrony prywatności, które w niej obowiązują.

Wybór i kontrola

Korzystając z pozycji **Sieć** w ustawieniach komputera, można dodać lub usunąć połączenie z siecią VPN, a także wyświetlić stan istniejących połączeń. Po skonfigurowania połączenia z siecią VPN można ręcznie nawiązać lub zakończyć połączenie, wybierając odpowiednią sieć z listy dostępnej w obszarze Ustawienia.

Góra strony

Program poprawy jakości obsługi klienta systemu Windows

Opis funkcji

W ramach Programu poprawy jakości obsługi klienta systemu Windows mogą być zbierane podstawowe informacje dotyczące sposobu korzystania z aplikacji, komputerów, podłączonych urządzeń i systemu Windows. Mogą być również zbierane dane dotyczące ewentualnych problemów w zakresie wydajności i stabilności. Jeśli użytkownik zadeklaruje chęć udziału w Programie poprawy jakości obsługi klienta systemu Windows, system Windows wyśle te dane do firmy Microsoft i będzie okresowo pobierał plik w celu zebrania dokładniejszych informacji na temat sposobu korzystania z systemu Windows i aplikacji. Raporty tworzone w ramach Programu poprawy jakości obsługi klienta są wysyłane do firmy Microsoft i pomagają jej w ulepszaniu funkcji najczęściej używanych przez klientów i opracowywaniu rozwiązań typowych problemów.

Informacje zbierane, przetwarzane lub przesyłane

Raporty Programu poprawy jakości obsługi klienta systemu Windows

mogą zawierać następujące informacje:

- Informacje konfiguracyjne dotyczące między innymi liczby procesorów w komputerze, liczby używanych połączeń sieciowych, rozdzielczości ekranu urządzeń wyświetlających i wersji systemu Windows zainstalowanej na komputerze.

- Informacje o wydajności i niezawodności dotyczące szybkości reakcji aplikacji na kliknięcie przycisku, liczby problemów występujących podczas korzystania z aplikacji lub urządzenia oraz szybkości wysyłania i odbierania danych przy użyciu połączenia sieciowego.

- Informacje o używaniu aplikacji dotyczące między innymi częstotliwości otwierania aplikacji, częstotliwości korzystania z Pomocy i obsługi technicznej systemu Windows, usług używanych do logowania się w aplikacjach oraz liczby folderów zwykle tworzonych na pulpicie.

Raporty tworzone w ramach Programu poprawy jakości obsługi klienta mogą także zawierać informacje o zdarzeniach (dane z dziennika zdarzeń), które zostały zarejestrowane na komputerze do siedmiu dni przed podjęciem decyzji o udziale w tym programie. Ponieważ większość użytkowników decyduje się na udział w Programie poprawy jakości obsługi klienta w ciągu kilku dni od zainstalowania systemu Windows, firma Microsoft używa tych informacji w celu analizy zainstalowanego systemu Windows i usprawnienia jego instalacji.

Te informacje są wysyłane do firmy Microsoft, gdy jest aktywne połączenie z Internetem. Raporty tworzone w ramach Programu poprawy jakości obsługi klienta celowo nie zawierają danych osobowych, takich jak imię i nazwisko, adres czy numer telefonu użytkownika, jednak w niektórych raportach mogą przypadkowo znaleźć się identyfikatory indywidualne, takie jak numer seryjny urządzenia podłączonego do komputera użytkownika. Firma Microsoft filtruje informacje zawarte w raportach tworzonych w ramach Programu poprawy jakości obsługi klienta, próbując w ten sposób usunąć wszelkie identyfikatory indywidualne, które mogą się znajdować w tych raportach. W przypadku otrzymania identyfikatorów indywidualnych firma Microsoft nie używa ich do ustalania tożsamości użytkownika ani do kontaktowania się z nim.

W ramach Programu poprawy jakości obsługi klienta losowo generowany jest numer nazywany unikatowym identyfikatorem globalnym (GUID), który jest wysyłany w każdym raporcie do firmy Microsoft. Identyfikator GUID pozwala stwierdzić, jakie dane zostały wysłane z określonego komputera w danym okresie. Niektóre raporty tego programu mogą również zawierać identyfikator GUID pobrany z konta Microsoft użytkownika.

W ramach programu okresowo będzie również pobierany plik umożliwiający zebranie dokładniejszych informacji na temat sposobu korzystania z systemu Windows i aplikacji. Dzięki temu plikowi system Windows ma więcej danych ułatwiających firmie Microsoft opracowywanie rozwiązań często występujących problemów i lepsze zrozumienie typowych sposobów korzystania z systemu Windows i aplikacji.

Używanie informacji

Informacje zbierane w ramach Programu poprawy jakości obsługi klienta są używane przez firmę Microsoft do udoskonalania jej produktów i usług, a także oprogramowania i sprzętu innych producentów, które są przeznaczone do użytku z tymi produktami i usługami. Mogą również być udostępniane w postaci zagregowanej partnerom firmy Microsoft, aby umożliwić im doskonalenie produktów i usług, ale te informacje nie mogą być używane do ustalania tożsamości użytkownika, do kontaktowania się z nim ani do kierowania do niego reklam.

Na podstawie identyfikatorów GUID firma Microsoft określa spektrum otrzymywanych opinii i przydziela im priorytety. Na przykład dzięki identyfikatorom GUID firma Microsoft może odróżnić jednego klienta, u którego dany problem wystąpił sto razy, od setki klientów, u których dany problem wystąpił tylko raz. Firma Microsoft nie używa informacji zebranych w ramach Programu poprawy jakości obsługi klienta do ustalania tożsamości użytkownika ani do kontaktowania się z nim.

Wybór i kontrola

Wybranie ustawień ekspresowych podczas konfiguracji systemu Windows, powoduje włączenie Programu poprawy jakości obsługi klienta systemu Windows: system Windows i aplikacje firmy Microsoft

ze Sklepu Windows mogą wysyłać raporty tworzone w ramach Programu poprawy jakości obsługi klienta dotyczące wszystkich użytkowników danego komputera. Jeśli użytkownik zdecyduje się dostosować ustawienia, może kontrolować Program poprawy jakości obsługi klienta przez wybranie opcji **Wysyłaj do firmy Microsoft informacje dotyczące sposobu używania mojego komputera w ramach Programu poprawy jakości obsługi klienta** w obszarze **Pomóż w ulepszaniu produktów i usług firmy Microsoft**. Po ukończeniu konfiguracji systemu Windows administratorzy mogą zmienić to ustawienie, korzystając z **Centrum akcji** w Panelu sterowania.

Aby uzyskać więcej informacji, przejrzyj często zadawane pytania dotyczące Programu poprawy jakości obsługi klientamożna wyświetlić oraz zarządzać nimi.

Góra strony

Windows Defender

Usługa Windows Defender przeszukuje komputer pod kątem złośliwego oprogramowania i innych potencjalnie niechcianych programów. Zawiera funkcje Społeczność Microsoft Active Protection Service i Historia.

Społeczność Microsoft Active Protection Service

W przypadku korzystania z usługi Windows Defender usługa społeczności Microsoft Active Protection Service (MAPS) może zapewnić lepszą ochronę komputera dzięki pobieraniu nowych sygnatur niedawno wykrytego złośliwego oprogramowania oraz monitorowaniu stanu zabezpieczeń komputera. Usługa społeczności MAPS będzie wysyłać informacje o złośliwym oprogramowaniu i innym potencjalnie niechcianym oprogramowaniu do firmy Microsoft. Może ona również wysyłać pliki zawierające złośliwe oprogramowanie. Jeśli usługa społeczności MAPS wykryje, że komputer jest zarażony określonym typem złośliwego oprogramowania, może ona automatycznie skontaktować się z użytkownikiem za pomocą jego konta Microsoft w celu rozwiązania problemu.

Informacje zbierane, przetwarzane lub przesyłane

Raporty MAPS zawierają informacje o potencjalnie złośliwych plikach, takie jak nazwy plików, skróty kryptograficzne, wydawca oprogramowania, rozmiary plików i oznaczenia daty. Oprócz tego usługa społeczności MAPS może zbierać pełne adresy URL w celu wskazania źródła pochodzenia pliku oraz adresy IP, z którymi potencjalnie złośliwe oprogramowanie może nawiązywać połączenia. Te adresy URL mogą czasami zawierać informacje osobiste, takie jak wyszukiwane terminy lub dane wprowadzone w formularzach. Raporty mogą też zawierać akcje zastosowane przez użytkownika po otrzymaniu od usługi Windows Defender powiadomienia o wykryciu potencjalnie niechcianego oprogramowania. Społeczność MAPS gromadzi te informacje, aby pomóc firmie Microsoft ocenić skuteczność usługi Windows Defender w wykrywaniu i usuwaniu złośliwego i potencjalnie niechcianego oprogramowania oraz aby identyfikować nowe złośliwe oprogramowanie.

Raporty są wysyłane automatycznie do firmy Microsoft w następujących przypadkach:

- Usługa Windows Defender wykrywa oprogramowanie, które nie zostało jeszcze przeanalizowane pod kątem zagrożeń.
- Usługa Windows Defender wykrywa zmiany wykonane na komputerze przez oprogramowanie, które nie zostało jeszcze przeanalizowane pod kątem zagrożeń.
- Usługa Windows Defender podejmuje działanie względem złośliwego oprogramowania (w ramach automatycznego rozwiązywania problemów) po jego wykryciu.
- Usługa Windows Defender wykonuje zaplanowane skanowanie i automatycznie podejmuje działania względem wykrytego oprogramowania zgodnie z ustawieniami wybranymi przez użytkownika.
- Usługa Windows Defender skanuje kontrolki ActiveX w programie Internet Explorer.

Jeśli podczas konfigurowania systemu Windows członkostwo w społeczności MAPS zostanie włączone, użytkownik dołączy do społeczności na poziomie podstawowym. Raporty członka na poziomie podstawowym zawierają informacje opisane w tej sekcji. Raporty

członka na poziomie zaawansowanym są bardziej wyczerpujące i mogą zawierać informacje osobiste, na przykład ścieżki plików i częściowe zrzuty pamięci. Te raporty, wraz z raportami innych użytkowników usługi Windows Defender uczestniczących w społeczności MAPS, pomagają badaczom firmy Microsoft w szybszym wykrywaniu nowych zagrożeń. Następnie są tworzone definicje złośliwego oprogramowania, a zaktualizowane definicje są udostępniane wszystkim użytkownikom w witrynie Windows Update.

W przypadku dołączenia do społeczności MAPS usługa Windows Defender może wysyłać konkretne pliki lub zawartość sieci Web z Twojego komputera, gdy firma Microsoft podejrzewa, że dany element może być potencjalnie niechcianym oprogramowaniem. Raport jest używany do dalszych analiz. Jeśli plik z dużym prawdopodobieństwem może zawierać informacje osobiste, przed jego wysłaniem zostanie wyświetlone pytanie. Jeśli przez pewien okres usługa Windows Update nie może uzyskać zaktualizowanych sygnatur dla usługi Windows Defender, usługa Windows Defender spróbuje pobrać sygnatury za pośrednictwem społeczności MAPS z innej lokalizacji pobierania.

W celu ochrony prywatności użytkownika informacje do społeczności MAPS są wysyłane w szyfrowanej postaci za pomocą protokołu SSL.

Aby pomóc w wykrywaniu i naprawianiu pewnych rodzajów infekcji złośliwego oprogramowania, usługa Windows Defender regularnie wysyła do społeczności MAPS informacje o stanie zabezpieczeń komputera. Obejmuje to informacje o ustawieniach zabezpieczeń komputera oraz pliki dzienników opisujące sterowniki i inne oprogramowanie ładowane w czasie uruchamiania komputera. Wysyłany jest także numer identyfikujący komputer.

Używanie informacji

Raporty społeczności MAPS służą do doskonalenia oprogramowania i usług firmy Microsoft. Raporty te mogą też być używane do celów statystycznych, testowych i do generowania definicji. Społeczność MAPS nie gromadzi celowo informacji osobistych. W razie otrzymania raportu społeczności MAPS przypadkowo zawierającego informacje osobiste firma Microsoft nie używa tych informacji do ustalania tożsamości użytkownika, do kontaktowania się z nim ani do kierowania do niego reklam.

Zbierane przez społeczność MAPS informacje o stanie zabezpieczeń komputera są używane do określania, czy komputer nie został zainfekowany przez pewne rodzaje złośliwego oprogramowania. W przypadku znalezienia takiego oprogramowania firma Microsoft użyje informacji kontaktowych na koncie Microsoft użytkownika w celu skontaktowania się z nim i przekazania szczegółowych informacji o problemie i sposobie jego rozwiązania.

Wybór i kontrola

Wybranie ustawień ekspresowych podczas konfiguracji systemu Windows powoduje włączenie społeczności MAPS. Jeśli użytkownik zdecyduje się dostosować ustawienia, może kontrolować usługę MAPS przez wybranie opcji **Uzyskaj lepszą ochronę przed złośliwym oprogramowaniem przez wysyłanie informacji i plików do usługi Microsoft Active Protection Service, gdy usługa Windows Defender jest włączona** w obszarze **Udostępniaj informacje firmie Microsoft i innym usługom**. Po ukończeniu konfiguracji systemu Windows poziom członkostwa w społeczności MAPS i inne ustawienia można zmienić (na przykład wyłączyć społeczność MAPS) przy użyciu menu **Ustawienia** w usłudze Windows Defender.

W przypadku pobrania Narzędzia do usuwania złośliwego oprogramowania za pośrednictwem usługi Windows Update może ono wysyłać podobne informacje do społeczności MAPS nawet w przypadku wyłączenia usługi Windows Defender. Aby uzyskać więcej informacji, zobacz Narzędzie Windows do usuwania złośliwego oprogramowania można wyświetlić oraz zarządzać nimi.

