Para obter informações atualizadas sobre as práticas de processamento de dados da Microsoft, leia a Política de Privacidade da Microsoft. Aqui você também pode saber mais sobre as ferramentas mais recentes que fornecemos para acessar e controlar seus dados e como entrar em contato conosco se você tiver uma consulta sobre privacidade.

Política de Privacidade do Windows 8.1 e do Windows Server 2012 R2

Última atualização: abril de 2014

Estes destaques da política de privacidade completa do Windows 8.1 e do Windows Server 2012 R2 (política de privacidade do "Windows") explicam em alto nível algumas das práticas de coleta e uso de dados do Windows 8.1 e do Windows Server 2012 R2 ("Windows"). Eles enfatizam os recursos online e não têm nenhuma pretensão de servirem como uma descrição completa. Eles não se aplicam a outros sites, produtos ou serviços da Microsoft, online ou offline.

Esta política de privacidade tem a seguintes seções:

- **Destaques** (esta página)
- Política, que é a política de privacidade completa do Windows 8.1 com links para políticas de privacidade de recursos do Windows que possuem políticas autônomas
- Suplemento de recursos, que descreve os recursos com impacto na privacidade do Windows 8.1 e do Windows Server 2012 R2

- Suplemento de aplicativos, que descreve os aplicativos com impacto na privacidade do Windows 8.1
- Suplemento de servidores, que descreve os recursos adicionais com impacto na privacidade do Windows Server 2012 R2

Para obter mais informações sobre como proteger seu computador, suas informações pessoais e sua família online, visite nosso Centro de Segurança e Proteção.

Suas informações

- Alguns recursos do Windows podem solicitar sua permissão para coletar ou usar informações do seu computador, inclusive dados pessoais. O Windows usa essas informações conforme descrito na Windows 8.1 política de privacidadecompleta do , bem como no Suplemento de recursos, no Suplemento de aplicativos e no Suplemento de servidores.
- Alguns recursos do Windows, mediante sua permissão, podem compartilhar informações pessoais pela Internet.
- Se você registrar seu software, deverá fornecer informações pessoais.
- O Windows exige ativação para reduzir a pirataria de software e garantir que os nossos clientes possam desfrutar da qualidade de software que esperam obter. A ativação envia algumas informações sobre seu computador para a Microsoft.
- Se você optar por entrar no Windows, com uma conta da Microsoft, o Windows sincronizará suas configurações nos dispositivos e conectará você automaticamente em alguns aplicativos e sites. O Windows não requer que você entre com uma conta da Microsoft para acessar serviços de email ou rede social de terceiros, mas, se esse terceiro oferecer um aplicativo por meio da Loja, você deve entrar na Loja com a conta da Microsoft para instalar o aplicativo. Se você criar uma conta da Microsoft, será solicitado a fornecer algumas informações pessoais, como sua região geográfica e sua data de nascimento.

Detalhes adicionais

Início da página

Suas escolhas

- O Windows oferece várias maneiras de controlar como os recursos do Windows transferem informações pela Internet. Há mais informações disponíveis sobre como controlar esses recursos no Suplemento de recursos, no Suplemento de aplicativos e no Suplemento de servidores.
- Para melhorar sua experiência, alguns recursos que usam a Internet são habilitados por padrão.
- Detalhes adicionais

Início da página

Uso das informações

- Usamos as informações coletadas para habilitar os recursos que você está usando ou para fornecer os serviços solicitados. Além disso, poderemos usá-las para aprimorar nossos produtos e serviços. Para facilitar o fornecimento de nossos serviços, oferecemos ocasionalmente informações a outras empresas que trabalham no nosso nome. Apenas as empresas que possuem necessidade comercial de usar as informações têm acesso a essas informações. Elas são obrigadas a manter essas informações em sigilo e são proibidas de as utilizar para qualquer outro fim.
- Detalhes adicionais

Início da página

Como falar conosco

Para obter mais informações sobre as nossas práticas de privacidade, leia a política de privacidade completa do Windows 8.1. Se preferir, escreva para nós usando nosso formulário na Internet.

Início da página

Para obter informações atualizadas sobre as práticas de processamento de dados da Microsoft, leia a Política de Privacidade da Microsoft. Aqui você também pode saber mais sobre as ferramentas mais recentes que fornecemos para acessar e controlar seus dados e como entrar em contato conosco se você tiver uma consulta sobre privacidade.

Política de Privacidade do Windows 8.1 e do Windows Server 2012 R2

Nesta página

Última atualização: abril de 2014

Esta política abrange o Windows 8.1 e o Windows Server 2012 R2 ("Windows"). Alguns componentes do Windows têm suas próprias políticas de privacidade, que estão listadas nesta página. As políticas de privacidade de softwares e serviços relacionados ao Windows e a versões anteriores também estão listadas nesse local.

Para obter informações sobre recursos específicos, consulte Suplemento de recursos, no Suplemento de aplicativose Suplemento de servidores. Para obter informações sobre o Windows Embedded Industry Pro e sobre o Windows Embedded Industry Enterprise, consulte esta política.

Esta é uma política que enfatiza recursos que se comunicam com a Internet, sem nenhuma pretensão de servir como uma lista completa.

Coleta e uso das suas informações

As informações pessoais que coletamos de você serão usadas pela

Microsoft e suas subsidiárias e afiliadas controladas para habilitar os recursos que você utiliza e para prestar os serviços ou desempenhar as transações que você solicitou ou autorizou. Essas informações também podem ser usadas para analisar e melhorar os produtos e serviços da Microsoft.

Salvo conforme descrito nesta política, as informações pessoais fornecidas por você não serão transferidas a terceiros sem o seu consentimento. Ocasionalmente, contratamos outras empresas para prestar serviços limitados em nosso nome, como a realização de análises estatísticas dos nossos serviços. Fornecemos a essas empresas apenas as informações pessoais necessárias para prestar o serviço. Elas estão proibidas de usar essas informações para qualquer outra finalidade.

A Microsoft pode acessar ou divulgar informações sobre você, incluindo o conteúdo de suas comunicações, para: (a) cumprir a lei ou responder a solicitações legítimas ou a processos judiciais; (b) proteger os direitos ou a propriedade da Microsoft ou dos nossos clientes, incluindo a aplicação dos nossos contratos ou políticas que regem o uso do software, ou (c) adotar providências quando acreditarmos, de boa-fé, que esse acesso ou divulgação seja necessário para proteger a segurança pessoal dos funcionários e dos cliente da Microsoft, bem como do público em geral.

As informações coletadas pela ou enviadas para a Microsoft pelo Windows 8.1 poderão ser armazenadas e processadas nos Estados Unidos ou em qualquer outro país onde a Microsoft ou suas afiliadas, subsidiárias ou fornecedores de serviços mantenham instalações. A Microsoft segue a Diretiva Safe Harbor estabelecida pelo Departamento de Comércio dos EUA referente à coleta, ao uso e à retenção de dados oriundos da União Europeia, da Área Econômica Europeia e da Suíça.

Início da página

Coleta e uso de informações sobre o seu computador

Quando você usar o software com os recursos habilitados para Internet, as informações sobre seu computador ("informações padrão do computador") serão enviadas para os sites que você visitar e para

os serviços online que você usar. Em geral, essas informações padrão do computador incluem dados como endereço IP, versões do sistema operacional e do navegador, além de configurações regionais e de idioma. Em alguns casos, elas também podem incluir uma ID de hardware, que informa o fabricante, o nome e a versão do dispositivo. Se um determinado recurso ou serviço enviar informações para a Microsoft, as informações padrão do computador também serão enviadas.

Os detalhes de privacidade de cada recurso do Windows no Suplemento de Recursos, no Suplemento de Aplicativos e no Suplemento de Servidores, além dos recursos listados em qualquer lugar desta página, descrevem as informações adicionais que são coletadas e como elas são usadas.

Os administradores podem usar a Política de Grupo para modificar muitas das configurações dos recursos descritos aqui. Para obter mais informações, consulte este white paper para administradores.

Início da página

Segurança das informações

A Microsoft tem o compromisso de ajudar a proteger a segurança de suas informações. Usamos diferentes tecnologias e procedimentos de segurança para ajudá-lo a proteger suas informações contra acesso, uso ou divulgação não autorizados. Por exemplo, armazenamos as informações fornecidas em sistemas de computador com acesso limitado, localizados em instalações controladas. Ao transmitirmos informações altamente confidenciais (como uma senha ou um número de cartão de crédito) pela Internet, nós as protegemos com o uso de criptografia, como o protocolo SSL.

Início da página

Alterações nesta política de privacidade

Ocasionalmente, atualizamos esta política de privacidade para que reflita as alterações em nossos produtos e serviços, bem como os comentários de nossos clientes. Quando postamos alterações, a data da "última atualização" na parte superior desta política é revisada. Se

houver alterações materiais nesta política ou em como a Microsoft utiliza suas informações pessoais, nós o notificaremos com um aviso anterior à implementação dessas alterações ou com o envio direto de uma notificação. Recomendamos que você revise periodicamente esta política para ficar informado sobre como a Microsoft está protegendo suas informações.

Início da página

Para obter mais informações

A Microsoft agradece os comentários a respeito desta política de privacidade. Em caso de dúvidas sobre esta política, ou se você achar que a Microsoft não está em conformidade com ela, escreva para nós usando nosso formulário na Internet.

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

Início da página

Para obter informações atualizadas sobre as práticas de processamento de dados da Microsoft, leia a Política de Privacidade da Microsoft. Aqui você também pode saber mais sobre as ferramentas mais recentes que fornecemos para acessar e controlar seus dados e como entrar em contato conosco se você tiver uma consulta sobre privacidade.

Política de Privacidade do Windows 8.1 e do Windows Server 2012 R2

Nesta página

Última atualização: abril de 2014

Observe que esta página é um suplemento da política de privacidade do Windows 8.1 e do Windows Server 2012 R2 ("Política de privacidade do Windows"), que inclui as seguintes seções:

- Destaques
- Política, que é a política de privacidade completa do Windows 8.1, com links para políticas de privacidade de recursos do Windows que possuem políticas autônomas
- **Suplemento de recursos** (esta página), que descreve os recursos com impacto na privacidade do Windows 8.1 e do Windows Server 2012 R2
- Suplemento de aplicativos, que descreve os aplicativos com impacto na privacidade do Windows 8.1
- Suplemento de servidores, que descreve os recursos adicionais com impacto na privacidade do Windows Server 2012 R2

descoberta de dispositivo

Criptografia de dispositivo

DirectAccess

Central de Facilidade de Acesso

Visualizador de Eventos

Proteção para a Família

Fax

Personalização de manuscrito: aprendizado automático

Grupo Doméstico

IME (Editor de Método de Entrada)

Compartilhamento de conexão com a internet

Impressão via Internet

Preferências de idioma

Serviços de localização

Gerenciar suas credenciais

Nome e imagem da conta

Reconhecimento de rede

Para entender as práticas de coleta e uso de dados relevantes a determinado recurso ou serviço do Windows, você deve ler a política de privacidade completa e todo suplemento ou política autônoma aplicável.

Ativação

O que este recurso faz

O recurso Ativação reduz a falsificação de software, que ajuda a garantir que os clientes da Microsoft recebam a qualidade de software esperada. Quando seu software é ativado, uma chave do produto específica é associada ao computador (ou ao hardware) no qual o software está instalado. Essa associação impede que a chave do produto seja usada para ativar a mesma cópia do software em vários computadores. Algumas alterações no hardware ou software de seu computador talvez exijam a reativação do Windows. A ativação detecta e desabilita explorações de ativação (softwares que desviam ou ignoram a ativação de software da Microsoft). Se houver uma exploração de ativação presente, um fornecedor de software ou hardware pode ter adulterado um software original da Microsoft para criar cópias falsificadas do software. As explorações de ativação podem afetar a operação normal do sistema.

Informações coletadas, processadas ou transmitidas

Durante a ativação, as seguintes informações são enviadas para a Microsoft:

- O código do produto da Microsoft (um código de cinco dígitos que identifica o produto Windows que você está ativando).
- Uma ID de canal ou um código do site que identifica como o produto do Windows foi obtido originalmente. Por exemplo, uma ID de canal ou um código do site identifica se o produto foi comprado originalmente de uma loja de varejo, obtido como uma cópia de avaliação, por meio de um programa de licenciamento por volume ou pré-instalado por um fabricante de computador.

Notificações, aplicativos da tela de bloqueio e atualizações de bloco

Encomendar cópias

Pré-busca e pré-início

Auxiliar de Compatibilidade de Programas

Propriedades

Proximidade

Conexões de Acesso Remoto

Conexões de RemoteApp e Área de Trabalho

Conexão de Área de Trabalho Remota

Entrar com uma conta da Microsoft

Armazenamento em nuvem do OneDrive

Sincronizar suas configurações

Tecnologia Teredo

Serviços TPM (Trusted Platform Module)

Certificados raiz da atualização

Update Services

- A data de instalação e se a instalação foi bem-sucedida.
- Informações que ajudam a confirmar se a chave do produto (Product Key) do Windows não foi alterada.
- Marca e modelo do computador.
- Informações de versão do sistema operacional e de software.
- Configurações regionais e de idioma.
- Um número único chamado GUID (identificador global exclusivo) atribuído ao seu computador.
- Chave do produto (com hash) e ID do produto.
- Nome BIOS, número e data da revisão.
- Número de série do volume do disco rígido (com hash).
- O resultado da verificação de ativação. Inclui códigos de erro e informações sobre todas as explorações de ativação e respectivos softwares mal-intencionados ou não autorizados encontrados ou desabilitados:
    - O identificador da exploração de ativação.
    - O estado atual da exploração de ativação, como limpa ou em quarentena.
    - Identificação do fabricante do computador.
    - O hash e o nome do arquivo da exploração de ativação e também um hash dos componentes de software relacionados, que podem indicar a presença de uma exploração de ativação.
- O nome e um hash do conteúdo do arquivo de instruções de inicialização de seu computador. Se sua licença do Windows for por assinatura, as informações também serão enviadas sobre como sua assinatura funciona. As informações padrão do computador também são enviadas.
- Se você usa uma cópia licenciada por volume do Windows que

Rede Virtual Privada

Programa de Aperfeiçoamento da Experiência do Usuário do Windows

Windows Defender

Windows Relatório de Erro do

Associação de arquivos do Windows

Ajuda do Windows

Assistência remota

Windows Search

Instalação do Windows

Compartilhamento do Windows

Windows SmartScreen

Reconhecimento de Fala do Windows

Windows Store

Serviço de Tempo do Windows

Windows Solução de Problemas

Pastas de trabalho

Local de trabalho

usa um servidor de ativação, o endereço IP desse servidor pode ser enviado para a Microsoft.

Uso das informações

A Microsoft usa as informações para confirmar se você tem uma cópia licenciada do software. A Microsoft não usa as informações para entrar em contato com cada consumidor. As informações do servidor de licença são usadas para garantir que os servidores de licença estejam em conformidade com os respectivos contratos de licença.

Faça suas escolhas e controle

A ativação é necessária e ocorre automaticamente quando você instala o Windows. Se não tiver uma licença válida para o software, você não poderá ativar o Windows.

Início da página

Cliente do AD RMS (Active Directory Rights Management Services)

O que este recurso faz

O cliente do Active Directory Rights Management Services (AD RMS) Client (AD RMS) é a tecnologia de proteção da informação que funciona com aplicativos ativados com AD RMS para ajudar a proteger as informações digitais de uso não autorizado. Os proprietários de informações digitais podem definir como os destinatários usam as informações contidas em um arquivo, como quem pode abrir, modificar, imprimir ou executar outras ações com o arquivo. Para criar ou visualizar um arquivo com permissões restritivas, seu computador deve estar executando um aplicativo ativado com AD RMS e ter acesso a um servidor AD RMS.

Informações coletadas, processadas ou transmitidas

O AD RMS usa seu endereço de email para identificar você em um servidor AD RMS. Dessa forma, seu endereço de email é armazenado no servidor e, em seu computador, nas licenças e nos certificados de identidade criados pelo servidor. Os certificados de identidade e as licenças são transferidos por servidores AD RMS quando você tenta abrir, imprimir ou realizar outras ações em um documento protegido por gerenciamento de direitos. Se seu computador está conectado a

uma rede corporativa, o servidor AD RMS normalmente é operado pela empresa. Se você usa os serviços AD RMS do Windows Live, o servidor é operado pela Microsoft. Para proteger sua privacidade, as informações enviadas aos servidores AD RMS da Microsoft são criptografas.

Uso das informações

A licença permite que você acesse arquivos protegidos. Os certificados de identidade são usados para identificar você em um servidor AD RMS e permitem que você proteja arquivos e acesse arquivos protegidos.

Faça suas escolhas e controle

Os recursos AD RMS devem ser ativados através de um aplicativo compatível com AD RMS. Por padrão, eles não estão ativados. Você pode escolher não ativar ou usá-los. No entanto, se você não ativá-los, não será possível acessar arquivos protegidos.

Início da página

ID de anúncio

O que este recurso faz

Para oferecer publicidade mais relevante, o Windows permite que os aplicativos acessem um identificador exclusivo de cada usuário em um dispositivo. Você pode redefinir ou desativar o acesso a esse identificador a qualquer momento.

Informações coletadas, processadas ou transmitidas

Se você permitir que aplicativos acessem o identificador de anúncio, o Windows fornecerá essas informações para todos os aplicativos que as solicitarem. Os aplicativos podem armazenar ou transmitir essas informações.

Uso das informações

Sua ID de anúncio é usada por desenvolvedores de aplicativos e redes de publicidade para lhe fornecer publicidade mais relevante, compreendendo quais são os aplicativos que você usa e como faz isso. Também pode ser usada por desenvolvedores de aplicativos para

melhorar a qualidade do serviço, permitindo que eles determinem a frequência e a eficácia dos anúncios e detectem fraudes e problemas de segurança.

Se permitir que os aplicativos acessem a ID do anúncio, cada uso do identificador pelo aplicativo ficará sujeito às práticas de privacidade desse aplicativo.

Faça suas escolhas e controle

Se você optar pelas configurações expressas ao configurar o Windows, o Windows permitirá que os aplicativos usem sua ID de anúncio. Se você personalizar as configurações, poderá controlar o acesso à sua ID de anúncio selecionando **Permitir que aplicativos usem minha ID de anúncio para experiências entre aplicativos** , em **Compartilhar informações com a Microsoft e outros serviços**. Após instalar o Windows, você poderá alterar essa configuração em **Privacidade** nas configurações do computador. Se desativar essa configuração, a ID de anúncio não será enviada aos aplicativos que a solicitarem. Se você optar por ativar essa configuração novamente, um novo identificador será gerado.

Início da página

Auditoria

A auditoria permite que um administrador configure Windows para registrar a atividade do sistema operacional em um log de segurança que pode ser acessado usando o Visualizador de Eventos e outros aplicativos. Esse log pode ajudar um administrador a detectar acesso não autorizado ao computador ou a seus recursos. Por exemplo, esse log pode ajudar os administradores a solucionarem problemas e identificarem se alguém se conectou ao computador, criou uma nova conta de usuário, alterou uma política de segurança ou abriu um documento.

Informações coletadas, processadas ou transmitidas

Os administradores determinam as informações a serem coletadas, por quanto tempo serão mantidas e se serão transmitidas para terceiros. As informações podem incluir informações pessoais, como nome de usuário ou nomes de arquivo. Para obter mais informações, contate o

administrador. Nenhuma informação é enviada para a Microsoft.

Uso das informações

Os administradores também determinam como serão usadas as informações de auditoria. Geralmente, o log de segurança é usado por auditores e administradores para rastrear a atividade do computador ou para identificar acesso não autorizado a ele ou a seus recursos.

Faça suas escolhas e controle

Os administradores determinam se esse recurso é habilitado e quantos usuários são notificados. Nenhum outro usuário pode exibir o log de segurança, a menos que o administrador permita o acesso a ele. Você pode configurar a Auditoria no seu computador abrindo a Política de Segurança Local em Ferramentas Administrativas.

Início da página

Biometria

O que este recurso faz

Se o seu computador tiver um leitor de impressão digital, você poderá usar sua impressão digital para entrar no Windows e identificar-se em aplicativos que dão suporte a esse recurso

Informações coletadas, processadas ou transmitidas

Quando você configura uma nova impressão digital, as leituras da sua impressão digital são armazenadas localmente no computador. Nenhuma informação é enviada para a Microsoft. Quando você usa sua impressão digital para se identificar em um aplicativo, o Windows compara a impressão digital com as impressões digitais salvas no seu computador e informa o aplicativo se a impressão digital digitalizada corresponde àquela associada à sua conta. O Windows não fornece ao aplicativo os dados da impressão digital digitalizada.

Uso das informações

O Windows usa as informações da impressão digital que você armazenou no computador para conectar você ao Windows usando sua impressão digital.

Faça suas escolhas e controle

Você pode adicionar ou remover impressões digitais em **Opções de entrada** em **Contas** nas configurações do computador.

Início da página

Criptografia de Unidade de Disco BitLocker

O que este recurso faz

A Criptografia de Unidade de Disco BitLocker criptografa seus dados para protegê-los, o que ajuda a impedir que usuários não autorizados acessem seus dados. Quando o BitLocker é habilitado em uma unidade com suporte, oWindows criptografa os dados na unidade.

Informações coletadas, processadas ou transmitidas

Quando BitLocker é ativado usando criptografia de software, as chaves criptográficas na memória criptografam e decodificam os dados continuamente como se eles fossem lidos a partir da ou gravados na unidade protegida. Quando BitLocker é ativado usando criptografia de hardware, a criptografia e a decodificação dos dados são executadas pela unidade.

Durante a BitLocker configuração, você pode escolher imprimir uma chave de recuperação ou salvá-la em um local na sua rede. Se você configurar BitLocker em uma unidade não removível, também será possível salvar sua chave de recuperação em uma unidade flash USB.

Se o seu computador não está associado a um domínio, é possível fazer backup da chave de recuperação do BitLocker, da ID da chave de recuperação e do nome do computador na MicrosoftOneDrive. Para ajudar a proteger sua privacidade, as informações são enviadas criptografadas por SSL.

É possível configurar o BitLocker para criptografar dados usando um certificado armazenado em um cartão inteligente. Quando você protege uma unidade de dados usando um cartão inteligente, a chave pública e o identificador único do cartão inteligente são armazenados sem criptografia na unidade. Essas informações podem ser usadas para localizar o certificado que foi originalmente usado para gerar o certificado de criptografia do cartão inteligente.

Se seu computador possuir um hardware de segurança com pelo menos a versão 1.2 do Módulo confiado da plataforma (TPM), BitLocker usa o TPM para fornecer proteção de dados de hardware aprimorada para a unidade na qual Windows está instalado. Para obter mais informações, consulte a seção Serviço do Módulo Confiado da Plataforma (TPM). Em computadores equipados com o TPM, você também pode configurar um número de identificação pessoal (PIN) para ajudar a adicionar uma camada extra de proteção para seus dados criptografados. BitLocker armazenará esse PIN baseado no TPM em um formulário criptografado e colocado em hash na unidade.

As informações coletadas pelo BitLocker não são enviadas para a Microsoft a menos que você escolha fazer backup da sua chave de recuperação para OneDrive.

Uso das informações

As chaves criptográficas e os identificadores globais únicos (GUIDs) são armazenados na memória do computador para darem suporte a operações do BitLocker. BitLocker as informações de recuperação permitem que você acesse seus dados protegidos no caso de falhas de hardware e outros problemas. Essas informações de recuperação permitem que BitLocker faça a distinção entre usuários autorizados e não autorizados.

A Microsoft não usa suas chaves de recuperação individuais para qualquer propósito. Quando as chaves de recuperação são enviadas para OneDrive, Microsoft pode usar dados agregados sobre elas para analisar as tendências e ajudar a aprimorar nossos produtos e serviços.

Faça suas escolhas e controle

Por padrão, o BitLocker é desabilitado. Em uma unidade removível, qualquer usuário pode ativar BitLocker ou desativar a qualquer momento abrindo BitLocker Criptografia de Unidade no Painel de Controle. Um administrador pode ativar BitLocker ou desativar todas as unidades.

Você pode exibir e gerenciar as chaves de recuperação armazenadas em sua conta do OneDrive.

Início da página

contatos

O que este recurso faz

Se você usar o aplicativo de Pessoas ou um aplicativo de terceiros suportado para gerenciar seus contatos, poderá escolher compartilhar contatos específicos com outros aplicativos de seu computador, exibir informações de contato em um cartão de visita ou compartilhar informações de um contato específico com outros aplicativos de seu computador para executar uma ação, como fazer uma chamada ou mapear um endereço.

Informações coletadas, processadas, armazenadas e transmitidas

Quando um aplicativo solicita informações de contato, o Windows permite que você escolha contatos específicos para compartilhar com o aplicativo. Os contatos podem vir do aplicativo de Pessoa ou e um aplicativo de contatos de terceiros suportado. O Windows não compartilha sua lista inteira de contatos com o aplicativo solicitante.

Se um aplicativo tiver acesso a uma informação sobre um de seus contatos, como o número de telefone ou endereço de email, o Windows poderá mostrar um cartão de visita com informações adicionais daquele contato em seu aplicativo de contatos. O Windows não compartilha as informações adicionais do contato com o aplicativo que está exibindo o cartão de visita.

Se você tocar ou clicar em um comando como **Ligar**, no **Email**ou **Mapear** no cartão de visita, o Windows abrirá o aplicativo adequado para executar aquela ação e fornecer ao aplicativo os detalhes necessários do contato para executar a ação, como fornecer o número do telefone para fazer uma chamada.

Uso das informações

O Windows usa as informações do contato de seus aplicativo de contatos para compartilhar os contatos específicos que você escolher, para exibir os cartões de visita, para abrir os aplicativos e compartilhar as informações de contato para executar as ações listadas nos cartões de visita e para exibir seus contatos do Windows Search. O uso das informações do aplicativo de Pessoas sobre seus contatos é descrito

na Política de privacidade de aplicativos de comunicação.

