Для отримання актуальної інформації щодо практики обробки даних корпорацією Майкрософт ознайомтеся з Положенням про конфіденційність корпорації Майкрософт. Тут ви також можете отримати інформацію про останні інструменти для отримання доступу до своїх даних і керування ними, а також про те, як із нами зв'язатися, якщо у вас виникне запитання щодо конфіденційності.

Положення про конфіденційність Windows 8.1 і Windows Server 2012 R2

Останнє оновлення: квітень 2014 року

У цьому витязі з декларації про конфіденційність для ОС Windows 8.1 і Windows Server 2012 R2 (далі – декларація про конфіденційність для ОС Windows) ідеться про правила збирання та використання даних системою Windows 8.1 і Windows Server 2012 R2 (далі – Windows). Витяг не є вичерпним описом. Основну увагу в ньому приділено онлайновим функціям. Його не можна застосувати до інших сайтів, продуктів або служб Microsoft, що працюють в Інтернеті чи в автономному режимі.

Ця декларація про конфіденційність містить такі розділи:

- **Витяг** (ця сторінка)
- Декларація, що є повною версією декларації про конфіденційність для ОС Windows 8.1, містить посилання на декларації про конфіденційність для засобів Windows, які мають свої власні декларації.

- Доповнення про засоби, у якому описуються засоби та функції, що впливають на конфіденційність в операційній системі Windows 8.1 і Windows Server 2012 R2

- Доповнення про програми, у якому описуються програми, що впливають на конфіденційність в операційній системі Windows 8.1

- Доповнення про сервер, у якому описуються додаткові засоби та функції, що впливають на конфіденційність в операційній системі Windows Server 2012 R2

Щоб отримати додаткові відомості про можливі способи захисту ПК, особистих відомостей і даних родини під час роботи в Інтернеті, відвідайте Центр захисту та безпеки.

Ваші відомості

- Деякі функції Windows можуть просити у вас дозволу на збирання або використання даних, отриманих із вашого ПК, зокрема особистих відомостей. Windows використовує ці відомості, як зазначено в повній версії декларації про конфіденційністьWindows 8.1, а також у Доповнення про засоби, Доповнення про програми й Доповнення про сервер.

- Деякі функції Windows можуть за вашої згоди надавати доступ до особистих відомостей через Інтернет.

- Якщо ви вирішите зареєструвати своє програмне забезпечення, вам буде запропоновано надати особисті відомості.

- Для протидії комп’ютерному піратству та з метою гарантованого надання споживачам очікуваної якості програмного забезпечення операційна система Windows потребує активації. Функція активації надсилає певні відомості про ПК до корпорації Майкрософт.

- У разі входу до ОС Windows за допомогою облікового запису Microsoft система Windows виконає синхронізацію настройок між пристроями та автоматично використовуватиме дані

облікового запису для входу до певних програм і на веб-сайти. ОС Windows не вимагає, щоб ви входили в систему з обліковим записом Microsoft, щоб отримати доступ до електронної пошти третьої сторони або служб соціальних мереж, та якщо третя сторона пропонує програму через Магазин, для інсталяції цієї програми необхідно увійти до Магазину з обліковим записом Microsoft. Під час створення облікового запису Microsoft відобразиться запит на ведення особистих відомостей, наприклад даних про географічне розташування та дати народження.

- Додаткові відомості

На початок сторінки

Можливості ваших дій

- Операційна система Windows пропонує вам численні можливості керування тим, як функції Windows передають інформацію через Інтернет. Додаткові відомості про керування цими функціями наведено в Доповнення про засоби, Доповнення про програми й Доповнення про сервер.

- Щоб розширити можливості користувача, певні функції, які використовують доступ до Інтернету, увімкнуто за замовчуванням.

- Додаткові відомості

На початок сторінки

Використання відомостей

- Зібрані відомості ми використовуємо з метою забезпечення роботи функцій, якими ви користуєтеся, або надання запитаних вами послуг. Ми також використовуємо ці відомості для вдосконалення наших продуктів і послуг. У рамках надання послуг ми час від часу надаємо відомості іншим компаніям, які працюють за нашим дорученням. Доступ надається лише компаніям, які мають ділову потребу у використанні цих відомостей. Від цих компаній вимагається

додержання конфіденційності ваших відомостей; їм забороняється використовувати ці відомості для будь-яких інших потреб.

- Додаткові відомості

На початок сторінки

Як із нами зв’язатись

Щоб отримати додаткові відомості про політику конфіденційності, перейдіть до повної версії декларації про конфіденційність для Windows 8.1. Окрім цього, нам можна надіслати повідомлення, заповнивши цю веб-форму.

На початок сторінки

Для отримання актуальної інформації щодо практики обробки даних корпорацією Майкрософт ознайомтеся з Положенням про конфіденційність корпорації Майкрософт. Тут ви також можете отримати інформацію про останні інструменти для отримання доступу до своїх даних і керування ними, а також про те, як із нами зв'язатися, якщо у вас виникне запитання щодо конфіденційності.

Положення про конфіденційність Windows 8.1 і Windows Server 2012 R2

На цій сторінці

Останнє оновлення: квітень 2014 року

Ця декларація стосується ОС Windows 8.1 і Windows Server 2012 R2 («Windows»). Для певних компонентів Windows передбачені окремі декларації про конфіденційність, які також перелічені на цій сторінці. Тут також перелічено декларації про конфіденційність для програмного забезпечення та послуг, пов'язаних з ОС Windows та попередніми випусками цієї операційної системи.

Додаткові відомості про окремі функції див. у Доповнення про засоби, Доповнення про програмита Доповнення про сервер. Додаткові відомості про Windows Embedded Industry Pro та Windows Embedded Industry Enterprise див. у цій декларації.

Ця декларація стосується функцій обміну даними через Інтернет і не може вважатися повним переліком функцій.

Збирання й використання інформації

Особисті відомості, які ми збираємо, використовуватимуться корпорацією Майкрософт і її підконтрольними дочірніми компаніями та філіями для забезпечення роботи використовуваних функцій і надання послуг або виконання запитаних і авторизованих транзакцій. Ця інформація також може використовуватися для аналізу та покращення продуктів і служб Microsoft.

Крім випадків, описаних у цій декларації, надані вами особисті відомості не передаватимуться третім сторонам без вашої згоди. Інколи ми доручаємо іншим компаніям надавати обмежений обсяг послуг від нашого імені, наприклад виконувати статистичний аналіз наших служб. Ці компанії отримуватимуть лише ту особисту інформацію, яка потрібна для надання послуг, і їм заборонено використовувати її з іншою метою.

Корпорація Майкрософт може отримувати доступ до особистих відомостей користувачів, включно зі змістом листування, або розкривати їх: (а) на вимогу закону або суду, а також у відповідь на запит правоохоронного органу; (б) щоб захистити права або власність корпорації Майкрософт чи її клієнтів, зокрема забезпечувати виконання умов угод або політик, які регулюють використання наших служб; (в) діючи згідно з переконанням, що доступ до цих відомостей і їх розкриття необхідні для захисту особистої безпеки працівників і клієнтів корпорації Майкрософт або громадськості.

Інформація, зібрана корпорацією Майкрософт або надіслана до неї цією ОС Windows 8.1, може зберігатися та оброблятися на території Сполучених Штатів Америки або будь-якої іншої країни, у якій є офіси корпорації Майкрософт, її афілійованих осіб, дочірніх компаній або постачальників послуг. Корпорація Майкрософт дотримується концепції «безпечної гавані», установленої Міністерством торгівлі США, щодо збирання, використання та зберігання даних у Європейському Союзі, Європейській економічній зоні та Швейцарії.

На початок сторінки

Збирання й використання інформації про ваш комп’ютер

Під час використання програмного забезпечення з функціями, які потребують активного інтернет-підключення, відомості про ваш комп'ютер (далі «стандартні відомості про комп'ютер») надсилаються до відвідуваних вами веб-сайтів і використовуваних онлайнових служб. До стандартних відомостей про комп'ютер зазвичай належить інформація про IP-адресу, версію операційної системи та браузера, а також мовні та регіональні настройки. Інколи стандартні відомості про комп'ютер можуть також містити ідентифікатор обладнання, що вказує на виробника пристрою, його модель і версію. Якщо певна функція або служба надсилає інформацію до корпорації Майкрософт, то разом із нею також надсилаються стандартні відомості про комп'ютер.

У відомостях про конфіденційність для кожної функції Windows у доповненні про функції, доповненні про програми, а також доповненні про сервер, наведених будь-де на цій сторінці, описано додаткові дані, яка збираються, і спосіб їх використання.

Адміністратори можуть змінити багато настройок для описаних у цьому розділі функцій за допомогою групової політики. Для отримання додаткових відомостей див. цей офіційний документ для адміністраторів.

На початок сторінки

Безпека вашої інформації

Корпорація Майкрософт вважає своїм обов'язком сприяти захисту вашої інформації. Ми використовуємо різні технології безпеки та процедури, які допомагають захистити вашу інформацію від неавторизованого доступу, використання або розголошення. Наприклад, ми зберігаємо надану вами особисту інформацію на комп'ютерах з обмеженим доступом, розміщених у закритих установах. Для пересилання суто конфіденційної інформації (наприклад, номерів або паролів кредитних карток) через Інтернет використовується шифрування, наприклад за протоколом SSL.

На початок сторінки

Зміни в декларації про конфіденційність

Зі зміненням наших продуктів і служб, а також у відповідь на відгуки користувачів час від часу до цієї декларації про конфіденційність вноситимуться зміни. Після внесення змін дата останнього оновлення вгорі тексту цієї декларації відповідно змінюється. У разі внесення суттєвих змін до цієї декларації або змінення порядку використання особистих відомостей корпорацією Майкрософт ми повідомимо про це, опублікувавши перед внесенням змін відповідне повідомлення або безпосередньо надіславши вам сповіщення. Радимо періодично переглядати цю декларацію, щоб завжди мати останні відомості про методи захисту вашої інформації корпорацією Майкрософт.

На початок сторінки

Додаткові відомості

Корпорація Майкрософт запрошує користувачів залишати коментарі стосовно цієї декларації про конфіденційність. Якщо у вас є запитання про цю декларацію або якщо ви вважаєте, що ми не дотримуємося її, зверніться до нас, заповнивши цю веб-форму.

Політика конфіденційності корпорації Майкрософт
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052
USA (США)

На початок сторінки

Для отримання актуальної інформації щодо практики обробки даних корпорацією Майкрософт ознайомтеся з Положенням про конфіденційність корпорації Майкрософт. Тут ви також можете отримати інформацію про останні інструменти для отримання доступу до своїх даних і керування ними, а також про те, як із нами зв'язатися, якщо у вас виникне запитання щодо конфіденційності.

Положення про конфіденційність Windows 8.1 і Windows Server 2012 R2

На цій сторінці

Останнє оновлення: квітень 2014 року

Ця сторінка є доповненням до декларації про конфіденційність Windows 8.1 і Windows Server 2012 R2 (далі «Декларація про конфіденційність Windows») і містить вказані нижче розділи.

- Витяг
- Декларація, що є повною версією декларації про конфіденційність для ОС Windows 8.1, містить посилання на декларації про конфіденційність для засобів Windows, які мають свої власні декларації.
- **Доповнення про засоби** (ця сторінка), у якому описуються засоби та функції, що впливають на конфіденційність в операційній системі Windows 8.1 та Windows Server 2012 R2.
- Доповнення про програми, у якому описуються програми, що впливають на конфіденційність в операційній системі

Виявлення та встановлення пристрою

Шифрування пристрою

DirectAccess

Центр легкого доступу

Переглядач подій

Безпека сім'ї

Факс

Персоналізація рукописного тексту – автоматичне навчання

Домашня група

Редактор засобів вводу (IME)

Спільний доступ до Інтернету

Друкування через Інтернет

Мовні параметри

Служби розташування

Керування обліковими даними

Ім'я та зображення облікового запису

Служба мережевого оповіщення

Windows 8.1

- Доповнення про сервер, у якому описуються додаткові засоби та функції, що впливають на конфіденційність в операційній системі Windows Server 2012 R2

Щоб зрозуміти принципи збирання та використання даних, пов'язані з певним засобом або службою Windows, ознайомтеся з повною версією декларації про конфіденційність та всіма застосовними або окремими доповненнями.

Активація

Властивості та завдання

Активація дає змогу зменшити кількість піратського програмного забезпечення, що, у свою чергу, допомагає гарантувати користувачам продуктів Microsoft належний рівень якості програмного забезпечення. Після активації програмного забезпечення певний ключ продукту зв'язується з ПК (або устаткуванням), на якому програмне забезпечення інстальовано. Цей зв'язок перешкоджає використанню ключа продукту для активації однієї копії програмного забезпечення на кількох ПК. Внесення певних змін до апаратного або програмного забезпечення ПК може вимагати повторної активації ОС Windows. Активація може виявити та вимкнути експлойти активації (програмне забезпечення, яке дає змогу уникнути активації програмного забезпечення Microsoft). Наявність експлойту активації може свідчити про те, що постачальник програмного або апаратного забезпечення підробив справжнє програмне забезпечення Microsoft для створення його піратських копій. Експлойти активації можуть перешкоджати належному функціонуванню системи.

Збирання, обробка та передавання інформації

Протягом активації до корпорації Майкрософт надсилаються зазначені нижче відомості.

- Код продукту Microsoft (п'ятизначний код, який дає змогу ідентифікувати продукт Windows, активація якого зараз триває).

Сповіщення, програми на екрані блокування й оновлення плиток

Замовлення друку

Попереднє завантаження та попередній запуск

Помічник із питань сумісності програм

Властивості

Наближення

Підключення для віддаленого доступу

Підключення до віддалених робочих столів і програм RemoteApp

Підключення до віддаленого робочого стола

Вхід за допомогою облікового запису Microsoft

Хмарне сховище OneDrive

Настройки синхронізації

Технологія Teredo

Служби модуля TPM

Відновлення кореневих

- Ідентифікатор каналу або код сайту, за яким можна визначити, як було отримано продукт Windows. Наприклад, ідентифікатор каналу або код сайту дає змогу визначати, як було отримано продукт: придбано в магазині, отримано як копію для ознайомлення, отримано в рамках програми корпоративного ліцензування чи попередньо інстальовано виробником ПК.
- Дата інсталяції та відомості про її успішність.
- Відомості, які допомагають переконатися в тому, що ключ продукту Windows не було змінено.
- Виробник і модель ПК.
- Відомості про версії операційної системи та програмного забезпечення.
- Регіональні та мовні параметри.
- Призначений ПК унікальний номер, що називається глобальним унікальним ідентифікатором (GUID).
- Ключ продукту (хешований) та ідентифікатор продукту.
- Назва, номер версії та дата версії системи BIOS.
- Серійний номер тому жорсткого диска (хешований).
- Результат перевірки активації. Зокрема, коди помилок і відомості про будь-які знайдені або вимкнуті експлойти активації та пов’язане з ними зловмисне або неавторизоване програмне забезпечення.
    - Ідентифікатор експлойту активації.
    - Поточний стан експлойту активації, наприклад «очищено» або «на карантині».
    - Ідентифікаційні дані виробника ПК.
    - Ім’я файлу експлойту та геш експлойту активації, а також геш пов’язаних компонентів програмного

сертифікатів

Служби оновлення

Віртуальна приватна мережа (VPN)

Програма підвищення якості ПЗ (CEIP) для Windows

Захисник Windows

Звітування про критичні помилки Windows

Зіставлення файлів Windows

Довідка Windows

Віддалена допомога

Служба пошуку Windows Search

Програма інсталяції Windows

Спільний доступ Windows

Windows SmartScreen

Засіб розпізнавання мовлення Windows

Магазин Windows

Служба часу Windows

Виправлення неполадок Windows

Служба Work Folders

Робоче місце

забезпечення, які можуть свідчити про наявність експлойту активації.

- Ім’я та геш вмісту файлу інструкцій із запуску ПК. Якщо операційна система Windows ліцензується за передплатою, будуть також надіслані відомості про принцип дії передплати. Також надсилатимуться стандартні відомості про комп’ютер.
- Якщо використовується копія Windows із корпоративною ліцензією, для якої використовується сервер активації, IP-адреса цього сервера може надсилатися до корпорації Майкрософт.

Використання інформації

Корпорація Майкрософт використовує відомості для підтвердження наявності ліцензованої копії програмного забезпечення. Корпорація Майкрософт не використовує ці відомості для звернення до окремих споживачів. Відомості про сервер ліцензій використовуються для забезпечення відповідності серверів ліцензій вимогам ліцензійних угод.

Вибір і керування

Активація є обов’язковою та здійснюється автоматично під час інсталяції ОС Windows. Якщо немає дійсної ліцензії для програмного забезпечення, активувати Windows буде неможливо.

На початок сторінки

Клієнт служби керування цифровими правами AD RMS

Властивості та завдання

Клієнт служби керування цифровими правами AD RMS – це технологія захисту інформації, яка застосовується із програмами, що її підтримують, для захисту цифрової інформації від несанкціонованого використання. Власники цифрової інформації можуть визначити, яким чином одержувачі використовуватимуть відомості, що містяться у файлі, наприклад указати, хто може відкривати, змінювати, друкувати файл або виконувати з ним інші дії. Щоб створити або переглянути файл з обмеженими дозволами, на ПК має виконуватися програма з підтримкою AD RMS, а також

має бути доступ до сервера AD RMS.

Збирання, обробка та передавання інформації

Служба AD RMS використовує адресу електронної пошти користувача для його ідентифікації на сервері AD RMS. Як наслідок, адреса електронної пошти зберігається на сервері та на ПК, у ліцензіях, і дає змогу ідентифікувати створені сервером сертифікати. Ідентифікаційні сертифікати та ліцензії передаються із серверів AD RMS під час спроби відкрити чи роздрукувати документ, захищений службою керування правами, або виконати з ним інші дії. Якщо ПК підключено до корпоративної мережі, сервером AD RMS зазвичай керує організація. У разі використання служби Windows Live AD RMS сервером керує корпорація Майкрософт. Щоб підвищити рівень конфіденційності, дані надсилаються на сервер AD RMS корпорації Майкрософт у зашифрованій формі.

Використання інформації

Ліцензія забезпечує доступ до захищених файлів. Ідентифікаційні сертифікати використовуються для встановлення особи користувача на сервері AD RMS і дають змогу захистити файли та отримати доступ до захищених файлів.

Вибір і керування

Для ввімкнення функцій AD RMS використовується програма з підтримкою AD RMS. За замовчуванням їх вимкнуто. Користувачу не обов’язково їх вмикати або використовувати. Проте, якщо їх не ввімкнути, захищені файли будуть недоступними.

На початок сторінки

Ідентифікатор реклами

Властивості та завдання

Система Windows дає змогу програмам отримувати доступ до унікального ідентифікатора кожного користувача пристрою, завдяки чому вони можуть надавати більш доречну рекламу. Доступ до цього ідентифікатора можна будь-коли скасувати або вимкнути.

Збирання, обробка та передавання інформації

Якщо дозволити програмам отримувати доступ до ідентифікатора реклами, ОС Windows надаватиме ці відомості всім програмам, які їх запитують. Програми можуть зберігати або передавати ці відомості.

Використання інформації

Ідентифікатор реклами використовується розробниками програм і рекламними мережами для надання користувачам більш доречної реклами завдяки відомостям про те, які саме програми використовуються та в який спосіб. Його також можуть використовувати розробники програм для підвищення якості обслуговування, оскільки він дає змогу визначати частоту та ефективність рекламних оголошень і виявляти шахрайство та проблеми в системі безпеки.

У разі надання програмам доступу до ідентифікатора реклами використання його кожною програмою регламентуватиметься процедурами забезпечення конфіденційності, застосовними до цієї програми.

Вибір і керування

У разі вибору швидкого настроювання під час інсталяції Windows система Windows дозволить програмам використовувати ідентифікатор реклами. У разі власноручного настроювання параметрів можна керувати доступом до ідентифікатора реклами, вибравши пункт **Дозволити програмам використовувати мій ідентифікатор реклами для покращення якості роботи в різних програмах** у розділі **Надати доступ до відомостей корпорації Майкрософт і службам інших виробників**. Після інсталяції Windows цю настройку можна змінити в розділі **Конфіденційність** у настройках ПК. Якщо вимкнути цей параметр, ідентифікатор реклами не надсилатиметься програмам, які його запитують. Якщо знов увімкнути цей параметр, буде створено новий ідентифікатор.

На початок сторінки

Аудит

Аудит дає змогу адміністратору настроїти в ОС Windows записування дій, що виконуються в операційній системі, у журналі безпеки, доступ до якого можна отримати за допомогою засобу перегляду подій та інших програм. Цей журнал може допомогти адміністратору виявити несанкціонований доступ до ПК або розташованих на ньому ресурсів. Наприклад, він може допомогти адміністраторам усунути неполадки та визначити, чи виконувався вхід на ПК, чи створювався новий обліковий запис користувача, чи вносилися зміни до політики безпеки або чи відкривався документ.

Збирання, обробка та передавання інформації

Адміністратори визначають, яка інформація має збиратися, як довго вона зберігається та чи може вона передаватися іншим сторонам. Ця інформація може включати особисті відомості, зокрема імена користувачів або імена файлів. За додатковими відомостями звертайтеся до адміністратора. До корпорації Майкрософт відомості не надсилаються.

Використання інформації

Адміністратори також визначають, як можуть використовуватися дані аудиту. Зазвичай аудитори та адміністратори використовують журнал безпеки для відстеження дій, які виконувалися на ПК, або для виявлення несанкціонованого доступу до ПК чи розташованих на ньому ресурсів.

Вибір і керування

Адміністратори визначають, чи слід вмикати цю функцію, а також задають спосіб сповіщення користувачів. Інші користувачі не можуть переглянути журнал безпеки, якщо адміністратор не надасть їм відповідні права доступу. Щоб настроїти перевірку на ПК, відкрийте локальну політику безпеки у вікні «Адміністрування».

На початок сторінки

Біометрія

Властивості та завдання

Якщо ПК оснащено сканером відбитків пальців, для входу в ОС Windows і підтвердження особи у програмах, що підтримують цю функцію, можна використовувати дактилоскопічні дані (відбиток пальця).

Збирання, обробка та передавання інформації

Під час настроювання нового відбитка пальця відомості про відбиток пальця зберігаються локально на ПК. До корпорації Майкрософт відомості не надсилаються. Коли відбиток пальця використовується для підтвердження особи у програмі, ОС Windows порівнює відбиток пальця з відбитками пальців, збереженими на ПК, і повідомляє програмі про те, чи відповідає відсканований відбиток пальця відбитку, пов’язаному з обліковим записом. ОС Windows не надає програмам дані щодо відсканованих відбитків пальця.

Використання інформації

В ОС Windows відомості про відбиток пальця, що зберігаються на ПК, використовуються для входу в ОС Windows за допомогою дактилоскопічних даних.

Вибір і керування

Щоб додати або видалити відбитки пальців, виберіть пункт **Параметри входу** в розділі **Облікові записи** в настройках ПК.

На початок сторінки

BitLocker Drive Encryption

Властивості та завдання

BitLocker Drive Encryption допомагає захистити дані завдяки їх шифруванню, що дає змогу запобігти доступу неавторизованих користувачів до ваших даних. Коли на підтримуваному диску ввімкнуто засіб BitLocker, ОС Windows шифрує дані на диску.

Збирання, обробка та передавання інформації

Якщо ввімкнути в засобі BitLocker використання програмного шифрування, система постійно виконуватиме шифрування та розшифровування даних у процесі їх зчитування та записування на

захищений диск за допомогою криптографічного ключа, що зберігається в пам’яті. Якщо ввімкнути в засобі BitLocker апаратне шифрування, шифрування та розшифровування даних виконуватиметься диском.

Під час інсталяції BitLocker можна також вибрати друк ключа відновлення або його збереження в певному мережевому розташуванні. У разі інсталяції BitLocker на незнімний диск можна також зберегти ключ відновлення у флеш-пам’яті USB.

Якщо ПК не приєднано до домену, резервну копію ключа відновлення BitLocker, ідентифікатора цього ключа та імені комп’ютера можна створити у службі Microsoft OneDrive. Щоб підвищити рівень конфіденційності, відомості надсилаються в зашифрованій формі за протоколом SSL.

У засобі BitLocker можна настроїти шифрування даних за допомогою сертифіката, збереженого на смарт-картці. У разі захисту диска з даними за допомогою смарт-картки відкритий ключ і унікальний ідентифікатор смарт-картки зберігаються на диску в незашифрованому вигляді. Ці відомості можна використовувати для пошуку сертифіката, який початково використовувався для створення сертифіката шифрування смарт-картки.

Якщо ПК оснащено апаратними засобами безпеки з модулем TPM щонайменше версії 1.2, засіб BitLocker використовує модуль TPM для забезпечення розширеного апаратного захисту даних для диска, на якому інстальовано ОС Windows. Для отримання додаткових відомостей див. розділ «Служби TPM». На оснащеному модулем TPM ПК можна також задати особистий ідентифікаційний номер (PIN-код), який допоможе додати ще один рівень захисту для шифрованих даних. Засіб BitLocker зберігатиме цей заданий у модулі TPM PIN-код на диску в гешованій і шифрованій формі.

Відомості, зібрані засобом BitLocker, не надсилатимуться до корпорації Майкрософт, окрім як у разі резервного копіювання ключа відновлення до служби OneDrive за бажанням користувача.

Використання інформації

Криптографічні ключі та глобальні унікальні ідентифікатори (GUID)

зберігаються в пам’яті ПК для виконання операцій у засобі BitLocker. Відомості про відновлення в засобі BitLocker дають змогу отримати доступ до захищених даних у разі виникнення неполадок у роботі устаткування та інших проблем. Ці відомості про відновлення дають змогу засобу BitLocker відрізнити авторизованих користувачів від неавторизованих.

Корпорація Майкрософт не використовує індивідуальні ключі відновлення з жодною метою. У разі надсилання ключів відновлення до служби OneDrive корпорація Майкрософт може використовувати агреговані дані про них для аналізу тенденцій і вдосконалення своїх продуктів і служб.

Вибір і керування

За замовчуванням засіб BitLocker вимкнуто. На знімному носії будь-який користувач може будь-коли ввімкнути або вимкнути засіб BitLocker, відкривши вікно BitLocker Drive Encryption на Панелі керування. Адміністратор може ввімкнути або вимкнути BitLocker для всіх дисків.

Ключі відновлення, що зберігаються в обліковому записі OneDrive, доступні для перегляду й керування .

На початок сторінки

Контакти

Властивості та завдання

Якщо для керування контактами використовується програма Люди або аналогічна підтримувана програма стороннього виробника, можна настроїти відображення відомостей про контакт у картці контакту або надання іншим програмам на ПК доступу до інформації про вибрані контакти чи до конкретних даних, необхідних для виконання певної дії, скажімо, здійснення виклику або пошуку адреси на карті.

Збирання, обробка, зберігання та передавання інформації

У системі Windows можна вибирати контакти, до чиїх даних надаватиметься доступ програмам, що використовують відомості про контакти. Ці контакти вибираються зі списку програми Люди

або аналогічної підтримуваної програми стороннього виробника. Програма, що надіслала запит, не отримує від системи Windows доступу до даних усіх контактів у списку.

Якщо програмі дозволено використовувати певні дані щодо одного з контактів, скажімо, номер його телефону або адресу електронної пошти, система Windows відображає картку контакту з додатковими відомостями про цього користувача, отриманими з програми для керування контактами. Система Windows не надає доступу до додаткових відомостей, відображуваних у картці контакту, жодній програмі.