Funkcja Historia

Opis funkcji

Funkcja Historia udostępnia listę wszystkich aplikacji na komputerze wykrytych przez usługę Windows Defender oraz akcji podjętych po wykryciu tych aplikacji.

Ponadto można wyświetlić listę aplikacji, których działanie na komputerze nie jest monitorowane przez usługę Windows Defender (elementy dozwolone). Można też wyświetlić aplikacje, których uruchamianie jest zablokowane przez usługę Windows Defender do momentu, gdy użytkownik wybierze ich usunięcie lub zezwoli na

ponowne uruchomienie (elementy poddane kwarantannie).

Informacje zbierane, przetwarzane lub przesyłane

Na komputerze użytkownika jest zapisywania lista programów wykrytych przez usługę Windows Defender, akcje podejmowane przez użytkownika i inne osoby oraz akcje podejmowane automatycznie przez usługę Windows Defender. Wszyscy użytkownicy mogą wyświetlać historię w usłudze Windows Defender, aby przejrzeć informacje o złośliwym oprogramowaniu i innych potencjalnie niechcianych programach, które próbowały się zainstalować i uruchomić na komputerze lub na których uruchomienie zezwolił inny użytkownik. Jeśli na przykład użytkownik dowiedział się o nowym zagrożeniu złośliwym oprogramowaniem, może sprawdzić w historii, czy usługa Windows Defender zapobiegła zainfekowaniu komputera przez ten program. Żadne informacje nie są wysyłane do firmy Microsoft.

Wybór i kontrola

Listy funkcji Historia mogą być usuwane przez administratora.

Góra strony

Raportowanie błędów systemu Windows

Opis funkcji

Funkcja Raportowanie błędów systemu Windows pomaga firmie Microsoft i partnerom firmy Microsoft w diagnozowaniu problemów związanych z używanym oprogramowaniem oraz ułatwiają udostępnianie rozwiązań. Nie wszystkie problemy mają rozwiązanie, ale jeśli rozwiązanie zostanie udostępnione, jest oferowane w formie procedury umożliwiającej usunięcie zgłoszonego problemu lub w postaci aktualizacji do zainstalowania. Aby zapobiec występowaniu problemów i zapewnić niezawodne działanie oprogramowania, niektóre rozwiązania są dołączane do dodatków Service Pack i przyszłych wersji oprogramowania.

Informacje zbierane, przetwarzane lub przesyłane

Raportowanie błędów systemu Windows jest obsługiwane przez wiele programów. Gdy w jednym z takich programów wystąpi błąd, może

zostać wyświetlony monit z pytaniem, czy użytkownik chce zgłosić ten błąd.

Funkcja Raportowanie błędów systemu Windows zbiera informacje pomocne w diagnozowaniu i rozwiązywaniu występujących problemów, takie jak miejsce wystąpienia problemu w oprogramowaniu lub sprzęcie, typ lub waga problemu, pliki pomocne w opisie problemu, podstawowe informacje dotyczące oprogramowania i sprzętu oraz ewentualne problemy dotyczące wydajności i zgodności oprogramowania. Jeśli system Windows służy do hostowania maszyn wirtualnych, raporty o błędach wysyłane do firmy Microsoft mogą zawierać informacje dotyczące maszyn wirtualnych.

Raportowanie błędów systemu Windows zbiera informacje o aplikacjach, sterownikach i urządzeniach, aby ułatwić firmie Microsoft badanie i udoskonalanie zgodności aplikacji oraz urządzeń. Informacje dotyczące aplikacji mogą zawierać nazwę plików wykonywalnych aplikacji. Informacje o urządzeniach i sterownikach mogą zawierać nazwy urządzeń zainstalowanych na komputerze i plików wykonywalnych skojarzonych ze sterownikami tych urządzeń. Mogą być gromadzone informacje o firmie, która opublikowała aplikację lub sterownik.

Włączenie raportowania automatycznego podczas konfiguracji systemu Windows powoduje automatyczne wysyłanie przez usługę raportowania podstawowych informacji o miejscach wystąpienia problemów. W niektórych przypadkach usługa raportowania będzie automatycznie wysyłać dodatkowe informacje pomocne w diagnozowaniu problemu, na przykład częściową migawkę pamięci komputera. Niektóre raporty o błędach mogą przypadkowo zawierać informacje osobiste. Na przykład raport zawierający migawkę pamięci komputera może zawierać imię i nazwisko użytkownika, część aktualnie używanego dokumentu lub dane przesłane ostatnio do witryny sieci Web.

Aby pomóc w diagnozowaniu niektórych typów problemów, Raportowanie błędów systemu Windows może utworzyć raport zawierający dodatkowe informacje, na przykład pliki dziennika. Przed wysłaniem raportu zawierającego dodatkowe informacje system Windows wyświetli monit o wysłanie raportu (nawet gdy włączono

raportowanie automatyczne).

Po wysłaniu raportu usługa raportowania może wyświetlić monit o podanie dalszych informacji na temat wykrytego błędu. Jeśli użytkownik poda w tych informacjach swój numer telefonu lub adres e-mail, raport dotyczący błędów nie będzie już anonimowy. Firma Microsoft może skontaktować się z użytkownikiem w celu uzyskania dodatkowych informacji, które mogą pomóc w rozwiązaniu zgłoszonego problemu.

Usługa raportowania błędów systemu Windows losowo generuje numer nazywany unikatowym identyfikatorem globalnym (GUID), który jest wysyłany do firmy Microsoft w każdym raporcie o błędach. Identyfikator GUID pozwala stwierdzić, jakie dane zostały wysłane z określonego komputera w danym okresie. Identyfikator GUID nie zawiera żadnych informacji osobistych.

W celu ochrony prywatności użytkownika informacje są wysyłane w szyfrowanej postaci za pomocą protokołu SSL.

Używanie informacji

Informacje dotyczące błędów i problemów zgłoszone przez użytkowników systemu Windows są używane przez firmę Microsoft do udoskonalania produktów i usług firmy Microsoft, a także oprogramowania i sprzętu innych producentów, które są przeznaczone do użytku z tymi produktami i usługami. Na podstawie identyfikatorów GUID firma Microsoft określa zakres otrzymywanych opinii i przydziela im priorytety. Na przykład dzięki identyfikatorom GUID firma Microsoft może odróżnić jednego klienta, u którego dany problem wystąpił sto razy, od setki klientów, u których dany problem wystąpił tylko raz.

Odpowiednie części gromadzonych informacji mogą być udostępniane pracownikom, kontrahentom, dostawcom i partnerom firmy Microsoft, ale mogą oni używać tych informacji tylko w celu naprawiania lub doskonalenia produktów i usług firmy Microsoft lub oprogramowania albo sprzętu innych firm przeznaczonego do użytku z produktami i usługami firmy Microsoft. Jeśli raport o błędach zawiera informacje osobiste, nie będą one używane przez firmę Microsoft do ustalania tożsamości użytkownika, do kontaktowania się z nim ani do kierowania do niego reklam. Jednak jeśli użytkownik zdecyduje się na podanie informacji kontaktowych, tak jak to opisano powyżej, możemy użyć

tych danych do skontaktowania się z nim.

Wybór i kontrola

Wybranie ustawień ekspresowych podczas konfiguracji systemu Windows powoduje wysyłanie przez usługę raportowania błędów systemu Windows raportów podstawowych w celu automatycznego sprawdzania dostępności rozwiązań problemów w trybie online. Jeśli użytkownik chce dostosować ustawienia, może kontrolować Raportowanie błędów systemu Windows przez wybranie opcji **Użyj funkcji raportowania błędów systemu Windows do wyszukiwania rozwiązań problemów** w obszarze **Wyszukiwanie rozwiązań problemów w trybie online**. Po ukończeniu konfiguracji systemu Windows można zmienić to ustawienie, korzystając z Centrum akcji w Panelu sterowania.

Aby uzyskać więcej informacji, należy zapoznać się z zasadami zachowania poufności informacji dotyczącymi usługi raportowania błędów firmy Microsoftmożna wyświetlić oraz zarządzać nimi.

Góra strony

Kojarzenie plików systemu Windows

Opis funkcji

Usługa kojarzenia plików systemu Windows umożliwia użytkownikom kojarzenie typów plików z określonymi aplikacjami. Jeśli użytkownik spróbuje otworzyć typ pliku, który nie ma skojarzonej aplikacji, system Windows pozwoli mu zdecydować, czy chce za pomocą usługi kojarzenia plików systemu Windows znaleźć aplikację dla pliku, co może wymagać między innymi przeszukania Sklepu Windows pod kątem zgodnej aplikacji. Zostaną wyświetlone aplikacje kojarzone zwykle z danym rozszerzeniem nazwy pliku.

Informacje zbierane, przetwarzane lub przesyłane

Jeśli użytkownik zdecydował się korzystać z usługi kojarzenia plików systemu Windows, do firmy Microsoft jest wysyłane rozszerzenie nazwy pliku (na przykład docx lub pdf) i język wyświetlania komputera. Pozostała część nazwy pliku nie jest wysyłana do firmy Microsoft. Kiedy plik zostaje skojarzony z określoną aplikacją, wysyłany jest unikatowy identyfikator aplikacji umożliwiający identyfikację aplikacji

domyślnej dla poszczególnych typów plików.

Używanie informacji

Jeśli użytkownik przesyła rozszerzenie nazwy pliku, usługa zwraca listę aplikacji, które firma Microsoft uznała za odpowiednie do otwierania plików z takim rozszerzeniem. Jeśli użytkownik nie zdecyduje się na pobranie i zainstalowanie aplikacji, skojarzenia typu pliku pozostają niezmienione.

Wybór i kontrola

Podczas próby otwarcia typu pliku, który nie ma skojarzonej aplikacji, można zdecydować, czy ma być używana usługa kojarzenia plików systemu Windows. Jeśli usługa nie jest używana, do firmy Microsoft nie są wysyłane żadne informacje o skojarzeniach plików.

Góra strony

Pomoc systemu Windows

Pomoc i obsługa techniczna online systemu Windows

Opis funkcji

Jeśli Pomoc i obsługa techniczna online systemu Windows jest włączona, po nawiązaniu połączenia z Internetem można korzystać z najnowszej dostępnej zawartości z zakresu pomocy i obsługi technicznej.

Informacje zbierane, przetwarzane lub przesyłane

W przypadku używania Pomocy i obsługi technicznej online systemu Windows do firmy Microsoft są wysyłane zapytania dotyczące pomocy oraz żądania dotyczące zawartości pomocy spowodowane kliknięciem linku. System Windows wysyła określone informacje o konfiguracji komputera, aby pomóc w znalezieniu jak najbardziej trafnej zawartości pomocy. Pomoc i obsługa techniczna online systemu Windows korzysta też ze standardowych technologii sieci Web, takich jak pliki cookie.

Używanie informacji

Firma Microsoft korzysta z tych informacji w celu wysyłania tematów Pomocy w odpowiedzi na zapytania funkcji wyszukiwania, zwracania

jak najdokładniejszych wyników oraz opracowywania nowej i poprawiania istniejącej zawartości. Informacje dotyczące konfiguracji komputera umożliwiają nam wyświetlanie odpowiedniej zawartości pomocy dla danej konfiguracji. Pliki cookie i inne technologie sieci Web ułatwiają przechodzenie do zawartości pomocy i pozwalają nam lepiej poznać sposoby korzystania z Pomocy systemu Windows w trybie online przez użytkowników.

Wybór i kontrola

Pomoc i obsługa techniczna online jest domyślnie włączona. Aby zmienić to ustawienie, należy nacisnąć lub kliknąć ikonę **Ustawienia** u góry okna Pomoc i obsługa techniczna, a następnie zaznaczyć lub wyczyścić pole wyboru **Uzyskaj Pomoc w trybie online**. Aby wyczyścić pliki cookie używane przez Pomoc systemu Windows, należy otworzyć aplet Opcje internetowe w Panelu sterowania, kliknąć lub nacisnąć przycisk **Usuń** w obszarze **Historia przeglądania**, zaznaczyć pole wyboru **Pliki cookie i dane witryn sieci Web**, a następnie kliknąć lub nacisnąć przycisk **Usuń**. Jeśli użytkownik zdecydował, że wszystkie pliki cookie mają być blokowane (w sekcji Prywatność apletu Opcje internetowe), Pomoc systemu Windows nie ustawi żadnych plików cookie.

Program udoskonalania Pomocy

Opis funkcji

Program udoskonalania Pomocy ułatwia firmie Microsoft identyfikowanie tendencji w sposobie korzystania z Pomocy i obsługi technicznej systemu Windows przez klientów w celu poprawienia dokładności wyników wyszukiwania oraz udostępnianej zawartości.

Informacje zbierane, przetwarzane lub przesyłane

W ramach Programu udoskonalania Pomocy do firmy Microsoft są wysyłane informacje o wersji systemu Windows uruchomionej na komputerze oraz o sposobie korzystania z Pomocy i obsługi technicznej systemu Windows, w tym także dotyczące zapytań wprowadzanych podczas przeszukiwania Pomocy i obsługi technicznej systemu Windows oraz ocen i opinii dotyczących przedstawionych tematów Pomocy. Do firmy Microsoft są wysyłane informacje dotyczące przeszukiwania i przeglądania tematów Pomocy, a także ocen i opinii

wystawionych im przez użytkownika.

W ramach Programu udoskonalania Pomocy losowo generowany jest numer nazywany unikatowym identyfikatorem globalnym (GUID), który jest wysyłany w każdym raporcie do firmy Microsoft. Identyfikator GUID pozwala stwierdzić, jakie dane zostały wysłane z określonego komputera w danym okresie. Identyfikator GUID nie zawiera żadnych informacji osobistych. Ten identyfikator GUID jest inny niż identyfikatory GUID używane w ramach usługi raportowania błędów systemu Windows i Programu poprawy jakości obsługi klienta systemu Windows.