Se você compartilhar informações de contato com um aplicativo de terceiros, a forma como o aplicativo usa as informações está sujeita às práticas de privacidade de terceiros. Se você compartilhar informações de contato com um aplicativo de Microsoft, as práticas de privacidade do aplicativo do aplicativo serão explicadas na política de privacidade do aplicativo.

Faça suas escolhas e controle

O Windows exibe e compartilha informações de contato apenas quando você escolhe compartilhar contatos específicos com um aplicativo, exibir um cartão de visita ou selecionar uma ação no cartão de visita.

Início da página

Instalação e descoberta de dispositivo

O Windows oferece diversos recursos para ajudá-lo a descobrir e instalar dispositivos em seu computador, incluindo Instalação de dispositivos, Instalação de dispositivos de banda larga móvel, Descoberta de rede e Emparelhamento de dispositivo sem fio.

Instalação de dispositivo

O que este recurso faz

Quando um novo dispositivo é instalado no computador, o Windows automaticamente pesquisa, baixa e instala o software de driver do dispositivo. O Windows também pode baixar informações sobre o dispositivo, como descrição, imagem e logotipo do fabricante. Alguns dispositivos, incluindo determinadas impressoras, webcams, dispositivos de banda larga móvel e dispositivos portáteis sincronizados com o Windows, têm um aplicativo que habilita completamente a funcionalidade e a experiência do usuário no dispositivo. Se o fabricante do dispositivo tiver fornecido um aplicativo para o dispositivo, o Windows poderá baixar e instalar automaticamente esse aplicativo da Windows Store, se você estiver conectado à Loja.

Informações coletadas, processadas ou transmitidas

Ao pesquisar drivers, o Windows entra em contato com o serviço online Windows Update para localizar e baixar drivers de dispositivos, caso ainda não haja um driver apropriado no computador. Para saber mais sobre as informações coletadas pelo Windows Update e como elas são usadas, veja a Política de privacidade do Update Services.

Para recuperar informações sobre seu dispositivo e determinar se um aplicativo está disponível para ele, o Windows envia dados sobre o dispositivo para a Microsoft, incluindo a ID do Dispositivo (por exemplo, ID de Hardware ou ID do Modelo do dispositivo em uso), sua região e idioma e a data em que as informações do dispositivo foram atualizadas pela última vez. Se houver um aplicativo disponível, o Windows automaticamente o baixará e instalará da Windows Store. O aplicativo estará disponível na sua conta da Windows Store, na lista dos seus aplicativos.

Uso das informações

As informações enviadas à Microsoft são usadas para determinar e baixar o driver adequado, as informações e o aplicativo para o seu dispositivo. A Microsoft não usa as informações enviadas para identificar ou contatar você.

Faça suas escolhas e controle

Se você optar pelas configurações expressas ao instalar o Windows, ative o download e a instalação automáticos de drivers, informações e aplicativos de dispositivos. Se optar pela personalização das configurações, poderá controlar o download e a instalação automáticos de drivers, aplicativos e informações de dispositivos selecionando **Obter automaticamente drivers de dispositivo, aplicativos e informações para novos dispositivos** , em **Ajude a proteger e atualizar seu computador**. Após instalar o Windows, você poderá alterar essas configurações no Painel de Controle selecionando Change device installation settings e **Não, deixe-me escolher o que fazer**.

Você pode desinstalar um aplicativo de dispositivo a qualquer momento sem desinstalar o dispositivo, embora talvez seja necessário que o aplicativo use determinados recursos do dispositivo. É possível reinstalar um aplicativo de dispositivo depois de desinstalá-lo, basta ir até sua lista de aplicativos na Windows Store.

Instalação de dispositivo de banda larga móvel

O que este recurso faz

Se seu computador possui um hardware de banda larga móvel fornecido por uma operadora móvel específica, Windows pode baixar e instalar automaticamente um aplicativo que permita a você gerenciar sua conta e plano de dados com a operadora móvel que fornece seu hardware de banda larga móvel do computador. Informações adicionais do dispositivo também são transferidas para ajudar a exibir sua conexão de banda larga móvel nas listas de rede.

Informações coletadas, processadas ou transmitidas

Para determinar quais informações e aplicativos de dispositivos baixar, o Windows envia uma parte dos identificadores de seu hardware de banda larga móvel para que possamos identificar sua operadora móvel. Para proteger sua privacidade, o Windows não envia os identificadores de hardware de banda larga móvel completos à Microsoft.

Se sua operadora móvel forneceu um aplicativo para a Microsoft, o Windows o baixará da Windows Store e o instalará. Quando você abrir o aplicativo após instalá-lo, ele terá acesso ao seu hardware de banda larga móvel, incluindo os identificadores de hardware exclusivos que a operadora móvel pode usar para identificar sua conta.

Uso das informações

A Microsoft usa a parte do identificador do hardware de banda larga móvel que o Windows envia para determinar qual aplicativo da operadora instalar em seu computador. Depois de instalado, o aplicativo pode usar suas identificações de hardware de banda larga móvel. Por exemplo, um aplicativo da operadora móvel pode usar esses identificadores para localizar a conta e planejar informações online. O uso dessas informações pelo aplicativo estará sujeito às práticas de privacidade da operadora móvel.

Faça suas escolhas e controle

Se você escolher as configurações expressas ao instalar o Windows pela primeira vez, o Windows automaticamente verificará e baixará os aplicativos da operadora móvel. Você pode habilitar e desabilitar esse recurso no Painel de Controle. Para obter mais informações, consulte a

seção Instalação de dispositivos abordada anteriormente.

Você pode desinstalar um aplicativo da operadora móvel a qualquer momento sem desinstalar o hardware de banda larga móvel.

Descoberta de rede

O que este recurso faz

Quando você conecta seu computador a uma pequena rede privada como pode possuir em casa, Windows pode descobrir automaticamente outros computadores e dispositivos compartilhados na rede e tornar o computador visível para outros na rede. Quando dispositivos compartilhados estão disponíveis, Windows pode automaticamente conectar-se a eles e instalá-los. Exemplos de dispositivos compartilhados incluem impressoras e extensores de mídia, mas não dispositivos pessoais como câmeras e celulares.

Informações coletadas, processadas ou transmitidas

Quando você habilita o recurso de compartilhamento e conexão com dispositivos, as informações sobre seu computador, como nome e endereço de rede, podem ser transmitidas pela rede local para permitir que outros computadores o descubram e se conectem a ele.

Para determinar se os dispositivos conectados à rede devem ser instalados automaticamente, algumas informações sobre a rede são coletadas e enviadas para a Microsoft. Essas informações incluem o número de dispositivos na rede, o tipo de rede (por exemplo, rede privada) e os tipos e nomes dos modelos dos dispositivos na rede. Nenhuma informação pessoal, como nome ou senha da rede, é coletada.

Dependendo das configurações de instalação do seu dispositivo, quando o Windows instala dispositivos compartilhados, o Windows pode enviar informações para a Microsoft e instalar o software do dispositivo no seu computador. Para obter mais informações, consulte a seção Instalação do dispositivo.

Uso das informações

As informações enviadas para a Microsoft sobre sua rede são usadas para determinar quais dispositivos na rede devem ser instalados automaticamente. A Microsoft não usa essas informações para

identificar, entrar em contato ou fazer propaganda para você.

Faça suas escolhas e controle

Se você optar por habilitar o recurso de compartilhamento e conexão de dispositivos ao ingressar em uma rede, a descoberta de rede será habilitada para essa rede. Você pode alterar essa configuração para sua rede atual clicando no tipo de rede listado sob o nome da rede em Central de Rede e Compartilhamento.

Você pode optar se deseja habilitar a descoberta de rede e a configuração automática dos dispositivos conectados à rede selecionando **Alterar as configurações de compartilhamento avançadas** na Central de Rede e Compartilhamento.

Emparelhamento de dispositivo sem fio

O que este recurso faz

Windows permite que você emparelhe seu computador com dispositivos sem fio que usam Bluetooth ou Wi–Fi Direct. Wi–Fi Direct é uma tecnologia sem fio que permite aos dispositivos se comunicarem diretamente entre si, sem a necessidade de se conectarem a uma rede Wi-Fi.

Informações coletadas, processadas ou transmitidas

Quando você seleciona **Permitir que dispositivos Bluetooth encontrem este computador** em Configurações de Bluetooth, o Windows transmite o nome do computador através do Bluetooth para permitir que dispositivos com Bluetooth habilitado detectem e identifiquem seu computador.

Quando você seleciona **Adicionar um dispositivo** em Dispositivos, nas configurações do computador, o Windows transmite o nome do computador através de Wi-Fi para permitir que dispositivos com Wi-Fi Direct o detectem e o identifiquem. Quando você escolhe **Adicionar um dispositivo**, Windows interrompe a transmissão do nome do seu computador por Wi–Fi.

Dependendo das configurações de instalação do seu dispositivo, quando o Windows instala dispositivos sem fio, o Windows pode enviar algumas informações para a Microsoft e instalar o software do dispositivo no seu computador. Para obter mais informações, consulte

a seção Instalação de dispositivos abordada anteriormente.

Uso das informações

O Windows difunde o nome do seu computador para permitir que outros dispositivos o identifiquem e se conectem a ele. O nome do seu computador não é enviado para a Microsoft.

Faça suas escolhas e controle

Para alterar se o Windows transmite o nome do seu computador usando Bluetooth, pressione e segure ou clique com o botão direito do mouse em Dispositivos e Impressoras no Painel de Controle do seu computador, selecione **Configurações de Bluetooth**e, em seguida, selecione **Permitir que dispositivos Bluetooth encontrem este computador**. Se você não quiser que o Windows transmita o nome do seu computador por Wi-Fi enquanto adiciona dispositivos, desabilite temporariamente o recurso Wi-Fi em Sem fio, nas configurações do computador, antes de adicionar um dispositivo.

Início da página

Criptografia de dispositivo

O que este recurso faz

A criptografia de dispositivo ajuda a proteger os dados criptografando-os com a tecnologia Criptografia de Unidade de Disco BitLocker, o que pode ajudar a prevenir ataques de software offline. Quando a criptografia de dispositivo está ativada, o Windows criptografa os dados da unidade em que o Windows está instalado.

Informações coletadas, processadas ou transmitidas

Quando você usa a criptografia de software, as chaves de criptografia na memória criptografam e decodificam os dados continuamente à medida que eles são lidos ou gravados na unidade protegida. Quando você usa a criptografia de hardware, a criptografia e a descriptografia dos dados são executadas pela unidade.

O Windows usa o TPM (Trusted Platform Module) no computador para armazenar e gerenciar as chaves de criptografia usadas para criptografar sua unidade. Quando a criptografia de dispositivo está habilitada, o Windows criptografa automaticamente a unidade em que

o Windows está instalado e gera uma chave de recuperação. A chave de recuperação pode ajudar você a acessar os dados protegidos, caso ocorram determinadas falhas de hardware ou outros problemas.

É feito o backup online automático da chave de recuperação do BitLocker do computador na conta do MicrosoftOneDrive de cada conta de administrador conectada a uma conta da Microsoft. O nome do computador e um identificador da chave de recuperação também são incluídos no backup na mesma conta do OneDrive. Para ajudar a proteger sua privacidade, as informações são enviadas criptografadas por SSL.

Uso das informações

As chaves de criptografia e os GUIDs (identificadores globais exclusivos) são armazenados na memória do computador para dar suporte a operações do BitLocker. As informações de recuperação permitem acessar seus dados protegidos no caso de algumas falhas de hardware ou outros problemas, e permitem que o BitLocker diferencie os usuários autorizados dos não autorizados.

A Microsoft faz backup de suas informações de recuperação em sua conta do OneDrive para que você possa acessá-las online. Não usamos as informações da chave de recuperação, nem as armazenamos em outro lugar que não seja a conta do OneDrive. Os dados agregados sobre as chaves de recuperação podem ser usados para analisar tendências e ajudar a aprimorar nossos produtos e serviços. Por exemplo, podemos usar essas informações para determinar a proporção de computadores em que a Criptografia de Dispositivo está ativada.

Faça suas escolhas e controle

Se você optar por usar uma conta da Microsoft ao configurar seu computador que, por sua vez, dá suporte para isso, a criptografia de dispositivo será ativada e será feito o backup da sua chave de recuperação na sua conta do OneDrive. Se você optar por usar uma conta local ao configurar o computador, a criptografia de dispositivo será desativada.

Se, posteriormente, você conectar uma conta da Microsoft a uma conta de administrador no computador:

- Se a criptografia de dispositivo ainda não estiver ativada, o Windows irá ativá-la automaticamente e fará backup das informações de recuperação na conta do OneDrive desse usuário.
- Se a criptografia de dispositivo já estiver ativada, será feito o backup das informações de recuperação do computador na conta do OneDrive desse usuário.

Você pode exibir e gerenciar as chaves de recuperação armazenadas em sua conta do OneDrive aqui.

Início da página

DirectAccess

O que este recurso faz

O DirectAccess permite que seu computador, quando conectado à Internet, estabeleça uma conexão remota e direta com a rede de seu local de trabalho, não importa onde você esteja.

Informações coletadas, processadas ou transmitidas

Cada vez que você iniciar seu computador, o DirectAccess tentará conectar-se à rede do seu local de trabalho, independentemente de sua presença física no local de trabalho. Uma vez conectado, o computador baixará a política do local de trabalho e você poderá acessar os recursos configurados na rede do local de trabalho. O administrador do seu local de trabalho poderá aproveitar a conectividade do DirectAccess para gerenciar e monitorar remotamente seu computador, inclusive os sites visitados, mesmo quando você não estiver fisicamente no local de trabalho.

O DirectAccess não envia informações para a Microsoft.

Uso das informações

As políticas da sua empresa determinam como as informações coletadas pelo administrador do seu local de trabalho são usadas.

Faça suas escolhas e controle

O DirectAccess deve ser configurado pelo administrador do seu local

de trabalho usando a Política de Grupo. Embora o administrador possa permitir que você desative temporariamente alguns elementos do DirectAccess, somente o administrador do local de trabalho pode impedir que o Windows tente se conectar ao seu local de trabalho para gerenciamento. Se você ou o administrador do local de trabalho remover seu computador do domínio do local de trabalho, o DirectAccess não mais poderá se conectar.

Início da página

Central de Facilidade de Acesso

O que este recurso faz

O recurso Central de Facilidade de Acesso permite que você habilite as opções e configurações de acessibilidade para facilitar a interação com o computador.

Informações coletadas, processadas ou transmitidas

Se você usa esse recurso, será necessário selecionar as declarações apropriadas.

Essas declarações incluem:

- É difícil enxergar as imagens e os textos na TV.
- É difícil enxergar as imagens no monitor por causa das condições de iluminação.
- Eu não uso um teclado.
- Sou cego.
- Sou surdo.
- Eu tenho comprometimento na fala.

Essas informações são salvas em um formato não legível por humanos e armazenadas localmente no seu computador.

Uso das informações

Um conjunto de recomendações de configuração é fornecido para você com base nas instruções escolhidas. Essas informações não são

enviadas para a Microsoft e não estão disponíveis para outros usuários, exceto para você e os administradores do seu computador.

Faça suas escolhas e controle

Você pode escolher quais declarações deseja selecionar acessando Facilidade de Acesso no Painel de Controle. Você pode alterar suas escolhas a qualquer momento. Também é possível escolher quais recomendações você deseja configurar no seu computador.

Início da página

Visualizador de Eventos

O que este recurso faz

Os usuários do computador, primeiramente os administradores, podem usar o Visualizador de Eventos para visualizar e gerenciar os logs de eventos. Os logs de eventos contêm informações sobre eventos de hardware, software e segurança no seu computador. Você também pode obter informações da Microsoft sobre eventos nos logs de eventos clicando em Ajuda online de log de eventos.

Informações coletadas, processadas ou transmitidas

Os logs de eventos contêm informações de evento geradas por todos os usuários e aplicativos no computador. Por padrão, todos os usuários podem exibir entradas dos logs de eventos; contudo, os administradores podem optar por restringir o acesso aos logs de eventos. Você pode acessar os logs de eventos do seu computador abrindo o Visualizador de Eventos. Para saber como abrir o Visualizador de Eventos, consulte Windows Ajuda e Suporte.

Se você usa a Ajuda Online do Log de Eventos para procurar informações adicionais sobre determinado evento, essas informações serão enviadas à Microsoft.

Uso das informações

Quando você usa a Ajuda Online do Log de Eventos para procurar informações sobre um evento, os dados do evento enviados de seu computador são usados para localizar e fornecer a você mais informações sobre o evento. Para eventos da Microsoft, os detalhes do evento serão enviados para a Microsoft. A Microsoft não usa essas

informações para identificar, entrar em contato ou fazer propaganda para você. Para eventos associados a aplicativos de terceiros, as informações serão enviadas para o local especificado pelo fornecedor ou fabricante de terceiros. Se você enviar informações sobre os eventos para editores de terceiros ou fabricantes, o uso das informações estará sujeito às práticas de privacidade de cada terceiro.

Faça suas escolhas e controle

Os administradores podem escolher restringir o acesso aos logs do Visualizador de Eventos. Os usuários com acesso total aos logs do Visualizador de Eventos podem limpar os logs. A menos que você já tenha autorizado o envio de informações do evento automaticamente ao clicar em Ajuda Online do Log de Eventos, será solicitado que você confirme se as informações apresentadas poderão ser enviadas pela Internet. Nenhuma informação do log de eventos será enviada pela Internet sem a sua autorização. Os administradores podem usar a Política de Grupo para selecionar ou alterar o site para o qual as informações do evento são enviadas.

Início da página

Proteção para a Família

O que este recurso faz

A Proteção para a Família ajuda os pais a protegerem seus filhos quando eles usam o computador. Os pais controlam quais aplicativos, jogos e sites os filhos podem usar. Os pais também definem limites de tempo e recebem relatórios regulares das atividades por email. Os pais gerenciam as restrições e visualizam os relatórios de atividades localmente no computador ou online, usando o site da Proteção para a Família da Microsoft.

Informações coletadas, processadas ou transmitidas

As configurações e os relatórios da Proteção para a Família das atividades dos filhos são armazenados no computador. Os relatórios de atividades podem incluir informações sobre o tempo de uso do computador, o tempo de uso de aplicativos e jogos e os sites visitados (incluindo as tentativas de visualizar sites bloqueados). Os administradores no computador podem alterar as configurações e

visualizar o relatório de atividades.

Se o gerenciamento online estiver habilitado para uma conta da criança, os responsáveis poderão ver o relatório de atividades da criança e alterar as respectivas configurações no site da Microsoft Proteção para a Família. O responsável pode permitir que outras pessoas vejam os relatórios de atividades e alterem as configurações adicionando-as como responsáveis no site da Microsoft Proteção para a Família. Se o responsável que está configurando a Proteção para a Família estiver conectado ao Windows com uma conta da Microsoft, o gerenciamento online será automaticamente habilitado.

Quando a Proteção para a Família é configurada para uma conta da criança com o gerenciamento online habilitado, são enviados automaticamente por email relatórios semanais das atividades da criança ao responsável.

Uso das informações

Os sites do Windows e da Microsoft Proteção para a Família usam as informações coletadas para oferecer o recurso Proteção para a Família. A Microsoft pode analisar as informações do log de atividades como um todo por questões de qualidade de dados, mas não as utiliza para identificar, entrar em contato ou fazer propaganda para os usuários individuais.

Faça suas escolhas e controle

A Proteção para a Família está desabilitada por padrão. É possível acessar a Proteção para a Família pelo Painel de Controle. Somente os administradores podem habilitar a Proteção para a Família, e apenas os usuários sem privilégios administrativos podem ser monitorados ou restritos. As crianças podem ver suas configurações, mas não conseguem alterá-las. Se a Proteção para a Família estiver habilitada, a criança receberá uma notificação de que a Proteção para a Família está monitorando sua conta toda vez que ela entrar no Windows. Se você indicar uma conta como sendo da criança durante a criação da conta, poderá habilitar a Proteção para a Família nessa conta.

Se o administrador que está configurando a conta da criança estiver conectado ao Windows com uma conta da Microsoft, o gerenciamento online será automaticamente habilitado e serão enviados relatórios

semanalmente com as atividades da criança. As contas dos pais podem ser adicionadas e removidas do site da Proteção para a Família da Microsoft. Qualquer pessoa adicionada como responsável no site pode exibir o relatório de atividades da criança e alterar suas configurações da Proteção para a Família, mesmo que o responsável não seja o administrador do computador que a criança usa.

Para usar corretamente a Proteção para a Família, somente os pais devem ser administradores do computador, e as crianças não devem ter privilégios administrativos. Observe que o uso desse recurso para monitorar outros usuários (como adultos) pode violar a lei aplicável.

Início da página

Fax

O que este recurso faz

O recurso Fax permite que você crie e salve capas de fax e envie e receba faxes usando seu computador e um modem de fax externo ou integrado ou um servidor de fax.

Informações coletadas, processadas ou transmitidas

As informações coletadas incluem as informações pessoais inseridas em uma folha de rosto de fax, assim como identificadores contidos nos protocolos de fax padrão da indústria, como TSID (ID do Assinante Transmissor) e CSID (ID do Assinante Chamado). Por padrão, Windows usa "Fax" como o valor para cada identificador.

Uso das informações

As informações inseridas na caixa de diálogo do remetente são apresentadas na capa do fax. Os identificadores, como o TSID e o CSID, podem conter texto arbitrário e geralmente são usados pela máquina de recebimento de fax ou computador para identificar o remetente. Nenhuma informação é enviada para a Microsoft.

Faça suas escolhas e controle

O acesso ao fax é determinado pelos privilégios da sua conta de usuário no computador. A menos que o administrador de fax altere as configurações de acesso, todos os usuários podem enviar e receber faxes. Por padrão, todos os usuários podem visualizar os documentos

que eles enviam e qualquer fax que é recebido no computador. Os administradores podem ver todos os documentos de fax, enviados ou recebidos, e podem definir as configurações de fax, incluindo quem tem permissões para exibir ou gerenciar fax, e os valores de TSID e CSID.

Início da página

Personalização de manuscrito: aprendizado automático

O que este recurso faz

O aprendizado automático é uma ferramenta de personalização de reconhecimento de manuscrito que está disponível em computadores com toque ou caneta eletrônica. Esse recurso coleta dados sobre as palavras que você usa e o modo como as escreve. Isso ajuda o software de reconhecimento de manuscrito a aprimorar sua interpretação do estilo e do vocabulário do manuscrito e também melhora a correção automática e as sugestões de texto para os idiomas sem IMEs.

Informações coletadas, processadas ou transmitidas

As informações coletadas pela aprendizagem automática são armazenadas no perfil do usuário para cada usuário no computador. Os dados são armazenados em um formato proprietário que não pode ser lido usando um aplicativo de visualização de texto (por exemplo, Bloco de Notas ou WordPad) e só estão disponíveis para outros usuários que forem administradores do computador.

As informações coletadas incluem:

- O texto das mensagem que você redigir e as entradas de calendário que criar usando os aplicativos de email (por exemplo, Office Outlook ou Windows Live Mail) incluindo quaisquer mensagens que você já tenha enviado.
- A tinta escrita no Painel de Entrada.
- O texto reconhecido a partir da tinta escrita no Painel de Entrada ou digitado usando os teclados virtuais.
- Os caracteres alternativos selecionados para corrigir o texto

reconhecido.

Uso das informações

As informações coletadas são usadas para ajudar a aprimorar o reconhecimento de manuscrito criando uma versão do software de reconhecimento personalizada de acordo com seu próprio estilo e vocabulário, bem como para habilitar a correção automática e as sugestões de texto conforme você digita usando teclados virtuais.

As amostras de texto são usadas para criar um dicionário estendido. As amostras de tinta são usadas para aprimorar o reconhecimento de manuscrito para cada usuário em um computador. Nenhuma informação é enviada para a Microsoft.

Faça suas escolhas e controle

O aprendizado automático é habilitado por padrão. Você pode habilitar ou desabilitar o aprendizado automático a qualquer momento em **Configurações avançadas** em **Idiomas** no Painel de Controle. Quando você desativar o aprendizado automático, todos os dados que foram coletados e armazenados pelo aprendizado automático serão excluídos.

Início da página

Grupo Doméstico

O que este recurso faz

O Windows permite vincular facilmente computadores à sua rede doméstica, assim você pode compartilhar imagens, músicas, vídeos, documentos e dispositivos. Ele também permite que os computadores transmitam mídia a dispositivos em sua rede doméstica, como um extensor de mídia. Esses computadores e dispositivos são o seu grupo doméstico. Você pode ajudar a proteger o seu grupo doméstico com uma senha e escolher o que deseja compartilhar.

Informações coletadas, processadas ou transmitidas

Você pode acessar seus próprios arquivos, como imagens, vídeos, músicas e documentos, a partir de qualquer computador no grupo doméstico. Quando você ingressar em um grupo doméstico, as

informações de todas as contas da Microsoft no computador (incluindo endereço de email, nome de exibição e imagem) serão compartilhadas com outros usuários do grupo doméstico para habilitar o compartilhamento com esses usuários.

Uso das informações

As informações coletadas permitem que os computadores em seu grupo doméstico saibam com quem compartilhar o conteúdo e como apresentá-lo. Nenhuma informação é enviada para a Microsoft.

Faça suas escolhas e controle

Você tem a capacidade de adicionar ou remover computadores de um grupo doméstico e decidir o que é compartilhado com outros membros do grupo doméstico. Você pode criar um grupo doméstico e gerenciar suas configurações acessando **Grupo Doméstico** , em **Rede** nas configurações do computador.

Início da página

IME (Editor de Método de Entrada)

Os IMEs da Microsoft são usados nos idiomas do Leste Asiático para converter a entrada de teclado em ideogramas. Esta seção explica vários recursos, incluindo autoajuste, previsão, relatório de erros de conversão e registro de palavras do IME.