Якщо на картці контакту вибрати команду **Зателефонувати**, **Надіслати листа**або **Знайти на карті** , ОС Windows відкриє відповідну програму та надасть їй доступ до даних, потрібних для виконання цієї команди (наприклад, телефонний номер для здійснення виклику).

Використання інформації

ОС Windows використовує відомості про контакт, що містяться у програмі для керування контактами, для надання іншим програмам доступу до відомостей про вказані вами контакти, відображення карток контактів, запуску програм та надання їм контактних даних, необхідних для виконання дій, перерахованих у картці контакту, а також для відображення контактів у службі пошуку Windows Search. Особливості використання відомостей про контакти програмою Люди описані в декларації про конфіденційність програм для соціальних мереж.

Якщо доступ до відомостей про контакти надається програмі стороннього виробника, ці відомості використовуватимуться нею у відповідності до правил забезпечення конфіденційності, визначених таким виробником. Якщо доступ до відомостей про контакти надається програмі Microsoft, особливості використання нею цих відомостей можна переглянути у декларації про конфіденційність цієї програми.

Вибір і керування

Система Windows відображає відомості про контакти та надає програмам доступ до них лише в разі вибору користувачем

відповідних настройок.

На початок сторінки

Виявлення та встановлення пристрою

У системі Windows є кілька функцій, які допомагають виявляти та настроювати пристрої на ПК, зокрема встановлення пристрою, установлення пристрою для мобільного широкосмугового зв’язку, виявлення мережі та створення пари з безпровідним пристроєм.

Установлення пристрою

Властивості та завдання

У разі встановлення нового пристрою на ПК система Windows може автоматично знайти, завантажити та інсталювати програмне забезпечення його драйвера. ОС Windows може також завантажити відомості про пристрій, наприклад його опис, зображення та емблему виробника. Для певних пристроїв, зокрема деяких принтерів, веб-камер, мобільних широкосмугових пристроїв і портативних пристроїв, що синхронізуються з ОС Windows, створено спеціальні програми, що активують всі функціональні можливості пристрою та підвищують зручність його використання. Якщо виробник пристрою надає для нього програму, ОС Windows може автоматично завантажити та інсталювати цю програму з Магазину Windows, якщо ви зареєстровані в Магазині.

Збирання, обробка та передавання інформації

Під час пошуку драйверів ОС Windows звертається до служби Windows Update через Інтернет для пошуку та завантаження драйверів пристрою, якщо на ПК користувача відповідний драйвер ще недоступний. Докладніше про відомості, які збирає служба Windows Update, і їх використання див. в декларації про конфіденційність для служб оновлення.

Щоб отримати відомості про пристрій і визначити, чи є для нього програма, ОС Windows надсилає до корпорації Майкрософт дані про цей пристрій, зокрема його ідентифікатор (наприклад, ідентифікатор устаткування або ідентифікатор моделі), регіон або мову, а також дату його останнього оновлення. За наявності програми для пристрою ОС Windows автоматично завантажує її з

Магазину Windows та інсталює. Програма стане доступною в обліковому записі Магазину Windows у списку ваших власних програм.

Використання інформації

Відомості, що надсилаються до корпорації Майкрософт, допомагають визначити та завантажити для пристрою правильний драйвер, відомості та програму. Корпорація Майкрософт не використовує надіслані відомості для встановлення особи користувача або звернення до нього.

Вибір і керування

У разі вибору швидкого настроювання під час інсталяції Windows вмикається автоматичне завантаження та інсталяція драйверів, відомостей про пристрої і програм для пристроїв. У разі вибіркової інсталяції користувач може ввімкнути або вимкнути автоматичне завантаження та інсталяцію драйверів, програм і відомостей для пристроїв за допомогою параметра **Автоматично завантажувати драйвери, програми та інформацію для нових пристроїв** у розділі **Допомога в питаннях захисту та оновлення ПК**. Після інсталяції Windows можна змінити ці настройки на Панелі керування. Для цього слід вибрати завдання Змінення параметрів встановлення пристроїв, а потім – пункт **Ні, я хочу вирішувати самостійно**.

Програму пристрою можна видалити будь-коли, не відключаючи сам пристрій, однак майте на увазі, що без неї певні функції пристрою можуть стати недоступними. Після видалення програму пристрою можна інсталювати повторно, власноруч відкривши список програм у Магазині Windows.

Установлення мобільного пристрою для широкосмугового зв’язку

Властивості та завдання

Якщо ПК оснащено устаткуванням для мобільного широкосмугового зв’язку, що надається певними операторами мобільної мережі, ОС Windows може автоматично завантажити та інсталювати програму, яка дає змогу керувати обліковими записами й тарифним планом такого мобільного оператора. Щоб

мобільне широкосмугове підключення відображалося у списку мереж, завантажуються також додаткові відомості про пристрій.

Збирання, обробка та передавання інформації

Щоб визначити, які відомості про пристрій і яку програму потрібно завантажувати, ОС Windows надсилає частину ідентифікаторів мобільного широкосмугового устаткування, які дають змогу ідентифікувати оператора мобільного зв’язку. Щоб покращити захист конфіденційності, ОС Windows не надсилає повні ідентифікатори мобільного широкосмугового устаткування до корпорації Майкрософт.

Якщо оператор мобільного зв’язку надав програму корпорації Майкрософт, система Windows завантажить її з Магазину Windows та інсталює на ПК. Якщо відкрити програму після її інсталяції, вона отримає доступ до устаткування для мобільного широкосмугового зв’язку, зокрема ідентифікаторів устаткування, які оператор мобільного зв’язку може використовувати для ідентифікації облікового запису.

Використання інформації

Корпорація Майкрософт використовує частину надісланого ОС Windows ідентифікатора устаткування для мобільного широкосмугового зв’язку для визначення програми оператора, яка має бути інстальована на комп’ютері. Після інсталяції програма може використовувати ідентифікатори устаткування для мобільного широкосмугового зв’язку. Наприклад, програма оператора мобільного зв’язку може використовувати ці ідентифікатори для пошуку відомостей про обліковий запис і тарифний план через Інтернет. Програма використовуватиме ці відомості відповідно до процедур забезпечення конфіденційності, яких дотримується оператор мобільного зв’язку.

Вибір і керування

У разі вибору швидкого настроювання під час першого настроювання ОС Windows система Windows автоматично перевірить наявність програм оператора мобільного зв’язку та завантажить доступні. Увімкнути та вимкнути цю функцію можна на Панелі керування. Додаткові відомості див. в розділі «Установка

пристрою» вище.

Програму оператора мобільного зв’язку можна видалити будь-коли, і для цього не потрібно відключати устаткування для мобільного широкосмугового зв’язку.

Пошук мережі

Властивості та завдання

У разі підключення ПК до невеликої приватної мережі, наприклад домашньої, система Windows може автоматично виявити інші ПК та надати спільний доступ до пристроїв у мережі, а також зробити ПК видимим для інших пристроїв у мережі. За наявності спільних пристроїв ОС Windows може автоматично підключитися до них і виконати їх встановлення. До спільних пристроїв, зокрема, належать принтери та медіарозширювачі, але не належать такі особисті пристрої, як камери та мобільні телефони.

Збирання, обробка та передавання інформації

Якщо ввімкнуто спільний доступ і підключення до пристроїв, відомості про ПК, зокрема його ім’я та мережева адреса, можуть передаватися через канал широкосмугового зв’язку локальної мережі, щоб інші ПК могли виявити його та підключитися до нього.

Щоб визначити, чи слід автоматично встановлювати пристрої, підключені до мережі, система збирає відомості про мережу та надсилає їх до корпорації Майкрософт. До цих відомостей належить кількість пристроїв у мережі, тип мережі (наприклад, приватна мережа), а також типи та назви моделей пристроїв у мережі. Особисті відомості, такі як мережеве ім’я або пароль, не збираються.

Залежно від настройок установлення пристроїв, коли ОС Windows установлює спільні пристрої, система Windows може надсилати певні відомості до корпорації Майкрософт та інсталювати програмне забезпечення пристрою на ПК. Додаткові відомості див. в розділі «Установка пристрою».

Використання інформації

До корпорації Microsoft надсилаються відомості про використовувану мережу, які дають змогу визначити в мережі

пристрої, що мають установлюватися автоматично. Корпорація Майкрософт не використовує ці відомості для встановлення особи користувача, зв'язку з ним або надсилання реклами.

Вибір і керування

Якщо ввімкнути спільний доступ і підключитися до пристроїв під час приєднання до мережі, для цієї мережі буде ввімкнуто виявлення мережевих ресурсів. Цю настройку можна змінити для поточної мережі, вибравши тип мережі, зазначений під ім'ям мережі в Центрі мереж і спільного доступу.

Виявлення мережевих ресурсів загалом і автоматичне встановлення підключених до мережі пристроїв можна ввімкнути, вибравши команду **Змінити додаткові параметри спільного доступу** в Центрі мережевих підключень і спільного доступу.

Створення пари з безпровідним пристроєм

Властивості та завдання

Система Windows дає змогу створювати пари між ПК та безпровідними пристроями, у яких використовується технологія Bluetooth або Wi-Fi Direct. Wi-Fi Direct – це безпровідна технологія, яка дає змогу пристроям взаємодіяти безпосередньо, без підключення до мережі Wi-Fi.

Збирання, обробка та передавання інформації

Якщо вибрати параметр **Дозволити пристроям Bluetooth знаходити цей комп'ютер** у настройках Bluetooth, ОС Windows передаватиме ім'я ПК через Bluetooth, щоб пристрої з підтримкою Bluetooth могли виявляти його та ідентифікувати.

Якщо вибрати параметр **Додати пристрій** у настройках ПК, ОС Windows передаватиме ім'я ПК через Wi-Fi, щоб пристрої з підтримкою Wi-Fi Direct могли виявляти його та ідентифікувати. Якщо закрити вікно **Додати пристрій**, ОС Windows припинить передавання імені ПК через мережу Wi-Fi.

Залежно від настройок установлення пристроїв, коли ОС Windows створює пару з безпровідним пристроєм, система Windows може надсилати певні відомості до корпорації Майкрософт та інсталювати програмне забезпечення пристрою на ПК. Додаткові

відомості див. в розділі «Установка пристрою» вище.

Використання інформації

Система Windows передає ім’я ПК на всі інші пристрої, щоб вони мали змогу ідентифікувати ПК та підключитися до нього. Ім’я ПК до корпорації Майкрософт не надсилається.

Вибір і керування

Щоб увімкнути або вимкнути в ОС Windows передавання імені ПК через Bluetooth, натисніть і утримуйте або клацніть правою кнопкою піктограму свого ПК у розділі «Пристрої та принтери» на Панелі керування, виберіть **Параметри Bluetooth**, а потім виберіть **Дозволити пристроям Bluetooth знаходити цей комп’ютер**. Щоб система Windows не передавала ім’я ПК через Wi-Fi, перед додаванням пристрою тимчасово вимкніть Wi-Fi у розділі «Безпровідне» у настройках ПК.

На початок сторінки

Шифрування пристрою

Властивості та завдання

Шифрування пристрою виконується за технологією BitLocker Drive Encryption і допомагає захистити дані та запобігти програмним атакам в автономному режимі. Якщо шифрування пристрою ввімкнуто, система Windows шифрує дані на диску, на якому інстальовано ОС Windows.

Збирання, обробка та передавання інформації

У разі використання програмного шифрування, система постійно виконуватиме шифрування та розшифровування даних у процесі їх зчитування та записування на захищений диск за допомогою криптографічного ключа, що зберігається в пам’яті. У разі використання апаратного шифрування, шифрування та розшифровування даних виконуватиметься диском.

В ОС Windows для збереження криптографічних ключів, що застосовуються для шифрування диска, і керування цими ключами використовується наявний на ПК модуль TPM. Якщо шифрування пристрою ввімкнуто, ОС Windows автоматично шифрує диск, на

якому інстальовано ОС Windows, і створює ключ відновлення. Ключ відновлення дає змогу отримати доступ до захищених даних у разі певних неполадок устаткування та інших проблем.

Копія ключа відновлення BitLocker для ПК автоматично зберігається в Інтернеті в обліковому записі MicrosoftOneDrive для кожного облікового запису адміністратора, який підключено до облікового запису Microsoft. Для ключа відновлення в тому ж обліковому записі OneDrive зберігаються його ідентифікатор та ім’я відповідного комп’ютера. Щоб підвищити рівень конфіденційності, відомості надсилаються в зашифрованій формі за протоколом SSL.

Використання інформації

Криптографічні ключі та глобальні унікальні ідентифікатори (GUID) зберігаються в пам’яті ПК для виконання операцій у засобі BitLocker. Відомості для відновлення дають змогу отримувати доступ до захищених даних у разі певних неполадок устаткування та інших проблем і забезпечують засобу BitLocker можливість відрізнити авторизованих користувачів від неавторизованих

Корпорація Майкрософт зберігає резервну копію відомостей для відновлення в обліковому записі OneDrive, тому до них можна отримати доступ через Інтернет. Дані про ключ відновлення не використовуються корпорацією Майкрософт і зберігаються лише в обліковому записі служби OneDrive. Корпорація Майкрософт може використовувати агреговані дані про ключі відновлення для аналізу тенденцій і вдосконалення продуктів і служб. Наприклад, ці відомості можуть використовуватися для визначення відсотку ПК, на яких увімкнуто шифрування пристрою.

Вибір і керування

Якщо під час настроювання ПК використовується обліковий запис Microsoft, шифрування пристрою буде ввімкнуто (за умови, що ПК підтримує цю функцію), а резервна копія ключа відновлення зберігатиметься в обліковому записі користувача у службі OneDrive. Якщо під час настроювання ПК використовується локальний обліковий запис, шифрування пристрою вимкнуто.

Якщо згодом підключити обліковий запис Microsoft до облікового запису адміністратора на ПК, відбудеться ось що.

- Якщо шифрування пристрою ще не ввімкнуто, система Windows увімкне його автоматично та створить резервну копію відомостей для відновлення в обліковому записі користувача у службі OneDrive.
- Якщо шифрування пристрою вже ввімкнуто, резервну копію відомостей для відновлення буде збережено в обліковому записі OneDrive.

Переглянути ключі відновлення, які зберігаються в обліковому записі OneDrive, і керувати ними можна тут.

На початок сторінки

DirectAccess

Властивості та завдання

DirectAccess, за наявності на ПК підключення до Інтернету, забезпечує можливість безперебійного віддаленого підключення до мережі на роботі, хай би де ви в цей момент перебували.

Збирання, обробка та передавання інформації

Під час кожного ввімкнення ПК засіб DirectAccess намагатиметься підключитися до мережі на роботі, навіть якщо ви цієї миті перебуваєте за межами офісу. Після підключення ПК завантажить політики для робочого місця та забезпечить доступ до настроєних ресурсів у мережі на роботі. Адміністратор робочого комп'ютера використовує можливості підключення DirectAccess для здійснення віддаленого моніторингу вашого ПК та керування ним, зокрема він може обмежити вам доступ до певних веб-сайтів, навіть якщо ви в цей момент перебуваєте не на робочому місці.

DirectAccess не надсилає жодних відомостей до корпорації Майкрософт.

Використання інформації

Правила збирання відомостей адміністратором робочого комп'ютера визначаються політиками компанії.

Вибір і керування

Адміністратор робочого комп'ютера має настроїти в DirectAccess використання групової політики. Адміністратор може дозволити тимчасово вимикати деякі елементи DirectAccess, однак припинити спроби системи Windows підключитися до робочого місця для здійснення керування може лише адміністратор робочого комп'ютера. Якщо ви або адміністратор робочого комп'ютера видалите ПК з домену в мережі на роботі, засіб DirectAccess більше не зможе встановлювати підключення.

На початок сторінки

Центр легкого доступу

Властивості та завдання

Центр легкого доступу дає змогу ввімкнути параметри та настройки спеціальних можливостей, які спрощують взаємодію з ПК.

Збирання, обробка та передавання інформації

Якщо використовується ця функція, буде запропоновано вибрати твердження, що відповідають вашій ситуації.

Пропонуються такі твердження.

- Погано видно зображення та текст на екрані телевізора.
- Умови освітлення ускладнюють перегляд зображень на моніторі.
- Я не користуюся клавіатурою.
- Я сліпий.
- Я глухий.
- У мене є вади мовлення.

Ці відомості зберігаються в не придатному для читання людиною форматі локально на ПК.

Використання інформації

На основі вибраних вами тверджень пропонується низка

рекомендацій щодо настроювання. Ці відомості не надсилаються до корпорації Майкрософт і не доступні нікому, крім вас і адміністраторів вашого ПК.

Вибір і керування

Щоб вибрати необхідні варіанти, відкрийте Центр легкого доступу на Панелі керування. Вибрані твердження можна будь-коли змінити. Крім того, можна вибрати рекомендації, яких слід дотримуватися на ПК.

На початок сторінки

Переглядач подій

Властивості та завдання

Користувачі ПК (переважно адміністратори) можуть скористатися переглядачем подій для перегляду журналів подій і керування ними. Журнал подій містить відомості про устаткування, програмне забезпечення та події системи безпеки ПК. Відомості про події в журналах подій можна також дізнатися в корпорації Майкрософт, скориставшись онлайновою довідкою журналу подій.

Збирання, обробка та передавання інформації

Журнали подій містять відомості про події, зареєстровані під час роботи всіх користувачів і програм на ПК. За замовчуванням записи журналу подій можуть переглядати всі користувачі; проте адміністратори можуть обмежити доступ до цих журналів. Щоб отримати доступ до журналів подій на ПК, слід відкрити переглядач подій. Щоб дізнатися про те, як відкрити переглядач подій, скористайтеся Центром довідки та підтримки Windows.

У разі використання онлайнової довідки журналу подій для пошуку додаткових відомостей про певну подію відомості про подію надсилаються до корпорації Майкрософт.

Використання інформації

У разі використання онлайнової довідки журналу подій для пошуку інформації про подію, пов’язані з нею дані, що надсилаються з ПК, використовуються для визначення місцезнаходження та надання додаткових відомостей про цю подію. Для подій Microsoft відомості

про подію надсилатимуться до корпорації Майкрософт. Корпорація Майкрософт не використовує ці відомості для встановлення особи користувача, зв'язку з ним або надсилання реклами. Для подій, пов'язаних із програмами стороннього виробника, відомості надсилатимуться в розташування, зазначене стороннім видавцем або виробником. У разі надсилання відомостей про події стороннім видавцям або виробникам, до цієї інформації застосовуватимуться процедури забезпечення конфіденційності відповідних третіх сторін.

Вибір і керування

Адміністратори можуть обмежити доступ до журналів подій. Користувачі, які мають повний доступ до журналів подій, можуть видаляти їх. Якщо ви ще не давали згоди на автоматичне надсилання відомостей про подію, після вибору посилання на онлайнову довідку для журналу подій відобразиться запит для підтвердження вашої згоди на надсилання зазначених відомостей через Інтернет. Жодна інформація журналу подій не передається через Інтернет без вашої згоди. Адміністратори можуть на основі групової політики вибрати або змінити сайт, на який надсилаються відомості про подію.

На початок сторінки

Безпека сім'ї

Властивості та завдання

Безпека сім'ї допомагає батькам захистити дітей, коли ті користуються ПК. Батьки можуть визначати, якими програмами, іграми та веб-сайтами дозволено користуватися дітям. Батьки можуть також установити часові обмеження та регулярно отримувати електронною поштою звіти про дії. Батьки можуть керувати обмеженнями та переглядати звіти про дії локально на ПК або в Інтернеті за допомогою веб-сайту Безпеки сім'ї (Microsoft).

Збирання, обробка та передавання інформації

Настройки Безпеки сім'ї та звіти про дії дітей зберігаються на ПК. Звіти про дії можуть містити відомості про час, проведений за

комп’ютером, час, протягом якого використовувалися окремі програми та ігри, а також інформацію про відвідані веб-сайти (а також про спроби переглянути заблоковані веб-сайти). Адміністратори на ПК можуть змінювати настройки та переглядати звіт про дії.

Якщо для облікового запису дитини ввімкнуто керування через Інтернет, батьки можуть переглянути звіт про дії дитини та змінити настройки на веб-сайті Безпеки сім’ї (Microsoft). Батьки можуть дозволити будь-кому переглядати звіти про дії та змінювати настройки, додавши відповідного користувача із правами дорослого на веб-сайті Безпеки сім’ї (Microsoft). Якщо один із батьків із правом настроювати Безпеку сім’ї увійшов до системи Windows за допомогою облікового запису Microsoft, керування через Інтернет вмикається автоматично.

Якщо для облікового запису дитини настроєно Безпеку сім’ї з увімкнутим керуванням через Інтернет, батькам автоматично надсилатимуться електронною поштою тижневі звіти про дії дитини.

Використання інформації

Система Windows і веб-сайт Безпеки сім’ї (Microsoft) використовують зібрані відомості для забезпечення роботи засобу безпеки сім’ї. Корпорація Майкрософт може аналізувати відомості, що містяться в журналі дій, в агрегованому вигляді для оцінки якості даних, але не використовуватиме їх для встановлення особи користувача, зв’язку з ним або надсилання реклами.

Вибір і керування

Безпеку сім’ї вимкнуто за замовчуванням. Щоб отримати доступ до Безпеки сім’ї, відкрийте розділ «Безпека сім’ї» на Панелі керування. Безпеку сім’ї можуть увімкнути лише адміністратори, а моніторинг і обмеження можна застосовувати лише для користувачів без прав адміністрування. Діти можуть переглянути свої настройки, але не можуть їх змінити. Якщо Безпеку сім’ї ввімкнуто, під час кожного входу до системи Windows дитина отримуватиме сповіщення про те, що її обліковий запис перебуває під наглядом Безпеки сім’ї. Якщо під час створення облікового запису вказано, що він належить дитині, для такого облікового

запису можна за бажання ввімкнути Безпеку сім'ї.

Якщо адміністратор, який настроїв обліковий запис дитини, входить до системи Windows за допомогою облікового запису Microsoft, керування через Інтернет вмикається автоматично та щотижня надсилаються звіти про дії дитини. Облікові записи батьків можна додати або видалити на веб-сайті Безпеки сім'ї (Microsoft). Будь-який користувач, доданий із правами дорослого на веб-сайті, може переглянути звіт про дії дитини та змінити настройки Безпеки сім'ї, навіть якщо він не є адміністратором на ПК, який використовує дитина.

Для належного використання Безпеки сім'ї адміністраторами на ПК мають бути лише дорослі. Дітям права адміністратора надавати не слід. Зауважте, що використання цієї функції для стеження за іншими користувачами (зокрема, дорослими) може вважатися порушенням відповідного закону.

На початок сторінки

Факс

Властивості та завдання

Функція факсу дає змогу створювати та зберігати титульні сторінки факсів, а також надсилати та отримувати факси за допомогою ПК та зовнішнього або вбудованого факс-модему або факс-сервера.

Збирання, обробка та передавання інформації

Збираються, зокрема, особисті відомості, введені на титульній сторінці факсу, а також ідентифікатори, записані в галузевих протоколах факсимільного зв'язку, такі як код абонента-відправника (TSID) і код абонента виклику (CSID). За замовчуванням Windows присвоює кожному ідентифікатору значення «Fax».

Використання інформації

Відомості, введені в діалоговому вікні відправника, відображаються на титульній сторінці факсу. Такі ідентифікатори, як TSID і CSID, можуть містити довільний текст і зазвичай використовуються для того, щоб факсимільний апарат або ПК, що отримують факс, могли

ідентифікувати відправника. До корпорації Майкрософт відомості не надсилаються.

Вибір і керування

Доступ до факсу залежить від прав, наданих на ПК обліковому запису користувача. Якщо адміністратор факсу не змінить настройки доступу, надсилати та приймати факси можуть усі користувачі. За замовчуванням усі користувачі можуть переглядати надіслані ними документи та будь-які факси, отримані на ПК. Адміністратори можуть переглядати всі факсимільні повідомлення, надіслані або прийняті, і можуть настроювати параметри факсу, зокрема встановлювати дозволи на перегляд факсів і керування ними, а також указувати значення TSID і CSID.

На початок сторінки

Персоналізація рукописного тексту – автоматичне навчання

Властивості та завдання

Автоматичне навчання – це засіб для персоналізації розпізнавання рукописного тесту, доступний на ПК із сенсорним екраном. Ця функція збирає дані про використовувані слова та спосіб їх написання. Це допомагає програмному забезпеченню для розпізнавання рукописного тексту вдосконалювати інтерпретацію рукописного стилю користувача, поповнювати словник і вдосконалювати автокоригування та пропозиції тексту для мов без редакторів засобів вводу (IME).

Збирання, обробка та передавання інформації

Відомості, зібрані функцією автоматичного навчання зберігаються на ПК у профілі кожного користувача. Дані зберігаються в закритому форматі, який неможливо прочитати за допомогою програм для перегляду тексту (наприклад, Блокноту або WordPad), і доступні іншим користувачам, якщо вони є адміністраторами на цьому ПК.

Зібрана інформація включає:

- Текст зі складених повідомлень і записів календаря, створених поштовими програмами (наприклад, Office Outlook

або Windows Live Mail), включно з усіма вже надісланими повідомленнями.

- Рукописний ввід на панелі вводу.
- Розпізнаний текст рукописного вводу, створеного на панелі вводу, або текст, набраний на сенсорній клавіатурі.
- Символи для заміни, вибрані вами для виправлення розпізнаного тексту.

Використання інформації

Зібрані відомості використовуються для вдосконалення розпізнавання рукописного тексту шляхом створення персональної версії програмного забезпечення для розпізнавання відповідно до вашого стилю та лексики, а також забезпечення автоматичного виправлення та пропонування тексту під час введення на сенсорних клавіатурах.

Зразки тексту використовуються для створення розширеного словника. Для вдосконалення розпізнавання рукописного тексту для кожного користувача на ПК використовуються зразки рукописного вводу. До корпорації Майкрософт відомості не надсилаються.

Вибір і керування

Автоматичне навчання ввімкнуто за замовчуванням. Автоматичне навчання можна будь-коли ввімкнути або вимкнути на вкладці **Додаткові настройки** в розділі **Мови** на Панелі керування. Після вимкнення функції автоматичного навчання зібрані дані, що досі зберігалися, видаляються.

На початок сторінки

Домашня група

Властивості та завдання

Система Windows надає змогу легко зв’язувати комп'ютери в домашній мережі для обміну зображеннями, музикою, відео та документами, а також для спільного використання пристроїв. Вона

також забезпечує можливість потокового передавання мультимедійних даних із ПК на пристрої в домашній мережі, наприклад на медіарозширювачі. Ці ПК та пристрої утворюють домашню групу. Домашню групу можна захистити паролем. Крім того, можна вибрати об’єкти, до яких надається спільний доступ.

Збирання, обробка та передавання інформації

Власні файли користувача, такі як зображення, відео, музика та документи будуть доступними з будь-якого ПК в домашній групі. Після приєднання до домашньої групи іншим користувачам у цій групі буде надано спільний доступ до відомостей про всі облікові записи Microsoft на вашому ПК (зокрема, до адрес електронної пошти, коротких імен і зображень), що дасть змогу спільно використовувати дані разом із цими користувачами.

Використання інформації

Зібрані відомості дають змогу комп'ютерам у домашній групі правильно визначати, кому надається спільний доступ до вмісту та яким чином він має бути представлений. До корпорації Майкрософт відомості не надсилаються.