Używanie informacji

Zebrane dane są używane do identyfikowania tendencji i wzorców użytkowania, co z kolei pozwala firmie Microsoft na poprawienie jakości udostępnianych informacji i dokładności wyników wyszukiwania. Na podstawie identyfikatorów GUID firma Microsoft określa zakres otrzymywanych problemów i przydziela im priorytety. Na przykład dzięki identyfikatorom GUID firma Microsoft może odróżnić jednego klienta, u którego dany problem wystąpił sto razy, od setki klientów, u których dany problem wystąpił tylko raz.

W ramach Programu udoskonalania Pomocy nie są zbierane informacje, które mogłyby posłużyć do identyfikacji użytkownika. W przypadku wpisania tego rodzaju informacji w polach wyszukiwania lub oceny zostaną one wysłane, ale firma Microsoft nie będzie ich używała do ustalania tożsamości użytkownika, kontaktowania się z nim ani do kierowania do niego reklam.

Wybór i kontrola

Wybranie ustawień ekspresowych podczas konfiguracji systemu Windows jest równoznaczne z przystąpieniem do Programu udoskonalania Pomocy. Jeśli użytkownik zdecyduje się dostosować ustawienia, może kontrolować Program udoskonalania Pomocy przez wybranie opcji **Wysyłaj do firmy Microsoft informacje dotyczące sposobu używania Pomocy w ramach Programu udoskonalania Pomocy** w obszarze **Pomóż w ulepszaniu produktów i usług firmy Microsoft**. Po ukończeniu konfiguracji systemu Windows można zmienić to ustawienie, korzystając z okna Pomoc i obsługa techniczna systemu Windows.

Góra strony

Pomoc zdalna

Opis funkcji

Korzystając z Pomocy zdalnej, użytkownik może poprosić inną osobę o połączenie się z jego komputerem i udzielenie pomocy dotyczącej problemu z komputerem bez względu na dzielącą odległość. Po nawiązaniu połączenia dana osoba ma wgląd w komputer użytkownika. Za zgodą użytkownika może ona sterować komputerem użytkownika za pomocą swojej myszy oraz klawiatury i wskazywać sposoby rozwiązania problemu.

Informacje zbierane, przetwarzane lub przesyłane

Funkcja Pomocy zdalna tworzy szyfrowane połączenie między dwoma komputerami w Internecie lub w sieci lokalnej. Gdy inna osoba nawiązuje połączenie z komputerem użytkownika przy użyciu Pomocy zdalnej, może zobaczyć jego pulpit, otwarte dokumenty oraz wszystkie widoczne informacje osobiste. Ponadto, jeśli użytkownik zezwoli osobie udzielającej pomocy na sterowanie komputerem za pomocą jej myszy i klawiatury, może ona wykonywać takie czynności, jak usuwanie plików czy zmienianie ustawień. Po nawiązaniu połączenia w ramach Pomocy zdalnej następuje wymiana informacji, takich jak nazwa użytkownika, nazwa komputera i awatar. Zapis wszystkich połączeń w ramach Pomocy zdalnej znajduje się w pliku dziennika sesji.

Używanie informacji

Informacje służą do nawiązania szyfrowanego połączenia i zapewnienia innej osobie dostępu do pulpitu użytkownika. Żadne informacje nie są wysyłane do firmy Microsoft.

Wybór i kontrola

Przed zezwoleniem innej osobie na połączenie z komputerem należy zamknąć wszystkie otwarte aplikacje lub dokumenty, których nie powinna ona oglądać. Jeśli w dowolnym momencie użytkownik uzna, że nie chce, aby ta osoba oglądała określoną zawartość lub wykonywała dane czynności na jego komputerze, może nacisnąć klawisz Esc, aby zakończyć sesję. Rejestrowanie sesji i wymianę

informacji kontaktowych można wyłączyć, czyszcząc pola wyboru tych opcji w ustawieniach Pomocy zdalnej.

Góra strony

Windows Search

Opis funkcji

Usługa Windows Search umożliwia przeszukiwanie zawartości danego urządzenia i Internetu z jednego miejsca. Aby dostarczać lepsze wyniki, usługa Windows Search może korzystać z usługi Bing i Platformy lokalizacji systemu Windows. Należy pamiętać, że na urządzeniu dostępne są osobne funkcje wyszukiwania udostępniane przez firmę Microsoft, na przykład wyszukiwanie w Sklepie Windows, program Internet Explorer i inne produkty firmy Microsoft.

Informacje zbierane, przetwarzane lub przesyłane

Jeśli użytkownik chce uzyskiwać wyniki wyszukiwania z sieci Web, system Windows będzie wysyłał ciągi wpisane w usłudze Windows Search do firmy Microsoft. Aby ulepszać zwracane wyniki wyszukiwania, usługa Windows Search wysyła też do firmy Microsoft informacje o charakterze interakcji z tą funkcją. Usługa Windows Search wysyła również identyfikator w celu dostarczania spersonalizowanych wyników wyszukiwania w oparciu o interakcje z usługą Bing i innymi produktami i usługami firmy Microsoft. W przypadku zalogowania się w systemie Windows za pomocą konta Microsoft identyfikator będzie skojarzony z kontem Microsoft użytkownika. Użytkownik może zdecydować, że nie chce otrzymywać spersonalizowanych wyników z usługi Windows Search; w takim przypadku identyfikator nie będzie wysyłany.

Jeśli użytkownik wyrazi zgodę na dostęp usługi Windows Search do jego lokalizacji, fizyczna lokalizacja urządzenia zwrócona przez Platformę lokalizacji systemu Windows zostanie wysłana do firmy Microsoft jako część każdego żądania wyszukiwania. Alternatywnie może zostać podjęta próba określenia przybliżonej lokalizacji fizycznej w oparciu o adres IP użytkownika.

W przypadku użycia usługi Windows Search do wyszukiwania w aplikacji wyszukiwane terminy są przekazywane do aplikacji.

Używanie informacji

W przypadku użycia usługi Windows Search do uzyskiwania wyników wyszukiwania z sieci Web podany przez użytkownika termin wyszukiwania oraz historia wyszukiwania (lokalna i online), informacje skojarzone z kontem Microsoft oraz lokalizacja urządzenia zostaną użyte do zwrócenia odpowiednich sugestii wyszukiwania, spersonalizowanych wyników wyszukiwania oraz spersonalizowanego środowiska w innych produktach i usługach Microsoft. Aby dowiedzieć się więcej o sposobie użycia danych, należy zapoznać się z zasadami zachowania poufności informacji usługi Bingmożna wyświetlić oraz zarządzać nimi.

Jeśli użytkownik za pomocą usługi Windows Search przeszukuje aplikację strony trzeciej, używanie zbieranych informacji podlega zasadom zachowania poufności informacji danej firmy. Jeśli użytkownik przeszukuje aplikację firmy Microsoft, odpowiednie informacje można znaleźć w zasadach zachowania poufności informacji danej aplikacji.

Wybór i kontrola

Wybranie ustawień ekspresowych podczas konfigurowania systemu Windows oznacza pozwolenie usłudze Windows Search na pobieranie sugestii wyszukiwania i wyników z sieci Web oraz pozwolenie firmie Microsoft na użycie danych z usługi Windows Search (w tym danych lokalizacji) do personalizowania środowiska usługi Windows Search oraz innych produktów Microsoft. Jeśli użytkownik zdecyduje się dostosować ustawienia, może zmienić te ustawienia usługi Windows Search. Po ukończeniu konfiguracji systemu Windows można zmienić to ustawienie, korzystając z opcji **Wyszukiwanie** w ustawieniach komputera.

Korzystając z pozycji **Wyszukiwanie** w obszarze **Wyszukiwanie i aplikacje** w ustawieniach komputera, można również wyczyścić lokalną historię wyszukiwania i część historii wyszukiwania w usłudze Bing używanej do personalizowania wyszukiwania w ramach usługi Windows Search. Wyczyszczenie historii wyszukiwania to sygnał dla firmy Microsoft, aby nie personalizowała sugestii wyszukiwania ani kolejności wyświetlania wyników wyszukiwania za pomocą wcześniej zgromadzonej historii wyszukiwania. Nie powoduje jednak

wyczyszczenia informacji reklamowych i innych danych z zakresu personalizacji (w tym informacji pochodzących z historii wyszukiwania) ani usunięcia informacji zagregowanych używanych przez firmę Microsoft do poprawienia wyników wyszukiwania i innych środowisk udostępnionych przez firmę Microsoft. Te informacje są zachowywane po usunięciu z nich informacji osobistych zgodnie z opisem w zasadami zachowania poufności informacji usługi Bing. Informacjami reklamowymi firmy Microsoft oraz innymi danymi umożliwiającymi personalizację można zarządzać w trybie online.

Góra strony

Instalator systemu Windows

W tej sekcji opisano funkcje dostępne w ramach procesu instalowania systemu Windows.

Aktualizacja dynamiczna

Opis funkcji

Aktualizacja dynamiczna umożliwia systemowi Windows jednorazowe sprawdzenie w witrynie Windows Update dostępności najnowszych aktualizacji dla danego komputera podczas instalacji systemu Windows. Jeśli aktualizacje zostaną odnalezione, funkcja ta pobiera je i instaluje automatycznie, zapewniając aktualność oprogramowania na komputerze już od pierwszego zalogowania lub użycia.

Informacje zbierane, przetwarzane lub przesyłane

Aby zainstalować zgodne sterowniki, funkcja Aktualizacja dynamiczna wysyła do firmy Microsoft informacje na temat sprzętu zainstalowanego w komputerze. Funkcja Aktualizacja dynamiczna może pobierać na komputer aktualizacje następujących typów:

- **Aktualizacje instalacjimożna wyświetlić oraz zarządzać nimi.** Ważne aktualizacje oprogramowania plików instalacyjnych, które zapewniają pomyślną instalację.
- **Aktualizacje sterowników wewnętrznychmożna wyświetlić oraz zarządzać nimi.** Ważne aktualizacje sterowników dla instalowanej wersji systemu Windows.

Oprócz tego w przypadku zainstalowania systemu Windows ze Sklepu

Windows funkcja Aktualizacja dynamiczna pobierze i zainstaluje najnowsze aktualizacje systemu Windows oraz sterowniki wymagane na komputerze.

Używanie informacji

Funkcja Aktualizacja dynamiczna przesyła do firmy Microsoft informacje o sprzęcie zainstalowanym w komputerze w celu określenia odpowiednich sterowników dla danego systemu.

Wybór i kontrola

W przypadku instalowania systemu Windows ze Sklepu Windows instalator automatycznie pobierze i zainstaluje aktualizacje. W przypadku instalowania systemu Windows z nośnika fizycznego zostanie wyświetlony monit z pytaniem, czy użytkownik chce przejść do trybu online, aby zainstalować aktualizacje.

Program poprawy jakości instalacji

Opis funkcji

Ta funkcja wysyła do firmy Microsoft jeden raport zawierający podstawowe informacje o komputerze oraz sposobie zainstalowania systemu Windows. Firma Microsoft używa tych informacji w celu usprawnienia instalacji oprogramowania i opracowania rozwiązań typowych problemów instalacyjnych.

Informacje zbierane, przetwarzane lub przesyłane

Zazwyczaj raport zawiera informacje na temat instalacji, takie jak data instalacji, czas trwania poszczególnych etapów instalacji, rodzaj instalacji (uaktualnienie czy instalacja od nowa), szczegółowe informacje o wersji, język systemu operacyjnego, typ nośnika, konfiguracja komputera oraz stan instalacji (powodzenie lub niepowodzenie) — wraz ze wszystkimi kodami błędów.

Jeśli użytkownik zdecyduje się na udział w Programie poprawy jakości instalacji, raport zostanie wysłany do firmy Microsoft, kiedy będzie dostępne połączenie z Internetem. Program poprawy jakości instalacji losowo generuje numer nazywany unikatowym identyfikatorem globalnym (GUID), który jest wysyłany w raporcie do firmy Microsoft. Identyfikator GUID pozwala stwierdzić, jakie dane zostały wysłane z określonego komputera w danym okresie. Identyfikator GUID nie

zawiera żadnych danych osobowych ani nie służy do identyfikacji użytkownika.

Używanie informacji

Firma Microsoft i jej partnerzy używają tego raportu do poprawy jakości jej produktów i usług. Identyfikator GUID służy do powiązania tych danych z danymi zebranymi w Programie poprawy jakości obsługi klienta systemu Windows, do którego można przystąpić w przypadku korzystania z systemu Windows.

Wybór i kontrola

Użytkownik może przystąpić do tego programu podczas instalowania systemu Windows, wybierając pozycję **Chcę pomóc w ulepszeniu instalacji systemu Windows** można wyświetlić oraz zarządzać nimi.

Aby uzyskać więcej informacji, zobacz sekcję Program poprawy jakości obsługi klienta systemu Windows.

Doradca zgodności instalacji

Opis funkcji

Podczas instalowania systemu Windows instalator ułatwia określenie, czy dany komputer można uaktualnić do systemu Windows 8.1, oraz udostępnia informacje na temat zgodności posiadanych programów i urządzeń.

Informacje zbierane, przetwarzane lub przesyłane

Po określeniu zgodności gromadzone są określone informacje na temat możliwości uaktualnienia, dotyczące na przykład wydajności sprzętu, urządzeń podłączonych do komputera oraz programów zainstalowanych na komputerze. Czasami zdarza się, że informacje dotyczące wydawcy programu zawierają informacje takie jak imię i nazwisko wydawcy lub jego adres e-mail.

Używanie informacji

Zbierane informacje posłużą do ustalenia właściwych dla komputera sterowników i do określenia zgodności komputera, programów i urządzeń z systemem Windows 8.1. Firma Microsoft używa ich też do udoskonalania swoich produktów i usług. Firma Microsoft nie używa tych informacji do ustalania tożsamości użytkownika, kontaktowania

się z nim ani do kierowania do niego reklam.