Candidatos IME à nuvem

O que este recurso faz

Quando você usa o Microsoft Pinyin IME para inserir caracteres em chinês simplificado, o IME pode usar um serviço online para examinar ideogramas candidatos à entrada digitada que ainda não existam em um dicionário no computador.

Informações coletadas, processadas ou transmitidas

Quando você digita caracteres em chinês simplificado usando o Microsoft Pinyin IME, o IME sugere ideogramas que talvez você deseje usar. Se o IME não encontrar boas sugestões no dicionário local, ele enviará a entrada do teclado para a Microsoft para determinar se há outros ideogramas candidatos a essa entrada que sejam melhores. Se

houver, eles serão exibidos na lista de candidatos e, se selecionados, serão adicionados ao dicionário local. Um identificador exclusivo gerado aleatoriamente também será enviado para nos ajudar a analisar o uso desse recurso. O identificador não é associado à sua conta da Microsoft, nem é usado para identificá-lo, contatá-lo ou direcionar propaganda para você.

Uso das informações

A Microsoft usa as informações coletadas para examinar os ideogramas em nuvem e aperfeiçoar nossos produtos e serviços. Não usamos essas informações para identificá-lo, contatá-lo nem direcionar propaganda para você.

Faça suas escolhas e controle

Candidatos IME à nuvem estão desativados por padrão para Microsoft Pinyin IME para chinês simplificado. Para exibir ou alterar essa configuração, abra Configurações do PC, clique em **Hora e idioma**, clique em **Região e idioma**, escolha o idioma e clique em **Opções**.

Proteção e autoajuste do IME

O que este recurso faz

Dependendo do IME utilizado suas configurações, os recursos de sugestão de texto e auto-tunning do IME podem gravar palavras ou sequências de palavras para aprimorar a seleção dos ideogramas exibidos.

Informações coletadas, processadas ou transmitidas

O recurso de auto-tunning do IME (auto-aprendizado) e sugestão de texto gravam uma palavra ou uma sequência de palavras e a frequência com a qual elas são usadas. As informações de auto-tuning (excluindo quaisquer sequências de caractere de símbolo/digito) são armazenadas em arquivos para cada usuário em um computador.

Uso das informações

Os dados de aprendizado automático e de sugestões de texto são usados pelo IME no computador para aprimorar a seleção de ideogramas exibidos quando o IME é usado. Se você escolher enviar esses dados para a Microsoft, eles serão usados para aprimorar o IME e produtos e serviços relacionados.

Faça suas escolhas e controle

Os recursos de aprendizado automático e sugestão de texto são habilitados por padrão nesses IMEs que dão suporte a eles. Os dados coletados não são enviados automaticamente para a Microsoft. Você pode escolher se deseja coletar ou enviar esses dados em Idioma no Painel de Controle.

Relatório de erro de conversão do IME

O que este recurso faz

Se ocorrerem erros na apresentação dos ideogramas ou na conversão da entrada de teclado, esse recurso pode coletar informações sobre os erros que podem ajudar a Microsoft aprimorar seus produtos e serviços.

Informações coletadas, processadas ou transmitidas

O Relatório de erro de conversão do IME coleta informações sobre os erros de conversão do IME, como o que foi digitado, o resultado da primeira conversão ou previsão, a cadeia de caracteres escolhida, informações sobre o IME usado e as informações sobre como ele foi usado. Além disso, se você usa o IME do japonês, é possível escolher incluir as informações do aprendizado automático nos relatórios de erro de conversão.

Uso das informações

A Microsoft usa as informações para aprimorar seus produtos e serviços. A Microsoft não usa essas informações para identificar, entrar em contato ou fazer propaganda para você.

Faça suas escolhas e controle

Após um determinado número de erros de conversão ser armazenado, a Ferramenta de Relatório de Conversão Ausente perguntará se você deseja enviar um relatório de erro de conversão. Você também pode escolher enviar um relatório de erro de conversão da Ferramenta de Relatório de Conversão Ausente do IME a qualquer momento. Você pode visualizar as informações contidas em cada relatório antes de escolher enviá-lo. Também é possível habilitar o envio automático de relatórios de erro de conversão nas Configurações do IME.

Registro de palavras do IME

O que este recurso faz

Dependendo do IME usado, você pode ser capaz de usar o registro de palavras para relatar palavras incompatíveis (palavras que não são convertidas corretamente para os ideogramas a partir da entrada do teclado).

Informações coletadas, processadas ou transmitidas

Os relatórios de registro podem incluir as informações que você fornece na caixa de diálogo Adicionar palavra sobre as palavras que estão sendo relatadas e o número da versão do software para um IME. Esses relatórios podem incluir informações pessoais, por exemplo, se você adicionar nomes pessoais usando o registro de palavras. Você tem a oportunidade de renovar os dados que estiverem sendo enviados com cada relatório antes de escolher enviá-los.

Uso das informações

A Microsoft usa as informações para aprimorar seus produtos e serviços. A Microsoft não usa essas informações para identificar, entrar em contato ou fazer propaganda para você.

Faça suas escolhas e controle

Cada vez que você criar um relatório de registro de palavra, é perguntado se você deseja enviar esse relatório para a Microsoft. Você pode visualizar as informações contidas no relatório antes de escolher enviá-lo.

Início da página

Compartilhamento de conexão com a internet

O que este recurso faz

O compartilhamento de conexão com a Internet permite compartilhar a conexão com a Internet de banda larga móvel com outros dispositivos via Wi-Fi. Você também pode iniciar remotamente um compartilhamento de conexão com a Internet em seu dispositivo de banda larga móvel do seu computador se você tiver entrado em ambos com a mesma conta da Microsoft.

Informações coletadas, processadas ou transmitidas

Quando você compartilha uma conexão com a Internet pela primeira vez, o Windows gera e armazena automaticamente um nome e uma senha de rede. Você pode alterar esses dados a qualquer momento.

Se o seu computador der suporte a esse recurso e você o tiver adicionado à sua conta da Microsoft como um dispositivo confiável, o Windows sincronizará o nome e a senha da rede com sua conta da Microsoft. O Windows também sincroniza outras informações para permitir que você inicie remotamente o compartilhamento de conexão com a Internet de seus outros dispositivos confiáveis. Essas informações incluem o endereço de hardware do rádio Bluetooth e um número aleatório usado para ajudar a proteger a conexão.

Uso das informações

Essas informações são usadas para configurar o compartilhamento de conexão com a Internet. A Microsoft não usa essas informações para identificá-lo, contatá-lo nem para enviar propaganda para você.

Faça suas escolhas e controle

Se você entrar em um dispositivo que dê suporte ao compartilhamento de conexão com a Internet usando sua conta da Microsoft e então adicionar o dispositivo como um dispositivo confiável, as informações necessárias para iniciar remotamente o compartilhamento de conexão com a Internet serão sincronizadas com o OneDrive. Você pode parar a sincronização de informações optando por não sincronizar senhas. Para obter mais informações, consulte a seção "Configurações de sincronização" nesta página.

Início da página

Impressão via Internet

O que este recurso faz

O recurso Impressão via Internet permite que você imprima via internet.

Informações coletadas, processadas ou transmitidas

Quando você imprime usando esse recurso, primeiro é necessário

conectar-se e autenticar-se em um servidor de impressão via internet. As informações que você precisará para enviar para o servidor de impressão vão variar dependendo do nível de segurança que o servidor de impressão suporta (por exemplo, é possível que seja solicitado o fornecimento de um nome de usuário e senha). Após você estar conectado, será apresentada uma lista de impressoras compatíveis. Se seu computador não tiver um driver para a impressora selecionada, você poderá baixar um do servidor de impressão. Como os trabalhos de impressão não são criptografados, é possível que outras pessoas vejam o conteúdo que está sendo enviado.

Uso das informações

As informações coletadas permitem que você imprima usando as impressoras remotas. Se você usar um servidor de impressão hospedado pela Microsoft, nós não usaremos as informações fornecidas para identificar ou contatar você, nem para direcionar propaganda para você. Se enviar informações a um servidor de impressão de terceiros, o uso das informações ficará sujeito às práticas de privacidade do terceiro.

Faça suas escolhas e controle

Você pode habilitar ou desabilitar a impressão via Internet abrindo **Programas e Recursos** no Painel de Controle e selecionando **Ativar ou desativar recursos doWindows**.

Início da página

Preferências de idioma

O que este recurso faz

Você pode adicionar os idiomas de sua preferência à lista de idiomas no Windows 8.1. Os aplicativos e sites aparecem no primeiro idioma disponível na lista.

Informações coletadas, processadas ou transmitidas

Quando você visita sites e instala aplicativos no computador, sua lista de idiomas preferidos é enviada aos sites visitados e fica disponível para os aplicativos utilizados para que eles possam fornecer conteúdo nos idiomas preferidos.

Uso das informações

Sua lista de idiomas preferidos é usada pelos sites e aplicativos da Microsoft para apresentar o conteúdo nos idiomas de sua preferência. A Microsoft não usa as informações de idioma para identificar ou entrar em contato com você. As informações de idiomas enviadas ou usadas por sites e aplicativos de terceiros estão sujeitas às práticas de privacidade do fornecedor do site ou aplicativo de terceiros.

Faça suas escolhas e controle

Sua lista de idiomas preferidos fica disponível aos aplicativos instalados e sites visitados. Você pode adicionar ou remover idiomas essa lista nas Preferências de idioma do Painel de Controle. Caso não tenha idiomas na lista, o idioma selecionado na guia Formatos da janela Região do Painel de Controle será enviado para os sites visitados.

Início da página

Serviços de localização

Os serviços de localização do Windows deixam você escolher quais aplicativos, sites e recursos do Windows podem determinar a localização do seu computador. Os serviços de localização do Windows consistem em dois componentes. O Localizador do Windows se conecta a um serviço online da Microsoft para determinar a localização. A Plataforma de Localização do Windows determina a localização do computador usando um hardware (por exemplo, um sensor de GPS) ou software, como o Localizador do Windows.

Plataforma de Localização do Windows

O que este recurso faz

Se você habilitar a Plataforma de Localização do Windows, os aplicativos instalados da Windows Store, bem como alguns recursos do Windows, poderão solicitar permissão para determinar a localização do computador. Se você permitir que um aplicativo use a sua localização, a Plataforma de Localização do Windows, além de fornecer sua localização enquanto você usa o aplicativo, poderá avisar o aplicativo quando o computador entrar ou sair dos limites geográficos definidos pelo aplicativo. Por exemplo, em determinado aplicativo, você pode

definir um lembrete para passar no supermercado quando sair do trabalho. Dependendo da configuração do sistema, a Plataforma de Localização do Windows pode determinar a localização do computador usando um hardware (por exemplo, um sensor de GPS) ou software, como o Localizador do Windows.

A Plataforma de Localização do Windows não impede que os aplicativos determinem a localização de outras maneiras. Por exemplo, você pode instalar dispositivos (como um receptor de GPS) que podem enviar informações de localização diretamente para um aplicativo e ignorar a plataforma. Independentemente das configurações da Plataforma de Localização do Windows, os serviços online podem usar o endereço IP para determinar sua localização aproximada, geralmente a cidade em que ele se encontra.

Informações coletadas, processadas ou transmitidas

A Plataforma de Localização do Windows propriamente dita não transmite nenhuma informação do computador, mas os localizadores individuais (como o Localizador do Windows) podem transferir informações quando a Plataforma de Localização do Windows solicita que o localizador determine a localização do computador. Os aplicativos, sites e recursos autorizados a usar a plataforma para determinar a localização do computador também podem transmitir ou armazenar essas informações. Se um aplicativo configurar limites geográficos a serem monitorados, esses limites serão armazenados de forma criptografada no computador. As informações armazenadas sobre esses limites incluem um nome, uma localização e se o computador estava dentro ou fora do limite na última vez em que a localização foi determinada. Os aplicativos que configuram limites geográficos podem transmitir ou armazenar essas informações

Uso das informações

Se você ativar a Plataforma de Localização do Windows, os aplicativos, sites e recursos do Windows autorizados poderão acessar a localização do computador e usá-la para fornecer conteúdo personalizado a você. Se usar um localizador ou aplicativo de terceiros, o uso que ele fizer da localização do computador estará sujeito às práticas de privacidade do respectivo fornecedor. Antes de baixar um aplicativo da Windows Store, você pode verificar se o aplicativo tem reconhecimento de local,

na descrição do aplicativo.

Faça suas escolhas e controle

Ao escolher as configurações expressas durante a Instalação do Windows, você habilita a Plataforma de Localização do Windows. Se você optar por personalizar configurações, poderá controlar a Plataforma de Localização do Windows selecionando Permita que o Windows e os aplicativos peçam o meu local da Plataforma de Localização do Windows em Compartilhar informações com a Microsoft e outros serviços. Quando cada aplicativo da Loja solicita pela primeira vez a localização do computador, o Windows pergunta se você deseja permitir que o aplicativo use sua localização. Você pode exibir e alterar essa configuração para cada aplicativo da Loja. Basta acessar Permissões nas configurações do aplicativo.

Se você usa um aplicativo de área de trabalho que utiliza a Plataforma de Localização do Windows, ele deverá solicitar sua permissão para usar a localização do computador e, ao acessá-la, será exibido um ícone na área de notificação para alertá-lo de que a localização do computador foi acessada. Cada usuário pode controlar suas próprias configurações de localização para os aplicativos em **Privacidade** , nas configurações do computador. Além disso, os administradores podem optar por desabilitar a plataforma de localização para todos os usuários em **Configurações de Localização** no Painel de Controle. Para impedir que os aplicativos sejam notificados quando os limites geográficos definidos por aplicativos forem acessados, um usuário administrador pode desabilitar o Serviço de Localização de Estrutura do Windows no Painel de Controle.

Localizador do Windows

O que este recurso faz

O Localizador do Windows se conecta ao Serviço de Localização da Microsoft online para determinar a localização aproximada do computador com base nas redes Wi-Fi perto do computador ou no respectivo endereço IP do computador.

Informações coletadas, processadas ou transmitidas

Quando um aplicativo autorizado solicitar sua localização, a Plataforma de Localização do Windows pedirá a todos os Localizadores instalados

(inclusive o Localizador do Windows) para determinar a localização atual do seu computador. Primeiro, o Localizador do Windows verifica se ele possui uma lista armazenada de pontos de acesso Wi-Fi próximos de uma solicitação anterior feita por um aplicativo com reconhecimento de local. Se ainda não houver uma lista de pontos de acesso Wi-Fi próximos, ou se a lista estiver desatualizada, o localizador enviará informações sobre os pontos de acesso Wi-Fi próximos e dados do GPS (se disponíveis) para o Serviço de Localização da Microsoft. O serviço retorna a localização aproximada do computador para o localizador, que a transmite para a Plataforma de Localização do Windows, que, por sua vez, a transfere para o aplicativo que a solicitou. O Localizador do Windows também pode atualizar sua lista armazenada de pontos de acesso Wi-Fi. O Localizador do Windows mantém essa lista para poder determinar a localização aproximada do seu computador sem precisar se conectar à Internet. Essa lista de pontos de acesso é criptografada quando armazenada em disco para que os aplicativos não tenham acesso direto a ela.

As informações enviadas sobre os pontos de acesso Wi-Fi próximos incluem o BSSID (o endereço MAC do ponto de acesso Wi-Fi) e a intensidade do sinal. As informações do GPS incluem a latitude, longitude, direção, velocidade e altitude observadas. Para proteger sua privacidade, o Localizador do Windows não envia nenhuma informação que identifique exclusivamente seu computador além das informações padrão do computador enviadas com todas as conexões com a Internet. Para proteger a privacidade dos proprietários de rede Wi-Fi, o Windows não envia informações sobre SSIDs (nomes dos pontos de acesso Wi-Fi) nem sobre redes Wi-Fi ocultas. Para fins de privacidade e segurança, as informações sobre redes Wi-Fi são enviadas com criptografia SSL.

Se você optar por ajudar a melhorar o Serviço de Localização da Microsoft, o Windows poderá enviar informações sobre pontos de acesso Wi-Fi próximos à Microsoft novamente depois que um aplicativo solicitar a localização de seu computador. Se você usa um plano de Internet limitado, o Windows limita o número de vezes por dia que envia essas informações para restringir o uso de sua conexão com a Internet.

Uso das informações

As informações são usadas pelo Localizador do Windows para fornecer à Plataforma de Localização do Windows o local aproximado de seu computador quando um aplicativo autorizado solicitá-lo.

Se você optar por melhorar o Serviço de Localização da Microsoft, as informações de Wi-Fi e GPS enviadas à Microsoft serão usadas para melhorar os serviços de localização da Microsoft, aperfeiçoando, assim, os serviços de localização oferecidos aos aplicativos. A Microsoft não armazena os dados coletados desse serviço que possam ser usados para identificar, contatar ou enviar anúncios para você, nem para rastrear ou criar um histórico da localização do seu computador.

Faça suas escolhas e controle

O Localizador do Windows é usado apenas quando um aplicativo autorizado solicita a localização de seu computador. Para obter mais informações sobre como controlar quando os aplicativos podem solicitar a localização do computador, veja a seção Plataforma de Localização do Windows. Se você autorizar aplicativos a solicitar a localização do computador, a lista armazenada em cache dos locais de pontos de acesso Wi-Fi próximos que são criptografados e armazenados pelo Localizador do Windows será excluída e substituída periodicamente.

Se você optar pelas configurações expressas ao instalar o Windows, ajudará a melhorar o Serviço de Localização da Microsoft. Se você optar por personalizar as configurações, poderá controlar se deseja ajudar a aperfeiçoar o Serviço de Localização da Microsoft selecionando **Enviar alguns dados de localização à Microsoft ao usar aplicativos com reconhecimento de local** , em **Ajudar a melhorar os produtos e serviços da Microsoft**. Após configurar o Windows, você pode alterar essa configuração em Configurações de Local no Painel de Controle. Se você optar por não ajudar a aperfeiçoar o serviço, ainda assim poderá usar o Localizador do Windows para determinar a localização aproximada do computador.

Você pode habilitar ou desabilitar o Localizador do Windows abrindo **Ativar ou desativar recursos doWindows** no Painel de Controle. Se você desabilitar o Localizador do Windows, ainda assim poderá usar outros localizadores (como um GPS) com a Plataforma de Localização do Windows.

Início da página

Gerenciar suas credenciais

O que este recurso faz

O Windows permite conectar aplicativos da Windows Store às contas que você usa em sites. Se já tiver salvo uma senha para um site no Internet Explorer, o Windows poderá usar a senha salva quando você conectar um aplicativo a esse site.

Informações coletadas, processadas ou transmitidas

Quando o aplicativo pedir as credenciais para entrar no site, você poderá optar por salvar essas credenciais. Se você já se conectou ao site no Internet Explorer e optou por salvar suas credenciais, o Windows preencherá automaticamente as credenciais salvas. As credenciais são armazenadas de forma criptografada no computador. Para obter mais informações sobre como essas e outras credenciais podem ser sincronizadas com o OneDrive, consulte a seção "Configurações de sincronização" desta página.

Uso das informações

O Windows só usa as credenciais salvas para ajudar você a entrar nos sites selecionados. Se você salvar credenciais para um site enquanto se conecta a um aplicativo, as credenciais salvas não serão usadas no Internet Explorer nem em outros aplicativos.

Faça suas escolhas e controle

Você pode gerenciar as credenciais salvas no Gerenciador de Credenciais no Painel de Controle. Para obter mais informações sobre como essas e outras credenciais podem ser sincronizadas com o OneDrive, consulte a seção "Configurações de sincronização" desta página.

Início da página

Nome e imagem da conta

O que este recurso faz

Para fornecer conteúdo personalizado, os aplicativos podem solicitar

seu nome e imagem da conta do Windows. O nome e a imagem da conta são exibidos em **Sua conta** em **Contas** , nas configurações do computador. Se você entrar no Windows com uma conta da Microsoft, o Windows usará o nome e a imagem associados a essa conta. Se não tiver escolhido uma imagem para a conta, será usada uma imagem padrão disponibilizada pelo Windows

Informações coletadas, processadas ou transmitidas

Se você permitir que aplicativos acessem o nome e a imagem de sua conta, o Windows passará essas informações a todos os aplicativos que os solicitarem. Os aplicativos podem armazenar ou transmitir essas informações.

Se você entrar no Windows com uma conta de domínio e permitir que aplicativos utilizem o nome e a imagem de sua conta, os aplicativos com permissão para usar suas credenciais do Windows poderão acessar alguns outros tipos de informações de sua conta de domínio. Essas informações incluem, por exemplo, seu nome UPN (como jack@contoso.com) e o nome de domínio DNS (como corp.contoso.com\jack).

Se você entrar no Windows com uma conta da Microsoft ou se entrar no Windows com uma conta de domínio conectada a uma conta da Microsoft, o Windows poderá sincronizar automaticamente a imagem da conta em seu computador com a imagem de sua conta da Microsoft.

Uso das informações

Se você usar um aplicativo de terceiros, o uso que ele faz de seu nome e de sua imagem da conta estará sujeito às práticas de privacidade do terceiro. Se você usa um aplicativo da Microsoft, as práticas de privacidade do aplicativo serão explicadas na sua política de privacidade.

Faça suas escolhas e controle

Se você escolher as configurações expressas durante a configuração do Windows, o Windows permitirá que os aplicativos acessem seu nome e imagem da conta. Se você optar por personalizar as configurações, poderá controlar o acesso ao seu nome e à imagem da conta selecionando **Permitir que aplicativos usem meu nome e**

minha imagem da conta , em **Compartilhar informações com a Microsoft e outros serviços**. Após instalar o Windows, você poderá alterar essa configuração em **Privacidade** nas configurações do computador. É possível alterar a imagem da conta em **Contas** , nas configurações do computador. Também é possível permitir que determinados aplicativos alterem sua imagem da conta.

Início da página

Reconhecimento de rede

O que este recurso faz

Se você possuir um plano de assinatura para acessar à rede (por exemplo, por uma conexão de banda larga móvel), esse recurso fornece informações sobre seu plano de assinatura para aplicativos e Windows recursos no computador. Windows Os recursos e aplicativos podem usar essas informações para otimizar seu funcionamento. Por exemplo, se você está em um plano de dados limitado, o Windows Update aguarda para enviar atualizações de prioridade baixa para o seu computador antes que você esteja conectado a outro tipo de rede. Esse recurso também fornece informações sobre sua conexão de rede, como a intensidade do sinal e se seu computador está conectado à internet.

Informações coletadas, processadas ou transmitidas

Esse recurso coleta informações de conectividade de rede de intranet e internet, como o sufixo do Serviço de Nomes de Domínio (DNS) do seu computador, nome de rede e endereço de gateway das redes às quais seu computador se conecta. Esse recurso também recebe informações do plano de assinatura, como a quantidade de dados restantes no plano.

Os perfis de conectividade de rede podem incluir um histórico de todas as redes visitadas e a data e hora da última conexão. Esse recurso pode tentar conectar-se a um servidor da Microsoft para determinar se você está conectado à internet. Os únicos dados enviados para a Microsoft durante as verificações da conectividade de rede são as informações de computador padrão.

Uso das informações

Se os dados forem enviados para a Microsoft, eles somente são usados para fornecer o status da conectividade de rede. O status de conectividade de rede é disponibilizado para os aplicativos e recursos no seu computador que solicitam informações de conectividade de rede. Se você usar um aplicativo de terceiros, o uso das informações coletadas estará sujeito às práticas de privacidade do terceiro.

Faça suas escolhas e controle

O Reconhecimento de Rede é habilitado por padrão. Um administrador pode desabilitá-lo usando as opções de Serviços em Ferramentas Administrativas no Painel de Controle. Não recomendamos desabilitar esse recurso, pois isso impedirá que alguns recursos do Windows funcionem corretamente.

Início da página

Notificações, aplicativos da tela de bloqueio e atualizações de bloco

Os aplicativos da Windows Store podem receber conteúdo e exibir notificações automaticamente de diversas maneiras. Por exemplo, eles recebem notificações que são exibidas rapidamente no canto da tela ou em blocos de aplicativo, quando os blocos estão fixados em Iniciar. Você também poderá receber as notificações na tela de bloqueio, se quiser. A tela de bloqueio também exibe um status resumido ou detalhado de alguns aplicativos. Os fornecedores de aplicativos podem enviar conteúdo para os seus aplicativos da Windows Store por meio dos Serviços de Notificação por Push do Windows que estiverem em execução nos servidores da Microsoft; ou então os aplicativos podem baixar as informações diretamente dos servidores de terceiros.

Notificações

O que este recurso faz

Os aplicativos da Windows Store podem fornecer informações periódicas ou em tempo real para você que serão exibidas de forma rápida como notificações no canto da tela.

Informações coletadas, processadas ou transmitidas

Os aplicativos exibem textos, imagens ou os dois nas notificações. O conteúdo das notificações é fornecido localmente pelo aplicativo (por

exemplo, o alarme de um aplicativo de relógio). É possível enviar notificações do serviço online de um aplicativo através dos Serviços de Notificação por Push do Windows (por exemplo, a atualização de uma rede social). As imagens exibidas nas notificações podem ser baixadas diretamente de um servidor especificado pelo fornecedor do aplicativo; quando isso acontece, as informações padrão do computador são enviadas a esse servidor.

Uso das informações

A Microsoft somente usa as informações de notificação para enviar notificações dos seus aplicativos para você. As notificações podem ser armazenadas temporariamente pelos Serviços de Notificação por Push do Windows antes de serem enviadas a seu computador. Se uma notificação não puder ser enviada imediatamente, ela somente será armazenada por alguns minutos antes de ser excluída.

Faça suas escolhas e controle

Você pode desabilitar as notificações em todos os aplicativos, ou em aplicativos individuais, em **Notificações** , em **Pesquisar aplicativos** nas configurações do computador. Se você desabilitar as notificações em um aplicativo ou desinstalá-lo, o fornecedor do aplicativo ainda poderá enviar atualizações aos Serviços de Notificação por Push do Windows, mas as notificações não serão exibidas no seu computador.