Вибір і керування

У домашній групі можна додавати та видаляти ПК, а також вказувати вміст, до якого надаватиметься спільний доступ іншим членам домашньої групи. Для створення домашньої групи та керування її настройками потрібно перейти до розділу **Домашня група** у розділі **Мережа** в настройках ПК.

На початок сторінки

Редактор засобів вводу (IME)

Редактори засобів вводу (IME) Microsoft використовуються для східноазійських мов із метою перетворення введених на клавіатурі символів на ієрогліфи. У цьому розділі розглянуто кілька функцій, зокрема автокоригування та прогнозування в редакторі IME, звітування про помилки перетворення в редакторі IME, а також реєстрація в ньому слів.

Пропозиції редактора IME із хмари

Властивості та завдання

Коли редактор Microsoft Pinyin IME використовується для введення спрощених китайських символів, він може звертатися до онлайнових служб із метою пошуку ієрогліфів-відповідників для введених символів, якщо такі відсутні в локальному словнику на ПК.

Збирання, обробка та передавання інформації

Під час введення спрощених китайських символів за допомогою редактора Microsoft Pinyin IME вам пропонуються для них відповідні варіанти ієрогліфів. Якщо редактор IME не знаходить потрібний ієрогліф у локальному словнику, він надсилає введені із клавіатури символи до корпорації Майкрософт, щоб отримати для них більш вдалі відповідники, якщо такі наявні. Якщо такі варіанти є, вони відобразяться у списку пропозицій, а в разі їх вибору додаватимуться до локального словника. До корпорації Майкрософт також надсилатиметься довільно згенерований унікальний ідентифікатор для аналізу використання цієї функції. Ідентифікатор не пов’язаний з обліковим записом Microsoft і не використовуватиметься для встановлення особи користувача, зв’язку з ним або надсилання реклами.

Використання інформації

Корпорація Майкрософт використовує зібрані відомості для пошуку ієрогліфів у хмарі та покращення своїх продуктів і служб. Вони не використовуються для встановлення особи користувача, зв’язку з ним або надсилання реклами.

Вибір і керування

Для китайської мови (спрощене письмо) пропозиції редактора IME із хмари за замовчуванням вимкнуто в редакторі Microsoft Pinyin IME. Щоб переглянути або змінити ці настройки, зайдіть у розділ **Час і мова**у настройках ПК, там відкрийте вікно **Регіональні та мовні параметри**, виберіть потрібну мову, а тоді клацніть пункт **Параметри**.

Автоматичне коригування та прогнозування в редакторі IME

Властивості та завдання

Залежно від використовуваного редактора IME й вибраних настройок засоби автоматичного коригування та пропонування тексту запам'ятовують слова або послідовності слів для подальшого відображення на екрані більш точних пропозицій ієрогліфів.

Збирання, обробка та передавання інформації

Функції автоматичного коригування (самонавчання) та пропонування тексту в редакторі IME реєструють вживані слова або послідовності слів, а також частоту їх використання. Відомості для автоматичного коригування (за винятком послідовностей цифр і символів) зберігаються у файлах для кожного користувача на ПК.

Використання інформації

Дані для автоматичного навчання та пропонування тексту використовуються редактором IME на ПК для вдосконалення функції підбору ієрогліфів, що відображатимуться у цьому редакторі. Якщо вибрати надсилання цих даних до корпорації Майкрософт, вони використовуватимуться для вдосконалення редактора IME та супутніх продуктів і служб.

Вибір і керування

У тих редакторах IME, які підтримують функції автоматичного навчання та пропонування слів, ці функції увімкнуто за замовчуванням. Зібрані дані не надсилаються автоматично до корпорації Майкрософт. Увімкнути або вимкнути збирання або надсилання цих даних можна в розділі «Мова» на Панелі керування.

Повідомлення про помилки перетворення в редакторі IME

Властивості та завдання

Ці функції збирають відомості про помилки представлення ієрогліфів або перетворення введених на клавіатурі символів на ієрогліфи, щоб допомогти корпорації Майкрософт вдосконалити свої продукти та служби.

Збирання, обробка та передавання інформації

Функція повідомлення про помилки перетворення IME збирає відомості про помилки перетворення IME, наприклад дані про текст, набраний на клавіатурі, перше перетворення або результати прогнозування, вибраний натомість рядок, відомості про редактор IME та особливості його використання. Крім того, у разі використання редактора IME для японської мови можна за необхідності включити до звітів про помилки перетворення відомості про автоматичне навчання.

Використання інформації

Корпорація Майкрософт використовує ці відомості для вдосконалення своїх продуктів і служб. Корпорація Майкрософт не використовує ці відомості для встановлення особи користувача, зв'язку з ним або надсилання реклами.

Вибір і керування

Коли накопичиться певна кількість зареєстрованих помилок перетворення, на екрані відобразиться запит від засобу звітування про неправильне перетворення із запитанням про те, чи слід надіслати звіт про помилки перетворення. У засобі звітування про помилки перетворення можна також у будь-який час вибрати надсилання звіту про помилки перетворення. Перед надсиланням звіту ви маєте змогу переглянути відомості, які він містить. У настройках редактора IME можна також увімкнути автоматичне надсилання звітів про помилки перетворення.

Реєстрація слів у редакторі IME

Властивості та завдання

У деяких редакторах IME можна скористатися функцією реєстрації слів для створення звіту про непідтримувані слова (слова, які не вдається правильно перетворити на ієрогліфи під час введення із клавіатури).

Збирання, обробка та передавання інформації

Звіти про реєстрацію містять інформацію про непідтримувані слова, надану користувачем у діалоговому вікні «Додавання слова», а також номер версії програмного забезпечення для редактора IME. Ці звіти можуть містити особисті відомості – наприклад, якщо під час реєстрації слів було додано власні назви

або імена. Перед надсиланням будь-якого звіту ви маєте змогу переглянути дані, які він містить.

Використання інформації

Корпорація Майкрософт використовує ці відомості для вдосконалення своїх продуктів і служб. Корпорація Майкрософт не використовує ці відомості для встановлення особи користувача, зв’язку з ним або надсилання реклами.

Вибір і керування

Щоразу під час створення звіту про реєстрацію слів відображатиметься запитання про те, чи слід надсилати цей звіт до корпорації Майкрософт. Перед надсиланням звіту можна завжди переглянути дані, які він містить.

На початок сторінки

Спільний доступ до Інтернету

Властивості та завдання

Завдяки технології спільного доступу до Інтернету можна надавати доступ до Інтернету через мобільне широкосмугове підключення іншим пристроям за допомогою Wi-Fi. Надання спільного доступу до Інтернету на пристрої мобільного широкосмугового зв’язку можна також розпочати віддалено з ПК, якщо вхід на мобільний пристрій і на ПК виконано за допомогою однакового облікового запису Microsoft.

Збирання, обробка та передавання інформації

Під час першого надання спільного доступу до Інтернету ОС Windows автоматично створить і збереже мережеве ім’я та пароль. Їх можна будь-коли змінити.

Якщо ПК підтримує таку функцію і його додано до облікового запису Microsoft як надійний пристрій, ОС Windows синхронізує мережеве ім’я та пароль з обліковим записом Microsoft. Система Windows також синхронізує інші відомості, які нададуть змогу віддалено розпочати надання спільного доступу до Інтернету з інших надійних пристроїв. До цих відомостей належать апаратна адреса радіомодуля Bluetooth і випадкове число, що

використовується для забезпечення безпеки з’єднання.

Використання інформації

Ці відомості використовуються для настроювання спільного доступу до Інтернету. Корпорація Майкрософт не використовує відомості для встановлення особи користувача, зв’язку з ним або надсилання реклами.

Вибір і керування

Якщо виконати вхід на пристрій, який підтримує спільний доступ до Інтернету, за допомогою облікового запису Microsoft і додати пристрій як надійний, відомості, необхідні для віддаленого ввімкнення спільного доступу до Інтернету, буде синхронізовано з OneDrive. Синхронізацію відомостей можна зупинити, відмовившись від синхронізації паролів. Додаткові відомості див. в розділі «Настройки синхронізації» на цій сторінці.

На початок сторінки

Друкування через Інтернет

Властивості та завдання

Завдяки цій технології можна друкувати матеріали через Інтернет.

Збирання, обробка та передавання інформації

Для використання цієї функції потрібно спочатку підключитися до сервера друку в Інтернеті й увійти на цей сервер, увівши необхідні облікові дані. Відомості, які необхідно надсилати на сервер друку, можуть бути різними, залежно від рівня безпеки, який підтримує сервер друку (наприклад, він може запитувати ім’я користувача та пароль). Після підключення відображається список сумісних принтерів. Якщо на ПК відсутній драйвер друку для вибраного принтера, його можна завантажити із сервера друку. Оскільки завдання для принтера не шифруються, надісланий вміст можуть побачити інші особи.

Використання інформації

Зібрана інформація дає вам змогу друкувати на віддалених принтерах. У разі вибору сервера друку, розміщеного в корпорації

Майкрософт, корпорація Майкрософт не використовуватиме надані відомості для встановлення особи користувача, зв’язку з ним або надсилання реклами. У разі надсилання відомостей на сервер друку третьої сторони, ця інформація використовуватиметься відповідно до процедур забезпечення конфіденційності цієї третьої сторони.

Вибір і керування

Щоб увімкнути або вимкнути друк через Інтернет, відкрийте на Панелі керування розділ **Програми та засоби** й виберіть завдання **Увімкнути або вимкнути засоби Windows**.

На початок сторінки

Мовні параметри

Властивості та завдання

Список мов у системі Windows 8.1 можна поповнити мовами, які ви плануєте часто використовувати. Програми та веб-сайти відображатимуться тією мовою, яку зазначено у списку першою.

Збирання, обробка та передавання інформації

Під час відвідування веб-сайтів та інсталяції програм на ПК список бажаних мов надсилається на відвідуваний веб-сайт і до нього надається доступ відповідним програмам, так що вміст можна буде отримати тими мовами, які ви найчастіше використовуєте.

Використання інформації

Список бажаних мов використовується веб-сайтами та програмами Microsoft для надання вмісту бажаними мовами. Корпорація Майкрософт не використовує жодні відомості про мови для встановлення особи користувача або зв’язку з ним. Використання інформації про мови, що надсилається на веб-сайти та застосовується програмами третіх сторін, здійснюватиметься відповідно до процедур забезпечення конфіденційності стороннього веб-сайту або видавця програми.

Вибір і керування

Список бажаних мов доступний для інстальованих програм і

відвідуваних веб-сайтів. Додати або видалити мови в цьому списку можна в розділі «Мовні параметри» на Панелі керування. Якщо в цьому списку немає мов, на відвідувані веб-сайти надсилатиметься мова, вибрана на вкладці «Формати» розділу «Регіон» Панелі керування.

На початок сторінки

Служби розташування

Служби розташування Windows дають змогу вказати, яким програмам, веб-сайтам і функціям Windows дозволено визначати розташування ПК. Служби розташування Windows складаються із двох компонентів. Засіб визначення розташування Windows підключається до онлайнової служби Microsoft для визначення розташування користувача. Платформа для визначення розташування Windows визначає розташування ПК за допомогою устаткування, наприклад датчика GPS, або такого програмного забезпечення, як засіб визначення розташування Windows.

Платформа визначення розташування Windows

Властивості та завдання

Якщо ввімкнуто платформу визначення розташування Windows, програми, інстальовані з Магазину Windows, а також деякі засоби Windows запитують дозвіл на доступ до відомостей про розташування ПК. Якщо дозволити програмі використовувати розташування, крім надання відомостей про розташування під час використання програми, платформа визначення розташування Windows сповіщає програмі, коли ПК перетинає географічні межі, визначені цією програмою. Наприклад, у програмі можна встановити нагадування про необхідність зайти після роботи в магазин і купити продуктів. Залежно від конфігурації системи платформа визначення розташування Windows може визначати розташування ПК за допомогою устаткування, наприклад датчика GPS, або такого програмного забезпечення, як засіб визначення розташування Windows.

Платформа визначення розташування Windows не перешкоджає програмам отримувати дані про розташування іншими способами.

Наприклад, деякі пристрої (скажімо, GPS-приймач) можуть надсилати відомості про розташування безпосередньо до програм, оминаючи платформу. Незалежно від настройок платформи визначення розташування Windows онлайнові служби можуть використовувати IP-адресу для визначення приблизного розташування (зазвичай, це місто, у якому наразі перебуває ПК).

Збирання, обробка та передавання інформації

Сама платформа визначення розташування Windows не передає жодних відомостей із ПК, але окремі засоби постачання даних про розташування (наприклад, засіб визначення розташування Windows) можуть передавати відомості, отримавши від платформи визначення розташування Windows запит на встановлення місцезнаходження ПК. Програми, веб-сайти та засоби, яким дозволено використовувати платформу з метою визначення розташування ПК, також передають або зберігають ці дані. Якщо програмою встановлені географічні межі, за перетином яких треба стежити, відомості про ці межі зберігаються в зашифрованому вигляді на ПК. До відомостей про ці межі належать ім’я, розташування й інформація про те, чи перебував ПК у встановлених межах останнього разу, коли визначалося його розташування. Програми, які встановлюють географічні межі, можуть передавати або зберігати ці відомості

Використання інформації

Якщо ввімкнути платформу визначення розташування Windows, авторизовані програми, веб-сайти та засоби Windows зможуть отримувати доступ до відомостей про місцезнаходження ПК та використовувати їх для надання персоналізованого вмісту. У разі використання програми або засобу визначення розташування від стороннього постачальника відомості про розташування ПК використовуватимуться відповідно до процедур забезпечення конфіденційності третьої сторони. Перед завантаженням програми з Магазину Windows з її опису можна дізнатися, чи використовує вона відомості про розташування.

Вибір і керування

Якщо вибрано експрес-настройки під час інсталяції Windows, платформа визначення розташування Windows вмикається

автоматично. Якщо застосовується настоювання параметрів, платформою визначення розташування Windows можна керувати, вибравши пункт «Дозволити системі Windows і програмам запитувати дані про розташування із платформи Windows для визначення розташування» в розділі «Надати доступ до відомостей корпорації Майкрософт і службам інших виробників». Коли програма з Магазину вперше запитує відомості про розташування ПК, в ОС Windows відобразиться запит на надання дозволу цій програмі використовувати дані про розташування. Цей параметр можна переглянути та змінити для кожної програми з Магазину Windows у розділі «Дозволи» в настройках відповідної програми.

У разі застосування класичної програми, що використовує платформу визначення розташування Windows, ця програма запитає дозвіл на використання даних про розташування ПК, і надалі, коли вона отримуватиме доступ до відповідних даних, в області сповіщень відображатиметься сповіщення про надання такого доступу. Кожен користувач може вибрати власні настройки розташування для програм із Магазину в розділі **Конфіденційність** у настройках ПК. Крім того, адміністратори можуть вимкнути платформу визначення розташування для всіх користувачів у розділі **Настройки розташування** на Панелі керування. Щоб програми не отримували сповіщень про перетинання визначених у них географічних меж, адміністратор може вимкнути на Панелі керування службу платформи Windows для визначення розташування.

Визначення розташування Windows

Властивості та завдання

Засіб визначення розташування Windows забезпечує підключення до онлайнової служби визначення розташування Microsoft, яка допомагає визначити приблизне розташування ПК за даними найближчих до нього мереж Wi-Fi і IP-адресою цього ПК.

Збирання, обробка та передавання інформації

Коли програма, якій користувач дозволив отримувати відомості про розташування, запитує ці відомості, платформа визначення розташування Windows надсилатиме запит усім інстальованим засобам визначення розташування (зокрема, засобу визначення

розташування Windows) для визначення поточного місцезнаходження. Засіб визначення розташування Windows спочатку перевірить, чи зберігся список точок доступу Wi-Fi після попереднього запиту програми, що використовує відомості про розташування. Якщо список найближчих точок доступу Wi-Fi відсутній або застарів, цей засіб надішле відомості про найближчі точки доступу Wi-Fi і дані GPS, за їх наявності, до служби визначення розташування Microsoft. Служба повертає дані про приблизне розташування ПК засобу визначення розташування Windows, а він передає ці дані платформі визначення розташування Windows, яка, у свою чергу, надає їх програмі, що запитувала ці дані. Засіб визначення розташування Windows може також оновити збережений список точок доступу Wi-Fi. Засіб визначення розташування Windows зберігає цей список, щоб для визначення приблизного розташування не потрібно було щоразу підключатися до Інтернету. Цей список точок доступу шифрується під час збереження на диску, тому програми не можуть отримувати до нього доступ безпосередньо.

Для найближчих точок доступу Wi-Fi надсилаються такі відомості, як BSSID (MAC-адреса точки доступу Wi-Fi) і рівень сигналу. Дані GPS включають зафіксовану широту, довготу, напрямок, швидкість і висоту над рівнем моря. Щоб покращити захист конфіденційності, засіб Windows не надсилає жодних відомостей для однозначної ідентифікації ПК, окрім стандартних відомостей про комп’ютер із даними про всі підключення до Інтернету. Для збереження конфіденційності власників мереж Wi-Fi, ОС Windows не надсилає відомості про ідентифікатори SSID (імена точок доступу Wi-Fi) і дані про приховані мережі Wi-Fi. З міркувань конфіденційності та безпеки дані про мережі Wi-Fi надсилаються в зашифрованому вигляді за протоколом SSL.

Якщо користувач вирішить посприяти вдосконаленню служби визначення розташування Microsoft, після того, як програма надішле запит на відомості про розташування ПК, ОС Windows може знову надіслати відомості про найближчі точки доступу Wi-Fi до корпорації Майкрософт. Якщо використовується лімітне підключення до Інтернету, ОС Windows надсилатиме ці відомості обмежену кількість разів протягом доби, щоб уникнути надмірного використання підключення до Інтернету.

Використання інформації

Засіб визначення розташування Windows використовує інформацію для надання відомостей про приблизне розташування ПК платформі визначення розташування Windows, коли тій надсилає відповідний запит авторизована програма.

Якщо ви вирішите посприяти вдосконаленню служби визначення розташування Microsoft, відомості про мережі Wi-Fi і дані системи GPS, надіслані до корпорації Майкрософт, використовуватимуться для покращення служб визначення розташування Microsoft, що, у свою чергу, сприятиме вдосконаленню служб визначення розташування, які надають відомості програмам на вашому ПК. Корпорація Майкрософт не зберігає жодні зібрані цією службою дані, які можна використовувати для встановлення особи, зв'язку з нею, надсилання реклами, відстеження місцезнаходження ПК або ведення журналу змін його розташування.

Вибір і керування

Засіб визначення розташування Windows використовується, лише коли від авторизованої програми надходить запит відомостей про розташування ПК. Додаткові відомості про те, як дозволити або заборонити надсилання програмами запитів відомостей про розташування, див. в розділі «Платформа визначення розташування Windows». Якщо програми авторизовано для запиту відомостей про розташування, кешований список розташувань найближчих точок доступу Wi-Fi, що шифрується та зберігається засобом визначення розташування Windows), періодично видалятиметься та замінюватиметься на новий.

Якщо вибрати швидке настроювання під час інсталяції Windows, автоматично ввімкнеться функція надання допомоги в удосконаленні служби визначення розташування Microsoft. У разі власноручного настроювання параметрів можна вказати, чи слід надавати допомогу в удосконаленні служби розташування Microsoft. Для цього виберіть пункт **Надсилати деякі дані про розташування до корпорації Майкрософт, якщо використовуються програми, функціонування яких залежить від розташування** у розділі **Допомога в покращенні продуктів і служб корпорації Майкрософт**.

Після інсталяції Windows цю настройку можна змінити в розділі «Настройки розташування» на Панелі керування. Навіть якщо ви відмовитеся допомагати нам удосконалювати службу, засіб визначення розташування Windows можна буде використовувати для визначення приблизного розташування ПК.

Увімкнути або вимкнути засіб визначення розташування Windows можна на вкладці **Увімкнути або вимкнути засоби Windows** на Панелі керування. Якщо визначення розташування Windows вимкнуто, можна скористатися іншими засобами постачання відомостей про розташування (наприклад, GPS) у поєднанні з платформою визначення розташування Windows.

На початок сторінки

Керування обліковими даними

Властивості та завдання

ОС Windows дає змогу підключати програми з Магазину Windows до облікових записів, що використовуються для веб-сайтів. Якщо пароль для веб-сайту було збережено у браузері Internet Explorer, ОС Windows може використовувати збережений пароль під час підключення програми до цього веб-сайту.

Збирання, обробка та передавання інформації

Коли у програмі відображається запит облікових даних для входу на веб-сайт, ці облікові дані можна зберегти. Якщо вхід на сайт за допомогою браузера Internet Explorer уже виконано й облікові дані збережено, ОС Windows автоматично підставить збережені облікові дані. Облікові дані зберігаються в зашифрованому вигляді на ПК. Додаткові відомості про ці та інші облікові дані, які можуть синхронізуватися зі сховищем OneDrive, див. в розділі «Настройки синхронізації» на цій сторінці.

Використання інформації

ОС Windows використовує збережені облікові дані лише для спрощення входу на вибрані веб-сайти. Якщо зберегти облікові дані під час підключення програми до веб-сайту, збережені облікові дані не використовуватимуться в браузері Internet Explorer або інших програмах.

Вибір і керування

Збереженими обліковими даними можна керувати за допомогою диспетчера облікових даних на Панелі керування. Додаткову інформацію про ці та інші облікові дані, які можуть синхронізуватися зі сховищем OneDrive, див. в розділі «Настройки синхронізації» на цій сторінці.

На початок сторінки

Ім’я та зображення облікового запису

Властивості та завдання

Для надання персоналізованого вмісту програми можуть запитувати в ОС Windows ім’я та зображення облікового запису. Ім’я та зображення облікового запису відображаються в підрозділі **Ваш обліковий запис** в розділі **Облікові записи** у настройках ПК. Якщо ввійти до Windows за допомогою облікового запису Microsoft, ОС Windows використовуватиме ім’я та зображення, пов’язані з цим обліковим записом. Якщо для облікового запису не вибрано зображення, для нього використовуватиметься зображення за замовчуванням, надане ОС Windows.

Збирання, обробка та передавання інформації

Якщо дозволити програмам доступ до імені та зображення облікового запису, ОС Windows надаватиме ці відомості всім програмам, які їх запитують. Програми можуть зберігати або передавати ці відомості.

Якщо виконати вхід до ОС Windows за допомогою облікового запису домену та дозволити програмам використовувати ім’я та зображення облікового запису, програмам, що можуть використовувати ваші облікові дані Windows, буде дозволено отримувати доступ до певних інших типів даних про обліковий запис у домені. До цих даних, зокрема, належить ваше ім’я учасника (наприклад, jack@contoso.com) та ім’я домену DNS (наприклад, corp.contoso.com\jack).

Якщо вхід до ОС Windows виконано за допомогою облікового запису Microsoft або ж вхід до ОС Windows здійснено за допомогою

облікового запису домену, підключеного до облікового запису Microsoft, система Windows автоматично синхронізує зображення облікового запису на ПК із зображенням облікового запису Microsoft.

Використання інформації

У разі використання програм сторонніх виробників, ім’я та зображення облікового запису використовуватимуться відповідно до процедур забезпечення конфіденційності третьої сторони. Процедури забезпечення конфіденційності в разі використання програми Microsoft будуть викладені в його декларації про конфіденційність.

Вибір і керування

Якщо вибрати швидке настроювання під час інсталяції Windows, система Windows дозволить програмам отримувати доступ до імені та зображення облікового запису. Якщо ви настроюєте параметри власноруч, для керування доступом до імені та зображення облікового запису можна вибрати параметр **Дозволити програмам використовувати моє ім’я та зображення облікового запису** у розділі **Надати доступ до відомостей корпорації Майкрософт і службам інших виробників**. Після настроювання ОС Windows цю настройку можна змінити в розділі **Конфіденційність** у настройках ПК. Зображення облікового запису можна змінити в розділі **Облікові записи** в настройках ПК. Крім того, можна дозволити певним програмам змінювати зображення облікового запису.

На початок сторінки

Служба мережевого оповіщення

Властивості та завдання

За наявності тарифного плану передплати для доступу до мережі (наприклад, через мобільне широкосмугове підключення) ця функція надає відомості про такий план програмам і засобам Windows на ПК. Програми та засоби Windows використовують ці відомості для оптимізації своєї поведінки. Наприклад, у разі використання лімітного тарифного плану служба Windows Update

відкладатиме оновлення ПК з низьким пріоритетом, доки комп’ютер не буде підключено до мережі іншого типу. Ця функція також надає відомості про підключення до мережі, наприклад рівень сигналу, і повідомляє, чи підключено ПК до Інтернету.

Збирання, обробка та передавання інформації

Цей засіб збирає відомості про підключення до Інтернету та інтрамережі, зокрема реєструє присвоєний ПК суфікс DNS, мережеве ім’я та адресу шлюзу мережі, до якої підключається ПК. Він також отримує відомості про план передплати, наприклад про невикористану частку передплаченого обсягу даних у рамках тарифного плану.

Профілі підключення до мережі можуть містити журнал підключення до всіх використовуваних мереж, а також відомості про дату й час останнього підключення. Цей засіб може спробувати підключитися до сервера Microsoft, щоб перевірити наявність підключення до Інтернету. Під час перевірки підключень до мережі до корпорації Microsoft надсилаються лише стандартні відомості про ПК.

Використання інформації

Якщо дані надсилаються до корпорації Microsoft, вони використовуються виключно для повідомлення про стан підключення до мережі. Відомості про стан підключення до мережі надаються тим програмам і засобам на ПК, які запитують інформацію про мережеве підключення. У разі застосування програми стороннього виробника зібрані відомості використовуватимуться відповідно до процедур забезпечення конфіденційності третьої сторони.

Вибір і керування

Службу мережевого оповіщення за замовчуванням увімкнуто. Адміністратор може її вимкнути у параметрах служб розділу «Адміністрування» на Панелі керування. Вимикати вказану функцію не рекомендовано, оскільки вона забезпечує належну роботу низки засобів Windows.

На початок сторінки

Сповіщення, програми на екрані блокування й оновлення плиток

Програми з Магазину Windows можуть автоматично отримувати вміст і відображати сповіщення кількома способами. Вони можуть, наприклад, отримувати сповіщення та відображати їх у стислому вигляді в куті екрана або на плитках програм, якщо ці плитки закріплені на початковому екрані. За необхідності сповіщення можна також отримувати на екрані блокування. Крім того, на екрані блокування можуть стисло або з подробицями відображатися відомості про стан певної програми. Видавці програм надсилають вміст до програм із Магазину Windows за допомогою служби push-сповіщень Windows, що виконується на серверах корпорації Майкрософт, або ж програми можуть завантажувати дані безпосередньо із серверів третіх сторін.

Сповіщення

Властивості та завдання

Магазин Windows може надавати відомості періодично або в реальному часі. Ця інформація відображається у стислому вигляді у формі сповіщень в куті екрана.

Збирання, обробка та передавання інформації

Програми можуть виводити текст і зображення на екран в області сповіщень. Вміст сповіщень може надаватися й у самій програмі (наприклад, сигнал будильника у програмі Годинник). Сповіщення можуть також надходити з онлайнових служб через службу push-сповіщень Windows (наприклад, останні новини із соціальних мереж). Зображення, що відображаються у сповіщеннях, можуть завантажуватися безпосередньо із сервера, указаного видавцем програми; у цьому разі на такий сервер будуть надіслані стандартні відомості про комп’ютер.

Використання інформації

Корпорація Microsoft використовує відомості про сповіщення виключно для надання сповіщень від програм. Перед доставкою на ПК сповіщення можуть тимчасово зберігатися у службі push-сповіщень Windows. Якщо сповіщення неможливо доставити негайно, вони зберігатимуться лише протягом кількох хвилин, а потім їх буде видалено.