Wybór i kontrola

W przypadku instalowania systemu Windows ze Sklepu Windows lub z nośnika fizycznego w ramach istniejącej instalacji systemu Windows informacje opisane w tej sekcji zostaną wysłane do firmy Microsoft. Jeśli użytkownik wykonuje rozruch z fizycznego nośnika instalacyjnego w celu zainstalowania systemu Windows, instalator nie sprawdza informacji dotyczących zgodności w trybie online.

Góra strony

Udostępnianie w systemie Windows

Opis funkcji

Usługa udostępniania w systemie Windows umożliwia udostępnianie zawartości między aplikacjami ze Sklepu Windows obsługującymi udostępnianie. Pozwala także udostępniać zawartość znajomym.

Informacje zbierane, przetwarzane lub przesyłane

Podczas udostępniania aplikacja źródłowa przekazuje zawartość do aplikacji docelowej tylko wtedy, gdy użytkownik wybrał odbiorcę lub aplikację docelową w okienku udostępniania. Jeśli aplikacja źródłowa nie obsługuje udostępniania, można udostępnić obraz bieżącej zawartości ekranu. Aby ułatwić dostęp do aplikacji docelowych i osób, którym użytkownik najczęściej udostępnia zawartość, są one umieszczone na liście w okienku udostępniania. Żadne informacje nie są wysyłane do firmy Microsoft.

Używanie informacji

Informacje dotyczące częstotliwości udostępniania zawartości aplikacjom docelowym i odbiorcom umożliwiają sortowanie listy w okienku udostępniania według popularności. Jeśli użytkownik udostępnia informacje aplikacji strony trzeciej, używanie zbieranych informacji podlega zasadom zachowania poufności informacji danej firmy. Jeśli użytkownik udostępnia zawartość w aplikacji firmy Microsoft, odpowiednie informacje można znaleźć w zasadach zachowania poufności informacji danej aplikacji.

Wybór i kontrola

Domyślnie system Windows przechowuje informacje o korzystaniu przez użytkownika z funkcji udostępniania w systemie Windows. Korzystając z pozycji **Udostępnianie** w obszarze **Wyszukiwanie i aplikacje** w ustawieniach komputera.

Góra strony

Windows SmartScreen

Opis funkcji

Filtr Windows SmartScreen pomaga dbać o bezpieczeństwo komputera przez sprawdzanie pobieranych plików i zawartości sieci Web w aplikacjach w celu ochrony przed złośliwym oprogramowaniem i potencjalnie niebezpieczną zawartością sieci Web. Zanim nieznany lub potencjalnie niebezpieczny pobrany plik zostanie otwarty, system Windows wyświetli ostrzeżenie. Jeśli filtr SmartScreen wykryje potencjalnie niebezpieczną zawartość sieci Web w aplikacji, system Windows zamiast zawartości wyświetli ostrzeżenie.

Informacje zbierane, przetwarzane lub przesyłane

Jeśli użytkownik zdecyduje się na korzystanie z filtru Windows SmartScreen do sprawdzania pobranych plików, system Windows wyśle informacje do usługi online SmartScreen. Wysyłane dane mogą zawierać nazwę pliku, identyfikator („skrót”) i informacje o certyfikacie cyfrowym wraz ze standardowymi informacjami o komputerze i numerze wersji filtru Windows SmartScreen. W celu ochrony prywatności użytkownika informacje wysyłane do firmy Microsoft są szyfrowane za pomocą protokołu SSL.

Jeśli filtr Windows SmartScreen jest używany do blokowania potencjalnie niebezpiecznej zawartości w aplikacjach, system Windows wyśle do usługi online SmartScreen informacje obejmujące adresy i typy zawartości, do których niektóre aplikacje ze Sklepu Windows uzyskują dostęp w czasie ich używania. W odpowiedzi usługa online zwróci do komputera informacje o tym, czy zawartość była zgłaszana do firmy Microsoft jako niebezpieczna lub podejrzana. Raporty wysyłane do firmy Microsoft obejmują informacje, takie jak nazwa lub identyfikator aplikacji i pełne adresy zawartości w sieci Web, do której aplikacja uzyskuje dostęp.

W celu ochrony prywatności użytkownika informacje wysyłane do firmy Microsoft są szyfrowane. W adresie wysyłanym do firmy Microsoft mogą znaleźć się informacje skojarzone z witryną, do której dostęp następuje z poziomu aplikacji (na przykład terminy wyszukiwania). Jeśli na przykład użytkownik sprawdził tłumaczenie określonego wyrazu w aplikacji słownika, sprawdzany wyraz może zostać wysyłany do firmy Microsoft jako część pełnego adresu użytego przez tę aplikację. Firma Microsoft filtruje takie adresy w celu usunięcia z nich danych osobowych, jeśli jest to możliwe.

System Windows generuje numer nazywany unikatowym identyfikatorem globalnym (GUID), który jest wysyłany w każdym raporcie do firmy Microsoft. Identyfikator GUID pozwala stwierdzić, jakie dane zostały wysłane z określonego komputera w danym okresie. Identyfikator GUID nie zawiera żadnych informacji osobistych.

Używanie informacji

Dzięki opisanym powyżej informacjom firma Microsoft może informować użytkowników o potencjalnie niebezpiecznych pobieranych plikach i zawartości w aplikacjach. Na przykład jeśli filtr SmartScreen wykryje potencjalne zagrożenie w aplikacji obsługującej filtr SmartScreen, system Windows zamiast zawartości wyświetli ostrzeżenie. Firma Microsoft używa też tych informacji do udoskonalania filtru SmartScreen oraz innych swoich produktów i usług. Firma Microsoft nie używa zebranych informacji do kierowania reklam do użytkownika.

Wybór i kontrola

Wybranie ustawień ekspresowych podczas konfiguracji systemu Windows powoduje włączenie filtru Windows SmartScreen. Jeśli użytkownik zdecyduje się dostosować ustawienia, może kontrolować filtr Windows SmartScreen przez wybranie opcji **Używaj usług online SmartScreen, aby zapewnić ochronę przed złośliwą zawartością w witrynach ładowanych przez aplikacje ze Sklepu Windows i program Internet Explorer oraz pobraną złośliwą zawartość** w obszarze **Pomóż chronić swój komputer i swoją prywatność**. Po ukończeniu konfiguracji systemu Windows można zmienić to ustawienie, korzystając z Centrum akcji w Panelu sterowania. Aby uzyskać informacje o filtrze SmartScreen programu

Internet Explorer, zobacz sekcję Filtr SmartScreen w zasadach zachowania poufności informacji programu Internet Explorermożna wyświetlić oraz zarządzać nimi.

Góra strony

Rozpoznawanie mowy w systemie Windows

Opis funkcji

Funkcja rozpoznawania mowy w systemie Windows umożliwia rozpoznawanie mowy w systemie Windows i w każdej aplikacji, w której jest używana. Dokładność rozpoznawania mowy w systemie Windows jest zwiększana dzięki temu, że funkcja uczy się sposobu używania języka przez użytkownika, w tym najczęściej używanych dźwięków i słów.

Informacje zbierane, przetwarzane lub przesyłane

Funkcja rozpoznawania mowy w systemie Windows przechowuje na komputerze użytkownika listę słów i ich wymowy. Słowa i ich wymowę można dodawać do tej listy, korzystając ze słownika mowy, a także dyktując i korygując słowa za pomocą funkcji rozpoznawania mowy w systemie Windows.

Jeśli w ramach rozpoznawania mowy w systemie Windows jest włączona funkcja przeglądania dokumentów, tekst z dokumentów programu Microsoft Office Word (z rozszerzeniem nazwy pliku doc lub docx) i wiadomości e-mail (z folderów poczty e-mail innych niż Elementy usunięte i Wiadomości-śmieci) na komputerze i wszelkich podłączonych udziałach plików uwzględnionych w lokalizacjach indeksu wyszukiwania w systemie Windows jest gromadzony i przechowywany w postaci fragmentów zawierających jeden, dwa lub trzy słowa. Fragmenty jednowyrazowe zawierają tylko słowa dodane do słowników niestandardowych, a fragmenty zawierające dwa lub trzy słowa to tylko słowa ze słowników standardowych

Wszystkie zebrane informacje są przechowywane w osobistym profilu mowy użytkownika na jego komputerze. Profile mowy są przechowywane dla poszczególnych użytkowników. Każdy użytkownik ma dostęp tylko do swojego profilu mowy. Tylko administratorzy mają dostęp do wszystkich profilów na komputerze. Informacje dotyczące

profilu nie są wysyłane do firmy Microsoft, jeśli użytkownik nie zgodzi się na to po wyświetleniu odpowiedniego monitu przez funkcję rozpoznawania mowy w systemie Windows. Przed wysłaniem możne przejrzeć te dane. Jeśli użytkownik zdecyduje się wysłać te informacje, wysyłane są także dane adaptacji akustycznej użyte w celu dostosowania charakterystyki dźwięku.

Jeśli użytkownik ukończy samouczek, funkcja rozpoznawania mowy w systemie Windows wyświetli monit z pytaniem, czy informacje o profilu mowy mają zostać wysłane do firmy Microsoft. Przed wysłaniem możne przejrzeć te informacje. Te informacje mogą zawierać nagrania głosu użytkownika wykonane podczas korzystania z samouczka, a także inne informacje z osobistego profilu mowy.

Używanie informacji

Funkcja rozpoznawania mowy w systemie Windows używa słów z profilu mowy do konwertowania mowy na tekst. Firma Microsoft korzysta z informacji z osobistego profilu mowy w celu udoskonalania swoich produktów i usług. Firma Microsoft nie używa tych informacji do ustalania tożsamości użytkownika, kontaktowania się z nim ani do kierowania do niego reklam.

Wybór i kontrola

Użytkownik może zdecydować, czy chce uruchomić rozpoznawanie mowy w systemie Windows. Jeśli funkcja rozpoznawania mowy w systemie Windows jest uruchomiona, funkcja przeglądu dokumentów zostaje domyślnie włączona. Ustawienia przeglądu dokumentów można zmienić po pierwszym uruchomieniu funkcji rozpoznawania mowy w systemie Windows. Otwierając aplet Rozpoznawanie mowy w Panelu sterowania i klikając pozycję **Zaawansowane opcje mowy**, można zmienić ustawienia przeglądu dokumentów lub usunąć osobiste profile mowy (i większość informacji dotyczących przeglądu dokumentów). Za pomocą opcji zmiany istniejących słów w słowniku mowy, można usuwać słowa dodane do profilu mowy. Jednak usunięcie osobistego profilu mowy nie spowoduje usunięcia słów dodanych za pomocą słownika mowy.

Lokalizacje, z których funkcja przeglądu dokumentów zbiera fragmenty tekstu, można określić, modyfikując lokalizacje w indeksie wyszukiwania systemu Windows. Aby wyświetlić lub zmodyfikować

lokalizacje uwzględnione w indeksie wyszukiwania systemu Windows, należy otworzyć aplet Opcje indeksowania w Panelu sterowania.

Na zakończenie sesji z samouczkiem użytkownik może zdecydować, czy chce wysłać do firmy Microsoft informacje z samouczka i inne dane dotyczące profilu. Informacje można wysłać także po uruchomieniu funkcji rozpoznawania mowy w systemie Windows. W tym celu wystarczy kliknąć prawym przyciskiem myszy pozycję **Mikrofon**, a następnie kliknąć polecenie **Pomóż w ulepszaniu rozpoznawania mowy**. W każdej z tych sytuacji przed wysłaniem danych można je przejrzeć, a także zrezygnować z ich wysyłania.

Góra strony

Sklep Windows

Sklep Windows umożliwia znajdowanie i instalowanie aplikacji dla danego komputera, a także zarządzanie nimi. W poniższych sekcjach opisano, jaki wpływ mogą mieć funkcje Sklepu oraz aplikacje nabyte w Sklepie na prywatność użytkownika i w jaki sposób można to kontrolować.

Sklep — aplikacje i usługa

Opis funkcji

Sklep umożliwia znajdowanie i instalowanie aplikacji dla danego komputera. Pozawala także śledzić zainstalowane aplikacje ze Sklepu, dzięki czemu można pobierać aktualizacje i instalować aplikacje na kilku komputerach.

Informacje zbierane, przetwarzane lub przesyłane

Aby znaleźć i zainstalować aplikacje, trzeba się zalogować w Sklepie za pomocą konta Microsoft. Dzięki temu Sklep ma dostęp do informacji z profilu konta Microsoft, takich jak imię i nazwisko, adres e-mail i awatar. Sklep zbiera i kojarzy z kontem użytkownika w Sklepie następujące informacje dodatkowe:

- Płatności na rzecz Sklepu. Informacje o kupionych produktach, zapłacone kwoty i sposób płatności za kupowane aplikacje lub za zakupy w aplikacji przy użyciu konta w Sklepie.

- Zainstalowane aplikacje. Lista zainstalowanych aplikacji ze

Sklepu, zasady licencjonowania poszczególnych aplikacji (licencja stała lub próbna na określony czas) oraz lista zakupów dokonanych w poszczególnych aplikacjach za pomocą konta w Sklepie. Oprócz przechowywania tych informacji w trybie online na koncie użytkownika w Sklepie, informacje dotyczące licencjonowania poszczególnych zainstalowanych aplikacji są także przechowywane na komputerze użytkownika. Te informacje umożliwiają zidentyfikowanie użytkownika jako właściciela licencji.

- Komputery, na których zainstalowano aplikacje. Marka, model i nazwa każdego komputera, na którym zainstalowano aplikacje a także numer identyfikujący komputer w sposób unikatowy. Ten numer jest generowany na podstawie konfiguracji sprzętu komputera i nie zawiera żadnych informacji o użytkowniku.