Aplicativos na tela de bloqueio

O que este recurso faz

Alguns aplicativos da Windows Store podem exibir status e notificações na tela quando o computador está bloqueado. Os aplicativos da tela de bloqueio também podem realizar tarefas enquanto o computador está bloqueado; por exemplo, sincronizar emails em segundo plano ou permitir que você atenda chamadas telefônicas. Você também pode usar a câmera do computador diretamente na tela de bloqueio.

Informações coletadas, processadas ou transmitidas

Os aplicativos na tela de bloqueio recebem atualizações de status do fornecedor do aplicativo através dos Serviços de Notificação por Push do Windows ou diretamente dos servidores do fornecedor do aplicativo (ou de outros). Os aplicativos na tela de bloqueio também transmitem

ou processam outras informações não relacionadas a notificações e atualizações.

Uso das informações

O Windows usa as informações de status e notificações fornecidas pelos aplicativos na tela de bloqueio para atualizar a tela de bloqueio.

Faça suas escolhas e controle

Após instalar o Windows, os aplicativos Email, Calendário e Skype são automaticamente definidos como aplicativos na tela de bloqueio. É possível adicionar ou remover esses e outros aplicativos da tela de bloqueio e desativar o uso da Câmera em **Tela de bloqueio** , em **PC e dispositivos** , nas configurações do computador. Você também pode escolher um aplicativo para que ele sempre exiba informações detalhadas (por exemplo, detalhes do próximo compromisso no seu calendário) na tela de bloqueio.

É possível também controlar se os aplicativos da tela de bloqueio podem exibir notificações na tela de bloqueio em **Notificações** , em **Pesquisar aplicativos** nas configurações do computador.

Atualizações de bloco

O que este recurso faz

Os aplicativos da Windows Store podem fornecer informações periódicas ou em tempo real para você que serão exibidas como atualizações para os blocos dos seus aplicativos na tela inicial.

Informações coletadas, processadas ou transmitidas

Os aplicativos da Loja que estão fixados à tela inicial podem atualizar seus blocos com textos, imagens ou ambos. O conteúdo exibido no bloco de um aplicativo é fornecido localmente pelo aplicativo, baixado periodicamente de um servidor especificado pelo fornecedor do aplicativo ou enviado do serviço online de um aplicativo através dos Serviços de Notificação por Push do Windows. Se o conteúdo do bloco for baixado diretamente de um servidor especificado pelo fornecedor do aplicativo, as informações padrão do computador serão enviadas a esse servidor.

Uso das informações

A Microsoft somente usa as informações do bloco para lhe enviar atualizações de bloco dos seus aplicativos. É possível armazenar essas informações temporariamente nos Serviços de Notificação por Push do Windows antes de enviar ao computador. Se uma atualização de bloco não puder ser enviada imediatamente, ela será armazenada somente por alguns dias antes de ser excluída.

Faça suas escolhas e controle

Depois que o aplicativo inicia o recebimento das atualizações de bloco, você pode desabilitá-las selecionando o bloco do aplicativo na tela inicial e selecionando **Desligar bloco dinâmico** nos comandos disponíveis ao aplicativo. Se você desafixar o bloco de um aplicativo da tela inicial, suas atualizações não serão exibidas. Se você desinstalar um aplicativo, o fornecedor do aplicativo ainda poderá enviar atualizações aos Serviços de Notificação por Push do Windows, mas elas não serão exibidas no computador.

Para limpar as atualizações atuais exibidas nos blocos da tela inicial, passe o dedo a partir do lado direito ou aponte para o canto superior direito da tela inicial, toque ou clique em **Configuraçõe**s em **Blocos**. Toque ou clique no botão **Limpar** em **Limpar informações pessoais de meus blocos**. As atualizações de bloco enviadas após a limpeza das atualizações atuais ainda serão exibidas.

Início da página

Encomendar cópias

O que este recurso faz

O Encomendar cópias permite que você envie imagens digitais armazenadas no seu computador ou em uma unidade de rede para um serviço de impressão de foto online da sua escolha. Dependendo do serviço, você pode ter suas imagens impressas e, em seguida, enviadas usando o endereço postal ou você pode pegar as impressões na loja local.

Informações coletadas, processadas ou transmitidas

Se você decidir fazer um pedido ao serviço de impressão de fotos online, suas fotos digitais serão enviadas pela Internet ao serviço selecionado. O caminho do arquivo para as imagens digitais que você

selecionar (que pode incluir seu nome de usuário) deve ser enviado ao serviço para que ele exiba e carregue as imagens. Os arquivos de imagem digital podem conter os dados sobre a imagem que foi armazenada com o arquivo pela câmera, como a data e a hora que a foto foi tirada ou o local onde a foto foi tirada se sua câmera possuir funcionalidades de GPS. Os arquivos também podem conter informações pessoais (como legendas) que podem ter sido associadas ao arquivo através de aplicativos de gerenciamento de imagem digital e do Explorador de Arquivos. Para obter mais informações, consulte a seção Propriedades a seguir.

Após selecionar um serviço de impressão de fotos online em Pedir Cópias, você será direcionado para o site do serviço na janela Pedir Cópias. As informações inseridas no site dos serviços de impressão de foto online são transmitidas para o serviço.

Uso das informações

As informações armazenadas pela câmera nos arquivos de fotos digitais podem ser usadas pelo serviço de impressão de fotos online durante o processo de impressão, por exemplo, para ajustar a cor ou a nitidez da imagem antes da impressão. As informações armazenadas pelos aplicativos de gerenciamento de imagem digital podem ser usadas pelo serviço de impressão de fotos online para imprimir como legendas na frente ou no verso da cópia impressa. O uso das informações dos serviços de impressão de foto online e outras informações que você fornecer para os serviços, como informações inseridas nos sites deles, estará sujeito às práticas de privacidade deles.

Faça suas escolhas e controle

Você pode usar Encomendar cópias para escolher quais imagens enviar e qual serviço usar para imprimir suas imagens. Alguns aplicativos de gerenciamento de imagem podem ser capazes de ajudar você a remover informações pessoais armazenadas antes de enviar as imagens para serem impressas. Também é possível editar as propriedades do arquivo para remover informações pessoais armazenadas.

Início da página

Pré-busca e pré-início

O que este recurso faz

O Windows ajuda os aplicativos e os recursos do Windows a abrirem mais rápido ao controlar quando e com que frequência esses aplicativos e recursos são usados e quais arquivos do sistema carregar.

Informações coletadas, processadas ou transmitidas

Quando você usa um aplicativo ou recurso do Windows, o Windows salva algumas informações no computador sobre os arquivos de sistema usados, bem como quando e com que frequência o aplicativo ou recurso foi utilizado.

Uso das informações

O Windows usa as informações sobre o uso do aplicativo e do recurso para ajudar a inicialização mais rápida de aplicativos e recursos. Em alguns casos, os aplicativos podem ser iniciados automaticamente em um estado de suspensão.

Faça suas escolhas e controle

Os aplicativos que são iniciados automaticamente e suspensos aparecem no Gerenciador de Tarefas e podem ser encerrados. Durante a suspensão, esses aplicativos não poderão acessar a webcam ou o microfone enquanto você não iniciá-los, mesmo que a funcionalidade tenha sido habilitada anteriormente.

Início da página

Auxiliar de Compatibilidade de Programas

O que este recurso faz

Se algum problema de incompatibilidade for encontrado no aplicativo de área de trabalho que você está tentando executar, o Auxiliar de Compatibilidade de Programas tentará ajudar você a resolvê-lo.

Informações coletadas, processadas ou transmitidas

Se um problema de incompatibilidade for encontrado em um aplicativo que você tentar executar, um relatório será gerado e incluirá

informações, como o nome do aplicativo, a versão do aplicativo, as configurações de compatibilidade necessárias e suas ações com o aplicativo. Os problemas com aplicativos incompatíveis são relatados à Microsoft através do Relatório de Erros do Windows ou do Programa de Aperfeiçoamento da Experiência do Usuário do Windows.

Uso das informações

Os relatórios de erros são usados para fornecer respostas para problemas que você relata para os seus aplicativos. As repostas contêm links (quando disponíveis) para o site do fornecedor do aplicativo para você saber mais sobre as possíveis soluções. Os relatórios de erros criados devido às falhas do aplicativo são usados para tentar determinar a configuração a ser ajustada quando você encontrar problemas de compatibilidade com os aplicativos em execução nessa versão do Windows. As informações relatadas pelo CEIP são usadas para identificar problemas de compatibilidade de aplicativos.

A Microsoft não usa nenhuma informação coletada através desse recurso para identificá-lo, contatá-lo nem para enviar propaganda para você.

Faça suas escolhas e controle

Para problemas relatados pelo Relatório de Erros do Windows, um relatório de erros é criado somente quando você seleciona a opção para buscar soluções na Internet. A menos que você tenha autorizado o relato de problemas de forma automática para buscar soluções, será perguntado se você deseja enviar o relatório de erros. Para obter mais informações, consulte a seção Relatório de Erros do Windows.

Alguns problemas são automaticamente relatados pelo Programa de Aperfeiçoamento da Experiência do Usuário do Windows, quando você habilita esse recurso. Para obter mais informações, consulte a seção Programa de Aperfeiçoamento da Experiência do Usuário do Windows.

Início da página

Propriedades

O que este recurso faz

As propriedades são informações do arquivo que permitem que você pesquise e organize seus arquivos rapidamente. Algumas propriedades estão intrínsecas ao arquivo (por exemplo, o tamanho do arquivo) enquanto outras podem ser específicas para um aplicativo ou dispositivo (por exemplo, as configurações da sua câmera quando você tira uma foto ou os dados da localização gravados pela câmera para a foto).

Informações coletadas, processadas ou transmitidas

O tipo de informação armazenado dependerá do tipo de arquivo e os aplicativos que o utilizam. Exemplos de propriedades incluem o nome do arquivo, a data de modificação, o tamanho do arquivo, autor, palavras-chave e comentários. As propriedades são armazenadas no arquivo e elas se movem com o arquivo se ele é movido ou copiado para outro local, como um arquivo compartilhado, ou enviado como um anexo de email.

Uso das informações

As propriedades podem ajudar você a pesquisar e organizar mais rápido seus arquivos. Elas também podem ser usadas pelos aplicativos para executar tarefas específicas do aplicativo. Nenhuma informação é enviada para a Microsoft.

Faça suas escolhas e controle

Você pode editar ou remover algumas propriedades de um arquivo selecionando o arquivo no Explorador de Arquivos e clicando em **Propriedades**. Algumas propriedades intrínsecas, como a data de modificação, o tamanho do arquivo, o nome do arquivo e algumas propriedades específicas do aplicativo, não podem ser removidas dessa forma. Para as propriedades específicas do aplicativo, você pode editá-las ou removê-las somente se o aplicativo usado gerar o arquivo compatível com esses recursos.

Início da página

Proximidade

Serviço de proximidade a curta distância

O que este recurso faz

Se o computador tiver um hardware NFC (comunicação a curta distância), será possível tocá-lo fisicamente em outro dispositivo ou acessório com o hardware NFC para compartilhar links, arquivos e outras informações. Existem dois tipos de conexões de proximidade: Tocar e Fazer e Tocar e Segurar. Com o recurso Tocar e Fazer, é possível criar uma conexão rápida ou de longo prazo entre dispositivos via Wi-Fi, Wi-Fi Direct ou Bluetooth. Com Tocar e Segurar, a conexão é ativada somente enquanto os dispositivos estiverem perto um do outro.

Informações coletadas, processadas ou transmitidas

Quando você toca em dispositivos compatíveis com proximidade juntos, eles trocam informações para estabelecer uma conexão entre si. Dependendo da configuração dos dispositivos, esses dados podem incluir informações de emparelhamento Bluetooth, endereços de rede Wi-Fi e o nome do computador.

Após uma conexão ser estabelecida, outras informações podem ser trocadas entre os dispositivos, dependendo do recurso ou aplicativo de proximidade específico que estiver sendo usado. Windows pode enviar arquivos, vínculos e outras informações entre dispositivos usando uma conexão de proximidade. Os aplicativos que usam proximidade podem enviar e receber quaisquer informações as quais eles tenham acesso. Essas informações podem ser enviadas pela sua rede ou conexão com a internet, ou diretamente pela conexão sem fio de dispositivo para dispositivo.

Uso das informações

As informações de rede e do computador trocadas através de uma conexão de proximidade são usadas para estabelecer uma conexão de rede e para identificar os dispositivos que estejam se conectando entre si. Os dados transferidos por uma conexão de proximidade iniciada em um aplicativo podem ser usados por esse aplicativo de qualquer maneira. Nenhuma informação é enviada para a Microsoft.

Faça suas escolhas e controle

O serviço de proximidade a curta distância é habilitado por padrão. Um administrador pode desabilitá-lo usando as opções fornecidas em Dispositivos e Impressoras no Painel de Controle.

Tocar e Enviar

O que este recurso faz

Windows O recurso Tocar e Enviar torna mais fácil compartilhar informações selecionadas com um amigo que está ao seu lado ou com outro dos seus dispositivos, como um celular. Por exemplo, quando você estiver em um navegador, é possível iniciar o recurso Tocar e Enviar a partir do painel Dispositivos. O próximo dispositivo no qual você tocar receberá um vínculo para a página da Web que estiver sendo exibida no momento. Isso também funciona com qualquer aplicativo que seja compatível com o compartilhamento de informações, como imagens, texto ou arquivos.

Informações coletadas, processadas ou transmitidas

O recurso Tocar e Enviar usa as informações que você está compartilhando e as informações descritas na seção Serviço de proximidade em campo próximo abordada anteriormente.

Uso das informações

Essas informações somente são usadas para criar uma conexão entre os dois dispositivos. As informações compartilhadas não são armazenadas pelo recurso Tocar e Enviar. Nenhuma informação é enviada para a Microsoft.

Faça suas escolhas e controle

Se o serviço de proximidade a curta distância estiver habilitado, o recurso Tocar e Enviar também será habilitado. Para obter mais informações, consulte a seção sobre o serviço de proximidade a curta distância.

Início da página

Conexões de Acesso Remoto

O que este recurso faz

O recurso Conexões de Acesso Remoto permitem que você se conecte a redes privadas usando uma conexão de rede virtual privada (VPN) e de Serviço de Acesso Remoto (RAS). O RAS é um componente que conecta o computador do cliente (geralmente seu computador) a um

computador principal (também conhecido como um servidor de acesso remoto) usando os protocolos padrão da indústria. As tecnologias de VPN permitem que os usuários se conectem a uma rede privada, como uma rede corporativa, através da Internet.

Um componente das conexões de Acesso Remoto, o Sistema de Rede de Conexão Discada permite que você acesse a Internet usando um modem de conexão discada ou uma tecnologia de banda larga, como um modem a cabo ou uma DSL (linha de assinante digital). A Rede de Conexão Discada inclui componentes de discador, como o Cliente do RAS, o Gerenciador de Conexões e o Telefone do RAS, assim como discadores de linha de comandos, como o rasdial.

Informações coletadas, processadas ou transmitidas

Os componentes de discador coletam informações do seu computador, como seu nome de usuário, senha e nome do domínio. As informações são enviadas para o sistema com o qual você está tentando se conectar. Para ajudar a proteger sua privacidade e a segurança do seu computador, informações relacionadas a segurança, como nome do usuário e senha, são criptografadas e armazenadas no seu computador.

Uso das informações

As informações do discador são usadas para ajudar seu computador a se conectar à internet. Um servidor de acesso remoto pode manter as informações de nome de usuário e do endereço IP para fins de contabilização e conformidade, mas nenhuma informação é enviada para a Microsoft.

Faça suas escolhas e controle

Para os discadores que não são de linha de comando, você pode escolher salvar sua senha selecionando **Salvar este nome de usuário e senha**. Você pode limpar essa opção a qualquer momento para excluir a senha salvada anteriormente a partir do discador. Como essa opção está desativada por padrão, pode ser solicitado que você forneça sua senha para conectar-se à internet ou à rede. Em discadores de linha de comando, como o rasdial, não existe a opção de salvar a senha.

Início da página

Conexões de RemoteApp e Área de Trabalho

O que este recurso faz

O recurso Conexões de RemoteApp e Área de Trabalho permite acessar aplicativos e áreas de trabalho em computadores remotos que tenham sido publicados na Internet para acesso remoto.

Informações coletadas, processadas ou transmitidas

Quando você ativar uma conexão, os arquivos de configuração serão transferidos para seu computador a partir do URL remota especificada. Esses arquivos de configuração vinculam aplicativos e áreas de trabalho em computadores remotos, assim você pode executá-los do seu computador. Seu computador verificará e baixará atualizações para esses arquivos de configuração de forma automática periodicamente. Esses aplicativos são executados em computadores remotos e as informações inseridas nos aplicativos serão transmitidas pela rede para os computadores remotos com os quais você escolheu se conectar.

Se a Microsoft estiver hospedando o computador ou o aplicativo ao qual você está se conectando, informações adicionais sobre sua conexão poderão ser enviadas à Microsoft para fins de suporte.

Uso das informações

As atualizações dos arquivos de configuração podem incluir alterações de configurações como a permissão para você acessar novos aplicativos; porém, os novos aplicativos serão executados somente se você decidir executá-los. Esse recurso também envia informações para os computadores remotos nos quais os aplicativos remotos são executados. O uso desses dados pelos aplicativos remotos está sujeito às políticas de privacidade dos provedores dos aplicativos e dos administradores dos computadores remotos. Nenhuma informação é enviada à Microsoft, a menos que a conexão remota seja hospedada pela Microsoft.

Faça suas escolhas e controle

Você pode escolher se deseja usar as Conexões do RemoteApp e da Área de Trabalho. Você pode adicionar ou remover as Conexões do

RemoteApp e da Área de Trabalho acessando Conexões do RemoteApp e da Área de Trabalho no Painel de Controle. Você pode adicionar uma nova conexão clicando em **Acessar RemoteApp e áreas de trabalho**e inserindo uma URL de Conexão na caixa de diálogo. Você também pode usar seu endereço de email para recuperar a URL de Conexão. Você pode remover uma conexão e seus arquivos de conexão clicando em **Remover** na caixa de diálogo de descrição das conexões. Se você desconectar uma conexão sem fechar todos os aplicativos abertos, esses aplicativos permanecerão abertos no computador remoto. As Conexões do RemoteApp e da Área de Trabalho não são exibidas em Adicionar ou remover lista de programas no Painel de Controle.

Início da página

Conexão de Área de Trabalho Remota

O que este recurso faz

O recurso Conexão de Área de Trabalho Remota permite que você estabeleça uma conexão remota com um computador host que executa Serviços de Área de Trabalho Remota.

Informações coletadas, processadas ou transmitidas

As configurações da Conexão de Área de Trabalho Remota são armazenadas localmente no aplicativo ou em um arquivo do protocolo RDP no computador. Essas configurações incluem o nome do seu domínio e os ajustes de configuração de conexão, como o nome do computador remoto, o nome de usuário, as informações da área de trabalho, as informações do dispositivo local, as informações de áudio, a área de transferência, as configurações da conexão, os nomes do aplicativo remoto e o ícone da sessão ou miniatura.

As credenciais dessas conexões e do Gateway de Área de Trabalho Remota, além de uma lista de nomes de servidor de Gateway de Área de Trabalho Remota são armazenadas localmente em seu computador. Uma lista é armazenada no Registro. Essa lista é armazenada permanentemente a menos que ela seja excluída por um administrador. Nenhuma informação é enviada à Microsoft, a menos que a conexão remota seja hospedada pela Microsoft.

Uso das informações

As informações coletadas pela Conexão de Área de Trabalho Remota permitem que você se conecte aos computadores host que executam Serviços de Área de Trabalho Remota usando as configurações de sua preferência. O nome de usuário, a senha e as informações do domínio são coletados para permitir que você salve suas configurações da conexão e permitir que você clique duas vezes no arquivo RDP ou clique em um favorito para iniciar a conexão sem ter de inserir novamente essas informações.

Faça suas escolhas e controle

Você pode optar se deseja usar a Conexão de Área de Trabalho Remota. Se decidir usá-la, seus arquivos RDP e os sites favoritos da Conexão de Área de Trabalho Remota incluirão as informações necessárias para um computador remoto, incluindo as opções e configurações que foram definidas quando a conexão foi salva automaticamente. Você pode personalizar os arquivos RDP e favoritos, incluindo os arquivos para conexão com o mesmo computador com configurações diferentes. Para modificar as credenciais salvas, abra o Gerenciador de Credenciais em Contas de usuário no Painel de Controle.

Início da página

Entrar com uma conta da Microsoft

O que este recurso faz

Uma conta da Microsoft (antes conhecida como Windows Live ID) é um endereço de email único, com senha, que você pode usar para entrar em aplicativos, sites e serviços da Microsoft e de parceiros da Microsoft. É possível inscrever-se para uma conta da Microsoft nos sites do Windows ou da Microsoft que exigem entrada com uma conta da Microsoft.

Você pode entrar no Windows com uma conta da Microsoft ou, em produtos que suportem isso, escolha conectar a sua conta local ou de domínio a uma conta da Microsoft. Se você fizer isso, o Windows pode sincronizar automaticamente as configurações e informações do Windows e dos aplicativos da Microsoft para manter seus

computadores com a mesma aparência. Se você visitar um site onde você usa uma conta da Microsoft para entrar, o Windows também conectará você automaticamente a esse site.

Informações coletadas, processadas ou transmitidas

Quando você insere um endereço de email a ser usado como uma conta da Microsoft ao configurar seu computador ou em **Contas** nas configurações do computador, o Windows envia o endereço de email à Microsoft para determinar se já existe uma conta da Microsoft associada a esse endereço de email. Se você já usa esse endereço de email como conta da Microsoft, poderá usá-lo com a senha da conta da Microsoft para entrar no Windows. Se você ainda não tiver informações de segurança suficientes para sua conta da Microsoft, pediremos primeiro a você algumas informações de segurança adicionais, por exemplo, o número do celular, para verificarmos se a conta é realmente sua. Se você não tiver uma conta da Microsoft, poderá criar uma usando qualquer endereço de email.

Quando você entra com uma conta da Microsoft, o Windows também envia informações padrão do computador para a Microsoft, incluindo o fabricante do dispositivo, o modelo e a versão.

Sempre que você entra no Windows com uma conta da Microsoft enquanto seu computador está conectado à Internet, o Windows verifica seu endereço de email e sua senha com os servidores da Microsoft. Quando você está conectado ao Windows através de sua conta da Microsoft ou de uma conta de domínio conectada à sua conta da Microsoft:

- Algumas configurações do Windows serão sincronizadas entre os computadores que você usa para entrar com sua conta da Microsoft. Para obter mais informações sobre quais configurações são sincronizadas e como controlá-las, consulte a seção Sincronizar suas configurações nesta página.

- Os aplicativos da Microsoft que usam uma conta da Microsoft para autenticação (como Email, Calendário, Pessoas, Microsoft Office, entre outros) podem começar a baixar automaticamente suas informações (por exemplo, o aplicativo Email baixará automaticamente as mensagens enviadas ao seu endereço do Outlook.com ou do Hotmail.com, se você tiver um). Os

navegadores da Web podem conectar você automaticamente a sites nos quais você entra com sua conta da Microsoft (por exemplo, se você visitar o Bing.com, poderá ser automaticamente conectado e não precisará reinserir a senha da sua conta da Microsoft).

O Windows solicitará sua permissão antes de deixar que aplicativos de terceiros usem informações de perfil ou outras informações pessoais associadas à sua conta da Microsoft. Se você entra no Windows com uma conta de domínio conectada à conta da Microsoft, as configurações e informações escolhidas são sincronizadas com a sua conta de domínio, e você é conectado automaticamente aos aplicativos e sites conforme descrito anteriormente. Como os administradores de domínio têm acesso a todas as informações no seu computador, eles também podem acessar todas as configurações e informações que você sincronizou com outros computadores através da sua conta da Microsoft. Isso pode incluir configurações como o nome, a imagem da conta e o histórico do navegador. Para obter mais informações sobre quais configurações são sincronizadas e como controlá-las, consulte a seção Sincronizar suas configurações nesta página.

Uso das informações

Quando você cria uma nova conta da Microsoft no Windows, nós usamos as informações inseridas para criar e proteger a conta. Por exemplo, as informações de segurança que você fornecer (como seu número de telefone ou endereço de email alternativo) serão usadas somente se você não puder entrar em sua conta. Quando você está conectado ao Windows com uma conta da Microsoft, o Windows usa as informações de sua conta da Microsoft para conectá-lo automaticamente a aplicativos e sites. Para obter mais informações sobre o impacto de ter uma conta da Microsoft sobre a privacidade, leia a Política de privacidade de conta da Microsoft. Para obter informações sobre como cada aplicativo da Microsoft usa as informações associadas à sua conta da Microsoft, consulte as políticas de privacidade de cada aplicativo. Você pode encontrar a política de privacidade de um aplicativo da Microsoft abrindo Configurações dentro do aplicativo ou na caixa de diálogo Sobre.

As informações padrão do dispositivo podem ser usadas para

personalizar determinadas comunicações para você – por exemplo, emails elaborados para ajudá-lo a usar o dispositivo.

Faça suas escolhas e controle

Quando você entra no Windows com uma conta da Microsoft, algumas configurações são automaticamente sincronizadas. Para aprender como alterar as configurações do Windows que são sincronizadas ou como parar a sincronização, consulte a seção Sincronizar suas configurações nesta página. Para aprender mais sobre os dados coletados pelos aplicativos da Microsoft que usam uma conta da Microsoft para autenticação, leia suas políticas de privacidade.

Em produtos que suportem isso, você pode criar uma conta local ou uma conta da Microsoft a qualquer momento em **Contas** nas configurações do computador. Se você entrar no Windows com uma conta de domínio, poderá conectar ou desconectar sua conta da Microsoft a qualquer momento em **Contas** nas configurações do computador.