Вибір і керування

Сповіщення можна вимкнути для всіх або лише для деяких програм у підрозділі **Сповіщення** у розділі **Пошук і програми** у настройках ПК. У разі вимкнення сповіщень для програми або видалення цієї програми її видавець може продовжувати надсилати оновлення до служби push-сповіщень Windows, але ці сповіщення не відображатимуться на ПК.

Програми на екрані блокування

Властивості та завдання

Деякі програми з Магазину Windows можуть відображати сповіщення й відомості про свій стан на екрані, коли ПК заблоковано. Програми на екрані блокування також можуть виконувати завдання, коли ПК заблоковано, наприклад синхронізувати електронну пошту у фоновому режимі або давати вам змогу відповідати на вхідні дзвінки. Камеру ПК також можна використовувати безпосередньо з екрана блокування.

Збирання, обробка та передавання інформації

Програми на екрані блокування можуть отримувати оновлення стану від свого видавця за допомогою служби push-сповіщень Windows чи безпосередньо із сервера видавця програми (або сервера іншої третьої сторони). Програми на екрані блокування можуть також передавати або обробляти інші відомості, не пов’язані зі сповіщеннями та оновленнями.

Використання інформації

Система Windows використовує відомості про стан і сповіщення, надані програмами на екрані блокування, для оновлення екрана блокування.

Вибір і керування

Після інсталяції Windows програми Пошта, Календар і Skype автоматично призначаються програмами на екрані блокування. Можна додавати на екран блокування ці або інші програми або видаляти їх із нього, а також вимикати використання камери в підрозділі **Екран блокування** у розділі **ПК та пристрої** в настройках ПК. Крім того, можна вибрати одну програму, для якої

на екрані блокування постійно відображатимуться докладні відомості про стан (наприклад, докладні відомості про наступну зустріч у Календарі).

Можливість відображення сповіщень програмами на екрані блокування можна настроїти в підрозділі **Сповіщення** у розділі **Пошук і програми** в настройках ПК.

Оновлення плиток

Властивості та завдання

Програми з Магазину Windows можуть періодично або в реальному часі надавати відомості, які відображатимуться як оновлення на плитках програм на початковому екрані.

Збирання, обробка та передавання інформації

Програми з Магазину, закріплені на початковому екрані, можуть оновлювати текст і зображення, що відображаються на їхніх плитках. Вміст, що відображається на плитці програми, може надаватися програмою локально, завантажуватися періодично із сервера, указаного видавцем програми, або надсилатися з онлайнової служби через службу push-сповіщень Windows. Якщо вміст плитки завантажено безпосередньо із сервера, указаного видавцем програми, на такий сервер надсилатимуться стандартні відомості про комп'ютер.

Використання інформації

Корпорація Microsoft використовує відомості про плитки виключно для надання для плиток оновлень від програм. Перед доставкою на ПК ці відомості можуть тимчасово зберігатися у службі push-сповіщень Windows. Якщо оновлення для плиток неможливо надати негайно, вони зберігатимуться лише протягом кількох днів, а потім їх буде видалено.

Вибір і керування

Якщо програма почала отримувати оновлення плиток, цю функцію можна вимкнути. Виділіть плитку програми на початковому екрані, а потім виберіть серед доступних у програмі команд пункт **Статична плитка** . У разі відкріплення плитки програми від початкового екрана оновлення плитки не відображатимуться. У

разі видалення програми її видавець може продовжувати надсилати оновлення до служби push-сповіщень Windows, але вони не відображатимуться на ПК.

Щоб видалити поточні оновлення, які відображаються на плитках на початковому екрані, проведіть пальцем від верхнього правого кута або підведіть вказівник до верхнього правого кута початкового екрана, виберіть **Настройки**, а потім – **Плитки**. Натисніть кнопку **Очистити** в області **Видалити особисту інформацію із плиток**. Оновлення плиток, надані після видалення поточних оновлень, будуть відображатися й надалі.

На початок сторінки

Замовлення друку

Властивості та завдання

Замовлення друку дає змогу надсилати цифрові зображення, збережені на ПК або мережевому диску, до вибраної служби друку фотографій в Інтернеті. Надрукувавши зображення, деякі служби надсилають їх поштою, інші передають знімки до місцевого магазину, де їх можна забрати особисто.

Збирання, обробка та передавання інформації

Якщо ви зробите замовлення в онлайновій службі друку фотографій, ваші цифрові фото буде надіслано до цієї служби через Інтернет. До служби може надсилатися шлях до файлів вибраних цифрових зображень (який іноді містить ім’я користувача) з метою забезпечити можливість відображення та передавання цих зображень. Файл цифрового зображення містить дані про зображення, які були збережені в ньому камерою, зокрема дату та час зйомки, а також відомості про місце зйомки (якщо камера підтримує функцію GPS). Файли можуть також містити особисті відомості (наприклад, підписи), які пов’язуються з файлом під час використання програм керування зображеннями та Файлового провідника. Додаткові відомості див. нижче в розділі «Властивості».

Після вибору онлайнової служби друку фотографій вас буде переспрямовано на веб-сайт відповідної служби у вікні

«Замовлення друку». Відомості, введені вами на веб-сайті онлайнової служби друку фотографій, передаються до цієї служби.

Використання інформації

Дані, збережені фотокамерою у файлах цифрових зображень, можуть використовуватися онлайновою службою друку фотографій, наприклад, для регулювання кольору та чіткості зображення перед їх друком. Відомості, що зберігаються у програмах для керування цифровими зображеннями, можуть використовуватися онлайновою службою друку фотографій для друку підписів на лицьовій або зворотній стороні зображення. Онлайнові служби друку фотографій використовують ці й інші надані їм відомості (наприклад, дані, введені на їхніх веб-сайтах) відповідно до власних процедур забезпечення конфіденційності.

Вибір і керування

У засобі замовлення друку можна вибрати зображення, які необхідно надрукувати, та відповідну службу, куди їх буде надіслано. У деяких програмах керування зображеннями можна видалити збережені особисті відомості перед надсиланням фотографій для друку. Ці відомості також можна видалити, змінивши властивості файлу.

На початок сторінки

Попереднє завантаження та попередній запуск

Властивості та завдання

ОС Windows сприяє швидшому запуску програм і засобів Windows, реєструючи час і частоту використання цих програм і засобів, а також відомості про системні файли, які вони завантажують.

Збирання, обробка та передавання інформації

Під час використання програми або засобу Windows система Windows зберігає на ПК відомості про час і частоту їх використання, а також про використані системні файли.

Використання інформації

ОС Windows застосовує відомості про використання програм і

засобів для пришвидшення їх запуску. В окремих випадках програми можуть автоматично запускатися у стані призупинення.

Вибір і керування

Програми, які автоматично запускаються та призупиняються, відображаються в диспетчері завдань, і їх роботу можна завершити. Програми у призупиненому стані не можуть отримувати доступ до веб-камери або мікрофона, доки їх не буде запущено, навіть якщо надання такого доступу вже було ввімкнуто.

На початок сторінки

Помічник із питань сумісності програм

Властивості та завдання

У разі виявлення проблеми несумісності під час запуску класичної програми помічник із питань сумісності програм спробує її усунути.

Збирання, обробка та передавання інформації

У разі виявлення проблеми несумісності під час запуску класичної програми створюється звіт, що містить такі відомості: ім’я та версія програми, необхідні параметри сумісності та дії, які були виконані щодо програми на цю мить. Повідомлення про проблеми із сумісністю програм надсилаються до корпорації Майкрософт за допомогою засобу звітування про критичні помилки Windows або програми підвищення якості ПЗ (програми CEIP) для ОС Windows.

Використання інформації

Звіти про помилки використовуються для надання відповідей стосовно проблем, про які було повідомлено стосовно програм. Відповіді містять посилання (за наявності) на веб-сайт видавця програми, за якими можна отримати додаткові відомості про можливі рішення. Звіт про помилки, створений з огляду на неполадки в роботі програм, використовується для визначення параметрів, які слід настроїти в разі виникнення проблем із сумісністю у програмах, які запускаються в цій версії Windows. Відомості, які надсилає програма CEIP, використовуються для визначення проблем несумісності програм.

Корпорація Майкрософт не використовує жодні відомості, зібрані за допомогою цих засобів, для встановлення особи користувача, зв’язку з ним або надсилання реклами.

Вибір і керування

Для проблем, про які повідомляє засіб звітування про критичні помилки Windows, звіт створюється, лише якщо вибрано команду «Виконати пошук рішення в Інтернеті». Якщо раніше не було дано згоду на автоматичне надсилання звітів про проблеми для пошуку рішень, на екрані відобразиться запит дозволу на надсилання такого звіту. Додаткові відомості див. в розділі «Звітування про критичні помилки Windows».

Якщо програму Windows CEIP увімкнуто, звіти про деякі проблеми надсилатимуться автоматично. Додаткові відомості див. в розділі «Програма підвищення якості ПЗ Windows».

На початок сторінки

Властивості

Властивості та завдання

Властивості – це відомості про файл, які забезпечують швидкий пошук і впорядкування файлів. Деякі властивості притаманні файлам (наприклад, розмір файлу), іншими володіють програми (наприклад, настройки камери під час фотографування або дані про розташування, записані камерою для фото).

Збирання, обробка та передавання інформації

Тип відомостей, що зберігаються, залежить від типу файлу та програм, які їх використовують. До властивостей можуть належати, наприклад, ім'я файлу, дата змінення, розмір файлу, ім'я автора, ключові слова та коментарі. Властивості зберігаються у файлі та переміщуються разом із файлом або копіюються разом із ним до іншого розташування, наприклад до спільної папки, чи надсилаються електронною поштою як вкладення.

Використання інформації

Властивості допомагають прискорити пошук і впорядкування

файлів. Їх також можна використовувати для виконання завдань, характерних для конкретних програм. До корпорації Майкрософт відомості не надсилаються.

Вибір і керування

Деякі значення властивостей можна змінити або видалити з файлу. Для цього потрібно виділити файл у Файловому провіднику та вибрати пункт **Властивості**. Таким чином можна видалити значення деяких основних атрибутів файлу, наприклад дату внесення змін, розмір, ім’я файлу, а також значення деяких атрибутів, притаманних конкретній програмі. Значення властивостей, притаманних конкретній програмі, можна змінити або видалити, лише якщо програма, за допомогою якої було створено файл, підтримує такі функції.

На початок сторінки

Наближення

Служба радіозв’язку на близькій відстані

Властивості та завдання

Якщо ПК оснащено устаткуванням для радіозв’язку на близькій відстані (NFC), можна фізично з’єднати його з іншим пристроєм, оснащеним устаткуванням NFC, для забезпечення спільного доступу до посилань, файлів та іншої інформації. Існує два типи підключень під час наближення: взаємодія зблизька та взаємодія поруч. У разі взаємодії зблизька можна створити коротко- або довготривале підключення між пристроями за допомогою Wi-Fi, Wi-Fi Direct або Bluetooth. У разі взаємодії поруч підключення активується, лише коли пристрої розташовано поруч.

Збирання, обробка та передавання інформації

Коли пристрої з увімкнутою функцією наближення розташовано на невеликій відстані один від одного, вони обмінюються даними для встановлення підключення. Залежно від настройок пристроїв цими даними можуть бути відомості про з'єднання за допомогою Bluetooth, мережеві адреси Wi-Fi, а також ім’я ПК.

Після встановлення підключення пристрої можуть обмінюватися й

іншими відомостями – це залежить того, яка програма чи засіб використовується для встановлення підключення під час наближення. За допомогою підключення під час наближення система Windows може надсилати файли, посилання та інші відомості з одного пристрою на інші. Програми, які використовують функцію наближення, можуть надсилати та отримувати відомості, до яких їм надано доступ. Ці відомості можуть надсилатися через мережу або підключення до Інтернету, або безпосередньо через пряме безпровідне підключення між пристроями.

Використання інформації

Відомості про мережу та ПК, якими обмінюються пристрої через підключення під час наближення, використовуються для встановлення підключення до мережі та визначення пристроїв, підключених один до одного. Дані, що передаються через установлене програмою підключення під час наближення, можуть використовуватися цією програмою яким завгодно чином. До корпорації Майкрософт відомості не надсилаються.

Вибір і керування

Службу радіозв'язку на близькій відстані за замовчуванням увімкнуто. Адміністратор може її вимкнути в параметрах розділу «Пристрої та принтери» на Панелі керування.

Засіб «Піднести й надіслати»

Властивості та завдання

Функція Windows «Піднести й надіслати» спрощує доступ до вибраних даних спільно із друзями, які перебувають поруч, або з іншим власним пристроєм, наприклад із мобільним телефоном. Наприклад, у браузері функцію «Піднести й надіслати» можна ввімкнути в області «Пристрої». Перший же пристрій, з яким буде встановлено з'єднання, отримає посилання на веб-сторінку, яка наразі відображається на екрані. Цю функцію можна використовувати в будь-якій програмі, що підтримує спільний доступ до даних, зокрема зображень, тексту або файлів.

Збирання, обробка та передавання інформації

Засіб «Піднести й надіслати» використовує відомості, до яких

надано спільний доступ, а також відомості, описані в розділі «Служба радіозв’язку на близькій відстані» вище.

Використання інформації

Ці відомості використовуються для встановлення підключення між двома пристроями. Засіб «Піднести й надіслати» не зберігає відомості, до яких надано спільний доступ. До корпорації Майкрософт відомості не надсилаються.

Вибір і керування

Якщо службу радіозв’язку на близькій відстані ввімкнуто, увімкнуто також і функцію «Піднести й надіслати». Для отримання додаткових відомостей див. розділ, присвячений службі радіозв’язку на близькій відстані.

На початок сторінки

Підключення для віддаленого доступу

Властивості та завдання

Підключення для віддаленого доступу дає змогу підключатися до приватних мереж за допомогою підключення до віртуальної приватної мережі (VPN) і служби віддаленого доступу (RAS). RAS – це компонент, який з’єднує клієнтський ПК (зазвичай це ваш ПК) з хост-комп'ютером (який також називається сервером віддаленого доступу) за стандартними для галузі протоколами. Технології VPN забезпечують підключення користувачів до приватної мережі, наприклад корпоративної, через Інтернет.

Компонент з’єднань для віддаленого доступу (комутований доступ) дає змогу отримати доступ до Інтернету за допомогою звичайного модему або технології широкосмугового зв’язку, наприклад кабельного модема або каналу DSL. Компонент «Комутоване з'єднання з мережею» містить підкомпоненти для набору номера, наприклад RAS-клієнт, диспетчер підключень і RAS-телефон, а також набирачі номера, які працюють у командному рядку, наприклад rasdial.

Збирання, обробка та передавання інформації

Компоненти набирача збирають на ПК такі відомості, як ім’я

користувача, пароль та ім’я домену. Ці відомості надсилаються до системи, до якої намагається підключитися користувач. Для захисту ПК та конфіденційності ваших даних пов’язані з безпекою відомості, наприклад ім’я користувача та пароль, шифруються та зберігаються на ПК.

Використання інформації

Відомості набирача допомагають ПК підключитися до Інтернету. Сервер віддаленого доступу може зберігати відомості про ім’я користувача та IP-адресу для обліку та забезпечення відповідності вимогам, але жодні з цих відомостей не надсилаються до корпорації Майкрософт.

Вибір і керування

У набирачах, за винятком набирачів для командного рядка, можна за необхідності зберегти свій пароль, установивши прапорець **Зберігати ім’я користувача та пароль**. Цей прапорець можна будь-якої миті зняти, щоб видалити з набирача збережений раніше пароль. Оскільки за замовчуванням цей параметр вимкнуто, може відобразитися запит на введення паролю для підключення до Інтернету або мережі. У засобах командного рядка можливості зберігати пароль не існує.

На початок сторінки

Підключення до віддалених робочих столів і програм RemoteApp

Властивості та завдання

Підключення до віддалених робочих столів і програм RemoteApp дає змогу отримати доступ до програм і робочих столів віддалених ПК, для яких передбачена можливість віддаленого доступу через Інтернет.

Збирання, обробка та передавання інформації

У разі ввімкнення підключення файли конфігурації завантажуються на ПК з указаної віддаленої URL-адреси. Ці файли конфігурації зв’язують програми та робочі столи на віддалених ПК, щоб їх можна було запускати з вашого комп’ютера. ПК автоматично перевірятиме наявність оновлень і час від часу завантажуватиме їх

до цих файлів конфігурації. Ці програми виконуються на віддалених ПК, а введені до них відомості передаються мережею на віддалений ПК, до якого встановлено підключення.

Якщо корпорація Майкрософт розміщує ПК або програми, до яких встановлюється підключення, до корпорації Майкрософт із метою надання підтримки можуть надсилатися додаткові відомості про підключення.

Використання інформації

Оновлення файлів конфігурації можуть включати зміни в настройках, зокрема надання доступу до нових програм, але нові програми виконуватимуться, лише якщо їх запустить користувач. Цей засіб також надсилає відомості на віддалені ПК, на яких запущено віддалені програми. Ці дані використовуються віддаленими програмами відповідно до політик конфіденційності їх постачальників і адміністраторів віддалених ПК. Відомості надсилаються до корпорації Майкрософт, лише якщо віддалене підключення розміщено корпорацією Майкрософт.

Вибір і керування

Використання підключень до віддалених робочих столів і програм RemoteApp можна вмикати та вимикати на власний розсуд. Додати або видалити підключення до віддалених робочих столів і програм RemoteApp можна в розділі «Підключення до віддалених робочих столів і програм RemoteApp» на Панелі керування. Щоб додати нове підключення, виберіть **Доступ до віддалених робочих столів і програм RemoteApp**і введіть URL-адресу для підключення в діалоговому вікні. Щоб отримати URL-адресу для підключення, можна також скористатися власною адресою електронної пошти. Щоб видалити підключення та відповідні файли підключення, слід натиснути кнопку **Видалити** в діалоговому вікні опису підключень. Якщо ви відключитеся від мережі, не закривши програми, ці програми лишаються відкритими на віддаленому ПК. Підключення до віддалених робочих столів і програм RemoteApp не відображаються у списку «Інсталяція та видалення програм» на Панелі керування.

На початок сторінки

Підключення до віддаленого робочого стола

Властивості та завдання

Підключення до віддаленого робочого стола дає змогу встановити віддалене підключення до хост-комп'ютера, на якому запущено служби віддалених робочих столів.

Збирання, обробка та передавання інформації

Настройки підключення до віддаленого робочого стола зберігаються в локальному (для програми) сховищі або у файлі протоколу RDP на ПК. До цих настройок належить ім’я домену та настройки конфігурації підключення, зокрема ім’я віддаленого ПК, ім’я користувача, відомості про екран, відомості про локальні пристрої, відомості про звук, буфер обміну, настройки підключення, ім’я програми, а також піктограма або ескіз сеансу.

Облікові дані для цих підключень, облікові дані для шлюзу віддаленого робочого стола та список імен надійних шлюзових серверів віддаленого робочого стола зберігаються локально на ПК. Список зберігається в реєстрі. Цей список зберігається постійно, доки його не видалить адміністратор. Відомості надсилаються до корпорації Майкрософт, лише якщо віддалене підключення розміщено корпорацією Майкрософт.

Використання інформації

Відомості, зібрані засобом підключення до віддаленого робочого стола, дають змогу підключатися до хост-комп'ютерів, на яких виконуються служби віддаленого робочого стола, з використанням визначених настройок. Зібрані відомості про ім’я користувача, пароль і домен дають змогу зберегти настройки підключення та встановлювати підключення без повторного введення цих відомостей, клацнувши двічі RDP-файл або вибравши рекомендовані підключення.

Вибір і керування

Використання підключення до віддаленого робочого стола можна вмикати та вимикати на власний розсуд. У разі використання такого підключення RDP-файли та рекомендовані підключення до віддаленого робочого стола містять відомості, необхідні для

підключення до віддаленого ПК, включно з параметрами та настройками, які було вказано під час автоматичного збереження параметрів підключення. RDP-файли та рекомендовані підключення можна настроювати. Зокрема, можна настроїти різні файли та рекомендовані підключення для з'єднання з одним і тим самим ПК з різними настройками. Щоб змінити збережені облікові дані, відкрийте диспетчер облікових даних у розділі «Облікові записи користувачів» на Панелі керування.

На початок сторінки

Вхід за допомогою облікового запису Microsoft

Властивості та завдання

Обліковий запис Microsoft (колишня назва – Windows Live ID) – це єдина адреса електронної пошти та пароль, які можна використовувати для входу до програм, на сайти та до служб Microsoft і вибору партнерів Microsoft. Обліковий запис Microsoft можна зареєструвати в ОС Windows або на веб-сайтах Microsoft, для входу на які потрібен обліковий запис Microsoft.

Для входу до ОС Windows можна використовувати обліковий запис Microsoft або, для продуктів, які це підтримують, підключити локальний обліковий запис чи обліковий запис у домені до облікового запису Microsoft. У такому разі ОС Windows може забезпечити однакові умови роботи на різних ПК, автоматично синхронізуючи настройки у Windows і програмах Microsoft. Під час відвідування веб-сайту, де для входу використовується обліковий запис Microsoft, ОС Windows також автоматично виконує вхід на цей веб-сайт.

Збирання, обробка та передавання інформації

У разі введення адреси електронної пошти, що використовується як обліковий запис Microsoft, під час настроювання ПК або в розділі **Облікові записи** в настройках ПК, ОС Windows надішле цю адресу електронної пошти до корпорації Майкрософт, щоб визначити, чи пов’язано який-небудь обліковий запис Microsoft із цією адресою електронної пошти. Якщо адреса електронної пошти вже використовується як обліковий запис Microsoft, її та

відповідний пароль облікового запису Microsoft можна використовувати для входу до ОС Windows. За відсутності достатньої кількості відомостей про безпеку для облікового запису Microsoft, можливо, спочатку потрібно буде надати ці відомості, наприклад номер мобільного телефону, який може використовуватися для перевірки особи власника облікового запису. За відсутності облікового запису Microsoft його можна створити, скориставшись адресою електронної пошти.

Під час виконання входу за допомогою облікового запису Microsoft ОС Windows також надсилатиме до корпорації Майкрософт стандартні відомості про комп’ютер, включно з відомостями про виробника пристрою, назвою моделі та версією.

Щоразу під час входу до ОС Windows за допомогою облікового запису Microsoft, коли ПК підключено до Інтернету, ОС Windows перевіряє адресу електронної пошти та пароль на серверах Microsoft. Вхід до ОС Windows за допомогою облікового запису Microsoft або облікового запису в домені, підключеного до облікового запису Microsoft, відкриває численні можливості.

- Певні настройки Windows на комп'ютерах, вхід на які здійснюється за допомогою облікового запису Microsoft, синхронізуватимуться між собою. Додаткові відомості про те, які саме настройки синхронізуються та як ними керувати, див. в розділі «Синхронізація настройок» на цій сторінці.

- Програми Microsoft, що використовують обліковий запис Microsoft для автентифікації (наприклад, Пошта, Календар, Люди, Microsoft Office та інші), можуть автоматично починати завантаження відомостей (наприклад, програма Пошта автоматично завантажуватиме повідомлення, надіслані на вашу адресу у службі Outlook.com або Hotmail.com, за наявності такої адреси). Браузери можуть автоматично виконувати вхід на веб-сайти, для входу на які використовується обліковий запис Microsoft (наприклад, у разі відвідування сайту Bing.com вхід може виконуватися автоматично без введення паролю облікового запису Microsoft).

ОС Windows запитуватиме ваш дозвіл, перш ніж надавати програмі

стороннього виробника відомості профілю або інші особисті дані, пов’язані з обліковим записом Microsoft. Якщо виконати вхід до системи Windows за допомогою облікового запису в домені, підключеного до облікового запису Microsoft, вибрані настройки та відомості синхронізуватимуться з обліковим записом у домені і вхід до програм і веб-сайтів виконуватиметься автоматично, як описано вище. Оскільки адміністратори домену можуть отримати доступ до будь-яких відомостей на ПК, вони також матимуть доступ до будь-яких настройок і відомостей, вибраних для синхронізації з іншими ПК через обліковий запис Microsoft. Це, зокрема, можуть бути такі параметри, як ім’я, зображення облікового запису та журнал браузера. Додаткові відомості про те, які саме настройки синхронізуються і як ними керувати, див. в розділі «Синхронізація настройок» на цій сторінці.

Використання інформації

Надані відомості використовуватимуться під час створення нового облікового запису Microsoft в ОС Windows, а також для його захисту. Наприклад, надані відомості про безпеку (зокрема, номер телефону або інша адреса електронної пошти) будуть використані, лише якщо неможливо виконати вхід до облікового запису. Якщо для входу в ОС Windows застосовується обліковий запис Microsoft, система Windows автоматично використовує дані облікового запису Microsoft для входу до програм і на веб-сайти. Щоб отримати додаткові відомості про те, як впливає на конфіденційність використання облікового запису Microsoft, ознайомтеся з декларацією про конфіденційність Microsoft. Відомості про те, як окремі програми Microsoft використовують дані, пов’язані з обліковим записом Microsoft, див. в декларації про конфіденційність для кожної програми. Декларацію про конфіденційність для програми Microsoft можна знайти в настройках кожної програми або в діалоговому вікні «Про програму».

Стандартні відомості про пристрій можуть використовуватися для персоналізації деяких повідомлень для користувачів, зокрема повідомлень електронної пошти з порадами щодо початку роботи із пристроєм.

Вибір і керування

Якщо ввійти до системи Windows з обліковим записом Microsoft, деякі настройки синхронізуватимуться автоматично. Відомості про те, як змінити список настройок Windows, для яких виконується синхронізація, або зупинити синхронізацію, див. в розділі «Синхронізація настройок» на цій сторінці. Щоб отримати додаткові відомості про дані, які збираються програмами Microsoft, що використовують для автентифікації обліковий запис Microsoft, ознайомтеся з деклараціями про конфіденційність цих програм.

Для продуктів, які це підтримують, можна в будь-який момент створити локальний обліковий запис Microsoft у розділі **Облікові записи** в настройках ПК. Якщо для входу в ОС Windows використовується обліковий запис у домені, обліковий запис Microsoft можна підключити або відключити будь-коли, відкривши розділ **Облікові записи** в настройках ПК.

У разі використання перегляду InPrivate в Internet Explorer, вхід на веб-сайти, де використовуються облікові записи Microsoft виконуватиметься автоматично.

На початок сторінки

Хмарне сховище OneDrive

Властивості та завдання

Під час входу на пристрій за допомогою облікового запису Microsoft можна автоматично зберігати певний вміст і параметри на серверах Microsoft для створення резервної копії на випадок, якщо із пристроєм щось станеться.

Збирання, обробка та передавання інформації

Якщо під час настроювання вибрати використання OneDrive як хмарного сховища, ОС Windows автоматично надсилатиме вміст на сервери Microsoft, включно з перерахованими нижче файлами й даними.

- Фотографії та відео на пристрої, які було збережено до папки **Фотографії з камери**
- Настройки, які є специфічними для пристрою й не

використовуються спільно з іншими пристроями.

- Описові відомості про пристрій, такі як назва пристрою та тип.

Можна також вибрати в настройках зберігання вмісту на серверах Microsoft, а для програм сервери Microsoft можна вибрати як місце розташування за замовчуванням для зберігання файлів.

Використання інформації

ОС Windows використовує цей вміст для надання служби зберігання даних у хмарі. Корпорація Майкрософт не використовує вміст або відомості користувача для встановлення особи користувача, зв'язку з ним або надсилання реклами.