- Oceny, recenzje i raporty o problemach. Po zainstalowaniu aplikacji można napisać jej recenzję lub ocenić aplikację w Sklepie. Z ocenami jest skojarzone konto Microsoft oceniającego użytkownika. Razem z recenzją napisaną przez użytkownika jest publikowana jego nazwa oraz awatar z konta Microsoft.

- Preferencje dotyczące Sklepu. Ustawione przez użytkownika preferencje dotyczące wyświetlania aplikacji w Sklepie (na przykład wyświetlanie tylko tych aplikacji, które są dostępne w języku ojczystym użytkownika).

W ustawieniach konta w Sklepie można też zapisać informacje dotyczące płatności, takie jak numer karty kredytowej. Ze względów bezpieczeństwa te dane są przesyłane za pośrednictwem połączenia SSL, a numer karty kredytowej jest przechowywany w postaci zaszyfrowanej (z wyjątkiem czterech ostatnich cyfr).

Usługa Sklepu zbiera określone informacje o kopii systemu Windows użytkownika, aby określić, czy produkt został kupiony w punkcie sprzedaży detalicznej, jest kopią ewaluacyjną, podlega programowi licencjonowania zbiorowego, czy też został preinstalowany przez producenta komputera. Kiedy użytkownik łączy się po raz pierwszy ze Sklepem, lista wszystkich aplikacji preinstalowanych na komputerze jest wysyłana do Sklepu i następuje skojarzenie licencji tych aplikacji z kontem użytkownika w Sklepie.

Kiedy użytkownik przegląda zawartość Sklepu i korzysta z jego aplikacji, firma Microsoft zbiera określone informacje pomagające w poznaniu tendencji i wzorców użytkowania — podobnie jak witryny sieci Web analizują metody przeglądania danych przez osoby, które je odwiedzają.

Używanie informacji

Firma Microsoft używa informacji kontaktowych, aby wysyłać użytkownikowi wiadomości e-mail niezbędne do zapewnienia obsługi związanej z korzystaniem ze Sklepu (na przykład w celu wysłania rachunku za kupione aplikacje). Informacje dotyczące płatności zapewniają obsługę płatności użytkownika za zakupy. W przypadku zapisania tych informacji nie trzeba ich ponownie podawać przy każdym kolejnym zakupie. Firma Microsoft używa informacji o zakupach do prowadzenia Sklepu i zapewnienia obsługi klienta.

Sklep prowadzi rejestr wszystkich aplikacji zainstalowanych przez użytkownika. Za pośrednictwem Sklepu można zatem zarządzać listą urządzeń, na których zainstalowano aplikacje. W zarządzaniu tymi informacjami może pomóc dział obsługi klienta. Zainstalowana aplikacja będzie zawsze widoczna w historii zakupów w Sklepie — nawet po jej odinstalowaniu. Dzięki tej liście w Sklepie można kontrolować przestrzeganie ograniczeń dotyczących liczby komputerów, na których można zainstalować aplikacje, zgodnie z opisem w warunkach użytkowania Sklepu Windows. Jeśli użytkownik napisze recenzję aplikacji, nazwa i awatar skojarzone z danym kontem w systemie Windows zostaną opublikowane obok recenzji w Sklepie. W przypadku zgłoszenia problemu z aplikacją raport o problemie zostaje udostępniony przedstawicielom Sklepu, aby umożliwić im ocenę problemu i podjęcie odpowiednich działań. Imię i nazwisko użytkownika oraz adres e-mail skojarzony z kontem w Sklepie mogą im posłużyć do kontaktowania się z użytkownikiem, jeśli będzie to konieczne podczas analizowania raportu.

Jeśli zostaną udostępnione aktualizacje aplikacji zainstalowanych przez użytkownika, w Sklepie zostanie wyświetlone powiadomienie, a na kafelku Sklepu będzie wyświetlana liczba dostępnych aktualizacji. Użytkownik może wyświetlić listę dostępnych aktualizacji i wybrać te, które chce zainstalować. Zaktualizowane aplikacje mogą korzystać z

innych funkcji systemu Windows niż ich wcześniejsze wersje, a zatem mogą uzyskać dostęp do innych zasobów na komputerze użytkownika. Zaktualizowane listy używanych funkcji można wyświetlić na stronach opisów aplikacji. Linki do tych stron znajdują się na stronie z dostępnymi aktualizacjami.

Sklep korzysta z zebranych informacji na temat kopii systemu Windows użytkownika w celu określenia sposobu zainstalowania systemu Windows na danym komputerze (na przykład, czy został preinstalowany przez producenta komputera). Dzięki tym informacjom Sklep umożliwia użytkownikowi dostęp do aplikacji dostarczonych przez danego producenta dla klientów korzystających z jego produktów. Dane te pozwalają także zapoznać się firmie Microsoft (a także producentowi — w niektórych przypadkach i w postaci zagregowanej) z wzorcami użytkowania systemu Windows.

Firma Microsoft korzysta z określonych zagregowanych informacji dotyczących zakupów aplikacji i danych dotyczących wykorzystania, aby dowiedzieć się, jak użytkownicy korzystają ze Sklepu (na przykład, jak znajdują instalowane aplikacje). Firma Microsoft może udostępnić część tych zagregowanych danych statystycznych deweloperom aplikacji. Firma Microsoft nie udostępnia deweloperom aplikacji żadnych informacji osobistych użytkownika. Dane dotyczące przeglądania i użycia zasobów zebrane przez Sklep służą do analizowania sposobów korzystania ze Sklepu przez użytkowników i do udoskonalania funkcji i usług Sklepu.

Wybór i kontrola

Jeśli użytkownik zdecydował się korzystać ze Sklepu, informacje opisane w tej sekcji będą wysyłane do firmy Microsoft zgodnie z powyższym opisem.

Aby usunąć opublikowaną recenzję aplikacji, należy przejść do opisu aplikacji w Sklepie, edytować recenzję i usunąć cały tekst.

Automatyczne aktualizacje aplikacji

Opis funkcji

Ta funkcja sprawdza dostępność aktualizacji aplikacji ze Sklepu Windows, pobiera te aktualizacje oraz je instaluje, aby zagwarantować, że na komputerze są obecne najnowsze wersje.

Aktualizacje aplikacji mogą obejmować aktualizacje zabezpieczeń, aktualizacje wydajności albo nowe funkcje lub nową zawartość. Zaktualizowane aplikacje mogą korzystać z innych funkcji systemu Windows niż ich wcześniejsze wersje, a zatem mogą uzyskać dostęp do innych zasobów na komputerze użytkownika. Informacje o zmianach funkcji można sprawdzić na stronie opisu produktu danej aplikacji w Sklepie Windows.

Informacje zbierane, przetwarzane lub przesyłane

Aby zapewnić dostęp do aktualizacji, Sklep wysyła do firmy Microsoft następujące informacje:

- Lista wszystkich aplikacji zainstalowanych ze Sklepu na danym komputerze przez wszystkich użytkowników.
- Informacje o licencji każdej aplikacji.
- Informacje o powodzeniach, niepowodzeniach i błędach związanych z aktualizacjami aplikacji ze Sklepu.
- Identyfikator GUID, czyli wygenerowany losowo numer, który nie zawiera żadnych informacji osobistych.
- Nazwa, numer wersji i data wersji systemu BIOS.
- Podstawowe informacje o komputerze, takie jak producent, model i używana wersja systemu Windows.

Używanie informacji

Te informacje są używane do świadczenia usługi aktualizacji. Są one również używane do generowania zbiorczych danych statystycznych, które pozwalają firmie Microsoft analizować tendencje oraz poprawiać produkty i usługi. Nie są używane do ustalania tożsamości użytkownika, kontaktowania się z nim ani do kierowania do niego reklam.

Wybór i kontrola

Wybranie ustawień ekspresowych podczas konfigurowania systemu Windows spowoduje, że Sklep Windows będzie automatycznie sprawdzał dostępność aktualizacji aplikacji, pobierał te aktualizacje oraz instalował je, nawet w przypadku wylogowania się ze Sklepu

Windows. W przypadku wyłączenia automatycznych aktualizacji aplikacji po zalogowaniu się w Sklepie Windows można zdecydować, czy zainstalować daną aktualizację.

Aby wyłączyć automatyczne aktualizacje aplikacji:

1. Otwórz Sklep Windows.
2. Przesuń palcem od prawej krawędzi ekranu, a następnie naciśnij polecenie **Ustawienia**można wyświetlić oraz zarządzać nimi.

   Jeśli używasz myszy, wskaż prawy dolny róg ekranu i kliknij pozycję **Ustawienia**można wyświetlić oraz zarządzać nimi.
3. Naciśnij lub kliknij pozycję **Aktualizacje aplikacji**można wyświetlić oraz zarządzać nimi.
4. Naciśnij lub kliknij pozycję **Automatycznie aktualizuj moje aplikacje** , aby wyłączyć automatyczne aktualizacje aplikacji

Aby zapoznać się z możliwościami najnowszej wersji aplikacji oraz sprawdzić, kiedy aplikacja została ostatnio zaktualizowana, należy przejrzeć stronę opisu produktu danej aplikacji w Sklepie Windows.

Uprawnienia dotyczące aplikacji ze Sklepu

Opis funkcji

Wiele aplikacji zainstalowanych ze Sklepu Windows korzysta z określonych funkcji urządzeń i oprogramowania na komputerze. Na przykład aplikacja do obsługi zdjęć może korzystać z kamery internetowej, a przewodnik po restauracjach może wymagać podania lokalizacji, aby polecić pobliskie restauracje.

Informacje zbierane, przetwarzane lub przesyłane

Oto lista funkcji, których używanie przez aplikacje musi być jawne:

- Połączenie internetowe. Umożliwia aplikacji połączenie się z Internetem.
- Połączenia przychodzące realizowane przez zaporę. Umożliwia aplikacji wysyłanie informacji przez zaporę do komputera lub z komputera użytkownika.
- Sieć domowa lub firmowa. Umożliwia aplikacji przesyłanie

informacji między danym komputerem a innymi komputerami w tej samej sieci.

- Biblioteki obrazów, muzyki, wideo i dokumentów. Umożliwia aplikacjom korzystanie z plików w bibliotekach użytkownika, a także ich zmienianie i usuwanie. Daje także dostęp do wszelkich dodatkowych danych osadzonych w tych plikach, takich jak informacje o lokalizacji zawarte w zdjęciach.

- Magazyn wymienny. Umożliwia aplikacji dostęp do plików na zewnętrznym dysku twardym, dysku flash USB lub urządzeniu wymiennym, a także dodawanie, zmienianie i usuwanie takich plików.

- Poświadczenia systemu Windows. Umożliwia aplikacji korzystanie z poświadczeń użytkownika w celu uwierzytelniania i zapewnienia dostępu do firmowego intranetu.

- Certyfikaty przechowywane na komputerze lub karcie inteligentnej. Umożliwia aplikacji korzystanie z certyfikatów w celu bezpiecznego łączenia się z organizacjami, takimi jak banki, agencje rządowe lub pracodawca użytkownika.

- Funkcja wiadomości SMS na komputerze. Umożliwia aplikacji wysyłanie i odbieranie wiadomości tekstowych.

- Kamera internetowa i mikrofon. Umożliwia aplikacji robienie zdjęć oraz nagrywanie dźwięku i obrazu wideo.

- Lokalizacja. Umożliwia aplikacji określanie przybliżonej lokalizacji użytkownika dzięki czujnikowi GPS lub informacjom dotyczącym sieci.

- Funkcja komunikacji zbliżeniowej komputera. Umożliwia aplikacji łączenie się z urządzeniami w pobliżu korzystającymi z tej samej aplikacji.

- Urządzenia przenośne. Umożliwia aplikacji komunikację z urządzeniami, takimi jak telefon komórkowy, cyfrowy aparat fotograficzny lub przenośny odtwarzacz muzyczny.

- Informacje użytkownika na urządzeniu przenośnym. Umożliwia

aplikacji korzystanie z kontaktów, kalendarzy, zadań, notatek, informacji o stanie oraz dzwonków na urządzeniu przenośnym, a także dodawanie, zmienianie i usuwanie tych danych.

- Konto komórkowego połączenia szerokopasmowego. Umożliwia aplikacji zarządzanie kontem komórkowego połączenia szerokopasmowego użytkownika.

Funkcje używane przez aplikację są wyświetlone na stronie opisu odpowiedniej aplikacji. Po zainstalowaniu aplikacji przez użytkownika system Windows umożliwia jej korzystanie z tych funkcji. Wyjątek stanowią funkcje lokalizacji, wiadomości tekstowych i kamery internetowej oraz mikrofonu, ponieważ korzystają z danych poufnych i są traktowane ze szczególną ostrożnością. Jeśli aplikacja po raz pierwszy żąda dostępu do jednej z funkcji używającej danych poufnych, system Windows wyświetla monit umożliwiający zdecydowanie, czy aplikacja może korzystać danej funkcji. W dowolnym momencie można zmienić tę decyzję.

Jeśli oprócz powyższych uprawnień aplikacja zażąda przechowywanych na określonym urządzeniu informacji dotyczących użytkownika lub jego działań, system Windows wyświetli monit z pytaniem, czy użytkownik chce udostępnić aplikacje te dane. Jeśli na przykład użytkownik podłączy urządzenie do monitorowania kondycji, które śledzi lokalizację użytkownika, system Windows zapyta, czy ma udostępnić aplikacji te dane.

Używanie informacji

Korzystanie z tych funkcji przez poszczególne aplikacje podlega zasadom zachowania poufności informacji obowiązującym u odpowiednich deweloperów. Jeśli aplikacja korzysta z jednej z opisanych powyżej funkcji używających danych poufnych, na stronie z opisem aplikacji w Sklepie jest dostępny link do zasad zachowania poufności informacji wydawcy tej aplikacji.