Ao usar a Navegação InPrivate no Internet Explorer, você não será conectado automaticamente a sites que usam contas da Microsoft.

Início da página

Armazenamento em nuvem do OneDrive

O que este recurso faz

Ao entrar no seu dispositivo com uma conta da Microsoft, você pode optar por salvar automaticamente algumas configurações e tipos de conteúdo em servidores da Microsoft para que tenha um backup se algo acontecer com seu dispositivo.

Informações coletadas, processadas ou transmitidas

Durante a instalação, se você optar por usar o OneDrive para armazenamento em nuvem, o Windows enviará automaticamente o conteúdo para os servidores da Microsoft, incluindo:

- Fotos e vídeos em seu dispositivo que estão salvos na pasta **Imagens da Câmera** .
- Configurações que são específicas ao dispositivo e que não são

compartilhadas entre seus dispositivos.

- Informações descritivas sobre o dispositivo, como nome e tipo.

Você também pode optar por salvar o conteúdo em servidores da Microsoft, e os aplicativos podem optar por selecionar servidores da Microsoft como o local de salvamento padrão para os seus arquivos.

Uso das informações

O Windows usa esse conteúdo para fornecer o serviço de armazenamento em nuvem. A Microsoft não usa seu conteúdo nem suas informações para identificá-lo, contatá-lo nem direcionar propaganda para você.

Faça suas escolhas e controle

Se você optar por "Usar OneDrive" ao configurar o seu computador, o Windows salvará o conteúdo descrito nesta seção no OneDrive. Você pode alterar essas configurações a qualquer momento na seção OneDrive nas configurações do computador.

Início da página

Sincronizar suas configurações

O que este recurso faz

Quando você entra no Windows com uma conta da Microsoft, o Windows sincroniza algumas de suas configurações e informações com os servidores da Microsoft para facilitar experiências personalizadas entre vários computadores. Depois que você entrar em um ou mais computadores com uma conta da Microsoft, quando você entrar em outro computador com a mesma conta da Microsoft pela primeira vez, o Windows baixará e aplicará as configurações e informações que você escolheu para serem sincronizadas com seus outros computadores. As configurações escolhidas para sincronização serão automaticamente atualizadas nos servidores da Microsoft e nos outros computadores à medida que você os utilizar.

Informações coletadas, processadas ou transmitidas

Se você escolher entrar no Windows com uma conta da Microsoft, o Windows sincronizará determinadas configurações com os servidores

da Microsoft. Essas configurações incluem:

- O layout da tela Inicial
- Os aplicativos que você instalou da Windows Store
- Preferências de idioma
- Preferências de Facilidade de Acesso
- Configurações de personalização, como sua imagem da conta, a imagem da tela de bloqueio, a tela de fundo e as configurações do mouse
- Configurações de aplicativos da Windows Store
- Dicionários de ortografia, dicionários IME e dicionários pessoais
- Histórico do navegador da Web, favoritos e sites que você abriu
- Senhas salvas de aplicativos, sites e redes
- Endereços de impressoras de rede compartilhadas às quais você se conectou

Para ajudar a proteger sua privacidade, todas as configurações sincronizadas são enviadas com criptografia SSL. Algumas dessas configurações serão sincronizadas em seu computador somente depois que você o adicionar à sua conta da Microsoft como um computador confiável.

Se você entrar no Windows com uma conta de domínio conectada a uma conta da Microsoft, as configurações e informações escolhidas serão sincronizadas com sua conta de domínio. As senhas salvas durante a entrada no Windows com uma conta de domínio conectada a uma conta da Microsoft nunca são sincronizadas. Como os administradores de domínio têm acesso a todas as informações no seu computador, eles também podem acessar todas as configurações e informações que você sincronizou com outros computadores usando sua conta da Microsoft.

Uso das informações

O Windows usa essas configurações e informações para oferecer o

serviço de sincronização. A Microsoft não usa suas configurações e informações sincronizadas para identificar, entrar em contato ou fazer propaganda para você.

Faça suas escolhas e controle

Quando você entra no Windows com uma conta da Microsoft, suas configurações são sincronizadas por padrão. Você pode optar por sincronizar suas configurações, bem como controlar o que é sincronizado, em **Sincronizar suas configurações** na seção do OneDrive, nas configurações do computador. Se você entrar no Windows com uma conta de domínio e conectá-la a uma conta da Microsoft, o Windows perguntará que configurações você deseja sincronizar antes de conectar sua conta da Microsoft.

Início da página

Tecnologia Teredo

O que este recurso faz

O recurso Tecnologia Teredo (Teredo) permite que os computadores e as redes se comuniquem através de vários protocolos de rede.

Informações coletadas, processadas ou transmitidas

Cada vez que você iniciar seu computador, o Teredo tentará localizar um serviço de Protocolo de Internet pública versão 6 (IPv6) na internet. Isso ocorre automaticamente quando seu computador é conectado a uma rede pública ou privada, mas não ocorre em redes gerenciadas, como domínios corporativos. Se você usar um aplicativo que requer o Teredo para usar conectividade de IPv6 ou se configurar o firewall pra sempre permitir a conectividade IPv6, o Teredo periodicamente entrará em contato com o serviço Microsoft Teredo através da Internet. A única informação enviada para a Microsoft é a informação padrão do computador e o nome do serviço solicitado (por exemplo, teredo.ipv6.microsoft.com).

Uso das informações

As informações enviadas do seu computador pelo Teredo são usadas para determinar se seu computador está conectado à internet e se ele podem localizar o serviço de IPv6 público. Assim que o serviço for

localizado, as informações serão enviadas para manter uma conexão com o serviço de IPv6.

Faça suas escolhas e controle

Com a ferramenta de linha de comando netsh, você pode alterar a consulta que o serviço envia pela internet para usar os servidores que não sejam da Microsoft ou pode desabilitá-la. Para obter instruções detalhadas, consulte a seção "Protocolo de Internet versão 6, Teredo e tecnologias relacionadas" deste white paper técnico.

Início da página

Serviços TPM (Trusted Platform Module)

O que este recurso faz

O TPM (Trusted Platform Module) é um hardware de segurança integrado a alguns computadores que, se apresentado e provisionado, permite que o computador aproveite todos os benefícios dos recursos de segurança avançados. Os recursos do Windows que usam o TPM incluem Criptografia do Dispositivo, Cartão Inteligente Virtual, Inicialização Segura, Windows Defender e Armazenamento de Certificado com base em TPM.

Informações coletadas, processadas ou transmitidas

Por padrão, Windows se apropria do TPM e armazena as informações completas de autorização do proprietário do TPM, então ele somente estará disponível para os Windows administradores. Os valores de autorização limitados são criados para executar as ações administrativas naturais e as ações de usuário padrão, e são gerenciados pelo Windows.

O Console de Gerenciamento do TPM permite que você provisione interativamente o TPM e salva o valor de autorização do proprietário do TMP para mídia externa, como uma unidade flash USB, após o TPM ter sido provisionado. Um arquivo salvo contém as informações de autorização do proprietário para o TPM. O arquivo também contém o nome do computador, a versão do sistema operacional, o usuário da criação e a data da criação para auxiliar você a reconhecer o arquivo.

Em um ambiente de domínio, a senha de proprietário do TPM

completa pode ser configurada pelo administrador do domínio para ser armazenada no Active Directory sob um objeto do TPM quando o TPM for provisionado.

Cada TPM possui uma Chave de endosso criptográfica única que ele usa para indicar sua autenticidade. A Chave de endosso pode ser criada e armazenada no TPM pelo fabricante do seu computador ou para computadores antigos, Windows pode precisar desencadear a criação da Chave de endosso dentro do TPM. A parte privada da Chave de endosso nunca será revelada fora do TPM, e após ter sido criada, ela geralmente não poderá ser redefinida. Um Certificado da Chave de endosso será armazenado no TPM da maioria dos computadores Windows. O Certificado da Chave de endosso indica que a Certificado da Chave de endosso existe em um TPM de hardware. O certificado é útil para verificadores remotos confirmarem se o TPM está em conformidade com as especificações do TPM. O Certificado da Chave de endosso é geralmente iniciado pelo fabricante do TPM ou o fabricante da plataforma.

Uso das informações

Quando o TPM for inicializado, os aplicativos podem usar o TPM para criar e ajudar a obter chaves criptográficas únicas adicionais. Por exemplo, a Criptografia do Dispositivo usa o TPM para proteger a chave que criptografa a unidade.

Se você salvar a senha de proprietário do TPM em um arquivo, o computador adicional e as informações de usuário salvas nesse arquivo ajudarão você a identificar o computador e o TPM correspondentes. A chave de endosso do TPM é usada para Windows durante a inicialização do TPM para criptografar o valor de autorização do proprietário do TMP antes de enviá-lo ao TPM. O Windows não transmite chaves criptográficas para fora do seu computador. Windows oferece uma interface para aplicativos de terceiros como software antimalware para usar a Chave de endosso para determinadas situações do TPM, como Inicialização Medida com Atestado. Para software antimalware, a chave de endosso e o certificado da chave de endosso também são úteis para confirmar as medidas de inicialização que são fornecidas por um TPM de determinado fabricante. Por padrão, somente administradores ou aplicativos com direitos administrativos podem usar a chave de

endosso do TPM.

Faça suas escolhas e controle

Os usuários ou administradores aceitam usar o TPM ativando um Windows recurso ou executando um aplicativo que usa o TPM.

Você pode escolher limpar o TPM e redefini-lo para os padrões de fábrica. Limpar o TPM remove as informações do proprietário, e com a exceção da chave de endosso, todas as informações criptográficas ou as chaves com base no TPM que os aplicativos possam ter criado quando o TPM estava em uso.

Início da página

Certificados raiz da atualização

O que este recurso faz

Os certificados são usados primeiramente para confirmar a identidade de uma pessoa ou dispositivo, autenticar um serviço ou criptografar arquivos. As autoridades em certificação raiz confiável são as organizações que emitem os certificados. Os Certificados raiz da atualização entram em contato com o serviço Windows Update online para verificar se a Microsoft adicionou uma autoridade de certificação para sua lista de autoridades confiáveis, mas somente quando um aplicativo é apresentado com um certificado emitido por uma autoridade de certificação que não seja diretamente confiável (um certificado que não esteja armazenado em uma lista de certificados confiáveis no seu computador). Se a autoridade de certificação tiver sido adicionada à lista de autoridades confiáveis da Microsoft, seu certificado será adicionado automaticamente à lista de certificados confiáveis no seu computador.

Informações coletadas, processadas ou transmitidas

Os Certificados raiz da atualização enviam uma solicitação para o serviço Windows Update online que solicita a lista atual de ACs raiz no Microsoft Root Certificate Program. Se o certificado não confiável estiver na lista, os Certificados raiz da atualização obterão esse certificado do Windows Update e o colocarão na loja de certificados confiáveis no seu computador. As informações transferidas incluem os nomes e hashes criptográficos dos certificados raiz.

Uso das informações

As informações são usadas pela Microsoft para atualizar a lista de certificados confiáveis no seu computador. A Microsoft não usa essas informações para identificar, entrar em contato ou fazer propaganda para você.

Faça suas escolhas e controle

O recurso Atualizar Certificados Raiz é habilitado por padrão. Os administradores podem configurar a Política de Grupo para desabilitar Atualizar Certificados Raiz em um computador.

Início da página

Update Services

O que este recurso faz

Os Update Services para Windows incluem o Windows Update e o Microsoft Update:

- **O Windows Update** é um serviço que oferece atualizações de software do Windows e outros softwares de suporte, como drivers fornecidos pelos fabricantes dos dispositivos.
- **O Microsoft Update** é um serviço que oferece atualizações de software do Windows e de outros softwares da Microsoft, como o Microsoft Office.

Informações coletadas, processadas ou transmitidas

O Update Services coleta informações do seu computador que permitem à Microsoft operar e melhorar os serviços; por exemplo:

- Softwares da Microsoft e outros softwares de suporte (como drivers e firmwares fornecidos por fabricantes de dispositivos) instalados no computador, para os quais os serviços de atualização têm atualizações disponíveis. Isso nos ajuda a determinar quais atualizações são apropriadas para você.
- Suas configurações do Windows Update e/ou do Microsoft Update; por exemplo, se você deseja que as atualizações sejam

baixadas ou instaladas automaticamente.

- Os êxitos, as falhas e os erros que ocorrem quando você acessa e usa os serviços de atualização.
- Números de Identificações de Plug and Play de dispositivos de hardware: um código atribuído pelo fabricante do dispositivo para identificá-lo (por exemplo, um tipo específico de teclado).
- GUID (identificador global exclusivo) – um número gerado aleatoriamente que não contém informações pessoais. Os GUIDs são usados para identificar computadores individuais sem identificar o usuário.
- Nome, número da revisão, fornecedor e data da revisão do BIOS: informações sobre o conjunto de rotinas de software essenciais que testam o hardware, iniciam o sistema operacional no computador e transferem dados entre dispositivos de hardware conectados ao computador.
- Fabricante, Modelo, Função da Plataforma e Número SKU: informações sobre o computador usadas para permitir investigações de diagnóstico em instalações de drivers.

Para usar o Update Services, acesse o Windows Update no Painel de Controle e verifique se há atualizações, ou altere suas configurações para permitir que o Windows instale atualizações automaticamente, à medida que são disponibilizadas (recomendado). No recurso WindowsUpdate, você pode escolher se deseja aceitar o Microsoft Update.

Se você escolher obter atualizações importantes de software para o seu computador, a Windows Ferramenta de Remoção de Software Mal-intencionado (MSRT) pode ser incluída nessas atualizações. A MSRT verifica infecções específicas, software malicioso ("malware") e ajuda a remover quaisquer infecções localizadas. Se o software for executado, ele removerá o malware listado no site de Suporte da Microsoft. Durante uma verificação de malware, um relatório será enviado para a Microsoft contendo informações específicas sobre o malware detectado, erros e outras informações sobre o computador. Para obter mais informações, leia a Windows política de privacidade da

Ferramenta de Remoção de Software Mal-intencionado .

Uso das informações

Os dados enviados à Microsoft são usados para operar e manter o Update Services. Eles também são usados para gerar estatísticas agregadas que nos ajudam a analisar tendências e aprimorar nossos produtos e serviços, inclusive o Update Services.

Para gerar estatísticas agregadas, os serviços de atualização usam o GUID coletado pelo Update Services para rastrear e registrar, além do número de computadores individuais que usam o Update Services, se houve êxito ou falha no download e na instalação de atualizações específicas. O Update Services registra o GUID do computador que tentou o download e a instalação, a ID do item que foi solicitado, se havia atualizações disponíveis e as informações padrão do computador.

As informações da MSRT descritas acima são usadas para ajudar a aprimorar nosso antimalware e outros produtos e serviços de segurança. As informações dos relatórios MSRT não são usadas para identificar ou contatar você.

Atualizações necessárias

Se você ativar o Update Services, para que esse serviço funcione corretamente, alguns componentes de software no seu sistema, os quais fazem parte ou estão diretamente relacionados com o Update Services, deverão ser atualizados periodicamente. Essas atualizações devem ser executadas para que o serviço possa verificar, baixar ou instalar outras atualizações. Essas atualizações necessárias corrigem erros, fornecem aperfeiçoamentos contínuos e mantêm a compatibilidade com os servidores da Microsoft que dão suporte ao serviço.

Se o Update Services for desativado, você não receberá essas atualizações.

As atualizações de software necessárias para instalar ou atualizar aplicativos da Windows Store serão baixadas e instaladas automaticamente. Essas atualizações devem ser realizadas para que os aplicativos funcionem corretamente.

Cookies e tokens

Um token é semelhante a um cookie. Ele armazena informações em um pequeno arquivo que é colocado no disco rígido pelo servidor do Update Services e é usado quando o computador se conecta ao servidor do Update Services, para manter uma conexão válida. É armazenado apenas no seu computador e não no servidor. Esse cookie ou token contém informações (como a hora da última verificação) para localizar as atualizações mais recentes disponíveis. Ele contém informações para gerenciar o conteúdo que deve ser baixado no seu computador, quando isso deve ocorrer, além do GUID para identificar seu computador para o servidor.

As informações contidas no cookie ou token são criptografadas pelo servidor (com exceção da hora de expiração do cookie ou token). Esse cookie ou token não é um cookie de navegador e, portanto, não pode ser controlado pelas configurações do navegador. Não é possível remover o cookie ou token; no entanto, se você não usar o Update Services, o cookie ou token não será usado.

Faça suas escolhas e controle

Se você optar pelas configurações expressas ao instalar o Windows, o serviço Windows Update será ativado e definido para instalar atualizações automaticamente.

Se você ativar o Update Services, independentemente da configuração escolhida, as atualizações necessárias de alguns componentes do serviço serão baixadas e instaladas automaticamente sem avisá-lo. Se você preferir não receber as atualizações necessárias, desative o Update Services.

Você também pode escolher se deseja verificar ou instalar automaticamente as atualizações importantes e recomendadas no seu computador ou apenas as atualizações importantes. As atualizações opcionais nunca são instaladas automaticamente. Depois de configurar o Windows, você poderá alterar suas configurações do Windows Update no Painel de Controle ou nas configurações do computador.

Se você tiver optado por verificar e instalar as atualizações importantes e receber a MSRT como parte dessas atualizações para seu computador, você poderá desabilitar a funcionalidade de relatório

do software.

Início da página

Rede Virtual Privada

O que este recurso faz

A VPN (Rede Virtual Privada) permite conectar a uma rede privada, como uma rede corporativa, através da Internet. A conexão VPN pode ser fornecida pelo cliente VPN do Windows ou por um aplicativo VPN de terceiros.

Informações coletadas, processadas ou transmitidas

Quando você se conecta a uma VPN, as credenciais inseridas no cliente VPN são enviadas para a rede remota. É possível armazenar essas credenciais no computador. Depois de você se conectar, dependendo da configuração da VPN, algumas atividades da sua rede poderão ser roteadas através da rede remota. Os administradores podem configurar aplicativos específicos para sempre rotear o tráfego através da VPN e para conectar automaticamente à VPN quando esses aplicativos são iniciados. Nenhuma informação é enviada para a Microsoft.

O software VPN de terceiros pode coletar informações adicionais; a coleta e o uso dessas informações estão sujeitos às práticas de privacidade do fornecedor.

Uso das informações

Os clientes VPN usam as credenciais que você fornece para efetuar a autenticação na rede remota e para rotear o tráfego da rede para/da rede remota. Se um cliente VPN de terceiros coletar informações adicionais, o uso dessas informações pelo fornecedor está sujeito às práticas de privacidade desse fornecedor.

Faça suas escolhas e controle

Você pode adicionar ou remover uma conexão VPN e ver o status das conexões existentes em **Rede** nas configurações do computador. Depois que uma conexão VPN é configurada, você pode conectá-la ou desconectá-la manualmente selecionando a rede na lista em Configurações.

Início da página

Programa de Aperfeiçoamento da Experiência do Usuário do Windows

O que este recurso faz

Os Programas de Aperfeiçoamento da Experiência do Usuário do Windows coletam informações sobre como você usa os aplicativos, computadores, dispositivos conectados e o Windows. Eles também podem coletar informações sobre problemas de desempenho e confiabilidade que podem ocorrer. Se você participar do Programa de Aperfeiçoamento da Experiência do Usuário do Windows, o Windows enviará esses dados à Microsoft e também baixará periodicamente um arquivo para coletar informações mais relevantes sobre como você usa o Windows e os aplicativos. Os relatórios do Programa de Aperfeiçoamento da Experiência do Usuário são enviados à Microsoft para melhorar os recursos que nossos clientes usam com mais frequência e criar soluções para problemas comuns.

Informações coletadas, processadas ou transmitidas

Os relatórios do Programa de Aperfeiçoamento da Experiência do Usuário podem incluir informações como:

- Informações de configuração, incluindo quantos processadores há no seu computador, o número de conexões de rede em uso, resoluções de tela para dispositivos de vídeo e qual versão do Windows está instalada no computador.

- Informações de desempenho e confiabilidade, incluindo a rapidez com que um aplicativo responde quando você clica em um botão, quantos problemas são encontrados em um aplicativo ou dispositivo e a velocidade com que as informações são enviadas ou recebidas através de uma conexão de rede.

- Informações de uso do aplicativo, incluindo informações como a frequência com que você abre os aplicativos e usa a Ajuda e Suporte do Windows, quais serviços você usa para entrar nos aplicativos e quantas pastas são normalmente criadas em sua área de trabalho.

Os relatórios do Programa de Aperfeiçoamento da Experiência do Usuário também contêm informações sobre eventos (dados de log de eventos) em seu computador de até sete dias antes da hora em que você decidiu começar a participar do Programa de Aperfeiçoamento da Experiência do Usuário. Como a maioria dos usuários decide participar do Programa de Aperfeiçoamento da Experiência do Usuário dentro de alguns dias após a instalação do Windows, a Microsoft usa essas informações para analisar e melhorar a experiência de instalação do Windows.

Essas informações são enviadas para a Microsoft quando você está conectado à Internet. Os relatórios do Programa de Aperfeiçoamento da Experiência do Usuário não contêm intencionalmente informações de contato, como seu nome, endereço ou número de telefone. No entanto, alguns relatórios podem, de forma não intencional, conter identificadores individuais, como um número de série de um dispositivo que esteja conectado ao seu computador. A Microsoft filtra as informações contidas nos relatórios do Programa de Aperfeiçoamento da Experiência do Usuário para tentar remover qualquer identificador individual que elas possam conter. Se forem recebidos identificadores individuais, a Microsoft não os utilizará para identificar ou entrar em contato com você.

O Programa de Aperfeiçoamento da Experiência do Usuário gera aleatoriamente um número chamado GUID (identificador global exclusivo) que é enviado para a Microsoft com cada relatório do Programa de Aperfeiçoamento da Experiência do Usuário. O GUID nos permite determinar quais dados são enviados de um computador particular ao longo do tempo. Alguns relatórios do Programa de Aperfeiçoamento da Experiência do Usuário também podem incluir GUIDs derivados da sua conta da Microsoft.

O Programa de Aperfeiçoamento da Experiência do Usuário também baixará periodicamente um arquivo para coletar informações mais relevantes sobre como você usa o Windows e os aplicativos. Esse arquivo auxilia o Windows a coletar outras informações que ajudam a Microsoft a criar soluções para problemas comuns e a entender melhor os padrões de uso do Windows e dos aplicativos.

Uso das informações

A Microsoft usa as informações do Programa de Aperfeiçoamento da Experiência do Usuário para melhorar seus produtos e serviços, bem como o software e o hardware de terceiros desenvolvidos para esses produtos e serviços. Nós podemos também compartilhar as informações agregadas do Programa de Aperfeiçoamento da Experiência do Usuário com parceiros da Microsoft, para que eles possam melhorar seus produtos e serviços, mas as informações não podem ser usadas para identificar ou contatar você, nem para direcionar publicidade para você.

Usamos o GUID para distinguir o grau de disseminação de comentários que recebemos e como priorizá-los. Por exemplo, o GUID permite à Microsoft distinguir entre um cliente enfrentando um problema várias vezes e vários clientes enfrentando o mesmo problema ao mesmo tempo. A Microsoft não usa as informações coletadas pelo Programa de Aperfeiçoamento da Experiência do Usuário para identificá-lo ou contatá-lo.

Faça suas escolhas e controle

Se você escolher as configurações expressas ao instalar o Windows, você habilitará o Programa Windows de Aperfeiçoamento da Experiência do Usuário do Windows: o Microsoft e os aplicativos da Windows Store poderão enviar relatórios do Programa de Aperfeiçoamento da Experiência do Usuário a todos os usuários de seu computador. Se você optar por personalizar configurações, poderá controlar o Programa de Aperfeiçoamento da Experiência do Usuário selecionando **Enviar informações à Microsoft sobre como eu utilizo meu computador, como parte do Programa de Aperfeiçoamento da Experiência do Usuário** , em **Ajudar a melhorar os produtos e serviços da Microsoft**. Após a instalação do Windows, os administradores poderão alterar essa configuração na **Central de Ações** do Painel de Controle.

Para obter mais informações, consulte do Programa de Aperfeiçoamento da Experiência do Usuário: perguntas frequentes.

Início da página

Windows Defender

O Windows Defender procura por malwares e outros softwares potencialmente indesejados em seu computador. Ele inclui os recursos Microsoft Active Protection Service e Histórico da Microsoft.

Microsoft Active Protection Service

Se você usa o Windows Defender, o MAPS (Microsoft Active Protection Service) pode ajudar a proteger o computador baixando automaticamente novas assinaturas de malwares recém-detectados e monitorando o status de segurança do computador. O MAPS envia informações sobre malwares e outros softwares potencialmente não desejados à Microsoft e também pode enviar arquivos que podem conter malware. Se o MAPS detectar que o computador está infectado com determinados tipos de malware, ele poderá entrar em contato com você automaticamente por meio da sua conta da Microsoft para ajudá-lo a solucionar o problema.

Informações coletadas, processadas ou transmitidas

Os relatórios do MAPS incluem informações sobre arquivos de malware potenciais, como nomes de arquivo, hash criptográfico, fornecedor de software, tamanho e carimbos de data. Além disso, o MAPS pode coletar URLs completas para indicar a origem dos arquivos, bem como os endereços IP aos quais os arquivos de malwares potenciais se conectam. Ocasionalmente, essas URLs podem conter informações pessoais, como dados ou termos de pesquisa inseridos em formulários. Os relatórios também podem incluir as ações que você executou ao ser notificado pelo Windows Defender sobre o software potencialmente indesejado que foi detectado. O MAPS inclui essas informações para que a Microsoft avalie a eficiência com que o Windows Defender detecta e remove malware e software potencialmente indesejado e tente identificar novo malware.

Os relatórios são enviados automaticamente à Microsoft quando:

- O Windows Defender detecta algum software que ainda não teve seus riscos analisados.
- O Windows Defender detecta alterações feitas no computador por software que ainda não teve seus riscos analisados.
- O Windows Defender executa uma ação com o malware detectado (como parte de sua correção automática).