Вибір і керування

Якщо під час настроювання ПК вибрати команду «Використовувати OneDrive», ОС Windows збереже вміст, описаний у цьому розділі, у OneDrive. Ці настройки завжди можна змінити в розділі OneDrive настройок ПК.

На початок сторінки

Настройки синхронізації

Властивості та завдання

Якщо виконати вхід до ОС Windows за допомогою облікового запису Microsoft, ОС Windows синхронізуватиме деякі настройки та відомості із серверами Microsoft, щоб у користувача були однаково зручні умови роботи на кількох ПК. Якщо після входу на один або кілька ПК з обліковим записом Microsoft уперше виконати вхід на інший ПК з цим самим обліковим записом Microsoft, ОС Windows завантажить і застосує настройки та відомості, які були вибрані для синхронізації на інших ПК. Настройки, вибрані для синхронізації, автоматично оновлюватимуться на серверах корпорації Майкрософт та інших ПК у процесі їх використання.

Збирання, обробка та передавання інформації

У разі входу до системи Windows за допомогою облікового запису Microsoft ОС Windows синхронізує певні настройки із сервером

Microsoft. Ці настройки перелічені нижче.

- Макет початкового екрана
- Програми, інстальовані з Магазину Windows
- Мовні параметри
- Настройки Центру легкого доступу
- Настройки персоналізації, наприклад зображення облікового запису, зображення на екрані блокування, фон і настройки миші
- Настройки для програм із Магазину Windows
- Словники для перевірки орфографії, словники IME й особисті словники
- Журнал браузера, уподобання та відкриті веб-сайти
- Збережені паролі програм, веб-сайтів і мереж
- Адреси спільних мережевих принтерів, до яких установлено підключення

Щоб підвищити рівень конфіденційності, усі синхронізовані настройки надсилаються в зашифрованій формі за протоколом SSL. Деякі з цих настройок не синхронізуватимуться на ПК, доки цей ПК не буде додано до облікового запису Microsoft як надійний.

Якщо виконати вхід до ОС Windows за допомогою облікового запису в домені, підключеного до облікового запису Microsoft, вибрані настройки та відомості синхронізуватимуться з обліковим записом у домені. Паролі, збережені під час сеансу Windows, коли обліковий запис у домені підключено до облікового запису Microsoft, ніколи не синхронізуватимуться. Оскільки адміністратори домену можуть отримати доступ до будь-яких відомостей на ПК, вони також зможуть отримувати доступ до будь-яких настройок і відомостей, вибраних для синхронізації з іншими ПК через обліковий запис Microsoft.

Використання інформації

Система Windows використовує ці настройки та відомості для забезпечення синхронізації. Корпорація Майкрософт не використовує ці синхронізовані настройки для встановлення особи користувача, зв’язку з ним або надсилання реклами.

Вибір і керування

Якщо ввійти до системи Windows за допомогою облікового запису Microsoft, деякі настройки синхронізуватимуться за замовчуванням. Щоб вибрати синхронізацію настройок і керувати елементами, для яких виконується синхронізація, перейдіть до підрозділу **Настройки синхронізації** в розділі OneDrive настройок ПК. Якщо виконати вхід до ОС Windows за допомогою облікового запису в домені та підключити цей обліковий запис до облікового запису Microsoft, система Windows запитає, які настройки потрібно синхронізувати перед підключенням до облікового запису Microsoft.

На початок сторінки

Технологія Teredo

Властивості та завдання

Технологія Teredo дає змогу ПК та мережам обмінюватися даними за кількома мережевими протоколами.

Збирання, обробка та передавання інформації

Щоразу під час запуску ПК технологія Teredo намагатиметься знайти в Інтернеті загальнодоступну службу протоколу Інтернету версії 6 (IPv6). Це виконується автоматично, коли ПК підключається до загальнодоступної або приватної мережі, але в разі підключення до керованих мереж, наприклад домену підприємства, ця технологія не використовується. У разі використання програми, що потребує Teredo для використання підключення за протоколом IPv6, або якщо підключення за протоколом IPv6 завжди ввімкнуте у брандмауері, технологія Teredo час від часу підключатиметься до служби Microsoft Teredo через Інтернет. До корпорації Microsoft надсилаються виключно стандартні відомості про ПК, а також ім’я запитуваної служби (наприклад, teredo.ipv6.microsoft.com).

Використання інформації

Відомості, що надсилаються з ПК за допомогою технології Teredo, використовуються для визначення наявності підключення ПК до Інтернету та можливості знайти загальнодоступну службу IPv6. Після того, як цю службу буде знайдено, надсилатиметься інформація, необхідна для підтримання з'єднання зі службою IPv6.

Вибір і керування

За допомогою знаряддя командного рядка netsh можна змінити запит, який служба надсилає через Інтернет, щоб натомість використовувати інший сервер (не Microsoft), або вимкнути цю функцію взагалі. Докладні вказівки див. в розділі «Протокол Інтернету версії 6, Teredo та супутні технології» цього офіційного технічного документа.

На початок сторінки

Служби модуля TPM

Властивості та завдання

Модуль TPM – це вбудоване в ПК устаткування для захисту, яке, за його наявності та за умови розподілення ресурсів, дає ПК змогу скористатися всіма перевагами розширених функцій безпеки. Модуль TPM використовує такі функції та засоби Windows, як шифрування пристрою, віртуальна смарт-картка, безпечне завантаження Захисника Windows і зберігання сертифікатів у модулі TPM.

Збирання, обробка та передавання інформації

За замовчуванням права власності на модуль TPM належать системі Windows, яка зберігає всі відомості щодо авторизації власника модуля TPM таким чином, що вони доступні лише для адміністраторів Windows. Для виконання типових завдань адміністрування створюються обмежені значення авторизації. Діями звичайного користувача керує система Windows.

Консоль керування модулем TPM дає змогу в інтерактивному режимі керувати ресурсами цього модуля та зберігати значення авторизації власника TPM на зовнішньому носії, наприклад у

флеш-пам’яті USB, після розподілення ресурсів TPM. Збережений файл містить відомості про авторизацію власника TPM для модуля TPM. Файл також містить відомості про ім’я ПК, версію операційної системи, користувача, який його створив, а також дату створення, які допомагають розпізнати його серед інших.

У середовищі домену адміністратор домену може настроїти зберігання повного пароля власника TPM у службі Active Directory в об’єкті TPM у разі розподілення ресурсу цього модуля.

Кожен модуль TPM має унікальний підтверджувальний криптографічний ключ, який використовується для позначення його автентичності. Виробник ПК може створити та зберегти підтверджувальний ключ у модулі TPM. На деяких старіших ПК система Windows має ініціювати створення підтверджувального ключа в модулі TPM. Відкрита частина підтверджувального ключа ніколи не потрапляє за межі модуля TPM, і після створення її зазвичай неможливо скинути. На більшості комп’ютерів під керуванням ОС Windows сертифікат підтверджувального ключа зберігатиметься в модулі TPM. Сертифікат підтверджувального ключа вказує на наявність цього ключа в устаткуванні TPM. За допомогою сертифіката віддалений засіб перевірки може переконатися в тому, що модуль TPM відповідає специфікаціям TPM. Сертифікат підтверджувального ключа зазвичай підписується виробником модуля TPM або виробником платформи.

Використання інформації

Після ініціалізації модуля TPM програми можуть використовувати цей модуль для створення та покращення захисту додаткових криптографічних ключів. Наприклад, засіб шифрування пристрою використовує модуль TPM для покращення захисту ключа, який використовується для шифрування диска.

Якщо вибрати збереження пароля власника TPM у файлі, додаткові відомості про ПК та користувача, що зберігаються в цьому файлі, допомагають визначити відповідний ПК та модуль TPM. Підтверджувальний ключ TPM використовується системою Windows під час ініціалізації модуля TPM для шифрування значення авторизації власника TPM перед його надсиланням до цього модуля. Система Windows не передає криптографічні ключі

за межі ПК. ОС Windows не надає програмам сторонніх виробників, зокрема програмному забезпеченню для захисту від зловмисних програм, інтерфейс для використання підтверджувального ключа в певних сценаріях TPM, таких як завантаження з оцінкою показників і засвідченням. У програмному забезпеченні для захисту від зловмисних програм підтверджувальний ключ і сертифікат ключа також використовуються для підтвердження того, що показники завантаження надані модулем TPM певного виробника. За замовчуванням підтверджувальний ключ TPM можуть використовувати лише адміністратори або програми, запущені із правами адміністратора.

Вибір і керування

Користувачі й адміністратори погоджуються на використання модуля TPM, увімкнувши засіб Windows або запустивши програму, що використовує TPM.

За необхідності можна очистити модуль TPM і відновити для нього заводські настройки за замовчуванням. Очищення модуля TPM призведе до видалення відомостей про власника, а також усіх ключів, що зберігаються в модулі TPM, окрім підтверджувального ключа, і криптографічних відомостей, створених програмами під час використання цього модуля.

На початок сторінки

Відновлення кореневих сертифікатів

Властивості та завдання

Сертифікати використовуються переважно для перевірки ідентичності користувача або ідентифікації пристрою, автентифікації служби або шифрування файлів. Довірені кореневі центри сертифікації – це організації, які видають сертифікати. Засіб оновлення кореневих сертифікатів підключається до служби Windows Update, щоб перевірити, чи додавала корпорація Майкрософт певний центр сертифікації до списку довірених центрів, але лише якщо для програми використовується сертифікат, виданий центром сертифікації, який не було визнано безпосередньо надійним (сертифікат, відсутній у списку надійних

сертифікатів на ПК). Якщо такий центр сертифікації було додано до списку довірених центрів корпорації Майкрософт, його сертифікат буде автоматично додано до списку надійних сертифікатів на ПК.

Збирання, обробка та передавання інформації

Засіб оновлення кореневих сертифікатів надсилає до онлайнової служби Windows Update запит на поточний список кореневих центрів сертифікації у програмі кореневих сертифікатів Microsoft. Якщо список містить сертифікат, що не є довіреним, засіб оновлення кореневих сертифікатів отримує цей сертифікат зі служби Windows Update і зберігає його у списку надійних сертифікатів на ПК. У цьому разі передаються такі відомості, як імена та криптографічні геші кореневих сертифікатів.

Використання інформації

Ці відомості використовуються корпорацією Майкрософт для оновлення списку надійних сертифікатів. Корпорація Майкрософт не використовує ці відомості для встановлення особи користувача, зв’язку з ним або надсилання реклами.

Вибір і керування

Оновлення кореневих сертифікатів увімкнуто за замовчуванням. Адміністратори можуть вимкнути оновлення кореневих сертифікатів на ПК, настроївши відповідну групову політику.

На початок сторінки

Служби оновлення

Властивості та завдання

До служб оновлення для ОС Windows належать Windows Update і Microsoft Update:

- **Windows Update** – це служба, яка надає оновлення для програмного забезпечення Windows та іншого підтримуваного програмного забезпечення, наприклад драйверів, що постачаються виробниками пристрою;
- **Microsoft Update** – це служба яка надає оновлення для

програмного забезпечення Windows, а також іншого програмного забезпечення Microsoft, наприклад Microsoft Office.

Збирання, обробка та передавання інформації

Служби оновлення збирають на ПК відомості, за допомогою яких корпорація Майкрософт забезпечує функціонування наведених нижче служб і покращує їхню якість.

- Програмне забезпечення Microsoft та інше інстальоване на ПК допоміжне програмне забезпечення (наприклад, драйвери та мікропрограми, що надаються виробником пристроїв), для якого доступні оновлення у службах оновлення. Це дає змогу визначити, які оновлення необхідні для користувача.

- Настройки конфігурації служб Windows Update і/або Microsoft Update, наприклад відомості про те, чи слід автоматично завантажувати й інсталювати оновлення.

- Випадки успішного та невдалого виконання операцій доступу до служб оновлення та їх використання, а також помилки, які виникали під час цього процесу.

- Ідентифікаційні номери Plug and Play для апаратних пристроїв – код, призначений виробником пристрою, що дає змогу ідентифікувати пристрій (наприклад, певний тип клавіатури).

- GUID (глобальний унікальний ідентифікатор) – створений довільним чином номер, який не містить особисті відомості. Ідентифікатори GUID використовуються для ідентифікації окремих ПК без встановлення особи користувачів.

- Ім’я BIOS, номер версії, постачальник і дата редакції – відомості про набір важливих програмних процедур, за допомогою яких виконується тестування устаткування, запуск операційної системи на ПК та забезпечується передавання даних між апаратними пристроями, підключеними до ПК.

- Виробник, модель, роль платформи та обліковий номер – відомості про ПК, які використовуються для діагностичного

дослідження інсталяції драйверів.

Службами оновлення можна скористатися, перейшовши до розділу Windows Update на Панелі керування та перевіривши наявність оновлень, або змінивши настройки та увімкнувши для ОС Windows автоматичну інсталяцію доступних оновлень (рекомендовано). У настройках засобу Windows Update можна вибрати, чи слід погоджуватися на використання Microsoft Update.

Якщо користувач погодився отримувати важливі оновлення програмного забезпечення на ПК, в ці оновлення може бути включено засіб Windows для видалення зловмисних програм. Засіб для видалення зловмисних програм перевіряє ПК на наявність поширених програм, створених зловмисниками (т. зв. «зловмисних програм»), і допомагає видалити виявлене шкідливе програмне забезпечення. У разі запуску це програмне забезпечення видаляє зловмисні програми, перелічені на веб-сайті підтримки Microsoft. Під час перевірки на наявність зловмисних програм до корпорації Майкрософт надсилається звіт із конкретними відомостями про виявлене шкідливе програмне забезпечення та помилки, а також іншою інформацією про ПК. Додаткові відомості див. в декларації про конфіденційність для засобу Windows для видалення зловмисних програм .

Використання інформації

Дані, надіслані до корпорації Майкрософт, використовуються для забезпечення функціонування та обслуговування служб Windows Update. Вони також використовуються для створення агрегованої статистики, яка допомагає корпорації Майкрософт аналізувати тенденції та вдосконалювати продукти та служби, зокрема служби Windows Update.

Для створення агрегованої статистики служби оновлення використовують отриманий службами Windows Update ідентифікатор GUID для відстеження та фіксування кількості окремих комп’ютерів, що використовують служби Windows Update, а також перевірки успішності завантаження та інсталяції певних оновлень. Служби оновлень Windows Update записують ідентифікатор GUID комп’ютера, з якого зроблено спробу завантаження та інсталяції, ідентифікатор елемента, щодо якого

було надіслано запит, відомості про доступність оновлень і стандартні відомості про комп’ютер.

Описані вище відомості засобу для видалення зловмисних програм використовуються для вдосконалення програмного забезпечення для захисту від зловмисних програм і покращення інших продуктів і служб безпеки. Відомості, що містяться у звітах засобу для видалення зловмисних програм, не використовуватимуться для встановлення особи користувача або зв’язку з ним.

Обов’язкові оновлення

Якщо включити служби оновлення, для їх правильного функціонування час від часу необхідно оновлювати деякі компоненти програмного забезпечення в системі, які входять до складу або безпосередньо стосуються служб оновлення. Ці оновлення необхідно виконати, перш ніж служба зможе перевірити наявність інших оновлень, завантажити їх або інсталювати. Ці обов’язкові оновлення забезпечують виправлення помилок і постійне покращення функціоналу, а також сумісність із серверами Microsoft, які підтримують цю службу.

Якщо служби оновлення вимкнуто, ці оновлення не надходитимуть.

Оновлення програмного забезпечення, необхідні для інсталяції або оновлення програм із Магазину Windows, буде завантажено й інстальовано автоматично. Ці оновлення необхідно виконати для належного функціонування програм.

Файли cookie та маркери

Маркери де в чому схожі на файли cookie. Пов’язані з ними відомості зберігаються на жорсткому диску користувача в невеликому файлі, розміщеному там сервером служб оновлення, і використовуються, коли комп’ютер підключається до сервера служб оновлення, для забезпечення припустимого підключення. Ці відомості зберігаються лише на комп’ютері користувача, а не на сервері. Такий файл cookie (або маркер) містить відомості (наприклад, час останнього сканування), які дають змогу знаходити найновіші доступні оновлення. За допомогою цих відомостей можна визначити, який вміст необхідно завантажити на

комп’ютер і коли саме це необхідно зробити. Сюди ж належить GUID для ідентифікації комп’ютера користувача сервером.

Відомості, що містяться у файлі cookie або маркері, шифруються сервером (окрім часу завершення терміну дії файлу cookie або маркера). Такий файл cookie (або маркер) відрізняється від файлів cookie браузера, тому ним не можна керувати за допомогою настройок браузера. Файл cookie (або маркер) неможливо видалити, проте, якщо служби Windows Update не застосовуються, не використовуватиметься й файл cookie (або маркер).

Вибір і керування

Якщо під час інсталяції ОС Windows вибрати швидкі настройки, службу Windows Update буде ввімкнуто й оновлення інсталюватимуться автоматично.

Якщо ввімкнути службу оновлення, незалежно від вибраної настройки, обов’язкові оновлення для деяких компонентів служби буде завантажено та інстальовано автоматично, без додаткового повідомлення. Якщо немає необхідності отримувати обов’язкові оновлення, вимкніть службу оновлення.

Також можна вибрати, наявність яких оновлень слід перевіряти або які з них потрібно інсталювати автоматично: важливі та рекомендовані для комп’ютера, чи лише важливі. Необов’язкові оновлення ніколи не інсталюються автоматично. Після інсталяції ОС Windows настройки служби Windows Update можна змінити на Панелі керування або в настройках ПК.

Якщо ввімкнуто перевірку наявності та інсталяцію важливих оновлень й у складі цих оновлень для ПК було отримано засіб для видалення зловмисних програм, можна вимкнути у програмному забезпеченні функцію звітування.

На початок сторінки

Віртуальна приватна мережа (VPN)

Властивості та завдання

Віртуальна приватна мережа дає змогу підключатися до приватної мережі (наприклад, корпоративної) через Інтернет. Підключення

VPN може бути надано VPN-клієнтом Windows або програмою для VPN сторонніх виробників.

Збирання, обробка та передавання інформації

Під час підключення до мережі VPN облікові дані, введені у VPN-клієнті, надсилаються до віддаленої мережі. Ці облікові дані можна зберігати на ПК. Після підключення, залежно від способу настройки мережі VPN, деякі або всі мережеві операції спрямовуються через віддалену мережу. Адміністратори можуть настроїти постійну маршрутизацію трафіку деяких програм через мережу VPN, а також автоматичне підключення до мережі VPN під час запуску цих програм. До корпорації Майкрософт відомості не надсилаються.

Програмне забезпечення для VPN сторонніх виробників може збирати додаткові відомості. Збір і використання цих відомостей регулюються політикою конфіденційності цих сторонніх виробників.

Використання інформації

VPN-клієнти використовують надані користувачем облікові дані для автентифікації у віддаленій мережі та спрямування мережевого трафіку до віддаленої мережі й у зворотному напрямку. Якщо VPN-клієнт стороннього виробника збирає додаткові відомості, використання стороннім виробником цих відомостей здійснюється відповідно до процедур забезпечення конфіденційності цього стороннього виробника.

Вибір і керування

Додати або видалити підключення VPN і переглянути стан наявних підключень можна в розділі **Мережа** в настройках ПК. Після настройки підключення VPN можна вручну підключати або відключати його, вибравши мережу у списку в настройках.

На початок сторінки

Програма підвищення якості ПЗ (CEIP) для Windows

Властивості та завдання

У рамках програми підвищення якості ПЗ (CEIP) для Windows

можуть збиратися відомості про використання програм, ПК, підключених пристроїв і ОС Windows. Можуть також збиратися відомості про проблеми із продуктивністю та надійністю, які виникають у системі. Якщо ви вирішите взяти участь у програмі CEIP для Windows, система Windows надсилатиме ці дані до корпорації Майкрософт, а також періодично завантажуватиме файли для збирання додаткових актуальних відомостей про використання ОС Windows і програм. Ці звіти надсилаються в рамках програми CEIP до корпорації Майкрософт для покращення засобів, якими користувачі користуються найчастіше, та створення рішень для найпоширеніших неполадок.

Збирання, обробка та передавання інформації

Звіти CEIP можуть містити зазначені нижче відомості.

- Відомості про про конфігурацію – це можуть бути дані про кількість процесорів на ПК, кількість використовуваних підключень до мережі, роздільну здатність пристроїв відображення та запущену на ПК версію Windows.

- Відомості про продуктивність і надійність – це може бути інформація про швидкість реагування програм на натискання кнопки, кількість проблем, які виникли під час використання пристрою або програми, а також швидкість надсилання або отримання даних через мережеве підключення.

- Відомості про використання програми – це можуть бути відомості про частоту відкриття програм, частоту звернення до Центру довідки й підтримки Windows, служби, що використовуються для входу до програм, а також кількість папок, які зазвичай створюються на настільному комп'ютері.

Звіти CEIP можуть також містити відомості про події (дані журналу подій) на ПК, які відбулися на ПК щонайбільше за сім днів до моменту приєднання до програми CEIP. Оскільки більшість користувачів вирішує взяти участь у програмі CEIP протягом кількох днів після інсталяції системи Windows, корпорація Майкрософт використовує ці відомості для аналізу та покращення зручності інсталяції ОС Windows.

Ці відомості надсилаються до корпорації Microsoft під час

підключення до Інтернету. До звітів CEIP не включаються контактні дані, зокрема ім’я, адреса або номер телефону; проте до деяких звітів можуть бути випадково додані індивідуальні ідентифікатори, наприклад серійний номер пристрою, підключеного до ПК. Корпорація Майкрософт фільтрує відомості, що містяться у звітах CEIP, намагаючись видалити всі індивідуальні ідентифікатори, які вони можуть містити. Отримавши індивідуальний ідентифікатор, корпорація Майкрософт не використовуватиме його для встановлення особи користувача або зв'язку з ним.

Програма CEIP довільним чином генерує номер GUID (глобальний унікальний ідентифікатор), який надсилається до корпорації Майкрософт із кожним звітом CEIP. GUID дає змогу визначити, які дані надсилалися з певного комп’ютера протягом певного періоду часу. Деякі звіти CEIP можуть також містити ідентифікатори GUID, отримані з облікового запису Microsoft.

Програма CEIP може також періодично завантажувати файл для збирання актуальніших відомостей про використання ОС Windows і програм. Ці файли дають змогу системі Windows збирати додаткові відомості, які допомагають корпорації Майкрософт створювати рішення для поширених проблем і краще зрозуміти особливості використання ОС Windows і програм.

Використання інформації

Корпорація Майкрософт використовує відомості, отримані в рамках програми CEIP, для вдосконалення своїх продуктів і служб, а також програмного забезпечення й устаткування сторонніх виробників, призначеного для використання з цими продуктами та службами. Агреговані відомості, отримані в рамках програми CEIP, можуть також надаватися партнерам корпорації Майкрософт, щоб вони могли вдосконалювати свої продукти та служби, але ці відомості неможливо буде використати для встановлення особи користувача, зв’язку з ним або надсилання реклами.

Ідентифікатор GUID використовується для визначення масштабності проблем, про які було повідомлено, і встановлення їх пріоритетності. Наприклад, ідентифікатор GUID дає корпорації Майкрософт змогу відрізнити ситуацію, коли одна й та ж проблема

виникла сто разів в одного користувача, від ситуації, коли ця проблема виникла один раз у ста користувачів. Корпорація Майкрософт не використовуватиме відомості, зібрані в рамках програми CEIP, для встановлення особи користувача або зв'язку з ним.

Вибір і керування

Якщо вибрати швидке настроювання під час інсталяції ОС Windows, програма CEIP для Windows вмикається автоматично: система Windows і програми Microsoft з Магазину Windows надсилатимуть звіти CEIP для всіх користувачів на ПК. У разі власноручного настроювання параметрів можна керувати програмою CEIP, вибравши пункт **Надсилати до корпорації Майкрософт відомості про використання ПК в рамках програми підвищення якості ПЗ** у розділі **Допомога в покращенні продуктів і служб корпорації Майкрософт**. Після інсталяції Windows адміністратор може змінити цю настройку в **Центрі підтримки** на Панелі керування.

Додаткові відомості див. в розділі Запитання й відповіді щодо програми CEIP.

На початок сторінки

Захисник Windows

Захисник Windows шукає на ПК зловмисні програми та інше потенційно небажане програмне забезпечення. Він містить службу Microsoft Active Protection Service і журнал.

Служба Microsoft Active Protection Service

У разі використання Захисника Windows служба Microsoft Active Protection Service (MAPS) допомагає покращити захист комп'ютера шляхом автоматичного завантаження відомостей про нещодавно виявлені зловмисні програми та стеження за станом безпеки вашого ПК. Служба MAPS надсилає відомості про зловмисні програми й інше потенційно небажане програмне забезпечення до корпорації Майкрософт. Вона також може надсилати файли, які, ймовірно, містять зловмисні програми. Якщо служба MAPS виявляє, що ПК інфіковано певним типом шкідливого програмного

забезпечення, вона, скориставшись даними облікового запису Microsoft, автоматично надсилає користувачу повідомлення, щоб допомогти вирішити цю проблему.

Збирання, обробка та передавання інформації

Звіти MAPS містять відомості про ймовірно зловмисні файли, наприклад імена файлів, криптографічний геш, відомості про видавця програмного забезпечення, розмір, позначки дати. Крім того, служба MAPS може збирати повні URL-адреси для позначення походження файлів, а також IP-адреси, із якими зв'язано файли, що потенційно містять шкідливе програмне забезпечення. Ці URL-адреси іноді можуть містити особисті відомості, наприклад умови пошуку або дані, введені у формах. Звіти можуть також включати дані про дії, які виконуються, коли Захисник Windows сповіщає про виявлення потенційно небажаного програмного забезпечення. Служба MAPS надає ці відомості, щоб допомогти корпорації Майкрософт оцінити ефективність виявлення та видалення зловмисних програм і потенційно небажаного програмного забезпечення, а також ефективність спроб виявлення нових зловмисних програм Захисником Windows.

Звіти автоматично надсилаються до корпорації Майкрософт у вказаних нижче випадках.

- Захисник Windows виявляє програмне забезпечення, для якого ще не було проведено аналіз ризиків.
- Захисник Windows виявляє зміни, внесені програмним забезпеченням, для якого ще не було проведено аналіз ризиків.
- Захисник Windows виконує певні дії зі зловмисною програмою після її виявлення (у рамках автоматичного виправлення).
- Захисник Windows здійснює планове сканування та автоматично виконує дії з виявленим програмним забезпеченням відповідно до визначених настройок.
- Захисник Windows сканує елемент керування ActiveX у браузері Internet Explorer.

У разі приєднання до служб MAPS під час інсталяції Windows

користувачу надається звичайне членство. Звіти в рамках звичайного членства містять відомості, описані в цьому розділі. Звіти в рамках розширеного членства більш вичерпні й можуть містити особисті відомості, наприклад дані про шлях до файлів і часткові дампи пам'яті. Ці звіти, а також звіти від інших користувачів Захисника Windows, що мають членство у службі MAPS, допомагають значно швидше виявляти нові загрози. Після цього створюються визначення зловмисних програм, і ці оновлені визначення надаються всім користувачам за допомогою служби Windows Update.