Wybór i kontrola

Przed zainstalowaniem aplikacji można sprawdzić w Sklepie, jakich funkcji ona wymaga. System Windows pyta użytkownika, czy chce zezwolić na dostęp do tych funkcji, które używają danych poufnych (dotyczących lokalizacji, wiadomości tekstowych, kamery internetowej

i mikrofonu), zanim dana aplikacja użyje ich po raz pierwszy.

Na stronie z opisem aplikacji w Sklepie Windows znajduje się skrócona lista funkcji używanych przez aplikację (u dołu kolumny z lewej strony). Pełną listę można zobaczyć na stronie szczegółów opisu aplikacji. Po zainstalowaniu aplikacji można w dowolnym momencie wyświetlić pełną listę funkcji używanych przez aplikację i kontrolować jej dostęp do funkcji korzystających z poufnych danych. W tym celu należy otworzyć aplikację, otworzyć panel **Ustawienia**, a następnie wybrać pozycję **Uprawnienia**można wyświetlić oraz zarządzać nimi.

Spersonalizowane wyszukiwanie w Sklepie i polecane aplikacje

Opis funkcji

Kiedy użytkownik przegląda lub wyszukuje aplikacje w Sklepie Windows, firma Microsoft udostępnia rekomendacje oraz wyniki wyszukiwania pomocne w znalezieniu odpowiednich aplikacji.

Informacje zbierane, przetwarzane lub przesyłane

Aby poprawić wyniki wyszukiwania, Sklep Windows wysyła do firmy Microsoft informacje dotyczące interakcji użytkownika ze Sklepem, takie jak wyszukiwane elementy oraz wybierane wyniki wyszukiwania. Sklep Windows wysyła także identyfikator skojarzony z kontem Microsoft użytkownika, aby udostępnić wyniki wyszukiwania spersonalizowane na podstawie interakcji użytkownika z usługą Bing oraz innymi produktami i usługami firmy Microsoft. Użytkownik może zdecydować, że nie chce otrzymywać spersonalizowanych wyników. W takim przypadku identyfikator nie będzie wysyłany.

Używanie informacji

Identyfikator użytkownika skojarzony z jego kontem Microsoft jest używany w Sklepie do udostępniania spersonalizowanych wyników wyszukiwania i polecanych produktów na podstawie interakcji użytkownika ze Sklepem oraz innymi produktami i usługami firmy Microsoft, takimi jak Bing i Sklep Windows Phone. Obejmuje to między innymi informacje dotyczące nabytych aplikacji, informacje udostępnione w profilu konta Microsoft oraz oceny i recenzje aplikacji. Te informacje te mogą być również używane do personalizowania innych produktów oraz usług firmy Microsoft.

Wybór i kontrola

W przypadku zalogowania się w systemie Windows za pomocą konta Microsoft spersonalizowane wyniki i polecane aplikacje są domyślnie włączone w Sklepie Windows. Aby nie korzystać ze spersonalizowanych wyników i polecanych aplikacji w Sklepie, należy to określić w sekcji **Preferencje** w ustawieniach Sklepu.

Pomóż ulepszyć Sklep Windows, wysyłając adresy URL zawartości, z której korzystają aplikacje

Opis funkcji

Niektóre aplikacje uzyskiwane ze Sklepu przypominają witryny sieci Web i mogą narazić komputer na niebezpieczeństwo — na przykład ze strony złośliwego oprogramowania. Po włączeniu ta funkcja zbiera informacje dotyczące zawartości sieci Web używanej przez takie aplikacje, aby ułatwić firmie Microsoft diagnozowanie potencjalnie niebezpiecznego zachowania. Te informacje mogą pomóc firmie Microsoft na przykład w usunięciu danej aplikacji ze Sklepu.

Informacje zbierane, przetwarzane lub przesyłane

Jeśli użytkownik zdecyduje się wysyłać informacje dotyczące zawartości sieci Web używanej przez aplikacje, firma Microsoft będzie zbierać informacje dotyczące typów zawartości i adresów URL używanych przez te aplikacje po ich uruchomieniu. Dzięki temu można określić, które z tych aplikacji otrzymują zawartość ze szkodliwych lub niebezpiecznych witryn sieci Web. Raporty wysyłane do firmy Microsoft mogą zawierać informacje, takie jak nazwa lub identyfikator aplikacji, pełne adresy URL używane przez aplikację oraz pełny adres URL identyfikujący lokalizację każdego kodu JavaScript, z którego aplikacja korzysta. System Windows generuje numer nazywany unikatowym identyfikatorem globalnym (GUID), który jest wysyłany w każdym raporcie do firmy Microsoft. Identyfikator GUID pozwala stwierdzić, jakie dane zostały wysłane z określonego komputera w danym okresie. Identyfikator GUID nie zawiera żadnych danych osobowych ani nie służy do identyfikacji użytkownika.

W celu ochrony prywatności użytkownika informacje wysyłane do firmy Microsoft są szyfrowane. Mogą też zostać dołączone informacje

związane ze stroną sieci Web, do której dostęp uzyskują aplikacje — na przykład wyszukiwane terminy lub dane wprowadzone w aplikacjach. Jeśli na przykład użytkownik sprawdził tłumaczenie określonego wyrazu w aplikacji słownika, sprawdzany wyraz może zostać uwzględniony w informacjach wysyłanych do firmy Microsoft jako część pełnego adresu użytego przez tę aplikację. Firma Microsoft filtruje takie adresy w celu usunięcia z nich danych osobowych, jeśli jest to możliwe.

Używanie informacji

Firma Microsoft okresowo przegląda wysłane informacje, aby wykryć aplikacje, które mogą korzystać z niebezpiecznej zawartości sieci Web, takiej jak szkodliwe adresy internetowe lub skrypty. Te informacje mogą zostać użyte w celu podjęcia odpowiednich działań dotyczących potencjalnie szkodliwych aplikacji. Adresy zawartości sieci Web mogą przypadkowo zawierać dane osobowe, które jednak nie są używane do ustalania tożsamości użytkownika, kontaktowania się z nim ani kierowania do niego reklam. Na podstawie identyfikatorów GUID firma Microsoft określa zakres otrzymywanych opinii i przydziela im priorytety. Identyfikator GUID umożliwia na przykład firmie Microsoft sprawdzenie, czy określone niebezpieczne zachowanie wystąpiło 100 razy na jednym komputerze, czy też raz na 100 komputerach.

Wybór i kontrola

Wybranie ustawień ekspresowych podczas konfiguracji systemu Windows powoduje wysyłanie przez system Windows informacji dotyczących zawartości sieci Web używanej przez aplikacje ze Sklepu, które zostały utworzone w języku JavaScript. Jeśli użytkownik zdecyduje się dostosować ustawienia, może kontrolować to ustawienie, wybierając pozycję **Używaj usług online SmartScreen, aby zapewnić ochronę przed złośliwą zawartością w witrynach ładowanych przez aplikacje ze Sklepu Windows i program Internet Explorer oraz pobraną złośliwą zawartość** w obszarze **Pomóż w ulepszaniu produktów i usług firmy Microsoft**. Po ukończeniu instalacji można zmienić to ustawienie, korzystając z pozycji **Prywatność** w ustawieniach komputera.

Góra strony

Usługa Czas systemu Windows

Opis funkcji

Usługa Czas systemu Windows umożliwia automatyczne synchronizowanie czasu na komputerze z serwerem czasu w sieci.

Informacje zbierane, przetwarzane lub przesyłane

Usługa łączy się z serwerem czasu w Internecie lub sieci lokalnej za pomocą standardowego protokołu NTP (Network Time Protocol). Domyślnie usługa przeprowadza synchronizację z serwerem time.windows.com raz na tydzień. Do serwera czasu są przesyłane tylko standardowe informacje o komputerze.

Używanie informacji

Informacje umożliwiają usłudze Czas systemu Windows automatyczne synchronizowanie czasu na danym komputerze.

Wybór i kontrola

Usługa Czas systemu Windows jest domyślnie włączona. Można ją wyłączyć, korzystając z pozycji **Data i godzina** w ustawieniach komputera. Wyłączenie funkcji Czas systemu Windows nie ma bezpośredniego wpływu na działanie aplikacji i innych usług, ale jeśli komputer nie ma dostępu do niezawodnego źródła danych dotyczących czasu, jego zegar może nie być zsynchronizowany z zegarami innych komputerów w sieci lub w Internecie. Jeśli wystąpi duża rozbieżność czasu między komputerami w sieci, aplikacje i usługi, których działanie zależy od czasu, mogą przestać działać lub mogą działać nieprawidłowo.

Góra strony

Rozwiązywanie problemów z systemem Windows

Opis funkcji

Funkcja rozwiązywania problemów z systemem Windows umożliwia diagnozowanie i rozwiązywanie typowych problemów dotyczących komputera.

Informacje zbierane, przetwarzane lub przesyłane

Po uruchomieniu pakietu wyniki są zapisywane na komputerze. Wyniki mogą zawierać informacje osobiste, takie jak nazwa użytkownika lub nazwa urządzenia. Funkcja rozwiązywania problemów z systemem Windows ułatwia wyszukiwanie rozwiązań problemów w Pomocy systemu Windows i społecznościach Windows w trybie online. Aby ułatwić znalezienie rozwiązania, do firmy Microsoft są wysyłane słowa kluczowe dotyczące danego problemu. Jeśli na przykład drukarka nie działa prawidłowo i użytkownik szuka rozwiązania tego problemu, do firmy Microsoft są wysyłane słowa, takie jak „drukarka”, „drukować” i „drukowanie”.

Używanie informacji

Firma Microsoft używa informacji zebranych przez usługę rozwiązywania problemów z systemem Windows, aby ułatwić rozwiązywanie problemów napotykanych przez użytkowników.

Wybór i kontrola

Aby usunąć wyniki rozwiązywania problemów, należy skorzystać z apletu Rozwiązywanie problemów w Panelu sterowania. W tym celu należy kliknąć pozycję **Wyświetl historię**, zaznaczyć wynik i kliknąć pozycję **Usuń**można wyświetlić oraz zarządzać nimi.

Góra strony

Foldery robocze

Opis funkcji

Foldery robocze to foldery na komputerze użytkownika, które są automatycznie synchronizowane z serwerem plików w jego miejscu pracy.

Zbierane, przetwarzane, przechowywane lub przesyłane informacje

Jeśli użytkownik zapisuje plik w folderze roboczym, plik jest automatycznie synchronizowany z serwerem plików obsługiwanym w jego miejscu pracy. Pliki zapisane w folderze roboczym użytkownika z poziomu innych komputerów zostaną zsynchronizowane z komputerem użytkownika.

Używanie informacji

System Windows wysyła pliki z folderów roboczych użytkownika i odbiera je w nich, aby zapewnić synchronizację tych folderów. Sposób użycia informacji przechowywanych na serwerach w miejscu pracy podlega zasadom zachowania poufności informacji obowiązującym w miejscu pracy.

Wybór i kontrola

Połączeniem komputera z folderami roboczymi można zarządzać w obszarze **Miejsce pracy** w ustawieniach komputera.

Góra strony

Miejsce pracy

Miejsce pracy umożliwia połączenie urządzenia z usługą Windows Intune (wymagającą osobnej subskrypcji od firmy Microsoft) lub inną usługą do zarządzania urządzeniami. Jeśli użytkownik zezwoli administratorowi w swojej firmie na zarządzanie jego komputerem za pomocą funkcji Miejsce pracy, administrator może wykonywać zadania, takie jak wymuszanie zasad zabezpieczeń na komputerze, instalowanie aplikacji, wyświetlanie określonych danych dotyczących konfiguracji i innych informacji na komputerze, oraz inne zadania z zakresu zarządzania. Aby uzyskać więcej informacji o sposobie korzystania z tej funkcji w danej firmie, należy zapoznać się z zasadami zachowania poufności informacji obowiązującymi w firmie lub skontaktować się z administratorem systemu.

Informacje zbierane, przetwarzane lub przesyłane

Kiedy użytkownik konfiguruje funkcję Miejsce pracy i korzysta z niej, komputer komunikuje się z używaną w danej firmie usługą do zarządzania urządzeniami, która może być obsługiwana przez firmę Microsoft. Poświadczenia wprowadzone w celu połączenia się z funkcją Miejsce pracy są wysyłane do tej usługi.

Używanie informacji

Informacje wysłane usłudze do zarządzania urządzeniami służą do nawiązania połączenia między usługą i danym komputerem oraz umożliwiają zainstalowanie samoobsługowej aplikacji ze Sklepu Windows. Aby uzyskać informacje o samoobsługowej aplikacji, zajrzyj

do zasad zachowania poufności informacji obowiązujących w firmie lub skontaktuj się z administratorem systemu.

Wybór i kontrola

Jeśli dana firma korzysta z funkcji Miejsce pracy, można nawiązać lub zakończyć połączenie w ramach funkcji Miejsce pracy, korzystając z pozycji Miejsce pracy w obszarze **Sieć**w ustawieniach komputera. Kiedy komputer połączy się z usługą, można wyświetlić informacje o połączeniu lub w dowolnym momencie zakończyć połączenie.

Góra strony

Aktualne informacje o praktykach przetwarzania danych stosowanych przez Microsoft zawiera Oświadczenie o ochronie prywatności w firmie Microsoft. Tam również możesz się dowiedzieć o najnowszych udostępnianych przez nas narzędziach służących uzyskiwaniu dostępu i kontrolowaniu danych oraz o metodach kontaktowania się z nami w razie pytań dotyczących prywatności.