- Windows Defender conclui a verificação agendada e automaticamente executa uma ação com o software que foi detectado com base em suas configurações.
- O Windows Defender verifica um controle ActiveX no Internet Explorer.

Se ingressar no MAPS ao instalar o Windows, você ingressará como uma associação básica. Os relatórios da associação básica contêm as informações descritas nesta seção. Relatórios de associação avançada são mais abrangentes e ocasionalmente podem conter informações pessoais; por exemplo, caminhos de arquivos e despejos parciais da memória. Esses relatórios, juntamente com os relatórios de outros usuários do Windows Defender que participam do MAPS, ajudam nossos pesquisadores a descobrir novas ameaças mais rapidamente As definições de malware serão criadas e essas definições atualizadas serão disponibilizadas por meio do Windows Update.

Se você ingressar no MAPS, o Windows Defender poderá enviar arquivos específicos ou conteúdo da Web do seu computador, os quais a Microsoft suspeita serem softwares potencialmente não desejados. O relatório de exemplo é usado para análises futuras. Se um arquivo tiver informações pessoais, você será avisado antes do envio do arquivo. Se o Windows Update não puder obter assinaturas atualizadas para o Windows Defender durante um período, o Windows Defender tentará usar o MAPS para baixar as assinaturas de um local alternativo de download.

Para ajudar a proteger sua privacidade, todas as informações são enviadas para o MAPS com criptografia SSL.

Para ajudar a detectar e corrigir determinados tipos de infecções de malware, o Windows Defender envia regulamente ao MAPS algumas informações sobre o estado da segurança do computador. Essas informações incluem as configurações de segurança do computador e os arquivos de log que descrevem os drivers e outros softwares que são carregados quando o computador é iniciado. Um número que identifica exclusivamente o computador também é enviado.

Uso das informações

Os relatórios enviados ao MAPS são usados para melhorar os

softwares e serviços da Microsoft. Os relatórios também podem ser usados para fins de estatísticas, testes ou análise, e para gerar definições. O MAPS não coleta informações pessoais intencionalmente. Como o MAPS pode coletar informações pessoais não intencionalmente, a Microsoft não usará as informações para identificar, entrar em contato ou fazer propaganda para você.

As informações sobre o estado da segurança do computador que o MAPS coleta são usadas para determinar se certos tipos de malware infectaram o computador. Nesse caso, a Microsoft usa as informações de contato em sua conta da Microsoft para contatá-lo com detalhes sobre o problema e como corrigi-lo.

Faça suas escolhas e controle

Se você escolher as configurações expressas durante a instalação do Windows, o MAPS será habilitado. Se preferir personalizar as configurações, você poderá controlar o MAPS selecionando **Obtenha melhor proteção contra malware enviando informações e arquivos ao Microsoft Active Protection Service quando o Windows Defender estiver ativado** , em **Compartilhar informações com a Microsoft e outros serviços**. Depois de instalar o Windows, você poderá alterar sua associação ao MAPS ou suas configurações, inclusive desabilitar o MAPS, no menu **Configurações** no Windows Defender.

Se você receber a Ferramenta de Remoção de Software Mal-intencionado através do Windows Update, ela poderá enviar informações similares ao MAPS mesmo se o Windows Defender estiver desabilitado. Para obter mais informações, leia sobre a Windows Ferramenta de Remoção de Software Mal-intencionado do .

Recurso Histórico

O que este recurso faz

O recurso Histórico oferece uma lista de todos os aplicativos em seu computador que o Windows Defender detecta e as ações que foram tomadas quando os aplicativos foram detectados.

Além disso, você pode visualizar uma lista de aplicativos que o Windows Defender não monitora enquanto eles são executados em seu computador (eles são chamados de itens permitidos). Também é

possível visualizar aplicativos que o Windows Defender impede de serem executados até que você escolha removê-los ou permitir que eles sejam executados novamente (esses são chamados de itens de quarentena).

Informações coletadas, processadas ou transmitidas

A lista de softwares que o Windows Defender detectar, as ações que você e outros usuários executam e as ações que o Windows Defender executa automaticamente são armazenadas no computador. Todos os usuários podem visualizar o histórico no Windows Defender para visualizar malwares e softwares potencialmente indesejados que tenham tentado se instalar ou executar no computador ou que tenham sido permitidos para serem executados por outro usuário. Por exemplo, se você descobrir uma nova ameaça de malware, poderá consultar o Histórico para ver se o Windows Defender a impediu de infectar seu computador. Nenhuma informação é enviada para a Microsoft.

Faça suas escolhas e controle

As listas do Histórico podem ser excluídas por um administrador.

Início da página

Windows Relatório de Erro do

O que este recurso faz

O Relatório de Erros do Windows ajuda a Microsoft e os parceiros da Microsoft a diagnosticar problemas no software que você usa e a oferecer soluções. Nem todos os problemas têm solução, mas, quando há soluções disponíveis, elas são oferecidas como etapas para resolver o problema relatado ou como atualizações a serem instaladas. Para ajudar a evitar problemas e tornar o software mais confiável, algumas soluções também são incluídas nos service packs e nas futuras versões do software.

Informações coletadas, processadas ou transmitidas

Muitos produtos de software são criados para funcionar com o Relatório de Erros do Windows. Se ocorrer um problema em um desses produtos, será perguntado se você deseja relatá-lo.

O Relatório de Erros do Windows coleta informações úteis para diagnosticar e solucionar um problema que tenha ocorrido; por exemplo, onde o problema ocorreu no software ou no hardware, o tipo ou a severidade do problema, os arquivos que ajudam a descrever o problema, informações básicas sobre o software e o hardware ou possíveis problemas de compatibilidade e desempenho do software. Se você usa o Windows para hospedar máquinas virtuais, os relatórios de erros enviados para a Microsoft poderão incluir informações sobre as máquinas virtuais.

O Relatório de Erros do Windows também coleta informações sobre aplicativos, drivers e dispositivos que ajudam a Microsoft a compreender e melhorar a compatibilidade de aplicativos e dispositivos. As informações sobre aplicativos podem incluir o nome dos arquivos executáveis do aplicativo. As informações sobre os dispositivos e drivers podem incluir os nomes dos dispositivos que você instalou no computador e os arquivos executáveis associados aos drivers desses dispositivos. As informações sobre a empresa que publicou um aplicativo ou driver podem ser coletadas.

Se você habilitar o relatório automático durante a instalação do Windows, o serviço de relatório enviará automaticamente as informações básicas sobre onde ocorrem os problemas. Em alguns casos, o serviço de relatório enviará automaticamente informações adicionais para ajudar a diagnosticar o problema, como um instantâneo parcial da memória do computador. Alguns relatórios de erros podem, não intencionalmente, conter informações pessoais. Por exemplo, um relatório que contém um instantâneo da memória do computador pode incluir seu nome, parte de um documento no qual você estava trabalhando ou dados que foram recentemente enviados a um site.

Para ajudar a diagnosticar certos tipos de problemas, o Relatório de Erros do Windows pode criar um relatório com informações adicionais, como arquivos de log. Antes de enviar um relatório com essas informações adicionais, o Windows perguntará se você deseja enviar o relatório, mesmo que você tenha habilitado o recurso de relatório automático.

Após o envio de um relatório, o serviço de relatórios poderá solicitar mais informações sobre o problema que ocorreu. Se você optar por

fornecer seu número de telefone ou endereço de email nessas informações, o relatório de erros será pessoalmente identificável. A Microsoft pode entrar em contato com você para solicitar informações adicionais a fim de solucionar o problema relatado.

O Relatório de Erros do Windows gera aleatoriamente um número chamado GUID (identificador global exclusivo) que é enviado para a Microsoft com cada relatório de erros. O GUID nos permite determinar quais dados são enviados de um computador particular ao longo do tempo. O GUID não contém informações pessoais.

Para ajudar a proteger sua privacidade, as informações são enviadas criptografadas por SSL.

Uso das informações

A Microsoft usa as informações sobre erros e problemas relatados por usuários do Windows para aperfeiçoar os produtos e serviços da Microsoft e software e hardware de terceiros criados para serem usados com esses produtos e serviços. Usamos o GUID para determinar o grau de disseminação dos comentários que recebemos e como priorizá-los. Por exemplo, o GUID permite à Microsoft distinguir entre um cliente enfrentando um problema várias vezes e vários clientes enfrentando o mesmo problema ao mesmo tempo.

Funcionários, prestadores de serviço, fornecedores e parceiros da Microsoft podem ter acesso a partes relevantes das informações coletadas, mas eles só poderão utilizar essas informações para reparar ou melhorar os produtos e serviços da Microsoft ou software e hardware de terceiros criados para serem usados com esses produtos e serviços da Microsoft. Se um relatório de erros incluir informações pessoais, a Microsoft não as usará para identificar, entrar em contato ou fazer propaganda para você. No entanto, se você optar por fornecer as informações de contato, conforme descrito acima, podemos usar essas informações para entrar em contato com você.

Faça suas escolhas e controle

Se você escolher as configurações expressas ao instalar o Windows, o Relatório de Erros do Windows enviará automaticamente relatórios básicos para verificar se há soluções para os problemas na Internet. Se você preferir personalizar as configurações, poderá controlar o

Relatório de Erros do Windows selecionando **Usar o Relatório de Erros do Windows para verificar soluções de problemas online** , em **Procurar soluções online**. Após a instalação do Windows, você poderá alterar essa configuração na Central de Ações do Painel de Controle.

Para obter mais informações, consulte a Microsoft Política de Privacidade dos Serviços de Relatório de Erro.

Início da página

Associação de arquivos do Windows

O que este recurso faz

Windows O recurso Associação de arquivos ajuda os usuários a associarem tipos de arquivo com aplicativos específicos. Se você tentar abrir um tipo de arquivo e ele não tiver um aplicativo associado a ele, Windows perguntará se você deseja usar o recurso Associação de Arquivos do Windows para localizar um aplicativo para o arquivo, que inclui a busca na Windows Store por um aplicativo compatível. Os aplicativos que geralmente são associados à extensão de nome de arquivo são exibidos.

Informações coletadas, processadas ou transmitidas

Se você escolher usar o recurso Windows Associação de arquivos, a extensão de nome de arquivo (por exemplo, docs ou pdf) e o idioma do monitor do seu computador serão enviados para a Microsoft. O restante do nome do arquivo não é enviado para a Microsoft. Quando uma associação de arquivo é feita com um aplicativo específico, um identificador exclusivo para o aplicativo é enviado para identificar o aplicativo padrão para cada tipo de arquivo.

Uso das informações

Quando você enviar uma extensão de nome de arquivo, o serviço retornará uma lista de aplicativos que a Microsoft está ciente de que podem abrir arquivos dessa extensão. A menos que você baixe e instale um aplicativo, nenhuma associação a tipo de arquivo será alterada.

Faça suas escolhas e controle

Quando você tentar abrir um tipo de arquivo sem um aplicativo associado, será possível escolher se deseja usar o recurso Windows Associação de arquivos. Nenhuma informação da associação do arquivo é enviada para a Microsoft a menos que você decida usar o serviço.

Início da página

Ajuda do Windows

Windows Ajuda e Suporte Online

O que este recurso faz

Windows Ajuda e Suporte Online, quando ativado, permite que você obtenha o conteúdo de ajuda e suporte atualizado disponível quando estiver conectado à internet.

Informações coletadas, processadas ou transmitidas

Quando você usa Windows Ajuda e Suporte Online, suas dúvidas sobre pesquisa da ajuda são enviadas para a Microsoft, assim como suas solicitações de conteúdo de ajuda quando um vínculo está clicado. O Windows envia algumas informações sobre a configuração de seu computador para localizar conteúdo de ajuda mais relevante. A Ajuda e Suporte Online do Windows também usa tecnologias padrão da Web, como cookies.

Uso das informações

A Microsoft usa as informações para retornar tópicos da Ajuda em resposta a suas consultas de pesquisa, retornar os resultados mais relevantes, desenvolver conteúdo novo e melhorar o conteúdo existente. Nós usamos as informações sobre a configuração de seu computador para exibir o conteúdo da Ajuda adequado à configuração. Nós usamos cookies e outras tecnologias da Web para facilitar a navegação pelo conteúdo da Ajuda e para compreender melhor como os usuários utilizam a Ajuda Online do Windows.

Faça suas escolhas e controle

Por padrão, a Ajuda e Suporte Online está habilitada. Para alterar essa configuração, toque ou clique no ícone **Configurações** na parte superior da janela da Ajuda e Suporte e marque ou desmarque **Obter**

ajuda online. Para limpar os cookies usados pela Ajuda do Windows, abra Opções da Internet no Painel de Controle, clique ou toque no botão **Excluir** em **Histórico de navegação**, selecione **Cookies e dados de sites**e clique ou toque em **Excluir**. Se você bloquear todos os cookies (na seção Privacidade das Opções da Internet), a Ajuda do Windows não definirá cookies.

Programa de Aperfeiçoamento da Experiência da Ajuda

O que este recurso faz

O Programa de Aperfeiçoamento da Experiência da Ajuda auxilia a Microsoft a identificar tendências na maneira como nossos clientes usam a Ajuda e Suporte Online do Windows, assim podemos melhorar nossos resultados de pesquisa e a relevância de nosso conteúdo.

Informações coletadas, processadas ou transmitidas

O Programa de Aperfeiçoamento da Experiência da Ajuda envia à Microsoft informações sobre a versão do Windows instalada em seu computador e sobre como você usa a Ajuda e Suporte do Windows, incluindo as consultas inseridas quando você pesquisa a Ajuda e Suporte do Windows e as classificações ou os comentários sobre os tópicos da Ajuda que são apresentados. Quando você pesquisa, navega ou fornece quaisquer classificações ou comentários nos tópicos de Ajuda apresentados a você, essas informações são enviadas para a Microsoft.

O Programa de Aperfeiçoamento da Experiência da Ajuda gera aleatoriamente um número chamado GUID (identificador global exclusivo) que é enviado à Microsoft com cada relatório do Programa de Aperfeiçoamento da Experiência da Ajuda. O GUID nos permite determinar quais dados são enviados de um computador específico ao longo do tempo. O GUID não contém informações pessoais. O GUID é separado dos GUIDs usados pelo Relatório de Erros do Windows e pelo Programa de Aperfeiçoamento da Experiência do Usuário do Windows.

Uso das informações

Os dados coletados são usados para identificar tendências e padrões de uso, assim a Microsoft pode aprimorar a qualidade do conteúdo que

fornecemos e a relevância de nossos resultados de pesquisa. Nós usamos o GUID para determinar o grau de disseminação dos problemas que recebemos e como priorizá-los. Por exemplo, o GUID permite à Microsoft distinguir entre um cliente enfrentando um problema várias vezes e vários clientes enfrentando o mesmo problema ao mesmo tempo.

O Programa de Aperfeiçoamento da Experiência da Ajuda não coleta intencionalmente informações que possam ser usadas para identificá-lo pessoalmente. Se você digitar essas informações nas caixas de pesquisa ou de comentários, as informações serão enviadas, mas a Microsoft não as usará para identificar, contatar ou direcionar publicidade para você.

Faça suas escolhas e controle

Ao escolher as configurações expressas quando instalar o Windows, você ingressará no Programa de Aperfeiçoamento da Experiência da Ajuda. Se você optar por personalizar configurações, poderá controlar as configurações do Programa de Aperfeiçoamento da Experiência da Ajuda selecionando **Enviar informações à Microsoft sobre como eu utilizo a Ajuda, como parte do Programa de Aperfeiçoamento da Experiência do Usuário** , em **Ajudar a melhorar os produtos e serviços da Microsoft**. Após instalar o Windows, você poderá alterar essa configuração na Ajuda e Suporte do Windows.

Início da página

Assistência remota

O que este recurso faz

Você pode usar o recurso Assistência Remota para convidar uma pessoa para se conectar ao seu computador e ajudar você a solucionar um problema nele, mesmo se ela não estiver por perto. Após fazer a conexão, a outra pessoa poderá visualizar seu computador. Com sua permissão, a outra pessoa pode usar o mouse e o teclado dela para controlar seu computador e mostrar a você como corrigir um problema.

Informações coletadas, processadas ou transmitidas

A Assistência Remota cria uma conexão criptografada entre os dois computadores através da internet ou de rede local. Quando uma pessoa usa o recurso Assistência Remota para se conectar ao seu computador, ela pode ver sua área de trabalho e os documentos abertos, incluindo informações privadas visíveis. Além disso, se você permitir que outra pessoa controle seu computador com o mouse e teclado dela, essa pessoa poderá fazer coisas como excluir arquivos ou alterar configurações. Após estabelecer a conexão, a Assistência Remota trocará informações de contato, incluindo nome de usuário, nome do computador e imagem da conta. Um arquivo de log de sessão mantém um registro de todas as conexões do recurso Assistência Remota.

Uso das informações

As informações são usadas para estabelecer uma conexão criptografada e para fornecer acesso a sua área de trabalho para outra pessoa. Nenhuma informação é enviada para a Microsoft.

Faça suas escolhas e controle

Antes de você permitir que alguém se conecte ao seu computador, feche quaisquer aplicativos ou documentos abertos que você não queira que a outra pessoa veja. Se a qualquer momento você se sentir desconfortável com o que essa pessoa está visualizando ou fazendo no seu computador, pressione a tecla Esc para encerrar a sessão. Você pode desabilitar o log de sessão e a troca de informações de contato desmarcando essas opções nas configurações da Assistência Remota.

Início da página

Windows Search

O que este recurso faz

O Windows Search permite que você pesquise no seu dispositivo e na Internet em um único local. Para fornecer melhores resultados de pesquisa, o Windows Search pode usar o Bing e a Plataforma de Localização do Windows Observe que há outros recursos de pesquisa no seu dispositivo, fornecidos pela Microsoft; por exemplo,pesquisar na Windows Store, no Internet Explorer e em outros produtos da Microsoft.

Informações coletadas, processadas ou transmitidas

Se você optar por obter resultados de pesquisa na Web, o Windows enviará o que você digitar no Windows Search para a Microsoft. Para ajudar a melhorar os resultados da pesquisa, o Windows Search também enviará informações para a Microsoft sobre como você interage com o recurso. O Windows Search também enviará um identificador para fornecer resultados de pesquisa personalizados com base nas suas interações com o Bing e outros produtos e serviços da Microsoft. Se você entrar no Windows com uma conta da Microsoft, o identificador será associado a essa conta da Microsoft. Você pode optar por não receber resultados personalizados no Windows Search; nesse caso, o identificador não será enviado.

Se você permitir que o Windows Search use sua localização, o local físico do seu dispositivo (conforme fornecido pela Plataforma de Localização do Windows) será enviado à Microsoft como parte de cada solicitação de pesquisa. Como alternativa, podemos tentar obter sua localização física aproximada com base no seu endereço IP.

Quando você usa o Windows Search para pesquisar em um aplicativo, seus termos de pesquisa são fornecidos ao aplicativo.

Uso das informações

Se você optar por usar o Windows Search para receber resultados de pesquisa da Web, usaremos o termo de pesquisa fornecido, seu histórico de pesquisa local e online, as informações associadas à sua conta da Microsoft e a localização do seu dispositivo para fornecer sugestões de pesquisa relevantes, resultados de pesquisa personalizados e experiências personalizadas em outros produtos e serviços da Microsoft. Para saber mais sobre como seus dados são usados, leia a Política de privacidade do Bing.

Se você usar o Windows Search para pesquisar em um aplicativo de terceiros, o uso das informações coletadas estará sujeito às práticas de privacidade desse terceiro. Se você pesquisar em um aplicativo da Microsoft, as práticas de privacidade do aplicativo serão explicadas na respectiva política de privacidade.

Faça suas escolhas e controle

Se escolher as configurações expressas ao configurar o Windows, você permitirá que o Windows Search obtenha sugestões de pesquisa e resultados da Web e permitirá que a Microsoft use os dados do Windows Search (incluindo a localização) para personalizar o Windows Search e outras experiências da Microsoft. Se você optar por personalizar as configurações, poderá decidir se deseja alterar essas configurações para o Windows Search. Depois de instalar o Windows, você poderá alterar essas configurações em **Pesquisar** nas configurações do computador.

Você pode limpar o histórico de pesquisas locais e o histórico de algumas pesquisas do Bing, usadas para personalizar sua experiência do Windows Search em **Pesquisar** em **Pesquisar aplicativos** nas configurações do computador. A limpeza do histórico de pesquisas instrui a Microsoft a não usar qualquer histórico de pesquisas coletadas anteriormente para personalizar sugestões de pesquisa ou ordenar resultados de pesquisa. Isso não limpa publicidades ou outras informações de personalização (incluindo informações derivadas do histórico de pesquisas), nem exclui informações que são usadas conjuntamente pela Microsoft para melhorar os resultados de pesquisa e outras experiências da Microsoft. Essas informações são retidas e tornadas anônimas, como descrito na Política de privacidade do Bing. Você pode gerenciar online a publicidade e outras informações de personalização da Microsoft.

Início da página

Instalação do Windows

Esta seção descreve os recursos disponibilizados como parte do processo de instalação do Windows

Atualização Dinâmica

O que este recurso faz

A Atualização Dinâmica permite que o Windows execute uma verificação única usando o Windows Update para obter as atualizações mais recentes para seu computador enquanto o Windows é instalado. Se forem encontradas atualizações, a Atualização Dinâmica baixará e instalará essas atualizações automaticamente para que o seu computador esteja em dia quando você entrar nele ou usá-lo pela

primeira vez.

Informações coletadas, processadas ou transmitidas

Para instalar drivers compatíveis, a Atualização Dinâmica envia informações para a Microsoft sobre o hardware do seu computador. Os tipos de atualizações que a Atualização Dinâmica pode baixar para o seu computador incluem:

- **Atualizações de instalação.** Atualizações de software importantes para arquivos de instalação para ajudar a garantir uma instalação bem-sucedida.
- **Atualizações de driver da caixa de entrada.** Atualizações de driver importantes para a versão do Windows que você está instalando.

Adicionalmente, se você instalar o Windows da Windows Store, a Atualização Dinâmica baixará e instalará as atualizações mais recentes para o Windows, bem como alguns drivers de hardware que o computador precisa.

Uso das informações

A Atualização Dinâmica relata informações para a Microsoft sobre o hardware do seu computador, para ajudar a identificar os drivers corretos para o seu sistema.

Faça suas escolhas e controle

Se você instalar o Windows da Windows Store, a Instalação baixará e instalará atualizações automaticamente. Se você instalar o Windows de mídia física, você será perguntado se deseja acessar a Internet para instalar atualizações.

Programa de Aperfeiçoamento da Instalação

O que este recurso faz

Esse recurso envia um único relatório para a Microsoft contendo as informações básicas sobre seu computador e como você instalou Windows. A Microsoft usa essas informações para ajudar a aprimorar a experiência da instalação e a criar soluções para problemas comuns de instalação.

Informações coletadas, processadas ou transmitidas

Em geral, o relatório inclui informações sobre sua experiência de instalação; por exemplo, a data de instalação, o tempo que cada fase da instalação levou, se ela foi uma atualização ou uma nova instalação do produto, os detalhes de versão, o idioma do sistema operacional, o tipo de mídia, a configuração do computador e o status de êxito ou falha, juntamente com eventuais códigos de erro.

Se você participar do Programa de Aperfeiçoamento da Instalação, o relatório será enviado para a Microsoft quando você estiver conectado à Internet. O Programa de Aperfeiçoamento da Instalação gera aleatoriamente um número chamado GUID (identificador global exclusivo) que é enviado para a Microsoft com o relatório. O GUID nos permite determinar quais dados são enviados de um computador particular ao longo do tempo. O GUID não contém qualquer informação pessoal e não é usado para identificar você.

Uso das informações

A Microsoft e seus parceiros usam o relatório para melhorar produtos e serviços. Usamos o GUID para correlacionar esses dados coletados pelo Programa de Aperfeiçoamento da Experiência do Usuário (CEIP) Windows, um programa do qual você poderá participar quando estiver usando o Windows.

Faça suas escolhas e controle

Você pode participar desse programa ao instalar o Windows selecionando **Eu quero ajudar a melhorar a instalação doWindows** .

Para obter mais informações, consulte a seção Programa de Aperfeiçoamento da Experiência do Usuário do Windows.

Assistente de Compatibilidade de Instalação

O que este recurso faz

Quando você instalar o Windows, a Instalação ajudará a determinar se o seu computador atual está pronto para uma atualização para o Windows 8.1 e fornecerá informações de compatibilidade em relação aos seus programas e dispositivos.

Informações coletadas, processadas ou transmitidas

Quando a compatibilidade é confirmada, nós coletamos determinadas informações sobre a sua potencial experiência de atualização, desde os recursos de hardware do seu computador até os dispositivos conectados e os aplicativos instalados nele. Ocasionalmente, as informações sobre o fornecedor do programa podem conter o nome ou o endereço de email do fornecedor.

Uso das informações

Usamos as informações coletadas para determinar os drivers certos para seu computador, bem como a compatibilidade do computador, de programas e dispositivos com o Windows 8.1. Além disso, poderemos usá-las para aprimorar nossos produtos e serviços. Nós não usamos essas informações para identificar, entrar em contato ou fazer propaganda para você.

Faça suas escolhas e controle

Se você instalar o Windows da Windows Store ou de mídia física dentro de uma instalação do Windows existente, as informações descritas nesta seção serão enviadas para a Microsoft. Se você inicializar via mídia de instalação física para instalar o Windows, a Instalação não verificará se há informações de compatibilidade na Internet.

Início da página

Compartilhamento do Windows

O que este recurso faz

Windows Compartilhamento permite que você compartilhe conteúdo entre aplicativos da Windows Store que deem suporte ao compartilhamento. Ele também permite que você compartilhe conteúdo com seus amigos.