У разі приєднання до служби MAPS Захисник Windows надсилатиме певні файли або веб-вміст із ПК, у яких, на думку спеціалістів корпорації Майкрософт, може міститися потенційно небажане програмне забезпечення. Звіт із такими зразками використовується для подальшого аналізу. Якщо файл, імовірно, містить особисті відомості, перед його надсиланням відобразиться запит дозволу. Якщо службі Windows Update не вдається отримати оновлені сигнатури для Захисника Windows протягом певного періоду часу, Захисник Windows спробує скористатися службою MAPS для завантаження сигнатур з іншого розташування.

Щоб підвищити рівень конфіденційності, усі відомості надсилаються до служби MAPS у зашифрованій формі за протоколом SSL.

Щоб допомогти виявити та виправити певні види зловмисних програм, Захисник Windows регулярно надсилає службі MAPS відомості про стан безпеки ПК. Сюди належать відомості про настройки безпеки ПК та файли журналу, у яких описуються драйвери й інше програмне забезпечення, що завантажується під час запуску ПК. Також надсилається унікальний ідентифікаційний номер вашого комп'ютера.

Використання інформації

Звіти, надіслані до служби MAPS, використовуються для вдосконалення програмного забезпечення та служб Microsoft. Звіти можуть використовуватися для статистичних, тестових або аналітичних цілей, а також для створення визначень. Служба MAPS не збирає жодних особистих відомостей. Якщо від служби

MAPS випадково надійдуть будь-які особисті відомості, корпорація Майкрософт не використовуватиме їх для встановлення особи користувача, зв’язку з ним або надсилання реклами.

Відомості про стан безпеки ПК, які збираються службою MAPS, використовуються для перевірки ПК на наявність шкідливого програмного забезпечення певного виду. У такому разі корпорація Майкрософт використовує контактні дані з облікового запису Microsoft, щоб звернутися до користувача та надати докладні відомості про проблему та способи її вирішення.

Вибір і керування

Якщо вибрати швидке настроювання під час інсталяції Windows, службу MAPS буде ввімкнуто автоматично. У разі власноручного настроювання параметрів можна керувати службою MAPS, вибравши команду **Скористатися кращим захистом від зловмисних програм, надсилаючи інформацію та файли у службу Microsoft Active Protection Service, коли Захисник Windows увімкнуто** у розділі **Надати доступ до відомостей корпорації Майкрософт і службам інших виробників**. Після інсталяції Windows можна змінити членство у службі MAPS або її настройки, зокрема вимкнути службу MAPS у меню **Настройки** програми Захисник Windows.

Якщо засіб для видалення зловмисних програм отримано через службу Windows Update, цей засіб може продовжувати надсилати відомості до служби MAPS, навіть якщо Захисник Windows вимкнуто. Додаткові відомості див. в декларації про конфіденційність для засобу видалення зловмисного програмного забезпеченняWindows .

Журнал

Властивості та завдання

Журнал містить список усіх програм на ПК, які були виявлені Захисником Windows, а також дії, виконані після їх виявлення.

Крім того, можна переглянути список програм, за виконанням яких на ПК Захисник Windows не стежить (вони називаються дозволеними елементами). Можна також переглянути програми, запуск яких блокується Захисником Windows, доки їх не буде

видалено або знову не буде дозволено їх запуск (такі об’єкти перебувають на карантині).

Збирання, обробка та передавання інформації

Список програмного забезпечення, виявленого Захисником Windows, відомості про дії, які були виконані користувачами, а також дії, які автоматично виконуються Захисником Windows, зберігаються на ПК. Усі користувачі можуть переглянути журнал Захисника Windows та дізнатися про зловмисні програми й інше потенційно небажане програмне забезпечення, яке спробувало інсталюватися або запуститися на ПК, або запуск якого було дозволено іншим користувачем. Наприклад, якщо стало відомо про нову загрозу з боку зловмисної програми, можна переглянути журнал, щоб дізнатися, чи блокує Захисник Windows запуск цієї програми на ПК. До корпорації Майкрософт відомості не надсилаються.

Вибір і керування

Адміністратор може видалити списки журналу.

На початок сторінки

Звітування про критичні помилки Windows

Властивості та завдання

Звітування про критичні помилки Windows допомагає корпорації Майкрософт і партнерам Microsoft діагностувати проблеми у використовуваному програмному забезпеченні та надати відповідні рішення. Деякі проблеми вирішити неможливо, але якщо рішення доступні, вони пропонуються у вигляді схеми вирішення проблеми, про яку повідомив користувач, або у вигляді оновлень, які необхідно інсталювати. Щоб запобігти виникненню проблем і підвищити надійність програмних продуктів, деякі рішення також включаються до складу пакетів оновлень і нових версій програмних продуктів.

Збирання, обробка та передавання інформації

Багато програмних продуктів підтримують роботу із засобом звітування про критичні помилки Windows. Якщо проблема

виникає в одному з цих продуктів, на екрані з'явиться вікно із запитанням, чи слід про неї повідомити.

Засіб звітування про критичні помилки Windows збирає корисні відомості для діагностування та вирішення проблеми, що виникла в користувача, наприклад інформацію про те, де у програмному або апаратному забезпеченні сталася проблема, дані про її тип і критичність, файли, які допоможуть описати проблему, основні відомості про програмне й апаратне забезпечення, інформацію про можливі проблеми із продуктивністю та сумісністю програмного забезпечення. Якщо ОС Windows використовується для розміщення віртуальних машин, звіт про помилки, що надсилається до корпорації Майкрософт, може містити відомості про віртуальні машини.

Засіб звітування про критичні помилки Windows також збирає відомості про програми, драйвери та пристрої, щоб допомогти корпорації Майкрософт зрозуміти проблеми та покращити сумісність програм і пристроїв. Відомості про програму можуть включати імена виконуваних файлів програми. Відомості про пристрої та драйвери можуть включати імена пристроїв, установлених на ПК, а також виконуваних файлів, пов’язаних із відповідними драйверами пристроїв. Можуть збиратися відомості про компанію, яка опублікувала програму або драйвер.

Якщо під час інсталяції ОС Windows було ввімкнуто автоматичне звітування, служба звітування автоматично надсилатиме базові відомості про місце виникнення проблеми. У деяких випадках служба звітування автоматично надсилатиме додаткові відомості, наприклад частковий знімок пам’яті ПК, щоб допомогти діагностувати проблему. Деякі звіти про помили можуть містити особисті відомості, які потрапили до них випадково. Наприклад, звіт зі знімком пам’яті ПК може містити ім’я, частину документа, з яким наразі працює користувач, або дані, які нещодавно надсилалися на веб-сайт.

Для діагностики певних типів проблем засіб звітування про критичні помилки Windows може створити звіт, що містить додаткові відомості, наприклад файли журналу. Перш ніж надіслати звіт, що містить ці додаткові відомості, в ОС Windows відобразиться запит на підтвердження надсилання звіту. Цей запит

відображатиметься, навіть якщо ввімкнуто функцію автоматичного звітування.

Після надсилання звіту служба звітування може запитати додаткові відомості про проблему, яка виникла в користувача. Якщо користувач вирішить у такому разі повідомити свій номер телефону або адресу електронної пошти, його звіт про помилки можна буде пов'язати з його особою. Корпорація Майкрософт може звернутися до користувача, щоб отримати додаткові відомості, що допоможуть вирішити проблему, про яку він повідомив.

Служба звітування про критичні помилки Windows довільним чином генерує номер GUID (глобальний унікальний ідентифікатор), який надсилається до корпорації Майкрософт разом із кожним звітом про помилки. GUID дає змогу визначити, які дані надсилалися з певного комп'ютера протягом певного періоду часу. Ідентифікатор GUID не містить жодних особистих відомостей.

Щоб підвищити рівень конфіденційності, відомості надсилаються в зашифрованій формі за протоколом SSL.

Використання інформації

Корпорація Майкрософт використовує відомості про помилки та проблеми, про які повідомляють користувачі Windows, для вдосконалення продуктів і служб Microsoft, а також програмного й апаратного забезпечення сторонніх виробників, призначеного для використання з цими продуктами та службами. Ідентифікатор GUID використовується для визначення масштабності проблем, про які було повідомлено, і встановлення їх пріоритетності. Наприклад, ідентифікатор GUID дає корпорації Майкрософт змогу відрізнити ситуацію, коли одна й та ж проблема виникла сто разів в одного користувача, від ситуації, коли ця проблема виникла один раз у ста користувачів.

Працівникам, підрядникам, постачальникам і партнерам корпорації Майкрософт може бути надано доступ до певних частин зібраної інформації, але їм дозволено використовувати ці відомості лише для виправлення або вдосконалення продуктів і служб Microsoft або програмного й апаратного забезпечення сторонніх виробників, призначеного для використання із продуктами та службами

Microsoft. Якщо звіт про помилки містить особисті відомості, корпорація Майкрософт не використовуватиме їх для встановлення особи користувача, зв’язку з ним або надсилання реклами. Проте якщо користувач сам надає свою контактну інформацію, як описано вище, вона може використовуватися для зв'язку з ним.

Вибір і керування

Якщо вибрати швидке настроювання під час інсталяції Windows, засіб звітування про критичні помилки Windows автоматично надсилатиме звіти для пошуку вирішень проблем. Якщо ви настроюєте параметри власноруч, для керування засобом звітування про критичні помилки Windows можна скористатися параметром **Використовувати засіб звітування про критичні помилки Windows для пошуку рішень проблем в Інтернеті** у розділі **Пошук рішень в Інтернеті**. Після інсталяції Windows цю настройку можна змінити в Центрі підтримки на Панелі керування.

Додаткові відомості див. в декларації про конфіденційність для служби звітування про критичні помилки Microsoft.

На початок сторінки

Зіставлення файлів Windows

Властивості та завдання

Зіставлення файлів Windows допомагає користувачам зіставляти типи файлів із певними програмами. Якщо ви намагаєтеся відкрити тип файлу, а з його типом не зіставлено жодну програму, в ОС Windows відобразиться запитання, чи слід скористатися засобом зіставлення файлів Windows, щоб знайти програму для цього файлу. Цей засіб, зокрема, виконує пошук сумісної програми в Магазині Windows. На екрані відображаються програми, які зазвичай зіставляються з таким розширенням імені файлу.

Збирання, обробка та передавання інформації

Якщо користувач погодиться на використання засобу зіставлення файлів Windows, до корпорації Майкрософт надсилатиметься розширення імені файлу (наприклад, docx або pdf), а також мова

інтерфейсу ПК. Інша частина імені файлу до корпорації Майкрософт не надсилатиметься. У разі зіставлення файлу з певною програмою надсилається унікальний ідентифікатор програми, який дає змогу визначати програму за замовчуванням для кожного типу файлів.

Використання інформації

Якщо надіслано розширення імені файлу, служба повертає список програм, які, за даними корпорації Майкрософт, можуть відкривати файли з таким розширенням. Якщо не вибрати завантаження та інсталяцію програми, зіставлення для цього типу файлу не зміниться.

Вибір і керування

У разі спроби відкрити файл, тип якого не зіставлено з жодною програмою, можна вказати, чи слід використовувати засіб зіставлення файлів Windows. Якщо користувач не бажає використовувати цей засіб, до корпорації Майкрософт не надсилаються жодні дані зіставлення файлів.

На початок сторінки

Довідка Windows

Онлайновий центр довідки та підтримки Windows

Властивості та завдання

Якщо ввімкнуто Онлайновий центр довідки та підтримки Windows, користувач буде отримувати найактуальнішу довідкову інформацію та відомості з підтримки, які лиш доступні в момент підключення до Інтернету.

Збирання, обробка та передавання інформації

У разі використання Онлайнового центру довідки та підтримки Windows до корпорації Майкрософт надсилаються пошукові запити користувача та його запити довідкової інформації, які реєструються під час вибору відповідного посилання. Система Windows надсилає певні відомості про конфігурацію ПК, які допоможуть знайти найбільш актуальну довідкову інформацію. Для

Онлайнового центру довідки та підтримки Windows також використовуються стандартні веб-технології, наприклад файли cookie.

Використання інформації

Корпорація Майкрософт використовує відомості для повернення розділів довідки у відповідь на пошуковий запит, надання найбільш відповідних результатів, а також створення нового та вдосконалення наявного вмісту. Відомості про конфігурацію ПК використовуються для відображення відповідного вмісту довідки для цієї конфігурації. Файли cookie та інші веб-технології використовуються для спрощення навігації у довідці та допомагають краще зрозуміти, як користувачі використовують Онлайновий центр довідки та підтримки Windows.

Вибір і керування

Онлайновий Центр довідки та підтримки увімкнуто за замовчуванням. Щоб змінити ці настройки, торкніться піктограми **Настройки** або клацніть її у верхній частині вікна «Центр довідки та підтримки», а потім установіть або зніміть прапорець **Отримати довідку в Інтернеті**. Щоб очистити файли cookie, які використовуються Центром довідки та підтримки Windows, відкрийте розділ «Властивості браузера» на Панелі керування, натисніть кнопку **Видалити** в області **Журнал браузера**, виберіть **Файли cookie та дані веб-сайтів**, а потім натисніть кнопку **Видалити**. Якщо вибрати блокування всіх файлів cookie (у розділі «Конфіденційність» вікна «Властивості браузера»), Центр довідки та підтримки Windows не встановлюватиме файли cookie.

Програма вдосконалення Центру довідки та підтримки

Властивості та завдання

Програма вдосконалення Центру довідки та підтримки (HEIP) допомагає корпорації Майкрософт визначати тенденції використання Онлайнового центру довідки та підтримки Windows, що дає змогу покращувати результати пошуку та відповідність вмісту.

Збирання, обробка та передавання інформації

Програма HEIP надсилає до корпорації Майкрософт відомості про версію Windows на ПК, а також інформацію про використання Центру довідки та підтримки Windows, зокрема запити, що вводяться під час пошуку даних у Центрі довідки та підтримки Windows, а також будь-які оцінки або відгуки щодо наданих розділів довідки. До корпорації Майкрософт надсилатимуться відомості про пошук, перегляд, оцінювання або відгуки стосовно розділів довідки, наданих користувачу.

Програма вдосконалення Центру довідки та підтримки довільним чином генерує номер GUID (глобальний унікальний ідентифікатор), який надсилається до корпорації Майкрософт із кожним звітом цієї програми. Номер GUID дає змогу визначити, які дані надсилалися з певного ПК протягом певного періоду часу. Ідентифікатор GUID не містить жодних особистих відомостей. Цей ідентифікатор GUID відрізняється від ідентифікаторів GUID, що використовуються засобом звітування про критичні помилки Windows і програмою Windows CEIP.

Використання інформації

Зібрані дані використовуються для виявлення тенденцій і схем використання довідки. Ці дані допомагають корпорації Майкрософт поліпшувати якість вмісту та точність результатів пошуку. Ідентифікатор GUID використовується для визначення масштабності проблем, про які стало відомо, і встановлення їх пріоритетності. Наприклад, ідентифікатор GUID дає корпорації Майкрософт змогу відрізнити ситуацію, коли одна й та ж проблема виникла сто разів в одного користувача, від ситуації, коли така проблема виникла один раз у ста користувачів.

Програма вдосконалення Центру довідки та підтримки не збирає свідомо жодних відомостей, які можна використати для встановлення особи користувача. Якщо такі відомості були введені в полях пошуку або відгуку, вони будуть надіслані, але корпорація Майкрософт не використовуватиме їх для встановлення особи користувача, зв’язку з ним або надсилання реклами.

Вибір і керування

У разі вибору швидкого настроювання під час інсталяції Windows

користувач автоматично зараховується до учасників програми вдосконалення Центру довідки та підтримки. У разі власноручного настроювання параметрів можна керувати настройками програми вдосконалення Центру довідки та підтримки, вибравши пункт **Надсилати до корпорації Майкрософт відомості про використання довідки в рамках програми HEIP** у розділі **Допомога в покращенні продуктів і служб корпорації Майкрософт**. Після інсталяції ОС Windows цю настройку можна змінити в Центрі довідки та підтримки Windows.

На початок сторінки

Віддалена допомога

Властивості та завдання

За допомогою служби віддаленої допомоги можна запросити іншого користувача підключитися до вашого ПК та допомогти, навіть якщо цей користувач наразі не поряд. Після підключення інший користувач зможе бачити ваш ПК. З вашого дозволу він може використовувати свою мишу та клавіатуру для керування вашим ПК й показати, як виправити певну неполадку.

Збирання, обробка та передавання інформації

Служба віддаленої допомоги створює шифроване підключення між двома ПК через Інтернет або локальну мережу. Коли інший користувач підключається до вашого ПК за допомогою служби віддаленої допомоги, він може бачити робочий стіл, усі відкриті документи та всі видимі особисті відомості. Крім того, якщо ви дозволяєте іншому користувачу керувати ПК за допомогою миші та клавіатури, він може виконувати так дії, як видалення файлів або змінення настройок. Після встановлення підключення служба віддаленої допомоги обмінюється контактними даними, до яких належать ім’я користувача, ім’я ПК та зображення облікового запису. Усі підключення віддаленої допомоги реєструються у файлі журналу сеансу.

Використання інформації

Надіслана інформація використовується для встановлення шифрованого з'єднання та для надання іншому користувачу

доступу до вашого робочого стола. До корпорації Майкрософт відомості не надсилаються.

Вибір і керування

Перш ніж дозволити іншому користувачу підключитися до ПК, закрийте всі програми або документи, які йому не слід бачити. Якщо ви почуваєтеся незручно через те, що бачить або робить на вашому ПК інший користувач, натисніть клавішу Esc для завершення сеансу. Ведення журналу сенсів і обмін контактними даними можна вимкнути, знявши відповідні прапорці в настройках віддаленої допомоги.

На початок сторінки

Служба пошуку Windows Search

Властивості та завдання

Служба пошуку Windows Search дає змогу виконувати пошук на пристрої та в Інтернеті з єдиного розташування. Для покращення результатів пошуку Служба пошуку Windows Search може використовувати службу Bing і платформу визначення розташування Windows. Зауважте, що на пристрої доступні також інші окремі засоби пошуку, надані корпорацією Майкрософт, наприклад пошук у Магазині Windows, пошук у браузері Internet Explorer, а також пошук в інших продуктах Microsoft.

Збирання, обробка та передавання інформації

Якщо ввімкнути отримання результатів пошуку в Інтернеті, ОС Windows надсилатиме відомості, введені користувачем у службі пошуку Windows Search, до корпорації Майкрософт. Щоб покращити результати пошуку, служба пошуку Windows Search також надсилає до корпорації Майкрософт відомості про використання цього засобу користувачем. Служба пошуку Windows Search також надсилає ідентифікатор для надання персоналізованих результатів пошуку на основі взаємодії користувача зі службою Bing та іншими продуктами та службами Microsoft. Якщо виконати вхід до ОС Windows за допомогою облікового запису Microsoft, ідентифікатор буде пов’язано з обліковим записом Microsoft. За бажання можна відмовитися від

отримання персоналізованих результатів пошуку у службі пошуку Windows Search. У такому разі ідентифікатор не надсилатиметься.

Якщо дозволити службі пошуку Windows Search використовувати дані про розташування, відомості про фізичне розташування пристрою, надані платформою визначення розташування Windows, надсилатимуться до корпорації Майкрософт у складі кожного пошукового запиту. Корпорація Майкрософт може також спробувати визначити приблизне фізичне розташування користувача на основі IP-адреси.

Якщо служба Windows Search використовується для пошуку у програмі, умови пошуку надаються цій програмі.

Використання інформації

Якщо служба Windows Search використовується для пошуку в Інтернеті, корпорація Майкрософт застосовує вказані умови пошуку, журнал локального пошуку та пошуку в Інтернеті, а також відомості, пов’язані з обліковим записом Microsoft, і відомості про розташування пристрою для надання відповідних пошукових пропозицій, персоналізованих результатів пошуку та функцій в інших продуктах і службах Microsoft. Додаткові відомості про використання даних користувача див. в декларації про конфіденційність для служби Bing.

Якщо служба Windows Search використовується для пошуку у програмі стороннього виробника, зібрані відомості використовуватимуться відповідно до процедур забезпечення конфіденційності цього виробника. Процедури забезпечення конфіденційності під час пошуку у програмі Microsoft викладені у декларації про конфіденційність цієї програми.

Вибір і керування

У разі вибору швидкого настроювання під час інсталяції ОС Windows службі пошуку Windows Search надається дозвіл отримувати пошукові пропозиції та результати пошуку в Інтернеті, а корпорації Майкрософт надається дозвіл використовувати дані зі служби пошуку Windows Search (зокрема, відомості про розташування) для персоналізації служби пошуку Windows Search та інших можливостей від корпорації Майкрософт. У разі вибору

настроювання параметрів ці настройки служби пошуку Windows Search можна змінити. Після інсталяції ОС Windows їх можна змінити у розділі **Пошук** в настройках ПК.

Журнал локального пошуку та, частково, журнал пошуку у службі Bing, що використовується для персоналізації можливостей пошуку Windows, можна очистити в підрозділі **Пошук** в розділі **Пошук і програми** в настройках ПК. Для корпорації Майкрософт очищення журналу пошуку означає, що вона не повинна використовувати зібрані раніше дані журналу пошуку для персоналізації пошукових пропозицій або впорядкування результатів пошуку. Це не призводить до видалення реклами або іншої інформації для персоналізації (зокрема, відомостей, отриманих із журналу пошуку), а також не спричиняє видалення відомостей, які використовуються корпорацією Майкрософт в агрегованій формі для покращення результатів пошуку та інших функцій, що надаються корпорацією Майкрософт. Ця інформація зберігається та знеособлюється, як описано в декларації про конфіденційність для служби Bing. Ви можете керувати параметрами служби Microsoft Advertising та іншими параметрами персоналізації через Інтернет.

На початок сторінки

Програма інсталяції Windows

У цьому розділі описано функції, доступні під час інсталяції ОС Windows.

Динамічне оновлення

Властивості та завдання

Динамічне оновлення дає змогу ОС Windows виконувати одноразову перевірку за допомогою служби Windows Update для отримання останніх оновлень для ПК під час інсталяції системи Windows. Якщо оновлення знайдено, засіб динамічного оновлення автоматично завантажує й інсталює їх на ПК, щоб забезпечити актуальність його стану під час першого входу або використання.

Збирання, обробка та передавання інформації

Щоб інсталювати сумісні драйвери, засіб динамічного оновлення

надішле до корпорації Майкрософт відомості про устаткування ПК. Нижче наведено типи оновлень, які засіб динамічного оновлення може завантажувати на ПК.

- **Оновлення інсталяції.** Важливі оновлення програмного забезпечення для інсталяційних файлів, що сприяють успішному завершенню інсталяції.
- **Оновлення драйверів у комплекті поставки.** Важливі оновлення драйверів для версії Windows, яку необхідно інсталювати.

Крім того, якщо інсталювати ОС Windows із Магазину Windows, засіб динамічного оновлення завантажить та інсталює останні оновлення для ОС Windows, а також деякі необхідні драйвери устаткування для ПК.

Використання інформації

Засіб динамічного оновлення повідомляє корпорації Майкрософт відомості про устаткування ПК, які допоможуть визначити правильні драйвери для системи.

Вибір і керування

Якщо інсталювати Windows із Магазину Windows, програма інсталяції завантажує й інсталює оновлення автоматично. У разі інсталяції ОС Windows із фізичного носія відображається запитання, чи слід підключитися до Інтернету для інсталяції оновлень.

Програма підвищення якості інсталяції

Властивості та завдання

Ця функція надсилає до корпорації Майкрософт один звіт, що містить базові відомості про ПК та спосіб інсталяції ОС Windows. Корпорація Майкрософт використовує ці відомості для покращення можливостей інсталяції та створення рішень для поширених проблем, які можуть виникати під час її здійснення.

Збирання, обробка та передавання інформації

Зазвичай звіт містить відомості про інсталяцію, зокрема дату інсталяції, час, витрачений на виконання кожної її фази, тип

інсталяції (оновлення чи інсталяція нового продукту), відомості про версію, мову операційної системи, тип носія, конфігурацію ПК та стан завершення інсталяції (успішно чи з помилками), а також коди всіх помилок.

Якщо користувач погодиться на участь у програмі покращення інсталяції, під час наступного підключення до Інтернету до корпорації Майкрософт буде надіслано звіт. Програма покращення інсталяції довільним чином генерує номер GUID (глобальний унікальний ідентифікатор), який надсилається до корпорації Майкрософт разом зі звітом. GUID дає змогу визначити, які дані надсилалися з певного комп'ютера протягом певного періоду часу. Ідентифікатор GUID не містить жодних особистих відомостей і не використовується для встановлення особи користувача.

Використання інформації

Корпорація Майкрософт і її партнери використовують звіт для вдосконалення своїх продуктів і служб. Ідентифікатор GUID використовується для зіставлення цих даних із даними, зібраними в рамках програми підвищення якості ПЗ Windows, у якій можуть брати участь користувачі системи Windows.

Вибір і керування

Приєднатися до цієї програми можна під час інсталяції Windows, установивши прапорець **Допомогти покращити інсталяцію ОС Windows** .

Додаткові відомості див. в розділі «Windows CEIP».

Порадник із сумісності інсталяції

Властивості та завдання

Під час інсталяції ОС Windows програма інсталяції допомагає визначити, чи готовий наявний ПК до оновлення до версії Windows 8.1, і надає інформацію про сумісність програм і пристроїв.

Збирання, обробка та передавання інформації

Під час визначення сумісності збираються певні відомості про потенційні можливості оновлення, зокрема характеристики вашого комп'ютерного устаткування, дані про підключені до комп'ютера

пристрої та інстальовані на ньому програми. Іноді відомості про видавця програми можуть містити його ім'я або адресу електронної пошти.

Використання інформації

Корпорація Майкрософт використовує зібрану інформацію для виявлення правильних драйверів для ПК та визначення сумісності ПК, програм і пристроїв з ОС Windows 8.1. Ці відомості також потрібні для подальшого вдосконалення продуктів і служб. Ці відомості не використовуються для встановлення особи користувача, зв’язку з ним або надсилання реклами.

Вибір і керування

У разі інсталяції Windows із Магазину Windows або з фізичного носія із пристрою, на якому вже інстальовано ОС Windows, відомості, описані в цьому розділі, будуть надіслані до корпорації Майкрософт. Якщо для інсталяції Windows комп’ютер завантажується з фізичного інсталяційного носія, програма інсталяції не перевірятиме відомості про сумісність в Інтернеті.

На початок сторінки

Спільний доступ Windows

Властивості та завдання

За допомогою спільного доступу Windows можна надавати спільний доступ до вмісту різним програмам із Магазину Windows, які підтримують таку функцію. Ця функція також дає змогу обмінюватися вмістом із друзями.

Збирання, обробка та передавання інформації

Під час надання спільного доступу вихідна програма передає вміст до цільової програми лише після вибору цієї цільової програми в області пошуку. Якщо вихідна програма не надає спільний доступ до вмісту, такий доступ надати до зображення, яке відображається на екрані. Щоб спростити процес, цільові програми та користувачі, яким найчастіше надається спільний доступ до вмісту, відображаються у відповідному списку в області пошуку. До корпорації Майкрософт відомості не надсилаються.

Використання інформації

Збережені відомості щодо періодичності надання спільного доступу цільовим програмам та користувачам, яким такий доступ надається найчастіше, використовуються для сортування елементів списку в області пошуку за частотою вибору. У разі надання спільного доступу до відомостей третій стороні, ці відомості використовуватимуться відповідно до політики конфіденційності такої третьої сторони. Процедури забезпечення конфіденційності в разі надання спільного доступу програмі Microsoft будуть викладені в її декларації про конфіденційність.