Oświadczenie o ochronie prywatności w systemach Windows 8.1 i Windows Server 2012 R2

Ta strona stanowi uzupełnienie zasad zachowania poufności informacji w systemach Windows 8.1 i Windows Server 2012 R2 („zasad zachowania poufności informacji w systemie Windows”), które składają się z następujących sekcji:

- Najważniejsze informacje
- Instrukcja, czyli pełny tekst zasad zachowania poufności informacji w systemie Windows 8.1 z uwzględnieniem linków do zasad zachowania poufności informacji dotyczących funkcji systemu Windows, które nie mają własnych zasad w tym zakresie
- Uzupełnienie dotyczące funkcjizawierające opis funkcji mających wpływ na ochronę prywatności w systemach Windows 8.1 i Windows Server 2012 R2

- **Uzupełnienie dotyczące aplikacji** (ta strona) zawierające opis aplikacji mających wpływ na ochronę prywatności w systemie Windows 8.1 i linki do zasad zachowania poufności informacji obowiązujących w przypadku poszczególnych aplikacji

- Uzupełnienie dotyczące wersji serwerowejzawierające opis dodatkowych funkcji mających wpływ na ochronę prywatności w systemie Windows Server 2012 R2

Aby zapoznać się z działaniami w zakresie zbierania i używania danych dotyczącymi określonej funkcji lub usługi systemu Windows, należy przeczytać pełny tekst zasad zachowania poufności informacji i odpowiednie uzupełnienia lub autonomiczne zasady zachowania poufności informacji.

W przypadku użytkowników, którzy podczas konfigurowania komputera zdecydowali się na udział w Programie poprawy jakości obsługi klienta te aplikacje zbierają informacje w postaci raportu dotyczącego sposobu korzystania z poszczególnych aplikacji, a także jej wydajności i niezawodności. Firma Microsoft korzysta z tych informacji w celu udoskonalania swoich produktów i usług. Te informacje nie są używane do ustalania tożsamości użytkownika, kontaktowania się z nim ani do kierowania do niego reklam. Ustawienie dotyczące tego programu można zmienić w ustawieniach komputera. Aby uzyskać więcej informacji, zobacz zasady zachowania poufności informacji Programu poprawy jakości obsługi klienta.

Poniższe linki prowadzą do zasad zachowania poufności informacji obowiązujących w przypadku poszczególnych aplikacji:

Alarm

Kalkulator

Kalendarz

Aparat

Finanse

Żywność

Gry

Zdrowie

Pomoc i porady

Poczta

Mapy

Muzyka

Wiadomości

Kontakty

Czytnik

Lista lektur

Skanowanie

Skype

Rejestrator dźwięku

Sport

Podróże

Wideo

Pogoda

Aktualne informacje o praktykach przetwarzania danych stosowanych przez Microsoft zawiera Oświadczenie o ochronie prywatności w firmie Microsoft. Tam również możesz się dowiedzieć o najnowszych udostępnianych przez nas narzędziach służących uzyskiwaniu dostępu i kontrolowaniu danych oraz o metodach kontaktowania się z nami w razie pytań dotyczących prywatności.

Oświadczenie o ochronie prywatności w systemach Windows 8.1 i Windows Server 2012 R2

Na tej stronie

Rejestrowanie dostępu użytkowników

Menedżer serwera

Usługi federacyjne Active Directory

Zarządzanie adresami IP

Ujednolicony dostęp zdalny

Usługi pulpitu zdalnego

Ta strona stanowi uzupełnienie zasad zachowania poufności informacji w systemach Windows 8.1 i Windows Server 2012 R2 („zasad zachowania poufności informacji w systemie Windows”). Zasady zachowania poufności informacji składają się z następujących sekcji:

- Najważniejsze informacje
- Instrukcja, czyli pełny tekst zasad zachowania poufności informacji w systemie Windows 8.1 z uwzględnieniem linków do zasad zachowania poufności informacji dotyczących funkcji systemu Windows, które nie mają własnych zasad w tym zakresie
- Uzupełnienie dotyczące funkcjizawierające opis funkcji mających wpływ na ochronę prywatności w systemach Windows 8.1 i Windows Server 2012 R2

Program poprawy jakości obsługi klienta systemu Windows i raportowanie błędów systemu Windows

Rejestrowanie spisu oprogramowania

- Uzupełnienie dotyczące aplikacjizawierające opis aplikacji mających wpływ na ochronę prywatności w systemie Windows 8.1
- **Uzupełnienie dotyczące wersji serwerowej** (ta strona) zawierające opis dodatkowych funkcji mających wpływ na ochronę prywatności w systemie Windows Server 2012 R2

Aby zapoznać się z działaniami w zakresie zbierania i używania danych dotyczącymi określonej funkcji lub usługi systemu Windows, należy przeczytać pełny tekst zasad zachowania poufności informacji w systemie Windows i odpowiednie uzupełnienia. Oprócz tego należy przeczytać ten ten oficjalny dokument techniczny dla administratorów.

Aby uzyskać informacje dotyczące wpływu funkcji zawartych w systemie Windows Server 2012 R2 Essentials na prywatność, zobacz Zasady zachowania poufności informacji systemu Windows Server 2012 R2 Essentials i środowiska Windows Server Essentials.

Rejestrowanie dostępu użytkowników

Opis funkcji

Usługa rejestrowania dostępu użytkowników (UAL) zbiera i agreguje rekordy żądań klientów ról serwera (żądań zarówno użytkowników, jak i urządzeń) oraz zainstalowanych produktów (jeśli są zarejestrowane w tej usłudze) na serwerze lokalnym. Te dane, w postaci adresów IP, nazw użytkowników, a w niektórych przypadkach nazw hostów lub tożsamości maszyn wirtualnych, są przechowywane w lokalnych bazach danych aparatu magazynu rozszerzonego i są dostępne tylko dla administratorów. Usługę rejestrowania dostępu użytkowników wyposażono w dostawcę WMI (w wersji 2) i skojarzone polecenia cmdlet programu Windows PowerShell do pobierania danych o dostępie użytkowników przeznaczonych do zarządzania uprawnieniami licencji dostępowych (CAL) w trybie offline, w którym korzystanie z bieżących rekordów żądań unikatowych klientów ma newralgiczne znaczenie.

Informacje zbierane, przetwarzane lub przesyłane

Gdy usługa rejestrowania dostępu użytkowników jest włączona, adresy IP, nazwy użytkowników, a w niektórych przypadkach nazwy hostów (jeśli zainstalowano rolę usługi DNS) i tożsamości maszyn wirtualnych (jeśli zainstalowano rolę funkcji Hyper-V) są zbierane lokalnie na serwerze. Żadne zebrane dane nie są wysyłane do firmy Microsoft.

Używanie informacji

Dane usługi rejestrowania dostępu użytkowników są udostępniane administratorom za pośrednictwem lokalnych baz danych aparatu magazynu rozszerzonego, dostawcy WMI i poleceń cmdlet programu Windows PowerShell. System Windows nie używa tych danych poza obrębem usługi rejestrowania dostępu użytkowników.

Wybór i kontrola

Usługa rejestrowania dostępu użytkowników jest domyślnie włączona. Usługę rejestrowania dostępu użytkowników można zatrzymać i uruchomić w trakcie działania serwera. Aby trwale wyłączyć usługę rejestrowania dostępu użytkowników, należy otworzyć program Windows PowerShell, wpisać polecenie Disable-UAL i ponownie uruchomić serwer. Administrator może usunąć wszystkie zebrane dane historyczne, zatrzymując, a następnie wyłączając usługę rejestrowania dostępu użytkowników i usuwając wszystkie pliki w folderze %SystemRoot%\System32\LogFiles\SUM\.

Góra strony

Menedżer serwera

Opis funkcji

Menadżer serwera to narzędzie do zarządzania, za pomocą którego administrator może monitorować jeden lub więcej serwerów oraz przeglądać ogólny lub charakterystyczny dla roli stan w celu wykonywania zadań administracyjnych i uzyskiwania dostępu do innych narzędzi do zarządzania serwerem.

Informacje zbierane, przetwarzane lub przesyłane

Menedżer serwera zbiera następujące typy informacji z serwera, którym zarządza administrator:

- **Ogólne informacje o serwerze:** nazwa NetBios i w pełni

kwalifikowana nazwa domeny (FQDN), poświadczenia konta wprowadzone w funkcji Zarządzaj jako, adres IPv4, adres IPv6, stan możliwości zarządzania, opis, wersja systemu operacyjnego, typ, ostatnia aktualizacja, procesory, pamięć, nazwa klastra, typ obiektu klastra, stan aktywacji, wersja produktu systemu, architektura systemu operacyjnego, producent, konfiguracja Programu poprawy jakości obsługi klienta i konfiguracja raportowania błędów systemu Windows.

- **Zdarzenia:** identyfikator, ważność, źródło, dziennik, data i godzina każdego zdarzenia z dzienników systemu Windows i innych dzienników wybranych przez administratora.
- **Wszystkie usługi:** nazwa, stan i typ uruchomienia.
- **Informacje o rolach serwera:** wyniki Analizatora najlepszych rozwiązań dla ról zainstalowanych na serwerze.
- **Informacje o wydajności:** próbki dla liczników wydajności i powiadomienia dotyczące użycia procesora i dostępnej pamięci.

Używanie informacji

Te informacje są przechowywane w Menedżerze serwera i nie są wysyłane do firmy Microsoft. Są wyświetlane w Menedżerze serwera, aby ułatwić administratorom monitorowanie systemów.

Wybór i kontrola

Administrator może włączyć lub wyłączyć zbieranie danych z dowolnego serwera (z wyjątkiem serwera lokalnego), dodając lub usuwając ten serwer w Menedżerze serwera. Administrator może jawnie podać poświadczenia do łączenia się z serwerem zdalnym. Menedżer serwera prosi administratora o jawną zgodę na zapisanie poświadczeń lokalnie w Menedżerze serwera. Administrator może je w dowolnej chwili usunąć.

Góra strony

Usługi federacyjne Active Directory

Opis funkcji

Usługi federacyjne Active Directory (AD FS) to rozwiązanie do obsługi logowania jednokrotnego i federacji gotowe do użytku w przedsiębiorstwie dla aplikacji bazujących na sieciach lokalnych lub innych. Usługi AD FS ułatwiają administratorom umożliwianie użytkownikom współpracy między organizacjami i łatwego dostępu do aplikacji w sieciach lokalnych i innych przy zachowaniu bezpieczeństwa aplikacji. W usługach AD FS jest używana usługa tokenu zabezpieczającego, która za pomocą usług domenowych Active Directory (AD DS) uwierzytelnia użytkowników i wystawia im tokeny zabezpieczające przy użyciu różnych protokołów. Token jest podpisany cyfrowo i zawiera oświadczenia dotyczące użytkownika pochodzące z usług AD DS, katalogu LDAP (Lightweight Directory Access Protocol), bazy danych programu SQL Server lub magazynu niestandardowego albo z dowolnego połączenia tych źródeł.

Informacje zbierane, przetwarzane lub przesyłane

Podczas uwierzytelniania użytkownika w usługach AD FS zbierane są poświadczenia użytkownika. Poświadczenia są natychmiast wysyłane do usług domenowych Active Directory na potrzeby uwierzytelniania: usługi AD FS nie zapisują ich lokalnie. Za pomocą atrybutów użytkownika w usługach domenowych Active Directory można wygenerować oświadczenia wychodzące, zależnie od reguł oświadczeń skonfigurowanych przez administratora usług AD FS. Oświadczenia wychodzące są wysyłane do zaufanych partnerów, z którymi administrator usług AD FS ustanowił relacje zaufania. Żadne informacje nie są wysyłane do firmy Microsoft.

Używanie informacji

Firma Microsoft nie ma dostępu do tych informacji. Te informacje są przeznaczone tylko do użytku klientów.

Wybór i kontrola

Usług AD FS można używać do zbierania danych lub wysyłania ich do zaufanych partnerów.

Góra strony

Zarządzanie adresami IP

Opis funkcji

Zarządzanie adresami IP (IPAM, IP Address Management) pozwala administratorom serwerów śledzić adresy IP, nazwy hostów i identyfikatory klientów (takie jak adres MAC w przypadku używania protokołu IPv4 i identyfikator DUID w przypadku protokołu IPv6) komputerów i urządzeń w sieci z informacjami logowania użytkowników.

Informacje zbierane, przetwarzane lub przesyłane

Serwer IPAM zbiera dzienniki inspekcji i zdarzenia z serwerów DHCP, kontrolerów domen oraz serwerów zasad sieciowych, a następnie zapisuje lokalnie adres IP, nazwę hosta, identyfikator klienta i nazwę zalogowanego użytkownika. Administrator serwera może za pomocą konsoli IPAM przeszukiwać zebrane dzienniki na podstawie adresu IP, identyfikatora klienta, nazwy hosta i nazwy użytkownika. Żadne z tych informacji nie są przesyłane do firmy Microsoft.

Używanie informacji

Firma Microsoft nie ma dostępu do tych informacji. Te informacje są przeznaczone tylko do użytku klientów.

Wybór i kontrola

Usługa IPAM nie jest domyślnie zainstalowana. Musi ją zainstalować administrator serwera. Po zainstalowaniu usługi IPAM inspekcja adresów IP jest automatycznie włączona. Aby wyłączyć inspekcję adresów IP na serwerze z zainstalowaną usługą IPAM, na serwerze IPAM należy uruchomić Harmonogram zadań, przejść do obszaru Zadanie inspekcji w gałęzi Microsoft\Windows\IPAM i wyłączyć to zadanie.

Góra strony

Ujednolicony dostęp zdalny

Opis funkcji

Ujednolicony dostęp zdalny umożliwia użytkownikom zdalnym łączenie się przez Internet z siecią prywatną, na przykład z siecią firmową. W ramach ujednoliconego dostępu zdalnego zdalnym komputerom klienckim z systemem Windows 8 jest udostępniana nieprzerwana i

obsługiwana jak bezpośrednia łączność z sieciami firmowymi za pomocą funkcji DirectAccess. Udostępniana jest też funkcja usługi dostępu zdalnego (RAS, Remote Access Service), która obejmuje tradycyjne usługi VPN, w tym łączność typu lokacja-lokacja z sieciami lokalnymi i innymi.