Informações coletadas, processadas ou transmitidas

Quando estiver compartilhando, o aplicativo de origem passa o conteúdo para o aplicativo de destino somente depois de você selecionar o destino no painel Compartilhar. Se o aplicativo de origem não tiver implementado o compartilhamento, você terá a opção de compartilhar uma imagem de qualquer coisa que for exibida na tela.

Dessa forma você pode acessá-los facilmente, os aplicativos de destino e as pessoas com as quais você compartilha conteúdo com frequência serão exibidos em uma lista no painel Compartilhar. Nenhuma informação é enviada para a Microsoft.

Uso das informações

As informações armazenadas sobre com que frequência você compartilha com os aplicativos de destino e pessoas com as quais você compartilha conteúdo com frequência são usadas para ordenar a lista no painel Compartilhar em ordem de frequência. Se você compartilhar informações com um aplicativo de terceiros, o uso das informações coletadas estará sujeito às políticas de privacidade do terceiro. Se você compartilhar com um aplicativo da Microsoft, as práticas de privacidade do aplicativo serão explicadas em sua política de privacidade.

Faça suas escolhas e controle

Por padrão, o Windows armazena as informações sobre o uso do Compartilhamento do Windows. Você pode parar de armazenar essas informações ou excluir todos os destinos armazenados em **Compartilhar** , em **Pesquisar aplicativos** nas configurações do computador.

Início da página

Windows SmartScreen

O que este recurso faz

O Windows SmartScreen ajuda a manter a segurança do seu computador verificando os arquivos baixados e o conteúdo da Web nos aplicativos, para ajudar a proteger contra software mal-intencionado e conteúdo da Web potencialmente não seguro. Antes que um arquivo baixado, mas desconhecido ou potencialmente não seguro, seja aberto, o Windows exibe um aviso. Se o SmartScreen detectar conteúdo da Web potencialmente não seguro em um aplicativo, o Windows exibirá um aviso no lugar do conteúdo.

Informações coletadas, processadas ou transmitidas

Se optar por usar o Windows SmartScreen para verificar os arquivos

baixados, o Windows enviará informações para o serviço SmartScreen online. Essas informações podem incluir um nome de arquivo, o identificador de arquivo ("hash") e as informações de certificado digital, juntamente com as informações padrão do computador e o número de versão de filtro do Windows SmartScreen. Para proteger sua privacidade, as informações enviadas à Microsoft são criptografadas por SSL.

Se você optar por usar o Windows SmartScreen para bloquear conteúdo potencialmente não seguro em aplicativos, o Windows enviará informações para o serviço SmartScreen online, incluindo os endereços e os tipos de conteúdo que alguns aplicativos da Windows Store acessa, quando você os utiliza. Em resposta, o serviço online informará ao seu computador se o conteúdo foi relatado à Microsoft como não seguro ou suspeito. Os relatórios enviados à Microsoft incluem informações como o nome ou o identificador do aplicativo e os endereços completos do conteúdo da Web acessado pelo aplicativo.

Para proteger sua privacidade, as informações enviadas à Microsoft são criptografadas. As informações que podem estar associadas a uma página da Web acessada dentro de um aplicativo, como termos de pesquisa, podem ser incluídas no endereço enviado à Microsoft. Por exemplo, se você procura uma palavra em um aplicativo de dicionário, a palavra procurada pode ser enviada para a Microsoft como parte do endereço completo acessado pelo aplicativo. A Microsoft filtra esses endereços para tentar remover as informações pessoais, onde possível.

O Windows gera aleatoriamente um número chamado GUID (identificador global exclusivo) que é enviado para a Microsoft com cada relatório. O GUID nos permite determinar quais dados são enviados de um computador particular ao longo do tempo. O GUID não contém informações pessoais.

Uso das informações

A Microsoft usa as informações descritas acima para enviar avisos a você sobre arquivos e tipos de conteúdo baixados potencialmente não seguros dentro de aplicativos. Por exemplo, se o SmartScreen detectar uma ameaça potencial dentro de um aplicativo com suporte para SmartScreen, o Windows exibirá um aviso no lugar do conteúdo.

Também usamos as informações para aperfeiçoar o SmartScreen e outros produtos e serviços. A Microsoft não usa as informações para enviar propaganda para você.

Faça suas escolhas e controle

Se você escolher as configurações expressas durante a configuração do Windows, o ativará o Windows SmartScreen. Se você optar por personalizar as configurações, poderá controlar o Windows SmartScreen selecionando **Use os serviços online SmartScreen para se proteger contra conteúdo mal-intencionado de sites, carregado por aplicativos da Windows Store e pelo Internet Explorer, bem como downloads mal-intencionados** , em **Ajude a proteger seu computador e sua privacidade**. Após a instalação do Windows, você poderá alterar essa configuração na Central de Ações do Painel de Controle. Para obter informações sobre o Internet ExplorerSmartScreen, consulte a seção SmartScreen Filtro da Internet Explorer Política de privacidade do.

Início da página

Reconhecimento de Fala do Windows

O que este recurso faz

Windows Reconhecimento de Fala fornece reconhecimento de fala em Windows e para quaisquer aplicativos que escolher usar. Windows Reconhecimento de Fala aumenta sua precisão aprendendo como você deve usar o idioma, incluindo os sons e as palavras que deseja usar.

Informações coletadas, processadas ou transmitidas

Windows Reconhecimento de Fala armazena uma lista de palavras e suas pronúncias no seu computador. As palavras e pronúncias são adicionadas a essa lista usando o Dicionário de Fala e usando o recurso Windows Reconhecimento de Fala para ditar e corrigir palavras.

Quando o recurso de revisão de documento do Reconhecimento de Fala do Windows é habilitado, o texto de documentos do Microsoft Office Word (com extensões de nome de arquivo doc ou docx) e os emails (de outras pastas de email que não sejam Itens Excluídos ou Lixo Eletrônico) em seu computador e em qualquer compartilhamento

de arquivos conectados incluídos nos locais de índice de pesquisa do Windows são coletados e armazenados em fragmentos de uma, duas ou três palavras. Os fragmentos de uma palavra incluem apenas palavras adicionadas aos dicionários personalizados, e os fragmentos de duas ou três palavras incluem somente palavras encontradas nos dicionários padrão.

Todas as informações coletadas são armazenadas no seu perfil de fala pessoal no seu computador. Os perfis de fala são armazenados para cada usuário e os usuários não podem acessar os perfis de outros usuários no seu computador. No entanto, os administradores podem acessar qualquer perfil no seu computador. As informações do perfil não são enviadas para a Microsoft a menos que você escolha enviá-las quando perguntado pelo recurso Reconhecimento de Fala do Windows. Você pode analisar os dados antes de enviá-los. Se você escolher enviar essas informações, os dados de adaptação acústica que foram usados para adaptar suas características de áudio também serão enviados.

Se você concluir uma sessão de treinamento de fala, o Reconhecimento de Fala do Windows perguntará se você deseja enviar suas informações do perfil de fala para a Microsoft. Você pode analisar as informações antes de enviá-las. Essas informações podem incluir gravações da sua voz enquanto você conclui a sessão de treinamento e as outras informações do seu perfil de fala pessoal.

Uso das informações

Windows Reconhecimento de Fala usa palavras do perfil de fala para converter sua fala para texto. A Microsoft usa as informações do perfil de fala pessoal para aprimorar seus produtos e serviços. Nós não usamos essas informações para identificar, entrar em contato ou fazer propaganda para você.

Faça suas escolhas e controle

Você pode escolher se deseja executar o recurso Windows Reconhecimento de Fala. Se você executar o recurso de Reconhecimento de Fala do Windows, a revisão de documento será habilitada por padrão. Você pode alterar as configurações de revisão de documento na primeira vez que executar o Reconhecimento de Fala do Windows. Você pode alterar as configurações de revisão do

documento ou excluir perfis de fala pessoal (e a maioria das informações de revisão do documento) acessando Reconhecimento de Fala no Painel de Controle e clicando nas opções de fala **Avançadas**. Você também pode usar a opção Alterar palavras existentes no Dicionário de Fala para excluir palavras que foram adicionadas para seu perfil de fala. No entanto, a exclusão de seu perfil de fala pessoal não exclui as palavras adicionadas através do Dicionário de Fala.

Você pode controlar os locais dos quais a revisão de documento coletará fragmentos de palavras modificando os locais incluídos em seu índice de pesquisa do Windows. Para visualizar ou modificar quais locais estão incluídos no seu Windows índice de pesquisa, abra Opções de Indexação no Painel de Controle.

No final da sessão de treinamento, será oferecida a você a opção de enviar seu treinamento e outras informações do perfil para a Microsoft. Você também pode enviar informações quando o recurso Windows Reconhecimento de Fala é iniciado clicando com o botão direito em **Microfone**e, em seguida, clicando em **Ajude a aprimorar o reconhecimento de fala**. Em ambos os casos, você pode visualizar todos os arquivos de dados antes de eles serem enviados e pode escolher não enviá-los.

Início da página

Windows Store

A Windows Store permite que você localize, gerencie e instale aplicativos no seu computador. As seções abaixo descrevem como os recursos da Loja, e os aplicativos que você obtém através da Loja, podem ter impacto na sua privacidade e o que pode ser feito para controlar isso.

Aplicativo e serviço da Loja

O que este recurso faz

A Loja permite que você localize e instale aplicativos no seu computador. Ela também mantém o acompanhamento dos aplicativos da Loja que foram instalados, então é possível obter atualizações para eles e instalá-las em mais de um computador.

Informações coletadas, processadas ou transmitidas

Para localizar e instalar aplicativos, você deve entrar na Loja com uma conta da Microsoft. Assim, a Loja tem acesso às informações do perfil de sua conta da Microsoft, como seu nome, email e imagem da conta. A Loja coleta e associa as seguintes informações adicionais à sua conta da Loja:

- Pagamentos à Loja. As informações sobre o que você comprou, quanto pagou e como pagou quando comprou aplicativos ou fez compras dentro do aplicativo com a sua conta da Loja.

- Aplicativos que você instalou. A lista de aplicativos que você instalou da Loja, a política de licença de cada aplicativo (licença permanente ou período limitado de avaliação) e uma lista de compras feitas com sua conta da Loja, em cada aplicativo. Além de armazenar essas informações online com sua conta da Loja, a Loja armazena as informações de licenciamento no seu computador para cada aplicativo instalado. Essas informações identificam você como o proprietário da licença.

- Computadores nos quais você instalou aplicativos. A marca, o modelo e o nome do computador de cada computador no qual você instalou aplicativos, junto com um número que identifica o computador de forma exclusiva. Este número é gerado com base na configuração de hardware do computador e não contém qualquer informação sobre você.

- Classificações, revisões e relatórios de problemas. Depois de instalar um aplicativo, será possível escrever uma análise ou deixar uma classificação para ele na Loja. Sua conta da Microsoft é associada a essas classificações. Se você escrever uma análise, o nome e a imagem de sua conta da Microsoft serão publicados com sua análise.

- Preferências da Loja. Preferências que você define para a visualização de aplicativos na Loja, por exemplo, exibir somente os aplicativos que estiverem disponíveis em seu idioma nativo.

Você pode escolher as suas informações de pagamento para a loja, como um número de cartão de crédito, com sua conta da Loja. Para fins de segurança, essas informações são transmitidas por SSL e todos

exceto os quatro últimos dígitos do número do seu cartão de crédito, são armazenados criptografados.

A Loja coleta algumas informações sobre sua cópia do Windows, para determinar se ela foi vendida no varejo, é uma cópia de avaliação, está sujeira ao programa de licenciamento do volume ou foi pré-instalada pelo fabricante do computador. Quando você se conecta pela primeira vez à Loja, uma lista de todos os aplicativos pré-instalados em seu computador é enviada para a Loja, que associa as licenças dos aplicativos à sua conta da Loja.

Conforme você navega pela Loja e usa os aplicativos dela, a Microsoft coleta algumas informações para nos ajudar a entender os padrões de uso e tendências, semelhante à maneira como os sites analisam os dados de navegação dos seus visitantes.

Uso das informações

A Microsoft usa suas informações de contato para enviar a você um email necessário para fornecer os serviços da Loja, como recibos de aplicativos que forem comprados. Ele usa suas informações de pagamento para permitir que você pague suas compras. Se você escolher armazenar essas informações, não será necessário inseri-las toda vez. A Microsoft usa informações sobre suas compras para operar a Loja e fornecer suporte ao cliente.

A Loja mantém o acompanhamento de todos os aplicativos que você tiver instalado. Você pode usar a Loja para gerenciar a lista de dispositivos nos quais você instalou aplicativos e o suporte ao cliente pode também ajudar você a gerenciar essas informações. Depois de instalar um aplicativo, sempre será possível visualizá-lo no histórico de compras da Loja, mesmo se você escolher desinstalá-lo. A Loja também usa essa lista para ajudar a aplicar o limite no número de computadores que podem ter aplicativos instalados, como descrito nos termos de uso da Windows Store. Quando você escreve uma análise para um aplicativo, o nome e a imagem da conta associados a sua Windows conta serão publicados ao lado da análise na Loja. Se você relatar um problema com um aplicativo, o relatório do problema ficará disponível para os representantes da Loja avaliarem e executarem ações. Eles podem usar seu nome e endereço de email associados com a sua conta da Loja para entrar em contato com você, se

necessário, quando eles analisarem o relatório.

Quando existirem atualizações disponíveis para os aplicativos instalados, uma notificação será exibida na Loja, e o bloco da Loja indicará o número de atualizações disponíveis. Você poderá então exibir a lista de atualizações disponíveis e escolher quais instalar. Os aplicativos atualizados podem usar funcionalidades do Windows diferentes das versões anteriores, o que pode fornecer a eles acesso a recursos diferentes no seu computador. Você pode ver as listas de atualizações de funcionalidades nas páginas de Descrição do Aplicativo vinculadas à página que lista as atualizações disponíveis.

A Loja usa as informações que ela coleta sobre sua copia do Windows para determinar como Windows foi instalado no seu computador (por exemplo, se o fabricante do seu computador a pré-instalou). Essas informações permitem que a Loja dê a você acesso para os aplicativos fornecidos exclusivamente por esse fabricante para os clientes dele. Elas também são usadas para fornecer informações para a Microsoft (e em conjunto para o fabricante, em alguns casos) sobre os padrões de uso do Windows.

A Microsoft usa alguns dados de uso e de compra do aplicativo em conjunto para saber como as pessoas usam a Loja (por exemplo, como os usuários localizam os aplicativos que instalam). A Microsoft pode compartilhar algumas dessas estatísticas agregadas com os desenvolvedores do aplicativo. A Microsoft não compartilha qualquer informação pessoal com os desenvolvedores do aplicativo. Nós utilizamos os dados de uso e navegação coletados pela Loja para entender melhor como as pessoas usam a Loja e para aprimorar os recursos e serviços da Loja.

Faça suas escolhas e controle

Se você escolher usar a Loja, as informações descritas nessa seção serão enviadas para a Microsoft conforme descrito acima.

Para remover uma análise de um aplicativo que você publicou, vá para a descrição do aplicativo na Loja, edite sua análise e exclua todo o texto.

Atualizações automáticas de aplicativos

O que este recurso faz

Esse recurso verifica, baixa e instala atualizações para aplicativos da Windows Store, para garantir que você tenha as versões mais recentes. As atualizações de aplicativos podem incluir atualizações de segurança, atualizações de desempenho ou nova funcionalidade ou conteúdo. Os aplicativos atualizados podem usar recursos do Windows diferentes das versões anteriores, o que pode fornecer a eles acesso a recursos diferentes no seu computador. Para saber mais sobre alterações de recursos, acesse a Página de Descrição do Produto do aplicativo na Windows Store.

Informações coletadas, processadas ou transmitidas

Para fornecer atualizações automáticas de aplicativos, a Loja envia as seguintes informações à Microsoft:

- Uma lista de todos os aplicativos instalados da Loja por todos os usuários no seu computador
- As informações de licenciamento de cada aplicativo
- Os sucessos, falhas e erros que ocorrem quando você atualiza aplicativos da Loja.
- GUID (identificador global exclusivo) – um número gerado aleatoriamente que não contém informações pessoais.
- Nome, número de revisão e data da revisão do BIOS
- Informações básicas sobre seu computador, como o fabricante, o modelo e a edição do Windows que você está usando

Uso das informações

Essas informações são usadas para fornecer o serviço de atualização. Elas também são usadas para gerar estatísticas agregadas que nos ajudam a analisar tendências e melhorar nossos produtos e serviços. Elas não são usadas para identificar, contatar ou fazer propaganda para você.

Faça suas escolhas e controle

Se você optar por configurações expressas ao instalar o Windows, a Windows verificará, baixará e instalará atualizações de aplicativos automaticamente, mesmo que você tenha saído da Windows Store. Se

você desabilitar as atualizações automáticas de aplicativos, poderá escolher se deseja ou não instalar uma atualização de aplicativo ao entrar na Windows Store.

Para desativar atualizações automáticas de aplicativos:

1. Abra a Windows Store
2. Passe o dedo pela borda direita da tela e toque em **Configurações**.

   Se você estiver usando um mouse, aponte para o canto inferior direito da tela e clique em **Configurações**.
3. Toque ou clique em **Atualizações de aplicativo**.
4. Toque ou clique em **Atualizar automaticamente meus aplicativos** para desabilitar atualizações automáticas de aplicativos.

Para saber o que a versão mais recente do aplicativo pode fazer e quando um aplicativo foi atualizado, você pode examinar a Página de Descrição do Produto do aplicativo na Windows Store.

Permissão para os aplicativos da Loja

O que este recurso faz

Muitos aplicativos que você instala a partir da Windows Store são projetados para aproveitar os recursos de hardware e software específicos do seu computador. Por exemplo, um aplicativo de foto pode precisar usar sua webcam e um guia de restaurante pode ser necessário para saber sua localização para fornecer recomendações próximas.

Informações coletadas, processadas ou transmitidas

Segue uma lista de recursos dos quais os aplicativos devem revelar o uso:

- Sua conexão de internet. Permite que o aplicativo se conecte à internet.
- Conexões de entrada através de um firewall. Permite que o aplicativo envie informações para ou a partir do seu computador através de um firewall.

- Uma rede doméstica ou corporativa. Permite que o aplicativo envie informações entre seu computador e outros computadores na mesma rede
- Suas bibliotecas de fotos, vídeos, músicas ou documentos. Permite que o aplicativo acesse, altere ou exclua arquivos em suas bibliotecas. Isso inclui acesso a dados tradicionais incorporados a esses arquivos, como informações de locais em fotos.
- Armazenamento removível. Permite que o aplicativo acesse, adicione, altere ou exclua arquivos em um disco rígido externo ou dispositivo portátil.
- Suas credenciais do Windows. Permitem que o aplicativo use suas credencias para autenticar e obter acesso a uma intranet corporativa.
- Certificados armazenados em seu computador ou em um cartão inteligente. Permite que o aplicativo use certificados para conectar-se com segurança às organizações como bancos, agências governamentais ou seu empregador.
- Recurso de mensagens de texto do computador. Permite que o aplicativo envie e receba as mensagens de texto.
- Sua webcam e microfone. Permite que o aplicativo tire fotos e grave áudio e vídeo.
- Sua localização. Permitir que o aplicativo determine sua localização aproximada com base em um sensor GPS ou informações de rede.
- Recurso de comunicação em campo próximo no seu computador. Permite que o aplicativo se conecte a outros dispositivos próximos que o mesmo aplicativo está executando.
- Seus dispositivos portáteis. Permite que o aplicativo se comunique com os dispositivos como seu celular, câmera digital ou player de música portátil.

Suas informações em um dispositivo portátil. Permite que o aplicativo acesse, adicione ou exclua contatos, calendários, tarefas, notas, status ou toque no seu dispositivo portátil.

- Sua conta de banda larga móvel. Permite que o aplicativo gerencie sua conta de banda larga móvel.

Você visualizará as características de uso do aplicativo listadas na página de Descrição do Aplicativo. Se você instalar um aplicativo, o Windows permitirá que ele use esses recursos, exceto localização, mensagens de texto, webcam e microfone, que são considerados extremamente confidenciais. Quando um aplicativo solicita acesso a um desses recursos confidenciais pela primeira vez, o Windows pergunta se você deseja permitir que o aplicativo os utilize. Você pode alterar se o aplicativo pode utilizá-lo a qualquer momento.

Além das permissões acima, se um aplicativo solicitar informações de um dispositivo que armazena informações sobre você e sobre seu comportamento, o Windows perguntará se você permite que o aplicativo utilize esse dispositivo. Por exemplo, se você se conectar a um dispositivo de atividades físicas que rastreia sua localização, o Windows perguntará se você permite que o aplicativo o acesse.

Uso das informações

O uso desses recursos por cada aplicativo estará sujeito às práticas de privacidade de seus desenvolvedores. Se um aplicativo usar um dos recursos sigilosos descritos acima, ficará disponível um link para a política de privacidade do fornecedor do aplicativo na página de Descrição do Aplicativo na Loja.

Faça suas escolhas e controle

Você pode visualizar quais recursos um aplicativo requer na Loja antes de instalá-lo. Windows perguntará se você deseja permitir ou negar o acesso aos recursos mais sensíveis (localização, mensagens de texto, webcam e microfone) antes de cada aplicativo utilizá-los.

Quando você visualiza a página de Descrição do Aplicativo do aplicativo na Windows Store, existirá uma lista abreviada dos recursos usados pelo aplicativo na parte inferior da coluna esquerda. Você pode visualizar a lista completa na página de Detalhes da Descrição do Aplicativo. Após instalar um aplicativo, você pode visualizar a lista

completa de recursos que ele usa a qualquer momento e controla seu acesso aos especialmente sensíveis. Para fazer isso, abra o aplicativo, abra **Configurações**e, em seguida, selecione **Permissões**.

Recomendações personalizadas de pesquisa e aplicativos da Loja

O que este recurso faz

Quando você navega ou pesquisa aplicativos na Windows Store, a Microsoft fornece recomendações e resultados de pesquisa para ajudar a localizar aplicativos que sejam relevantes para você.

Informações coletadas, processadas ou transmitidas

Para ajudar a aperfeiçoar os resultados da pesquisa, a Windows Store envia informações à Microsoft sobre como você interage com a pesquisa, incluindo o que você pesquisa e os resultados da pesquisa selecionados. O Windows Search também envia um identificador associado à sua conta da Microsoft para fornecer resultados de pesquisa personalizados com base em suas interações com o Bing e com outros produtos e serviços da Microsoft. Você pode optar por não obter resultados personalizados; nesse caso, o identificador não será enviado.

Uso das informações

A Loja usa o identificador associado à sua conta da Microsoft para fornecer resultados personalizados de pesquisa e recomendações com base nas suas interações com a Loja e com outros produtos e serviços da Microsoft, como o Bing e a Windows Store. Isso inclui algumas informações, como os aplicativos comprados, as informações de perfil fornecidas na sua conta da Microsoft e suas classificações e avaliações de aplicativos. Essas informações também podem ser usadas para personalizar outros produtos e serviços da Microsoft.

Faça suas escolhas e controle

Quando você está conectado ao Windows com uma conta da Microsoft, os resultados e recomendações personalizados da Windows Store são ativados por padrão. Você pode optar por não obter resultados e recomendações personalizados da Loja na seção **Preferências** das configurações da Loja.

Ajuda a aprimorar a Windows Loja enviando URLs para o conteúdo da Web que os aplicativos usam

O que este recurso faz

Alguns aplicativos obtidos da Loja são parecidos com sites e podem expor o computador a softwares potencialmente não seguros, como malware. Se você ativar esse recurso, ele coletará informações sobre o conteúdo da Web usado por esses aplicativos para ajudar a Microsoft a diagnosticar comportamento potencialmente não seguro. Por exemplo, a Microsoft pode usar essas informações para remover um aplicativo da Loja.

Informações coletadas, processadas ou transmitidas

Se você enviar as informações sobre o conteúdo da Web usado por seus aplicativos, a Microsoft coletará informações sobre os tipos de conteúdo e as URLs que esses aplicativos acessam quando são utilizados. Isso pode nos ajudar a identificar quais desses aplicativos estão recebendo conteúdo de sites mal-intencionados ou não seguros. Os relatórios enviados para a Microsoft incluem informações, como o nome ou identificador do aplicativo, os URLs completos dos endereços que o aplicativo acessa e os URLs completos indicam qualquer JavaScript que o aplicativo acesse. O Windows gera aleatoriamente um número chamado GUID (identificador global exclusivo) que é enviado para a Microsoft com cada relatório. O GUID nos permite determinar quais dados são enviados de um computador particular ao longo do tempo. O GUID não contém qualquer informação pessoal e não é usado para identificar você.

Para proteger sua privacidade, as informações enviadas à Microsoft são criptografadas. As informações que podem ser associadas à página inicial que esses aplicativos acessam, como termos ou dados de pesquisa inseridos nos aplicativos, podem ser incluídos. Por exemplo, se você procura uma palavra em um aplicativo de dicionário, a palavra procurada pode ser incluída mas informações enviadas para a Microsoft como parte do endereço completo acessado pelo aplicativo. A Microsoft filtra esses endereços para tentar remover as informações pessoais, onde possível.

Uso das informações

A Microsoft periodicamente revisa as informações enviadas para ajudar a detectar os aplicativos que podem estar interagindo com conteúdo inseguro da Web, como endereços e scripts prejudiciais. Podemos usar essas informações para executar uma ação contra aplicativos potencialmente prejudiciais. Endereços de conteúdo da Web podem conter involuntariamente informações pessoais, mas essas informações não são usadas para identificar, entrar em contato ou direcionar publicidade para você. Usamos o GUID para determinar o grau de disseminação dos comentários que recebemos e como priorizá-los. Por exemplo, o GUID permite à Microsoft distinguir entre funcionamento potencialmente inseguro ocorrendo 100 vezes em um único computador e o mesmo funcionamento ocorrendo uma vez em cada um dos 100 computadores.