Вибір і керування

За замовчуванням в ОС Windows зберігаються відомості про використання засобу надання спільного доступу Windows. Зберігання цієї інформації можна припинити. Крім того, можна видалити всі збережені цільові об’єкти в підрозділі **Спільний доступ** у розділі **Пошук і програми** в настройках ПК.

На початок сторінки

Windows SmartScreen

Властивості та завдання

Фільтр Windows SmartScreen допомагає захистити ПК, перевіряючи завантажені файли та дані з Інтернету в програмах, щоб убезпечити ПК від зловмисного ПЗ і потенційно небезпечного вмісту з Інтернету. Перед відкриттям невідомого або потенційно небезпечного завантаженого файлу на екрані відобразиться попередження. Якщо засіб SmartScreen виявить у програмі потенційно небезпечний вміст з Інтернету, в ОС Windows замість цього вмісту відобразиться попередження.

Збирання, обробка та передавання інформації

Якщо засіб Windows SmartScreen використовується для перевірки завантажуваних файлів, ОС Windows надсилає інформацію до онлайнової служби SmartScreen, зокрема ім’я файлу, ідентифікатор файлу (його «геш») та інформацію про цифровий сертифікат, а також стандартні відомості про ПК та номер версії фільтра

Windows SmartScreen. Щоб підвищити рівень конфіденційності, відомості надсилаються до корпорації Майкрософт у зашифрованій формі за протоколом SSL.

У разі використання Windows SmartScreen, для блокування потенційно небезпечного вмісту у програмах, ОС Windows надсилає інформацію до онлайнової служби SmartScreen, зокрема дані про адреси та типи вмісту, до яких отримують доступ деякі програми з Магазину Windows під час їх використання. У відповідь на це онлайнова служба повідомляє, чи не надходили до корпорації Майкрософт повідомлення про те, що цей вміст є небезпечним або підозрілим. Звіти, що надсилаються до корпорації Майкрософт, містять таку інформацію, як назва або ідентифікатор програми та повні адреси веб-вмісту, до якого отримує доступ програма.

Щоб підвищити рівень конфіденційності, відомості надсилаються до корпорації Майкрософт у зашифрованій формі. Адреса, що надсилається до корпорації Майкрософт, може містити відомості, пов’язані з веб-сторінкою, яка відкривається всередині програми (зокрема умови пошуку). Наприклад, у разі пошуку слова у програмі-словнику це слово може надсилатися до корпорації Майкрософт у складі повної адреси, до якої отримує доступ програма. Корпорація Майкрософт фільтрує ці адреси, намагаючись видалити особисті відомості, якщо є така змога.

Система Windows довільним чином генерує номер GUID (глобальний унікальний ідентифікатор), який надсилається до корпорації Майкрософт із кожним звітом. GUID дає змогу визначити, які дані надсилалися з певного комп’ютера протягом певного періоду часу. Ідентифікатор GUID не містить жодних особистих відомостей.

Використання інформації

Корпорація Майкрософт використовує описані вище відомості для попередження користувача про потенційно небезпечні завантажені файли та вміст програм. Наприклад, якщо SmartScreen виявляє потенційну загрозу всередині програми, яка підтримує SmartScreen, в ОС Windows замість вмісту відобразиться відповідне попередження. Ця інформація також використовується

для вдосконалення засобу SmartScreen та інших продуктів і служб. Корпорація Майкрософт не використовує відомості для надсилання реклами.

Вибір і керування

У разі вибору швидкого настроювання під час інсталяції Windows фільтр Windows SmartScreen вмикається автоматично. Якщо ви настроюєте параметри власноруч, для керування настройками Windows SmartScreen виберіть завдання **Використовувати мережеві служби SmartScreen для кращого захисту від шкідливого вмісту на сайтах, завантажених програмами з Магазину Windows і браузером Internet Explorer, а також від шкідливих завантажень** у розділі **Допомога у захисті ПК та конфіденційності даних**. Після інсталяції Windows цю настройку можна змінити в Центрі підтримки на Панелі керування. Відомості про службу Internet ExplorerSmartScreen див. в розділі «Фільтр SmartScreen» декларації про конфіденційність для браузера Internet Explorer.

На початок сторінки

Засіб розпізнавання мовлення Windows

Властивості та завдання

Засіб розпізнавання мовлення Windows забезпечує розпізнавання мовлення в системі Windows та для будь-яких програм, що використовують цю технологію. Точність розпізнавання мовлення Windows підвищується за рахунок дослідження особливостей використання мови користувачем, зокрема реєстрації звуків і слів, які він використовує.

Збирання, обробка та передавання інформації

Засіб розпізнавання мовлення Windows зберігає список слів і їхню вимову на ПК. Слова та вимова додаються до цього списку за допомогою словника розпізнавання, а також шляхом диктування слів та їх виправлення в засобі розпізнавання мовлення Windows.

Якщо в засобі розпізнавання мовлення Windows увімкнуто функцію перегляду документів, текст із документів Microsoft Office Word (з розширенням імені файлу DOC або DOCX) і електронна пошта (з

папок електронної пошти, окрім папок «Видалені» або «Небажана пошта») на ПК та в будь-якій підключеній спільній папці, включеній до списку розташувань індексу пошуку Windows, збирається та зберігається у вигляді фрагментів з одного, двох або трьох слів. Фрагменти з одного слова містять лише слова, додані до користувацьких словників, а фрагменти із двох і трьох слів містять лише слова, які містяться у стандартних словниках.

Усі зібрані відомості зберігаються у персональному мовленнєвому профілі на ПК. Мовленнєві профілі зберігаються окремо для кожного користувача. Користувач може отримати доступ лише до власного мовленнєвого профілю, але не до профілів інших людей на цьому ПК. Проте адміністратори мають доступ до будь-якого профілю на ПК. Відомості профілю не надсилаються до корпорації Майкрософт, якщо користувач не надасть відповідний дозвіл у відповідь на запит засобу розпізнавання мовлення Windows. Дані можна переглянути перед надсиланням. Якщо користувач вирішить надіслати ці відомості, будуть надіслані також дані акустичної адаптації, що використовуються для адаптації до вимови користувача.

Після завершення сеансу навчання розпізнаванню у засобі розпізнавання мовлення Windows відобразиться запитання про те, чи слід надсилати відомості мовленнєвого профілю до корпорації Майкрософт. Відомості можна переглянути перед надсиланням. Вони можуть включати записи голосу, зроблені під час сеансу навчання та іншу інформацію з особистого мовленнєвого профілю.

Використання інформації

Засіб розпізнавання мовлення Windows використовує слова із мовленнєвого профілю для перетворення мовлення на текст. Корпорація Майкрософт використовує відомості мовленнєвого профілю для вдосконалення своїх продуктів і служб. Ці відомості не використовуються для встановлення особи користувача, зв’язку з ним або надсилання реклами.

Вибір і керування

Розпізнавання мовлення Windows можна ввімкнути або вимкнути на власний розсуд. У разі запуску засобу розпізнавання мовлення Windows функцію перегляду документів буде ввімкнуто за

замовчуванням. Настройки засобу перегляду документів можна змінити під час першого запуску засобу розпізнавання мовлення Windows. У розділі «Розпізнавання мовлення» на Панелі керування можна змінити настройки розпізнавання мовлення або видалити особисті мовленнєві профілі, вибравши **Додатково в параметрах мовлення**. Також за допомогою засобу «Змінити наявні слова» у словнику розпізнавання мовлення можна видаляти слова, особисто додані до мовленнєвого профілю. Проте видалення особистого мовленнєвого профілю не означатиме видалення слів, доданих за допомогою словника розпізнавання.

Змінити розташування, з яких засіб перегляду документів повинен збирати слова, можна в індексі пошуку Windows. Щоб переглянути або змінити розташування, включені до індексу пошуку Windows, відкрийте розділ «Параметри індексування» на Панелі керування.

Наприкінці сеансу навчання відобразиться запит стосовно того, чи слід надсилати дані навчання та інші відомості мовленнєвого профілю до корпорації Майкрософт. Коли розпізнавання мовлення Windows запущено, відомості можна також надсилати, клацнувши правою кнопкою елемент **Мікрофон**і вибравши команду **Допомогти покращити розпізнавання мовлення**. У будь-якому разі можна переглянути всі файли даних перед надсиланням або відмовитися від їх надсилання.

На початок сторінки

Магазин Windows

У Магазині Windows можна шукати програми, інсталювати їх на ПК та керувати ними. У розділі нижче описано, як функції Магазину та отриманих із нього програм можуть вплинути на рівень конфіденційності, а також наведено процедури, які дають змогу контролювати цей вплив.

Програма та служба Магазин

Властивості та завдання

У Магазині можна шукати програми та інсталювати їх на ПК. У ньому також відстежуються інстальовані на ПК програми з Магазину, що дає змогу отримувати оновлення для цих програм та

інсталювати їх на кілька ПК.

Збирання, обробка та передавання інформації

Щоб знайти та інсталювати програму, необхідно виконати вхід до Магазину за допомогою облікового запису Microsoft. Це надає Магазину доступ до відомостей, зазначених у профілі облікового запису Microsoft, зокрема до імені, адреси електронної пошти та зображення облікового запису. Магазин збирає та зв’язує наведені нижче додаткові відомості з обліковим записом Магазину.

- Платежі в магазині. Відомості про придбані товари, сплачені суми та спосіб оплати під час придбання програм або здійснення покупок у програмах за допомогою облікового запису Магазину.

- Інстальовані програми. Список програм, інстальованих із Магазину, політика ліцензування кожної з них (постійна ліцензія чи ознайомлювальна версія з обмеженим терміном дії), а також список покупок, зроблених із використанням облікового запису в Магазині в кожній із програм. Ця інформація зберігається в Інтернеті в обліковому записі Магазину, крім того, відомості про ліцензування кожної інстальованої програми зберігаються Магазином на ПК. Вони дають змогу ідентифікувати користувача як власника ліцензії.

- ПК, на яких інстальовано програми. Марка, модель та ім’я кожного ПК, на якому інстальовано програми, разом із номером, який дає змогу однозначно ідентифікувати ПК. Цей номер створюється на основі конфігурації устаткування ПК та не містить відомостей про користувача.

- Оцінки, відгуки та звіти про проблеми. Після інсталяції програми користувач може написати про неї відгук або оцінити її в Магазині. З цими оцінками пов’язується обліковий запис Microsoft. У разі написання відгуку разом із ним буде опубліковано ім’я та зображення облікового запису Microsoft.

- Особисті настройки Магазину. Настройки перегляду програм у Магазині, наприклад відображення лише тих програм, які доступні рідною мовою користувача.

За бажання в обліковому записі Магазині можна зберігати відомості про оплату, наприклад номер кредитної картки. З міркувань безпеки ці відомості передаються за допомогою SSL, а номер кредитної картки, окрім останніх чотирьох цифр, зберігається в зашифрованому вигляді.

Магазин збирає відомості про вашу копію Windows, щоб визначити її тип: проданий у роздрібному магазині екземпляр, оцінювальна копія, копія, отримана в рамках програми корпоративного ліцензування, чи екземпляр, попередньо інстальований виробником ПК. Під час першого підключення до Магазину до нього надсилається список усіх програм, попередньо інстальованих на ПК, а потім ліцензії цих програм зв'язуються з обліковим записом Магазину.

Під час перегляду вмісту в Магазині та використання отриманих із нього програм корпорація Майкрософт збирає певні відомості, які допомагають зрозуміти структуру та тенденції використання (так само, як веб-сайти аналізують дані перегляду своїх сторінок відвідувачами).

Використання інформації

Корпорація Майкрософт використовує контакті відомості користувача для надсилання повідомлень електронної пошти, необхідних для надання послуг Магазину, наприклад квитанцій для програм, які купує користувач. Вона використовує відомості про оплату, щоб надавати користувачу змогу оплатити покупку; у разі зберігання цих відомостей їх не потрібно вводити щоразу. Корпорація Майкрософт використовує відомості про покупки для забезпечення функціонування Магазину та його служби підтримки.

Магазин відстежує всі інстальовані програми. Його можна використовувати для керування списком пристроїв, на які інстальовано програми. Служба підтримки також може допомогти в керуванні цими відомостями. Після інсталяції програми вона завжди відображається в журналі покупок Магазину, навіть якщо її потім було видалено. Крім того, Магазин використовує цей список для обмеження кількості ПК, на які можна інсталювати програму, відповідно до умов використання Магазину Windows. У разі написання відгуку про програму, поруч із цим відгуком у Магазині

публікується ім’я користувача та зображення облікового запису, пов’язане з обліковим записом Windows. Повідомлення про проблеми із програмою надсилаються представникам Магазину, щоб вони оцінили проблему та вжили необхідних заходів. За необхідності під час перевірки звіту може використовуватись ім’я та адреса електронної пошти, пов’язані з обліковим записом Магазину.

Коли для інстальованих програм з’являються оновлення, у Магазині відображається сповіщення, а на плитці Магазину вказується кількість доступних оновлень. Користувач може переглянути список доступних оновлень і вибрати, які з них слід інсталювати. Оновлені програми можуть використовувати ширше коло можливостей Windows, ніж попередні версії, що дає їм змогу отримати доступ до інших ресурсів на ПК. Оновлений список можливостей можна переглянути на сторінці опису програми, на яку веде посилання на сторінці зі списком доступних оновлень.

Магазин використовує зібрані відомості щодо копії Windows для визначення способу інсталяції ОС Windows на ПК (наприклад, чи було її попередньо інстальовано виробником). Ці відомості дають змогу Магазину надавати користувачам доступ до програм, які виробники ПК розробляють спеціально для своїх клієнтів. Вони також використовуються для надання відомостей корпорації Майкрософт (інколи також, в агрегованому вигляді, – виробнику ПК) щодо схем використання ОС Windows.

Корпорація Майкрософт використовує певні дані про придбання та використання програми в агрегованому вигляді для визначення способів використання Магазину (наприклад, способів застосування користувачами інстальованих програм). Корпорація Майкрософт може надавати деякі агреговані статистичні дані розробникам програм. Корпорація Майкрософт не надає жодних особистих відомостей розробникам програм. Зібрані Магазином дані про перегляд і використання сторінок застосовуються для кращого розуміння принципів використання Магазину та вдосконалення його функцій і служб.

Вибір і керування

Якщо користувач вирішує використовувати Магазин, указані в

цьому розділі відомості надсилатимуться до корпорації Майкрософт, як описано вище.

Якщо необхідно видалити опублікований відгук про програму, відкрийте опис програми в Магазині, перейдіть у режим редагування відгуків і видаліть текст.

Автоматичні оновлення програм

Властивості та завдання

Ця функція дає змогу перевірити наявність оновлень для програм із Магазину Windows, завантажити їх та інсталювати, щоб забезпечити використання найновіших версій. Оновлення програм можуть передбачати оновлення системи безпеки, виконання оновлень або додавання нових функціональних можливостей чи вмісту. Оновлені програми можуть використовувати ширше коло можливостей Windows, ніж попередні версії, що дає їм змогу отримати доступ до інших ресурсів на ПК. Ви можете дізнатися про зміни в можливостях на сторінці опису програми в Магазині Windows.

Збирання, обробка та передавання інформації

Для автоматичного оновлення програм Магазин надсилає до корпорації Майкрософт зазначені нижче відомості.

- Список усіх програм, інстальованих із Магазину всіма користувачами цього ПК
- Відомості про ліцензування для кожної програми
- Випадки успішного та невдалого виконання операцій оновлення програм із Магазину, а також помилки, які виникали під час здійснення цього процесу
- GUID (глобальний унікальний ідентифікатор) – створений довільним чином номер, який не містить особистих відомостей
- Ім’я BIOS, номер редакції та дата редакції
- Основна інформація про ПК, наприклад дані про виробника, модель і використовуваний випуск Windows

Використання інформації

Ця інформація використовується для забезпечення роботи служби оновлення. Вона також використовується для створення агрегованої статистики, яка дає змогу корпорації Майкрософт аналізувати тенденції та вдосконалювати свої продукти та служби. Ці відомості не використовуються для встановлення особи користувача, зв’язку з ним або надсилання реклами.

Вибір і керування

У разі вибору швидкого настроювання під час інсталяції ОС Windows Магазин Windows буде автоматично перевіряти наявність оновлень програм, завантажувати їх та інсталювати, навіть після виходу з Магазину Windows. Вимкнувши автоматичні оновлення програм, можна самостійно вирішувати, чи слід інсталювати оновлення програм, під час входу до Магазину Windows.

Щоб вимкнути автоматичні оновлення програм, виконайте вказані нижче дії.

1. Відкрийте програму Магазин Windows.
2. Проведіть пальцем від правого краю екрана, потім виберіть пункт **Настройки**.

   Якщо ви використовуєте мишу, наведіть вказівник на правий нижній кут екрана та клацніть елемент **Настройки**.
3. Натисніть кнопку **Оновлення програми**.
4. Натисніть кнопку **Автоматично оновлювати програми** , щоб вимкнути автоматичні оновлення програм.

Дізнатися про можливості найновішої версії програми та дату її останнього оновлення можна на сторінці опису цієї програми в Магазині Windows.

Дозвіл для програм із Магазину

Властивості та завдання

Багато програм, що інсталюються з Магазину Windows, розраховані на використання переваг певного апаратного та програмного забезпечення. Наприклад, для програми з обробки

фотографій не завадить мати веб-камеру, а такому засобу, як ресторанний гід, потрібно знати розташування користувача, щоб надати рекомендації про заклади поблизу.

Збирання, обробка та передавання інформації

Ось список функцій, про використання яких мають повідомляти програми.

- Підключення до Інтернету. Дає змогу програмам підключатися до Інтернету.
- Вхідні підключення за допомогою брандмауера. Дають змогу програмам надсилати відомості на ПК та з нього через брандмауер.
- Домашня мережа або мережа на роботі. Дає змогу програмам надсилати відомості з одного ПК на інші в межах однієї мережі.
- Бібліотеки зображень, відео, музики або документів. Дає змогу програмам отримувати доступ до файлів у бібліотеках, вносити до них зміни або видаляти їх. Це передбачає можливість доступу до будь-яких додаткових даних, вбудованих у ці файли, наприклад відомостей про місце зйомки у файлах фотографій.
- Знімні носії. Дає змогу програмам отримувати доступ до файлів, вносити в них зміни та видаляти їх на зовнішньому диску, у флеш-пам’яті USB або на портативному пристрої.
- Облікові дані Windows. Дає змогу програмі використовувати облікові дані для автентифікації та надання доступу до корпоративної інтрамережі.
- Сертифікати, що зберігаються на ПК або смарт-картці. Дає змогу програмі використовувати сертифікати для для безпечного підключення до різноманітних організацій, наприклад банку, урядових установ або організації, у якій працює користувач.
- Функція обміну текстовими повідомленнями на ПК. Дає змогу програмі надсилати та отримувати текстові повідомлення.

- Веб-камера та мікрофон. Дає змогу програмі записувати звук, знімати фотографії та відео.
- Розташування. Дає змогу програмі визначити приблизне розташування на основі даних від датчика GPS або відомостей про мережу.
- Датчик ПК для радіозв'язку на близькій відстані. Дає змогу програмі підключитися до іншого розташованого поблизу пристрою, на якому запущено таку саму програму.
- Портативні пристрої. Дає змогу програмі обмінюватися даними з такими пристроями, як мобільний телефон, цифрова камера або портативний музичний програвач.
- Відомості на портативному пристрої. Дають змогу програмі отримувати доступ до контактів, календарів, приміток, станів і звукових сигналів на портативному пристрої, а також додавати, змінювати або видаляти їх.
- Обліковий запис мобільного широкосмугового зв'язку. Дає змогу програмам керувати обліковим записом мобільного широкосмугового зв'язку.

Функції, що їх використовує програма, можна переглянути на сторінці її опису. У разі інсталяції програми, ОС Windows дозволить їй використовувати перераховані вище функції – крім засобів визначення розташування, обміну текстовими повідомленнями, веб-камери та мікрофону, за допомогою яких можна отримати конфіденційну інформацію. Коли програма вперше запитує дозвіл на доступ до засобу, що використовує конфіденційну інформацію, ОС Windows запитує в користувача, чи слід надати програмі такий дозвіл. Дозвіл на використання цих функцій і засобів програмами можна надати чи скасувати будь-коли.

Окрім того, якщо програма запитає дозвіл на надсилання даних із пристрою, на якому зберігаються відомості про користувача та його поведінку, система Windows запитає користувача, чи слід дозволяти програмі використовувати ці дані. Наприклад, у разі підключення пристрою, який відстежує ваше місцезнаходження, ОС Windows запитає, чи слід надавати програмі доступ до цих

відомостей.

Використання інформації

Ці засоби та функції використовуватимуться кожною програмою відповідно до процедур забезпечення конфіденційності їх розробників. Якщо програма використовує засіб, що застосовує конфіденційну інформацію, на сторінці з її описом у Магазині відображатиметься посилання на декларацію про конфіденційність відповідного видавця.

Вибір і керування

Перед інсталяцію програми можна переглянути в Магазині засоби, які для неї необхідні. Перед першим використанням кожної програми система Windows запитуватиме, надати чи заборонити цій програмі доступ до засобів, що використовують конфіденційну інформацію (засобів визначення розташування, обміну текстовими повідомленнями, веб-камери та мікрофону).

На сторінці опису програми в Магазині Windows у нижній частині лівого стовпця відображається список скорочених назв функцій, що використовуються програмою. Повний список можна переглянути сторінці «Докладно» в описі програми. Після інсталяції програми в будь-який час можна переглянути повний список засобів, які вона використовує, і керувати її доступом до найбільш конфіденційної інформації. Для цього запустіть програму, відкрийте вікно **Настройки**, а потім виберіть **Дозволи**.

Персоналізований пошук у Магазині та рекомендації щодо програм

Властивості та завдання

Під час перегляду програм або їх пошуку в Магазині Windows корпорація Майкрософт надає рекомендації та результати пошуку, допомагаючи знаходити актуальні програми.

Збирання, обробка та передавання інформації

Щоб покращити результати пошуку, Магазин Windows надсилає до корпорації Майкрософт відомості про взаємодію користувача з Магазином, зокрема інформацію про шукані програми та вибрані результати. Магазин Windows також надсилає пов’язаний з

обліковим записом ідентифікатор Microsoft для надання персоналізованих результатів пошуку на основі взаємодії користувача зі службою Bing та іншими продуктами та службами Microsoft. За бажання можна відмовитися від отримання персоналізованих результатів пошуку. У такому разі ідентифікатор не надсилатиметься.

Використання інформації

Магазин використовує ідентифікатор, пов’язаний з обліковим записом Microsoft для надання персоналізованих результатів пошуку та рекомендацій на основі взаємодії користувача з Магазином та іншими продуктами та службами Microsoft, зокрема службою Bing і Магазином Windows Phone. Зокрема, використовується така інформація, як придбані програми, відомості про профіль, зазначені в обліковому записі Microsoft, а також оцінки й відгуки про програми. Ці дані також можуть використовуватися для персоналізації інших продуктів і служб Microsoft.

Вибір і керування

Якщо вхід до ОС Windows виконується за допомогою облікового запису Microsoft, персоналізація результатів і надання рекомендацій у Магазині Windows вмикається за замовчуванням. За бажання можна відмовитися від отримання персоналізованих результатів і рекомендацій із Магазину, вибравши відповідні параметри в розділі **Настройки** у вікні настройок Магазину.

Допомога у вдосконаленні Магазину Windows через надсилання URL-адрес, які використовують програми

Властивості та завдання

Деякі програми, отримані з Магазину, використовують веб-вміст і можуть надавати доступ до комп’ютера потенційно небезпечному програмному забезпеченню, наприклад зловмисним програмам. Якщо цей засіб увімкнуто, він починає збирати відомості про веб-вміст, який використовується згаданими програмами, щоб допомогти корпорації Майкрософт діагностувати потенційно небезпечну поведінку. Корпорація Майкрософт може, наприклад,

використовувати ці відомості для видалення програми з Магазину.

Збирання, обробка та передавання інформації

Якщо користувач дозволить надсилання відомостей про веб-вміст, що використовується програмами, корпорація Майкрософт збиратиме відомості про URL-адреси та типи вмісту, до якого отримує доступ програма під час її використання. Це допоможе виявити програми, які отримують вміст зі шкідливих або небезпечних веб-сайтів. Звіти, що надсилаються до корпорації Майкрософт, включають такі відомості, як ім’я або ідентифікатор програми, повні URL-адреси, до яких вона отримує доступ, а також повні URL-адреси, які вказують на розташування будь-якого коду JavaScript, що використовується програмою. Система Windows довільним чином генерує номер GUID (глобальний унікальний ідентифікатор), який надсилається до корпорації Майкрософт із кожним звітом. GUID дає змогу визначити, які дані надсилалися з певного комп’ютера протягом певного періоду часу. Ідентифікатор GUID не містить жодних особистих відомостей і не використовується для встановлення особи користувача.

Щоб підвищити рівень конфіденційності, відомості надсилаються до корпорації Майкрософт у зашифрованій формі. Вони можуть містити дані, пов’язані з веб-сторінкою, до якої отримує доступ програма, наприклад відомості про умови пошуку або дані, введені у програмі. Наприклад, у разі пошуку слова у програмі-словнику це слово може бути включено до відомостей, які надсилаються до корпорації Майкрософт у складі повної адреси веб-сайту, до якого програма отримувала доступ. Корпорація Майкрософт фільтрує ці адреси, намагаючись видалити особисті відомості, якщо є така змога.

Використання інформації

Корпорація Майкрософт час від часу перевіряє надіслані відомості, щоб покращити виявлення програм, які можуть взаємодіяти з небезпечним веб-вмістом, шкідливими веб-сайтами або сценаріями. Ці відомості використовуються для вживання заходів проти потенційно шкідливих програм. До адрес веб-вмісту можуть бути випадково додані особисті відомості, але ці відомості не використовуватимуться для встановлення особи користувача,

зв'язку з ним або надсилання реклами. Ідентифікатор GUID використовується для визначення масштабності проблем, про які було повідомлено, і встановлення їх пріоритетності. Наприклад, ідентифікатор GUID дає змогу корпорації Майкрософт відрізнити випадок потенційно небезпечної поведінки, зареєстрованої сто разів на одному ПК, від випадку такої ж поведінки, зареєстрованої один раз на ста комп'ютерах.

Вибір і керування

У разі вибору швидкого настроювання під час інсталяції системи Windows, ОС Windows надсилатиме відомості про веб-вміст, що використовується програмами з Магазину, якщо вони були створені за допомогою мови JavaScript. Якщо ви настроюєте параметри власноруч, для керування цими настройками можна вибрати завдання **Використовувати онлайнові служби SmartScreen для покращення захисту від шкідливого вмісту, завантаженого із сайтів програмами з Магазину Windows і браузером Internet Explorer, а також від шкідливих завантажень** у розділі **Допомога в покращенні продуктів і служб корпорації Майкрософт**. Після інсталяції цю настройку можна змінити в розділі **Конфіденційність** в настройках ПК.

На початок сторінки

Служба часу Windows

Властивості та завдання

Служба часу Windows автоматично синхронізує час на ПК із сервером часу в мережі.

Збирання, обробка та передавання інформації

Служба з'єднується із сервером часу через Інтернет або локальну мережу за допомогою стандартного протоколу NTP. За замовчуванням ця служба виконує синхронізацію із сервером time.windows.com щотижня. На сервер часу не надсилаються жодні дані, крім стандартних відомостей про ПК.

Використання інформації

Ці відомості використовуються службою часу Windows для автоматичної синхронізації часу на ПК.