Informacje zbierane, przetwarzane lub przesyłane

Na potrzeby monitorowania użytkowników ujednoliconego dostępu zdalnego na serwerze funkcji DirectAccess są przechowywane szczegóły dotyczące użytkowników zdalnych łączących się z siecią prywatną. Obejmuje to takie informacje, jak nazwa hosta użytkownika zdalnego, nazwa użytkownika usługi Active Directory oraz publiczny adres IP klienta zdalnego, a jeśli klient znajduje się za translatorem adresów sieciowych (NAT) — jego publiczny adres IP. Te dane mogą też być przechowywane w wewnętrznej bazie danych systemu Windows lub na serwerach RADIUS (jedynie za zgodą administratora). Tylko administrator funkcji DirectAccess (użytkownik domeny z kontem administratora lokalnego) uzyskujący dostęp do serwera może uzyskać dostęp do tych informacji i je wyświetlać.

Używanie informacji

Administratorzy używają tych informacji podczas rozwiązywania problemów z łącznością klientów oraz na potrzeby inspekcji i zapewniania zgodności z przepisami. Żadne informacje nie są wysyłane do firmy Microsoft.

Wybór i kontrola

Monitorowanie klientów zdalnych jest domyślnie włączone i nie można go wyłączyć. Dane monitorowania są przechowywane w wewnętrznej bazie danych systemu Windows lub na serwerach RADIUS tylko w przypadku, gdy administrator skonfigurował używanie którejś z tych opcji w ewidencjonowaniu. Jeśli administrator nie skonfigurował ewidencjonowania, żadne z tych informacji nie są przechowywane. Administrator może też tak skonfigurować ewidencjonowanie na serwerze dostępu zdalnego, aby nie były przechowywane nazwy użytkowników i adresy IP.

Góra strony

Usługi pulpitu zdalnego

Opis funkcji

Usługi pulpitu zdalnego (RDS, Remote Desktop Services) udostępniają platformę ułatwiającą firmom wdrażanie scentralizowanej strategii dotyczącej komputerów, zarządzanie komputerami i aplikacjami oraz zwiększanie elastyczności i zgodności przy jednoczesnym ulepszaniu bezpieczeństwa danych.

Informacje zbierane, przetwarzane lub przesyłane

Na potrzeby monitorowania użytkowników usług RDS serwer hosta sesji usług pulpitu zdalnego przechowuje informacje o użytkownikach zdalnych łączących się z zasobami usług RDS. Obejmuje to takie informacje, jak nazwa hosta użytkownika zdalnego, nazwa użytkownika usługi Active Directory oraz publiczny adres IP klienta zdalnego, a jeśli klient znajduje się za translatorem adresów sieciowych (NAT) — jego publiczny adres IP. Te dane są automatycznie zapisywane w wewnętrznej bazie danych systemu Windows lub na serwerach SQL, gdy użytkownicy nawiązują połączenia. Żadne informacje nie są wysyłane do firmy Microsoft. Tylko użytkownik domeny z kontem administratora lokalnego może uzyskać dostęp do tych informacji i je wyświetlać.

Używanie informacji

Administratorzy używają tych informacji podczas rozwiązywania problemów z łącznością klientów oraz na potrzeby wewnętrznej inspekcji i zapewniania zgodności z przepisami. Żadne informacje nie są wysyłane do firmy Microsoft.

Wybór i kontrola

Monitorowanie klientów jest domyślnie włączone i nie można go wyłączyć. Informacje monitorowania są przechowywane w wewnętrznej bazie danych systemu Windows lub na serwerze SQL.

Góra strony

Program poprawy jakości obsługi klienta systemu Windows i raportowanie błędów systemu Windows

Opis funkcji

Aby uzyskać więcej informacji o tych funkcjach, zobacz kartę Uzupełnienie dotyczące funkcji lub ten oficjalny dokument techniczny dla administratorów.

Informacje zbierane, przetwarzane lub przesyłane

Aby dowiedzieć się, jakie konkretnie informacje są zbierane, przetwarzane i przesyłane przez te funkcje, zobacz fragmenty dotyczące Programu poprawy jakości obsługi klienta oraz raportowania błędów systemu Windows w części Uzupełnienie dotyczące funkcji .

Używanie informacji

Aby dowiedzieć się, do czego są używane informacje zbierane przez te funkcje, zobacz fragmenty dotyczące Programu poprawy jakości obsługi klienta oraz raportowania błędów systemu Windows w części Uzupełnienie dotyczące funkcji .

Wybór i kontrola

Program poprawy jakości obsługi klienta jest domyślnie wyłączony, a raportowanie błędów systemu Windows jest domyślnie skonfigurowane do monitowania użytkownika przed wysłaniem do firmy Microsoft raportu o awarii. Program poprawy jakości obsługi klienta można włączyć lub wyłączyć w Menedżerze serwera i Panelu sterowania oraz metodami sterowania używanymi w wierszu polecenia. Raportowaniem błędów systemu Windows można sterować tylko metodami używanymi w wierszu polecenia.

Aby włączyć lub wyłączyć Program poprawy jakości obsługi klienta za pomocą Panelu sterowania, należy kliknąć pozycję **System i konserwacja**i kliknąć pozycję **Raporty i rozwiązania problemów**. Następnie w obszarze **Zobacz też**, kliknąć pozycję **Ustawienia Programu poprawy jakości obsługi klienta** , aby uzyskać dostęp do opcji włączenia lub wyłączenia programu.

Kontrolki Menedżera serwera

Serwer lokalny

- Włączanie Programu poprawy jakości obsługi klienta
  Otwórz Menedżera serwera i wybierz pozycję **Serwer lokalny**. Kliknij link Program poprawy jakości obsługi klienta, w oknie dialogowym wybierz pozycję **Tak, chcę wziąć udział w**

Programie poprawy jakości obsługi klienta , a następnie kliknij przycisk **OK**.

- Wyłączanie Programu poprawy jakości obsługi klienta
  Otwórz Menedżera serwera i wybierz pozycję **Serwer lokalny**. Kliknij link Program poprawy jakości obsługi klienta, w oknie dialogowym wybierz pozycję **Nie, nie chcę brać udziału** , a następnie kliknij przycisk **OK**.

- Włączanie raportowania błędów systemu Windows
  Otwórz Menedżera serwera i wybierz pozycję **Serwer lokalny**. Kliknij link Raportowanie błędów systemu Windows, wybierz pozycję **Tak, automatycznie wysyłaj raporty podsumowujące**, a następnie kliknij przycisk **OK**.

- Wyłączanie raportowania błędów systemu Windows
  Otwórz Menedżera serwera i wybierz pozycję **Serwer lokalny**. Kliknij link Raportowanie błędów systemu Windows, wybierz pozycję **Nie chcę brać udziału w programie i nie pytaj mnie ponownie**, a następnie kliknij przycisk **OK**.

Wiele komputerów

- Włączanie Programu poprawy jakości obsługi klienta
  Otwórz Menedżera serwera i wybierz pozycję **Wszystkie serwery**. Na kafelku Serwery zaznacz wszystkie serwery (Ctrl+A), kliknij prawym przyciskiem myszy i wybierz pozycję **Konfiguruj automatyczne przesyłanie opinii o systemie Windows** . Na karcie Program poprawy jakości obsługi klienta wybierz pozycję **Tak, chcę wziąć udział (zalecane)**. Zastosuj to ustawienie do wszystkich serwerów, zaznaczając pole wyboru obok pozycji Nazwa serwera w kontrolce wybierania serwerów, a następnie kliknij przycisk **OK**.

- Wyłączanie Programu poprawy jakości obsługi klienta
  Otwórz Menedżera serwera i wybierz pozycję Wszystkie serwery. Na kafelku Serwery zaznacz wszystkie serwery (Ctrl+A), kliknij prawym przyciskiem myszy i wybierz pozycję **Konfiguruj automatyczne przesyłanie opinii o systemie Windows** . Na karcie Program poprawy jakości obsługi klienta wybierz pozycję **Nie, nie chcę brać udziału**. Zastosuj to ustawienie do

wszystkich serwerów, zaznaczając pole wyboru obok pozycji Nazwa serwera w kontrolce wybierania serwerów, a następnie kliknij przycisk **OK**.

- Włączanie raportowania błędów systemu Windows
  Otwórz Menedżera serwera i wybierz pozycję **Wszystkie serwery**. Na kafelku Serwery zaznacz wszystkie serwery (Ctrl+A), kliknij prawym przyciskiem myszy i wybierz pozycję **Konfiguruj automatyczne przesyłanie opinii o systemie Windows** . Na karcie Raportowanie błędów systemu Windows wybierz pozycję **Tak, automatycznie wysyłaj raporty podsumowujące (zalecane)**. Zastosuj to ustawienie do wszystkich serwerów, zaznaczając pole wyboru obok pozycji Nazwa serwera w kontrolce wybierania serwerów, a następnie kliknij przycisk **OK**.

- Wyłączanie raportowania błędów systemu Windows
  Otwórz Menedżera serwera i wybierz pozycję **Wszystkie serwery**. Na kafelku Serwery zaznacz wszystkie serwery (Ctrl+A), kliknij prawym przyciskiem myszy i wybierz pozycję **Konfiguruj automatyczne przesyłanie opinii o systemie Windows** . Na karcie Raportowanie błędów systemu Windows wybierz pozycję **Nie, nie chcę brać udziału**. Zastosuj to ustawienie do wszystkich serwerów, zaznaczając pole wyboru obok pozycji Nazwa serwera w kontrolce wybierania serwerów, a następnie kliknij przycisk **OK**.

Góra strony

Rejestrowanie spisu oprogramowania

Opis funkcji

Rejestrowanie spisu oprogramowania (SIL) zawiera nowy zestaw klas WMI i poleceń cmdlet programu Powershell, aby uprościć podstawową funkcję spisu wersji systemu Windows Server, oprogramowania zainstalowanego w systemie Windows Server oraz cech serwera, na którym działa oprogramowanie. Ponadto po ustawieniu odpowiedniej opcji przez administratora funkcja SIL ma możliwość zbierania danych z jej dostawcy WMI co godzinę i przekazania ich w sieci do serwera

agregacji, jeśli został on określony przy użyciu polecenia cmdlet Set-SilLogging -TargerUri.

Informacje zbierane, przetwarzane lub przesyłane

Dane mogą zostać przesłane do serwera agregacji w sieci, jeśli został on skonfigurowany przez administratora. Domyślnie żadne dane nie są zbierane, przetwarzane lub przesyłane. Dane obejmują:

- Nazwę i wersję zainstalowanego systemu operacyjnego Windows Server.
- Lista nazw, wersji i wydawców oprogramowania zainstalowanego na serwerze i datę zainstalowania oprogramowania.
- Pełni kwalifikowaną nazwę domeny systemu serwera.
- Numer, typ i producenta procesorów, procesorów logicznych i rdzeni zainstalowanych w systemie serwera lub do niego przypisanych.

Dane zbierane i przetwarzane, ale nie przekazywane domyślnie, nawet jeśli zadanie zbierania danych co godzinę jest włączone i obiekt docelowy agregatora został określony przez administratora:

- Klasa MsftSil_UalAccess i polecenie cmdlet Get-SilUalAccess przetwarza całkowitą liczbę unikatowych użytkowników i urządzeń każdej roli lub produktu zarejestrowanego za pomocą funkcji rejestrowania dostępu użytkownika (UAL) z dwóch dni przed zapytaniem. Są to tylko sumy — żadne informacje o użytkowniku ani o urządzeniu nie są zwracane ani przesyłane. Funkcja SIL musi przetworzyć informacje o użytkownikach i o urządzeniach z klas UAL w celu obliczenia samej liczby elementów. Te dane są dostępne tylko dla administratora komputera lokalnego. Funkcja SIL nie zmienia praw dostępu do interfejsów API klas UAL.

Żadne zebrane dane nie są wysyłane do firmy Microsoft.

Używanie informacji

Dostawcy SIL WMI agregują dane dostarczone przez inne interfejsy API już istniejące w systemie. Dane mogą zostać przesłane do serwera agregacji w sieci, jeśli został on skonfigurowany przez administratora.

Domyślnie żadne dane nie są zbierane, przetwarzane lub przesyłane. W przypadku polecenia cmdlet Get-SilUalAccess i klasy MsftSil_UalAccess przetworzone dane zawierają całkowitą liczbę unikatowych użytkowników i urządzeń każdej roli lub produktu zarejestrowanych za pomocą funkcji rejestrowania dostępu użytkownika (UAL) z dwóch dni przed zebraniem danych, ale nie zawierają żadnych danych identyfikujących użytkownika lub urządzenie. Mimo że to polecenie Cmdlet i klasa WMI występują w systemie, nie są one częścią ładunku danych funkcji SIL zbieranych i przekazywanych do agregatora co godzinę, gdy funkcję SIL skonfigurowano do przesyłania danych przez administratora systemu.

Wybór i kontrola

Zadania funkcji SIL wykonywane co godzinę są domyślnie wyłączone. Wszystkie interfejsy API SIL są domyślnie dostępne do odpytywania dla administratorów systemu lokalnego. Zadania funkcji SIL wykonywane co godzinę można uruchamiać i zatrzymywać w czasie działania serwera za pomocą poleceń cmdlet Start-SilLogging i Stop-SilLogging. Użycie polecenia cmdlet Set-SilLogging pozwala administratorom serwera ustawić datę i godzinę, o której uruchamiane jest wykonywane co godzinę zadanie (wartość domyślna to 3:00 czasu systemu lokalnego), identyfikator URI (Uniform Resource Identifier) docelowego serwera agregacji i niezbędny w celu zapewnienia poufnej transmisji danych odcisk palca certyfikatu.

Wszystkie ustawienia konfiguracji funkcji SIL, takie jak uruchamianie i zatrzymywanie zadania wykonywanego co godzinę, można zmienić w rejestrze, ale należy zrobić przed pierwszym uruchomieniem systemu i tylko wówczas, gdy system jest maszyną wirtualną.

Góra strony