Вибір і керування

Службу часу Windows увімкнуто за замовчуванням. Цю функцію можна вимкнути в розділі **Дата й час** у настройках ПК. Вимкнення служби часу Windows не матиме безпосереднього впливу на програми й інші служби, але без надійного джерела відомостей про час годинник ПК може показувати інший час, ніж решта ПК в мережі або Інтернеті. У разі суттєвих розбіжностей у часі на підключених до мережі ПК, у роботі програм та служб, функціонування яких залежить від часу, виникатимуть помилки та неполадки.

На початок сторінки

Виправлення неполадок Windows

Властивості та завдання

Засіб виправлення неполадок Windows дає змогу діагностувати та усувати на ПК проблеми загального характеру.

Збирання, обробка та передавання інформації

Після запуску пакета виправлення неполадок результати зберігаються на ПК. Ці результати можуть містити особисті відомості, наприклад ім’я користувача або ім’я пристрою. Засіб виправлення неполадок Windows може допомогти знайти рішення проблеми в довідці Windows і спільнотах Windows в Інтернеті. До корпорації Microsoft будуть надіслані пов’язані із проблемою ключові слова, які допоможуть знайти для неї рішення. Наприклад, якщо принтер не працює належним чином і потрібна довідка, до корпорації Майкрософт надсилатимуться слова «принтер», «друкувати», «друк».

Використання інформації

Корпорація Майкрософт використовує відомості, зібрані засобом виправлення неполадок Windows, щоб допомагати користувачам вирішувати проблеми, які можуть у них виникати.

Вибір і керування

Щоб видалити результати в засобі виправлення неполадок, перейдіть до розділу «Виправлення неполадок» на Панелі керування. Натисніть кнопку **Переглянути журнал**, виберіть потрібний результат, а потім натисніть кнопку **Видалити**.

На початок сторінки

Служба Work Folders

Властивості та завдання

Work Folders – це папки на ПК, які автоматично синхронізуються з файловим сервером на роботі.

Збирання, обробка, зберігання та передавання інформації

Якщо файл зберігається в папці Work Folders, він автоматично синхронізується з файловим сервером, керування яким здійснюється на робочому місці. Файли, збережені в папці Work Folders з інших ПК, синхронізуватимуться з вашим ПК.

Використання інформації

ОС Windows надсилає та отримує файли в папках Work Folders для синхронізації цих папок. Інформація, що зберігається на серверах на роботі, використовується відповідно до політики конфіденційності роботодавця.

Вибір і керування

Для керування доступом ПК до папок Work Folders перейдіть до розділу **Робоче місце** в настройках ПК.

На початок сторінки

Робоче місце

Робоче місце дає змогу підключити пристрій до служби Windows Intune (потрібно оформити окрему передплату в корпорації Майкрософт) або служби керування пристроєм стороннього постачальника. Якщо ви дозволите системному адміністратору керувати вашим ПК за допомогою засобу робочого місця, він зможе застосовувати політики безпеки на вашому ПК, інсталювати

програми, переглядати певні настройки та іншу інформацію на ПК, а також виконувати інші завдання з керування. Докладнішу інформацію про використання вашою компанією засобу робочого місця див. в політиці конфіденційності компанії. Ці відомості також можна отримати в системного адміністратора.

Збирання, обробка та передавання інформації

Під час налаштування та використання робочого місця ПК обмінюється даними зі службою керування пристроєм, яку використовує компанія. Ця служба може бути розміщена в корпорації Майкрософт. До неї надсилаються введені облікові дані, що використовуються для підключення до робочого місця.

Використання інформації

Інформація, що надсилається до служби керування пристроєм, використовується для встановлення зв’язку між службою та ПК, а також для забезпечення можливості інсталювати самонастроювані програми з Магазину Windows. Докладнішу інформацію про самонастроювані програми отримайте з політики конфіденційності компанії або в системного адміністратора.

Вибір і керування

Якщо компанія використовує засіб робочого місця, можна підключитися до робочого місця або відключитися від нього в розділі **Мережа**в настройках ПК. Після підключення ПК до служби ви зможете переглядати інформацію про підключення або відключитися у будь-який час.

На початок сторінки

Для отримання актуальної інформації щодо практики обробки даних корпорацією Майкрософт ознайомтеся з Положенням про конфіденційність корпорації Майкрософт. Тут ви також можете отримати інформацію про останні інструменти для отримання доступу до своїх даних і керування ними, а також про те, як із нами зв'язатися, якщо у вас виникне запитання щодо конфіденційності.

Положення про конфіденційність Windows 8.1 і Windows Server 2012 R2

Зважайте, що ця сторінка є доповненням до декларації про конфіденційність Windows 8.1 і Windows Server 2012 R2 (далі – «Декларація про конфіденційність Windows»), яка містить такі розділи.

- Витяг
- Декларація, яка є повною версією декларації про конфіденційність Windows 8.1, містить посилання на декларації про конфіденційність для засобів Windows, для яких існують окремі декларації
- Доповнення про засоби, у якому описуються засоби та функції, що впливають на конфіденційність в операційній системі Windows 8.1 і Windows Server 2012 R2
- **Доповнення про програми** (ця сторінка), де описано програми, які впливають на конфіденційність в операційній системі Windows 8.1, і яке містить посилання на декларації

про конфіденційність, що застосовуються для кожної програми

- Доповнення про сервер, у якому описуються додаткові засоби та функції, що впливають на конфіденційність в операційній системі Windows Server 2012 R2

Щоб зрозуміти принципи збирання та використання даних, пов’язані з певним засобом або службою Windows, ознайомтеся з повною версією декларації про конфіденційність та всіма застосовними або окремими доповненнями.

У разі участі у програмі підвищення якості ПЗ (CEIP) під час настоювання комп’ютера ці програми збиратимуть відомості для створення звіту про використання кожної програми, а також про продуктивність і надійність цих програм. Корпорація Майкрософт використовує відомості, зібрані в рамках програми CEIP, для вдосконалення своїх продуктів і служб. Ці відомості не використовуватимуться для встановлення особи користувача, зв’язку з ним або надсилання реклами. CEIP можна вимкнути в настройках ПК. Додаткові відомості див. у декларації про конфіденційність для програми CEIP.

За допомогою наведених нижче посилань можна перейти до декларацій про конфіденційність, які застосовуються до кожної з наведених нижче програм.

Будильник

Калькулятор

Календар

Камера

Фінанси

Харчування

Ігри

Здоров’я

Довідка+підказки

Пошта

Карти

Музика

Новини

Люди

Переглядач

Список переглядів

Сканування

Skype

Звукозаписувач

Спорт

Подорожі

Відео

Погода

Для отримання актуальної інформації щодо практики обробки даних корпорацією Майкрософт ознайомтеся з Положенням про конфіденційність корпорації Майкрософт. Тут ви також можете отримати інформацію про останні інструменти для отримання доступу до своїх даних і керування ними, а також про те, як із нами зв'язатися, якщо у вас виникне запитання щодо конфіденційності.

Положення про конфіденційність Windows 8.1 і Windows Server 2012 R2

На цій сторінці

Ця сторінка є доповненням до декларації про конфіденційність Windows 8.1 і Windows Server 2012 R2 (далі – "Декларація про конфіденційність Windows"). Декларація про конфіденційність містить такі розділи:

- Витяг
- Декларація, що є повною версією декларації про конфіденційність для ОС Windows 8.1, містить посилання на декларації про конфіденційність для засобів Windows, які мають свої власні декларації.
- Доповнення про засоби, у якому описано засоби, що впливають на конфіденційність в операційних системах Windows 8.1 і Windows Server 2012 R2
- Доповнення про програми, у якому описуються програми, що впливають на конфіденційність в операційній системі Windows 8.1

вдосконалення програмного забезпечення Windows (CEIP) і звітування про критичні помилки Windows (WER)

Журналювання інвентаризації програмного забезпечення

- **Доповнення про сервер** (ця сторінка), у якому описано додаткові засоби та функції, що впливають на конфіденційність в операційній системі Windows Server 2012 R2

Щоб зрозуміти принципи збирання та використання даних, пов’язані з певним засобом або службою Windows, ознайомтеся з повною версією декларації про конфіденційність Windows і всіма відповідними доповненнями. Крім того, прочитайте цей офіційний документ для адміністраторів.

Щоб дізнатися про вплив на конфіденційність засобів, які містяться в операційній системі Windows Server 2012 R2 Essentials, див. розділ Декларація про конфіденційність для Windows Server 2012 R2 Essentials і Windows Server Essentials Experience.

Журналювання доступу користувачів

Властивості та завдання

Засіб журналювання доступу користувачів (UAL) збирає й акумулює дані про запити клієнтом ролей сервера (запити користувачів і пристроїв) та інстальованих продуктів (якщо вони зареєстровані в UAL) на локальному сервері. Ці дані (у формі IP-адрес, імен користувачів, а в деяких випадках імен хостів і/або посвідчень віртуальних машин) зберігаються в локальних базах даних розширюваного засобу зберігання (ESE), і доступ до них можуть отримувати лише адміністратори. UAL містить постачальник WMIv2 і пов’язані командлети Windows PowerShell для отримання даних про доступ користувача, призначених для керування правами на окремі клієнтські ліцензії (CAL) для автономних користувачів, у яких критично важливими є поточні записи про унікальні запити клієнта.

Збирання, обробка та передавання інформації

IP-адреси, імена користувачів і, в деяких випадках, імена хостів (якщо інстальовано роль DNS), а також посвідчення віртуальних машин (якщо інстальовано роль Hyper–V) збираються локально на сервері, коли увімкнуто засіб UAL. Зібрані дані не надсилаються

корпорації Майкрософт.

Використання інформації

Доступ до даних UAL надається адміністраторам за допомогою баз даних ESE, постачальника WMI і командлетів Windows PowerShell. Система Windows використовує такі дані лише для забезпечення функціонування самого засобу UAL.

Вибір і керування

Функцію UAL увімкнуто за замовчуванням. Службу UAL можна зупиняти та запускати під час роботи сервера. Щоб вимкнути UAL остаточно, відкрийте Windows PowerShell, введіть команду Disable-UAL і перезапустіть сервер. Адміністратори можуть видаляти всі зібрані дані журналу. Для цього їм потрібно зупинити службу й вимкнути UAL, а потім видалити всі файли у папці %SystemRoot%\System32\LogFiles\SUM\.

На початок сторінки

Диспетчер серверів

Властивості та завдання

Диспетчер серверів – це засіб керування, який дає змогу адміністратору контролювати один або кілька серверів і переглядати загальний стан або стан для конкретної ролі, щоб виконувати завдання з керування й отримувати доступ до інших засобів керування серверами.

Збирання, обробка та передавання інформації

Диспетчер серверів отримує із сервера, яким керує адміністратор, наведені нижче типи даних.

- **Загальні відомості про сервер:** ім’я NetBios і повне доменне ім’я (FQDN), облікові дані, внесені під час використання функції "Керувати як", IPv4-адреса, IPv6-адреса, стан керованості, опис, версія операційної системи, тип, останнє оновлення, процесори, пам’ять, ім’я кластера, тип об’єкта кластера, стан активації, обліковий номер (SKU), архітектура операційної системи, виробник,

конфігурація програми підвищення якості ПЗ (CEIP) і конфігурація Звітування про критичні помилки Windows.

- **Події:** ідентифікатор, важливість, джерело, журнал, дата та час для кожної події з журналу Windows та інших журналів на вибір адміністратора.
- **Усі служби:** ім’я, стан і тип запуску.
- **Відомості про роль сервера:** результати Best Practice Analyzer (BPA) для ролей, інстальованих на сервері.
- **Відомості про продуктивність:** зразки для лічильників продуктивності, повідомлення про використання ЦП та доступну пам’ять.

Використання інформації

Ці відомості зберігаються в диспетчері серверів і не надсилаються до корпорації Майкрософт. Вони відображаються у диспетчері серверів і допомагають адміністраторам контролювати системи.

Вибір і керування

Адміністратор може надавати та відкликати свою згоду на збирання даних із будь-якого сервера, за винятком локального сервера, додаючи відповідний сервер до диспетчера серверів або видаляючи його звідти. Адміністратор може прямо надавати облікові дані для підключення до віддаленого сервера. Диспетчер серверів відображає запит на надання адміністратором явної згоди на зберігання облікових даних локально в диспетчері серверів. Адміністратор може видалити такі облікові дані будь-коли.

На початок сторінки

Служба об’єднання AD CS

Властивості та завдання

Служби об’єднання Active Directory (AD FS) – це корпоративне рішення з об’єднання та єдиного входу для локальних або інших мережевих програм. За допомогою служби AD FS адміністратори забезпечують користувачам різних організацій можливість

взаємодії та доступу до програм у локальних або інших мережах, дбаючи водночас про безпеку цих програм. Служба AD FS використовує службу маркерів безпеки, яка, у свою чергу, застосовує службу доменів Active Directory (AD DS) для автентифікації користувачів і надання їм маркерів безпеки з використанням різноманітних протоколів. Маркер містить цифровий підпис і твердження про користувача, які надходять від AD DS, полегшеного протоколу доступу до каталогів (LDAP), SQL Server, користувацького сховища або будь-якої їх комбінації.

Збирання, обробка та передавання інформації

Облікові дані користувача збираються під час автентифікації користувача за допомогою AD FS. Ці облікові дані негайно надсилаються до служби доменів Active Directory для автентифікації, і служба AD FS не зберігає їх локально. Атрибути користувача у службі доменів Active Directory можуть використовуватися для створення вихідних тверджень залежно від правил тверджень, налаштованих адміністратором AD FS. Вихідні твердження надсилаються довіреним партнерам, з якими адміністратор AD FS установив довірчі відносини. До корпорації Майкрософт відомості не надсилаються.

Використання інформації

Корпорація Майкрософт не має доступу до цієї інформації. Ця інформація призначена тільки для використання клієнтом.

Вибір і керування

Використовуйте службу AD FS, якщо необхідно, щоб служба AD FS збирала або надсилала дані довіреним партнерам.

На початок сторінки

Керування IP-адресами

Властивості та завдання

Служба керування IP-адресами (IPAM) дозволяє адміністраторам серверів відстежувати IP-адресу, ім’я хоста та ідентифікатор клієнта (наприклад, MAC-адресу в IPv4 та DUID в IPv6) для комп’ютерів або пристроїв у мережі за допомогою відомостей, які

користувач надає для входу.

Збирання, обробка та передавання інформації

Сервер IPAM збирає журнали аудиту та події із серверів DHCP, контролерів доменів і серверів мережевої політики, а тоді локально зберігає IP-адресу, ім’я хоста, ідентифікатор клієнта та ім’я користувача, який виконав вхід. Адміністратор сервера може виконувати пошук у зібраних журналах за IP-адресою, ідентифікатором клієнта, іменем хоста та іменем користувача з використанням консолі IPAM. Жодні з цих відомостей не надсилаються до корпорації Майкрософт.

Використання інформації

Корпорація Майкрософт не має доступу до цієї інформації. Ця інформація призначена тільки для використання клієнтом.

Вибір і керування

Службу IPAM не інстальовано за замовчуванням, її повинен інсталювати адміністратор сервера. Після інсталяції служби IPAM автоматично вмикається аудит IP-адрес. Щоб вимкнути аудит IP-адрес на сервері, де інстальовано службу IPAM, запустіть на сервері IPAM планувальник завдань, перейдіть до завдання аудиту в папці Microsoft\Windows\IPAM і вимкніть це завдання.

На початок сторінки

Уніфікований віддалений доступ

Властивості та завдання

За допомогою засобу уніфікованого віддаленого доступу віддалені користувачі можуть підключатися до приватної мережі (наприклад, корпоративної) через Інтернет. Засіб уніфікованого віддаленого доступу використовує DirectAccess для надання віддаленим клієнтським комп’ютерам на платформі Windows 8 можливості безперервного та прозорого підключення до корпоративних мереж. Він також забезпечує роботу служби віддаленого доступу (RAS), тобто традиційних служб VPN включно з локальним підключенням "вузол-вузол" або іншими мережевими підключеннями.

Збирання, обробка та передавання інформації

Для контролю користувачів уніфікованого віддаленого доступу сервер DirectAccess зберігає відомості про віддалених користувачів, які підключаються до приватної мережі. Сюди належать такі відомості, як ім’я хоста віддаленого користувача, ім’я користувача Active Directory та публічна IP-адреса віддаленого користувача (якщо на клієнті використовується перетворення мережевих адрес (NAT), то це буде публічна IP-адреса). Ці дані також можуть зберігатися на серверах внутрішньої бази даних Windows (WID) або RADIUS лише з дозволу адміністратора. Отримувати доступ до таких відомостей і користуватися ними може лише адміністратор DirectAccess (користувач домену з локальним обліковим записом адміністратора), який входить на сервер.

Використання інформації

Ці відомості буде використовувати лише адміністратор для виправлення неполадок із підключенням клієнта, а також із метою аудиту або виконання нормативних вимог. До корпорації Майкрософт відомості не надсилаються.

Вибір і керування

Контроль віддалених клієнтів увімкнуто за замовчуванням, і його не можна вимкнути. Дані контролю зберігаються на серверах WID/RADIUS, лише якщо адміністратор налаштував ведення облікових записів на використання будь-яких із цих параметрів. Якщо адміністратор не налаштував ведення облікових записів, ці відомості не зберігаються. Адміністратор може також налаштувати ведення облікових записів на сервері віддаленого доступу таким чином, щоб ім’я користувача та IP-адреса не зберігались.

На початок сторінки

Служби віддаленого керування робочими столами

Властивості та завдання

Служби віддаленого керування робочими столами (RDS) надають платформу, яка допомагає компаніям запроваджувати

централізоване керування робочими столами, керувати програмами, підвищувати гнучкість системи та забезпечувати відповідність нормативним вимогам, водночас підвищуючи рівень безпеки даних.

Збирання, обробка та передавання інформації

Для контролю користувачів RDS на сервері сеансу віддаленого робочого стола зберігаються відомості про віддалених користувачів, які підключаються до ресурсів RDS. Сюди належать такі відомості, як ім'я хоста віддаленого користувача, ім'я користувача Active Directory та публічна IP-адреса віддаленого користувача (якщо на клієнті використовується перетворення мережевих адрес (NAT), то це буде публічна IP-адреса). Ці дані зберігаються автоматично у внутрішній базі даних Windows (WID) або на сервері SQL під час підключення користувачів. Відомості не надсилаються до корпорації Майкрософт. Лише користувач домену з обліковим записом локального адміністратора може отримати доступ і переглядати цю інформацію.

Використання інформації

Ці відомості буде використовувати лише адміністратор для виправлення неполадок із підключенням клієнта, а також із метою внутрішнього аудиту або виконання нормативних вимог. До корпорації Майкрософт відомості не надсилаються.

Вибір і керування

Моніторинг клієнтів увімкнуто за замовчуванням, і його не можна вимкнути. Відомості моніторингу зберігаються у WID/сервери SQL.

На початок сторінки

Програма вдосконалення програмного забезпечення Windows (CEIP) і звітування про критичні помилки Windows (WER)

Властивості та завдання

Додаткові відомості про ці засоби див. на вкладці Доповнення про засоби або в цьому офіційному документі для адміністраторів.

Збирання, обробка та передавання інформації

Щоб дізнатися про те, які саме дані збирають, обробляють і передають ці засоби, див. відомості про програму CEIP і засіб звітування про критичні помилки на вкладці Доповнення про засоби .

Використання інформації

Щоб дізнатися про те, як ми використовуємо дані, зібрані цими засобами, див. відомості про програму CEIP і засіб звітування про критичні помилки на вкладці Доповнення про засоби .

Вибір і керування

Програму CEIP за замовчуванням вимкнуто, а засіб звітування про критичні помилки за замовчуванням налаштовано, щоб відображати запит на підтвердження перед надсиланням звітів про аварійне завершення роботи до корпорації Майкрософт. Програму CEIP можна вмикати та вимикати в диспетчері серверів і на Панелі керування, а також за допомогою командного рядка. Роботою засобу звітування про критичні помилки можна керувати лише за допомогою командного рядка.

Щоб увімкнути або вимкнути програму CEIP на Панелі керування, виберіть пункт **Система й обслуговування**та натисніть кнопку **Неполадки: звіти та вирішення**. Після цього в розділі **Див. також**у настройках ПК, там відкрийте вікно **Параметри підвищення продуктивності ПЗ** , щоб увімкнути або вимкнути CEIP.

Елементи керування диспетчера серверів

Локальний сервер

- Увімкнення CEIP
  Відкрийте диспетчер серверів і виберіть пункт **Локальний сервер**. Перейдіть за посиланням "Програма підвищення якості ПЗ", у діалоговому вікні виберіть пункт **Так, я бажаю взяти участь у програмі CEIP** і натисніть кнопку **ОК**.

- Вимкнення CEIP
  Відкрийте диспетчер серверів і виберіть пункт **Локальний сервер**. Перейдіть за посиланням "Програма підвищення якості ПЗ", у діалоговому вікні виберіть пункт **Ні, я не бажаю брати участь у програмі CEIP** і натисніть кнопку

ОК.

- Увімкнення засобу звітування про критичні помилки
  Відкрийте диспетчер серверів і виберіть пункт **Локальний сервер**. Перейдіть за посиланням "Звітування про критичні помилки Windows", виберіть пункт **Так, автоматично надсилати загальні звіти**та натисніть кнопку **ОК**.

- Вимкнення засобу звітування про критичні помилки
  Відкрийте диспетчер серверів і виберіть пункт **Локальний сервер**. Перейдіть за посиланням "Звітування про критичні помилки Windows", виберіть пункт **Я не бажаю брати участь у програмі, і надалі не запитувати**та натисніть кнопку **ОК**.

Використання на кількох комп’ютерах

- Увімкнення CEIP
  Відкрийте диспетчер серверів і виберіть пункт **Усі сервери**. На плитці "Сервери" виберіть усі сервери (Ctrl+A), клацніть правою кнопкою миші та виберіть пункт **Настроїти автоматичний відгук Windows** . На вкладці "Програма підвищення якості ПЗ" виберіть пункт **Так, я бажаю взяти участь (рекомендовано)**. Застосуйте цей параметр до всіх серверів, установивши прапорець поруч з іменем сервера в елементі керування "Вибір серверів", і натисніть кнопку **ОК**.

- Вимкнення CEIP
  Відкрийте диспетчер серверів і виберіть пункт "Усі сервери". На плитці "Сервери" виберіть усі сервери (Ctrl+A), клацніть правою кнопкою миші та виберіть пункт **Настроїти автоматичний відгук Windows** . На вкладці "Програма підвищення якості ПЗ" виберіть пункт **Ні, я не бажаю брати участь у програмі CEIP**. Застосуйте цей параметр до всіх серверів, установивши прапорець поруч з іменем сервера в елементі керування "Вибір серверів", і натисніть кнопку **ОК**.

- Увімкнення засобу звітування про критичні помилки
  Відкрийте диспетчер серверів і виберіть пункт **Усі сервери**. На плитці "Сервери" виберіть усі сервери (Ctrl+A), клацніть правою кнопкою миші та виберіть пункт **Настроїти**

автоматичний відгук Windows . На вкладці "Звітування про критичні помилки Windows" виберіть пункт **Так, автоматично надсилати загальні звіти (рекомендовано)**. Застосуйте цей параметр до всіх серверів, установивши прапорець поруч з іменем сервера в елементі керування "Вибір серверів", і натисніть кнопку **ОК**.

- Вимкнення засобу звітування про критичні помилки
  Відкрийте диспетчер серверів і виберіть пункт **Усі сервери**. На плитці "Сервери" виберіть усі сервери (Ctrl+A), клацніть правою кнопкою миші та виберіть пункт **Настроїти автоматичний відгук Windows** . На вкладці "Звітування про критичні помилки Windows" виберіть пункт **Ні, я не бажаю брати участь у програмі CEIP**. Застосуйте цей параметр до всіх серверів, установивши прапорець поруч з іменем сервера в елементі керування "Вибір серверів", і натисніть кнопку **ОК**.

На початок сторінки

Журналювання інвентаризації програмного забезпечення

Властивості та завдання

Журналювання інвентаризації програмного забезпечення (SIL) надає новий набір класів WMI і командлетів Powershell для полегшення інвентаризації операційної системи випуску Windows Server, інстальованого у Windows Server програмного забезпечення та характеристик сервера, на якому працює це програмне забезпечення. Крім того, адміністратор може ввімкнути в SIL можливість щогодини збирати дані від постачальника WMI і надсилати їх у мережі до сервера агрегації, якщо його вказано за допомогою параметра -TargetUri командлета Set-SilLogging.

Збирання, обробка та передавання інформації

Адміністратор може налаштувати передачу даних на сервер агрегації в мережі. За замовчуванням збирання, обробка та передавання даних не відбуваються. Ці дані включають:

- ім’я Windows Server і випуск інстальованої операційної системи;

- перелік назв, версій і видавців усього програмного забезпечення, інстальованого на сервері, і дату його інсталяції;
- повне доменне ім’я серверної системи;
- кількість, тип і виробника процесорів, логічних процесорів і ядер, установлених у серверній системі або призначених їй.

За замовчуванням дані збираються й обробляються, але не передаються, навіть якщо ввімкнено щогодинне завдання та вказано цільовий вузол агрегації:

- Вибрано клас MsftSil_UalAccess і командлет Get-SilUalAccess для обробки загальної кількості унікальних користувачів і пристроїв для кожної ролі або продукту, зареєстрованих у засобі журналювання доступу користувачів (UAL) за два дні до запиту. Підраховується тільки кількість, жодні дані про самих користувачів або пристрої не виводяться й не передаються. Щоб підрахувати кількість, SIL потрібно обробити дані про користувачів і пристрої з класів засобу журналювання доступу користувачів (UAL). Ці дані доступні лише адміністратору локального комп’ютера. SIL не змінює доступ, необхідний для API-інтерфейсів UAL.

Зібрані дані не надсилаються корпорації Майкрософт.

Використання інформації

Постачальники WMI засобів журналювання інвентаризації програмного забезпечення збирають дані, отримані від інших, уже наявних у системі, інтерфейсів API. Адміністратор може налаштувати передавання даних у мережі на сервер для подальшої агрегації. За замовчуванням збирання, обробка та передавання даних не відбуваються. Що стосується класу MsftSil_UalAccess і командлета Get-SilUalAccess, оброблені дані містять загальну кількість унікальних користувачів і пристроїв для кожної ролі або продукту, зареєстрованих у засобі журналювання доступу користувачів (UAL) за два дні до збирання. Але дані, які можуть ідентифікувати користувачів або пристрої, не виводяться. Хоча цей клас WMI і командлет існують у системі, вони не входять

до пакета даних SIL, які щогодини збираються та передаються для агрегації, після того як адміністратор системи виконав відповідні налаштування.

Вибір і керування

За замовчуванням щогодинне завдання SIL вимкнено. За замовчуванням усі API-інтерфейси SIL доступні для запитів адміністраторам локальної системи. Щогодинне завдання SIL можна запустити або зупинити під час роботи сервера за допомогою командлетів Start-SilLogging і Stop-SilLogging. За допомогою командлета Set-SilLogging адміністратори сервера можуть установити дату й час запуску щогодинного завдання (за замовчуванням це відбувається о третій ранку за часом локальної системи), універсальний ідентифікатор ресурсу (URI) цільового сервера агрегації та відбиток сертифіката, необхідний для забезпечення довіреної передачі даних.

Усі параметри налаштування SIL, включно із запуском і зупинкою щогодинного завдання, можна змінити в реєстрі, який має використовуватися, тільки якщо систему інстальовано на віртуальній машині та тільки до першого запуску системи.

На початок сторінки