Faça suas escolhas e controle

Se você escolher as configurações expressas ao instalar o Windows, o Windows enviará informações sobre o conteúdo da Web usado pelos seus aplicativos da Loja criados em JavaScript. Se você optar por personalizar configurações, poderá controlar essa configuração selecionando **Usar o serviços SmartScreen online para proteger-se contra conteúdo mal-intencionado em sites carregados por aplicativos da Windows Store e pelo Internet Explorer, bem como contra downloads mal-intencionados,** , em **Ajudar a melhorar os produtos e serviços da Microsoft**. Após a instalação, você pode alterar essa configuração em **Privacidade** nas configurações do computador.

Início da página

Serviço de Tempo do Windows

O que este recurso faz

O recurso Windows Serviço de Tempo sincroniza automaticamente a hora dos seus computadores com um servidor de horário em uma rede.

Informações coletadas, processadas ou transmitidas

O serviço se conecta a um servidor de horário através da internet ou uma rede local usando o protocolo SNTP padrão da indústria. Por

padrão, esse serviço é sincronizado com o time.windows.com uma vez por semana. Nenhuma outra informação além das informações do computador padrão é enviada para o servidor de horário.

Uso das informações

As informações são usadas pelo serviço Tempo do Windows para sincronizar automaticamente o horário local do computador.

Faça suas escolhas e controle

O serviço Tempo doWindows está ativado por padrão. Você pode desativar esse recurso em **Data e Hora** nas configurações do computador. A desativação do serviço Tempo do Windows não tem efeito direto em aplicativos ou em outros serviços, mas, sem uma fonte de tempo confiável, o relógio local do computador poderá sair de sincronia com outros computadores na rede ou internet. Os aplicativos e serviços que dependem de horário poderão falhar ou interromper o funcionamento correto se houver uma discrepância significativa entre os computadores em rede.

Início da página

Windows Solução de Problemas

O que este recurso faz

Windows Solução de Problemas permite que você diagnostique e corrija problemas comuns no seu computador.

Informações coletadas, processadas ou transmitidas

Após executar o pacote de solução de problemas, os resultados são salvos no seu computador. Esses resultados podem conter informações pessoais, como seu nome de usuário ou o nome de um dispositivo. Windows Solução de Problemas pode ajudar você a pesquisar por soluções de problemas em Windows Ajuda e Windows comunidades online. As palavras-chave associadas ao problema serão enviadas para a Microsoft para ajudar a localizar uma solução. Por exemplo, se sua impressora não estiver funcionando corretamente e você estiver buscando ajuda, as palavras "impressora", "imprimir" e "impressão" são enviadas para a Microsoft.

Uso das informações

A Microsoft usa as informações coletadas da Solução de Problemas do Windows para ajudar a solucionar problemas que nossos usuários encontrarem.

Faça suas escolhas e controle

Para excluir resultados de solução de problemas, vá para Soluções de Problemas no Painel de Controle. Clique em **Exibir histórico**, selecione um resultado e clique em **Excluir**.

Início da página

Pastas de trabalho

O que este recurso faz

As pastas de trabalho são pastas do computador que são sincronizadas automaticamente com o servidor de arquivos do espaço de trabalho.

Informações coletadas, processadas, armazenadas ou transmitidas

Quando você salva um arquivo em uma pasta de trabalho, o arquivo é sincronizado automaticamente com um servidor de arquivos gerenciado pelo espaço de trabalho. Os arquivos salvos na pasta de trabalho de outros computadores serão sincronizados ao seu computador.

Uso das informações

O Windows envia e recebe os arquivos nas pastas de trabalho para mantê-las sincronizadas. O uso das informações armazenadas em servidores do espaço de trabalho estão sujeitas à política de privacidade do espaço de trabalho.

Faça suas escolhas e controle

Você pode gerenciar a conexão do computador com pastas de trabalho em **Local de trabalho** nas configurações do computador.

Início da página

Local de trabalho

O recurso Local de Trabalho permite que você conecte seu dispositivo ao Windows Intune (requer uma assinatura separada da Microsoft) ou a outro serviço de gerenciamento de dispositivos de terceiros. Se você permitir que o administrador de sua empresa gerencie seu computador usando o recurso Local de Trabalho, ele poderá realizar determinadas tarefas, como especificar políticas de segurança para o computador, instalar aplicativos, exibir determinadas configurações e informações sobre o computador e outras tarefas de gerenciamento. Consulte a política de privacidade ou o administrador de sistema da sua empresa para obter mais informações sobre o uso desse recurso na empresa.

Informações coletadas, processadas ou transmitidas

Quando você configura e usa o recurso Local de Trabalho, seu computador se comunica com o serviço de gerenciamento de dispositivos usado pela empresa, que pode ser hospedado pela Microsoft. As credenciais que você insere para se conectar ao seu local de trabalho são enviadas ao serviço.

Uso das informações

As informações enviadas ao serviço de gerenciamento de dispositivos são usadas para estabelecer uma conexão entre o serviço e o seu computador, bem como para permitir a instalação de um aplicativo de autoatendimento da Windows Store. Consulte a política de privacidade ou o administrador do sistema de sua empresa para obter mais informações sobre o aplicativo de autoatendimento.

Faça suas escolhas e controle

Se sua empresa usa o recurso Local de Trabalho, você pode conectar ou desconectá-lo nas configurações do computador em **Rede**. Depois que você conectar seu computador ao serviço, poderá exibir informações sobre a conexão ou desconectar-se a qualquer momento.

Início da página

Para obter informações atualizadas sobre as práticas de processamento de dados da Microsoft, leia a Política de Privacidade da Microsoft. Aqui você também pode saber mais sobre as ferramentas mais recentes que fornecemos para acessar e controlar seus dados e como entrar em contato conosco se você tiver uma consulta sobre privacidade.

Política de Privacidade do Windows 8.1 e do Windows Server 2012 R2

Destacar Política Recursos Aplicativos Servidor

Observe que esta página é um suplemento da política de privacidade do Windows 8.1 e do Windows Server 2012 R2 ("Política de privacidade do Windows"), que inclui quatro seções:

- Destaques
- Política, que é a política de privacidade completa do Windows 8.1, com links para políticas de privacidade de recursos do Windows que têm suas próprias políticas autônomas
- Suplemento de recursos, que descreve os recursos com impacto na privacidade do Windows 8.1 e do Windows Server 2012 R2
- **Suplemento de aplicativos** (esta página), que descreve os aplicativos que impactam a privacidade no Windows 8.1; inclui links para políticas de privacidade aplicáveis a cada aplicativo
- Suplemento de servidores, que descreve os recursos adicionais com impacto na privacidade do Windows Server 2012 R2

Para entender as práticas de coleta e uso de dados relevantes a

determinado recurso ou serviço do Windows, você deve ler a política de privacidade completa e todo suplemento ou política autônoma aplicável.

Se optar por participar do CEIP (Programa de Aperfeiçoamento da Experiência do Usuário) quando configurar o seu computador, esses aplicativos coletarão informações em um relatório sobre como você usa cada aplicativo e também sobre o desempenho e a confiabilidade do aplicativo. A Microsoft usa as informações do CEIP para aprimorar seus produtos e serviços. Essas informações não serão usadas para identificar, contatar ou fazer propaganda para você. Você também pode desativar o CEIP nas configurações do computador. Para saber mais, veja Política de privacidade do CEIP.

Os links a seguir levam às políticas de privacidade aplicáveis a cada aplicativo:

Alarme

Calculadora

Calendário

Câmera

Finanças

Alimentação

Jogos

Saúde

Ajuda e Dicas

Email

Mapas

Músicas

Notícias

Pessoas

Leitor

Lista de Leitura

Verificação

Skype

Gravador de Som

Esportes

Viagem

Vídeo

Clima

Para obter informações atualizadas sobre as práticas de processamento de dados da Microsoft, leia a Política de Privacidade da Microsoft. Aqui você também pode saber mais sobre as ferramentas mais recentes que fornecemos para acessar e controlar seus dados e como entrar em contato conosco se você tiver uma consulta sobre privacidade.

Política de Privacidade do Windows 8.1 e do Windows Server 2012 R2

Nesta página

Esta página é um suplemento da política de privacidade do Windows 8.1 e do Windows Server 2012 R2 ("Política de privacidade do Windows"). A política de privacidade contém estas seções:

- Destaques
- Política, que é a política de privacidade completa do Windows 8.1 com links para políticas de privacidade de recursos do Windows que possuem políticas autônomas
- Suplemento de recursos, que descreve os recursos com impacto na privacidade do Windows 8.1 e no Windows Server 2012 R2
- Suplemento de aplicativos, que descreve os aplicativos com impacto na privacidade do Windows 8.1
- **Suplemento de servidores** (esta página), que descreve os recursos adicionais com impacto na privacidade do Windows Server 2012 R2

Para entender as práticas de coleta e uso de dados relevantes para um

Experiência do Usuário doWindows) e WER (Relatório de Erros do Windows)

Log de Inventário de Software

determinado recurso ou serviço do Windows, você deve ler a política de privacidade completa do Windows e qualquer suplemento aplicável. Além disso, leia este white paper para administradores.

Para obter informações sobre o impacto na privacidade dos recursos incluídos no Windows Server 2012 R2 Essentials, consulte a Política de privacidade do Windows Server 2012 R2 Essentials e do Windows Server Essentials Experience.

Log de Acesso do Usuário

O que este recurso faz

O UAL (Log de Acesso de Usuário) coleta e agrega registros de solicitações de clientes de funções de servidor (tanto do usuário quanto do dispositivo), bem como de produtos instalados (se registrados com o UAL) no servidor local. Esses dados – na forma de endereços IP, nomes de usuários e, em alguns casos, nomes de hosts e/ou identidades de máquina virtual – ficam armazenados nos bancos de dados ESE (Mecanismo de Armazenamento Extensível) locais e só estão acessíveis aos administradores. O UAL tem um provedor WMIv2 e cmdlets associados do Windows PowerShell para recuperar dados de acesso do usuário destinados ao gerenciamento de direitos de CAL (Licença de Acesso para Cliente) do cliente offline, onde os registros reais de solicitações exclusivas de clientes são críticos.

Informações coletadas, processadas ou transmitidas

Endereços IP, nomes de usuários e, em alguns casos, nomes de hosts (se a função DNS estiver instalada), bem como identidades de máquina virtual (se a função Hyper–V estiver instalada), são coletados localmente no servidor quando o UAL é ativado. Os dados coletados não são enviados à Microsoft.

Uso das informações

Os dados do UAL são disponibilizados aos administradores através de bancos de dados ESE locais, do provedor WMI e de cmdlets do Windows PowerShell. O Windows não utiliza esses dados fora do recurso UAL.

Faça suas escolhas e controle

O UAL está habilitado por padrão. O serviço do UAL pode ser interrompido e iniciado enquanto o servidor está em execução. Para desabilitar o UAL permanentemente, abra o Windows PowerShell, digite Disable-UAL e reinicie o servidor. Um administrador pode excluir todos os dados de histórico coletados interrompendo o serviço, desabilitando o UAL e excluindo todos os arquivos da pasta %SystemRoot%\System32\LogFiles\SUM.

Início da página

Gerenciador do Servidor

O que este recurso faz

O Gerenciador do Servidor é uma ferramenta de gerenciamento que permite a um administrador monitorar um ou vários servidores e ver o status geral ou específico de uma função, a fim de realizar tarefas de gerenciamento e acessar outras ferramentas de gerenciamento de servidores.

Informações coletadas, processadas ou transmitidas

O Gerenciador do Servidor coleta os seguintes tipos de informações de um servidor gerenciado pelo administrador:

- **Informações gerais sobre o servidor:** nome NetBios e FQDN (nome de domínio totalmente qualificado), credenciais de conta inseridas no recurso "Gerenciar como", endereço IPv4, endereço IPv6, status da capacidade de gerenciamento, descrição, versão do sistema operacional, tipo, última atualização, processadores, memória, nome do cluster, tipo de objeto do cluster, status da ativação, SKU, arquitetura do sistema operacional, fabricante, configuração do CEIP (Programa de Aperfeiçoamento da Experiência do Usuário) e configuração do WER (Relatório de Erros do Windows).

- **Eventos:** ID, gravidade, origem, log, data e hora de cada evento do Windows e outros logs que o administrador escolher.

- **Todos os serviços:** nome, status e tipo de início.

- **Informações sobre a função de servidor:** resultados do BPA

(Analisador de Práticas Recomendadas) para funções que estão instaladas no servidor.

- **Informações sobre desempenho:** exemplos de contadores de desempenho e notificações sobre uso de CPU e memória disponível.

Uso das informações

Essas informações são armazenadas no Gerenciador do Servidor e não são enviadas à Microsoft. Elas são exibidas no Gerenciador do Servidor para ajudar os administradores a monitorar os sistemas.

Faça suas escolhas e controle

O administrador pode aceitar ou recusar coletar dados de qualquer servidor, exceto do servidor local, adicionando o servidor ao Gerenciador do Servidor ou removendo-o. O administrador pode explicitamente fornecer credenciais para se conectar a um servidor remoto. O Gerenciador do Servidor solicita ao administrador consentimento explícito para armazenar as credenciais localmente no Gerenciador do Servidor, e o administrador pode excluir essas credenciais a qualquer momento.

Início da página

Serviços de Federação do Active Directory

O que este recurso faz

O recurso AD FS (Serviços de Federação do Active Directory) é uma solução de federação e logon único pronta para a empresa, para aplicativos locais ou baseados em rede. Com o AD FS, os administradores podem habilitar os usuários a colaborar em diferentes organizações e acessar facilmente os aplicativos em redes locais ou em outras redes, ao mesmo tempo em que a segurança dos aplicativos é mantida. O AD FS usa um serviço de token de segurança que utiliza o AD DS (Serviços de Domínio Active Directory) para autenticar usuários e emitir para eles tokens de segurança usando vários protocolos. O token é assinado digitalmente e contém declarações sobre o usuário, que provêm do AD DS, do protocolo LDAP, do SQL Server ou de um repositório personalizado.

Informações coletadas, processadas ou transmitidas

As credenciais do usuário são coletadas quando o usuário faz autenticação com o AD FS. As credenciais são imediatamente enviadas aos Serviços de Domínio Active Directory para autenticação, e o AD FS não as armazena localmente. Os atributos do usuário nos Serviços de Domínio Active Directory podem ser usados para gerar declarações de saída, dependendo das regras de declaração configuradas pelo administrador do AD FS. As declarações de saída serão enviadas para parceiros confiáveis com os quais o administrador do AD FS tenha estabelecido uma relação de confiança. Nenhuma informação é enviada à Microsoft.

Uso das informações

A Microsoft não terá acesso a essas informações. As informações destinam-se ao uso exclusivo do cliente.

Faça suas escolhas e controle

Use o AD FS se quiser que ele colete ou envie dados para parceiros confiáveis.

Início da página

Gerenciamento de endereço IP

O que este recurso faz

O IPAM (Gerenciamento de Endereço IP) permite que os administradores do servidor rastreiem o endereço IP, nome do host e identificador do cliente (como o endereço MAC no IPv4 e o DUID no IPv6) de computadores ou dispositivos em uma rede com informações de logon do usuário.

Informações coletadas, processadas ou transmitidas

O servidor IPAM coleta logs de auditoria e eventos de servidores DHCP, controladores de domínio e servidores de política de rede, e depois armazena localmente o endereço IP, nome do host, identificador do cliente e nome do usuário conectado. O administrador do servidor pode pesquisar os logs coletados com base no endereço IP, identificador do cliente, nome do host e nome de usuário usando o

console do IPAM. Nenhuma dessas informações é enviada à Microsoft.

Uso das informações

A Microsoft não tem acesso a essas informações. As informações destinam-se ao uso exclusivo do cliente.

Faça suas escolhas e controle

O IPAM não é instalado por padrão e deve ser instalado pelo administrador do servidor. Depois que o IPAM é instalado, a auditoria de endereço IP é habilitada automaticamente. Para desabilitar a auditoria de endereço IP em um servidor onde o IPAM esteja instalado, inicie o Agendador de Tarefas no servidor IPAM, navegue até Tarefa de Auditoria em Microsoft\Windows\IPAM e desabilite a tarefa.

Início da página

Acesso Remoto Unificado

O que este recurso faz

O Acesso Remoto Unificado permite que usuários remotos se conectem a uma rede privada, como uma rede corporativa, através da Internet. O Acesso Remoto Unificado usa o DirectAccess para fornecer conectividade ininterrupta e transparente com redes corporativas a computadores cliente remotos que executam o Windows 8. Ele também fornece funcionalidade de Serviço de Acesso Remoto (RAS), que são serviços tradicionais de VPN, incluindo conectividade site a site de rede local ou outra.

Informações coletadas, processadas ou transmitidas

Para monitoramento de usuários do Acesso Remoto Unificado, o servidor DirectAccess armazena os detalhes dos usuários remotos que se conectam à rede privada. Isso inclui informações como nome do host do usuário remoto, nome de usuário do Active Directory e endereço IP público do cliente remoto (se o cliente estiver atrás de uma NAT (conversão de endereços de rede), será o endereço IP público). Esses dados também podem ser armazenados nos servidores RADIUS/WID (Banco de Dados Interno do Windows), apenas com o consentimento do administrador. Somente um administrador do

DirectAccess (um usuário de domínio com uma conta de administrador local) que acessa um servidor pode acessar e ver essas informações.

Uso das informações

Essas informações serão usadas pelo administrador para solucionar problemas de conectividade do cliente e também para fins de auditoria ou conformidade. Nenhuma informação é enviada à Microsoft.

Faça suas escolhas e controle

O monitoramento de cliente remoto é ativado por padrão e não pode ser desabilitado. Os dados de monitoramento só são armazenados nos servidores RADIUS/WID quando o administrador configura a contabilização para usar qualquer uma dessas opções. Se o administrador não configurar a contabilização, nenhuma dessas informações será armazenada. O administrador também pode configurar a contabilização em um servidor de acesso remoto para não armazenar informações de nome de usuário e endereço IP.

Início da página

Serviços de Área de Trabalho Remota

O que este recurso faz

O RDS (Serviços de Área de Trabalho Remota) fornece uma plataforma para ajudar as empresas a implementar uma estratégia de área de trabalho centralizada, gerenciar áreas de trabalho e aplicativos, bem como aprimorar a flexibilidade e a conformidade, ao mesmo tempo em que aperfeiçoa a segurança dos dados.

Informações coletadas, processadas ou transmitidas

Para monitoramento de usuários de RDS, o servidor Host da Sessão da Área de Trabalho Remota armazena informações sobre usuários remotos que se conectam a recursos de RDS. Isso inclui informações como nome do host do usuário remoto, nome de usuário do Active Directory e endereço IP público do cliente remoto (se o cliente estiver atrás de uma NAT (conversão de endereços de rede), será o endereço IP público). Esses dados são armazenados automaticamente nos servidores WID (Banco de Dados Interno do Windows) ou SQL quando os usuários se conectam. Nenhuma informação é enviada à

Microsoft. Somente um usuário de domínio com uma conta de administrador local pode acessar e exibir essas informações.

Uso das informações

Essas informações serão usadas pelo administrador para solucionar problemas de conectividade do cliente e também para fins de auditoria interna ou conformidade. Nenhuma informação é enviada à Microsoft.

Faça suas escolhas e controle

O monitoramento de cliente é habilitado por padrão e não pode ser desabilitado. As informações de monitoramento são armazenadas no servidor WID/SQL.

Início da página

CEIP (Programa de Aperfeiçoamento da Experiência do Usuário doWindows) e WER (Relatório de Erros do Windows)

O que este recurso faz

Para obter mais informações sobre esses recursos, consulte a guia Suplemento de recursos ou este white paper para administradores.

Informações coletadas, processadas ou transmitidas

Para saber as informações específicas que são coletadas, processadas e transmitidas por esses recursos, consulte o Programa de Aperfeiçoamento da Experiência do Usuário e o WER na guia Suplemento de recursos .

Uso das informações

Para saber como usamos as informações que são coletadas por esses recursos, consulte o Programa de Aperfeiçoamento da Experiência do Usuário e o WER na guia Suplemento de recursos .

Faça suas escolhas e controle

O Programa de Aperfeiçoamento da Experiência do Usuário permanece desabilitado por padrão, e o WER é definido como padrão para consultar você antes de enviar relatórios de falhas à Microsoft. Você pode habilitar ou desabilitar o Programa de Aperfeiçoamento da Experiência do Usuário no Gerenciador do Servidor e no Painel de

Controle, além de usar os métodos de controle de linha de comando. O WER pode ser controlado usando apenas os métodos de linha de comando.

Para ativar ou desativar o CEIP via Painel de Controle, clique em **Sistema e Manutenção**e em **Relatórios de Problemas e Soluções**. Em seguida, em **Veja também**, clique em **Configurações do Programa de Aperfeiçoamento da Experiência do Usuário** para acessar a opção de ativar ou desativar o CEIP.

Controles do Gerenciador do Servidor

Servidor local

- Habilitar o Programa de Aperfeiçoamento da Experiência do Usuário
  Abra Gerenciador do Servidor e selecione **Servidor local**. Clique no link Programa de Aperfeiçoamento da Experiência do Usuário, selecione **Sim, Aperfeiçoamento da Experiência do Usuário** na caixa de diálogo e clique em **OK**.

- Desabilitar o Programa de Aperfeiçoamento da Experiência do Usuário
  Abra Gerenciador do Servidor e selecione **Servidor local**. Clique no link Programa de Aperfeiçoamento da Experiência do Usuário, selecione **Não quero participar** na caixa de diálogo e clique em **OK**.

- Habilitar o WER
  Abra Gerenciador do Servidor e selecione **Servidor local**. Clique no link do Relatório de Erros do Windows, selecione **Sim, enviar relatórios resumidos automaticamente**e clique em **OK**.

- Desabilitar o WER
  Abra Gerenciador do Servidor e selecione **Servidor local**. Clique no link do Relatório de Erros do Windows, selecione **Não quero participar; não perguntar novamente**e clique em **OK**.

Vários computadores

- Habilitar o Programa de Aperfeiçoamento da Experiência do Usuário

Abra Gerenciador do Servidor e selecione **Todos os Servidores**. No bloco Servidores, selecione todos os servidores (Ctrl+A), clique com o botão direito do mouse e selecione **Configurar Comentários Automáticos do Windows** . Na guia Programa de Aperfeiçoamento da Experiência do Usuário, selecione **Sim, desejo participar (Recomendado)**. Aplique essa configuração a todos os servidores marcando a caixa de seleção ao lado de Nome do Servidor no controle Selecionar Servidores e depois clique em **OK**.

- Desabilitar o Programa de Aperfeiçoamento da Experiência do Usuário
  Abra Gerenciador do Servidor e selecione Todos os Servidores. No bloco Servidores, selecione todos os servidores (Ctrl+A), clique com o botão direito do mouse e selecione **Configurar Comentários Automáticos do Windows** . Na guia Programa de Aperfeiçoamento da Experiência do Usuário, selecione **Não quero participar**. Aplique essa configuração a todos os servidores marcando a caixa de seleção ao lado de Nome do Servidor no controle Selecionar Servidores e depois clique em **OK**.

- Habilitar o WER
  Abra Gerenciador do Servidor e selecione **Todos os Servidores**. No bloco Servidores, selecione todos os servidores (Ctrl+A), clique com o botão direito do mouse e selecione **Configurar Comentários Automáticos do Windows** . Na guia Relatório de Erros do Windows, selecione **Sim, enviar relatórios resumidos automaticamente (Recomendado)**. Aplique essa configuração a todos os servidores marcando a caixa de seleção ao lado de Nome do Servidor no controle Selecionar Servidores e depois clique em **OK**.

- Desabilitar o WER
  Abra Gerenciador do Servidor e selecione **Todos os Servidores**. No bloco Servidores, selecione todos os servidores (Ctrl+A), clique com o botão direito do mouse e selecione **Configurar Comentários Automáticos do Windows** . Na guia Relatório de Erros do Windows, selecione **Não quero participar**. Aplique essa configuração a todos os servidores marcando a caixa de

seleção ao lado de Nome do Servidor no controle Selecionar Servidores e depois clique em **OK**.

Início da página

Log de Inventário de Software

O que este recurso faz

O SIL (Log de Inventário de Software) fornece um novo conjunto de classes WMI e cmdlets do PowerShell para simplificar o inventário básico da edição do sistema operacional Windows Server, o software instalado no Windows Server e as características do servidor em que o software é executado. Além disso, o SIL tem a capacidade de coletar por hora, se habilitado por um administrador, dados do seu provedor WMI e encaminhá-los pela rede a um servidor de agregação, caso um seja especificado com o cmdlet Set-SilLogging -TargerUri.

Informações coletadas, processadas ou transmitidas

Os dados podem ser transmitidos para um servidor de agregação pela rede, caso isso tenha sido configurado por um administrador. Por padrão, nada é coletado, processado ou transmitido. Esses dados incluem:

- O nome e a edição do sistema operacional instalado do Windows Server.
- Uma lista de nomes, versões e fornecedores de todos os softwares instalados no servidor e a data em que eles foram instalados.
- O nome de domínio totalmente qualificado do sistema do servidor.
- O número, o tipo e o fabricante de processadores, processadores lógicos e núcleos instalados ou atribuídos ao sistema do servidor.

Dados coletados e processados, mas não transmitidas por padrão, mesmo que a tarefa por hora esteja habilitada e um agregador de destino seja especificado pelo administrador:

- A classe MsftSil_UalAccess e o cmdlet Get-SilUalAccess

processam a contagem do total de usuários e dispositivos exclusivos de cada produto registrado no recurso UAL (Log de Acesso do Usuário) a partir de dois dias antes da consulta. Essas são apenas contagens, nenhuma informação de usuário ou dispositivo é gerada ou transmitida. O SIL precisa processar as informações de usuário e dispositivo, de classes UAL, para calcular as contagens propriamente ditas. Esses dados podem ser acessados apenas por um administrador do computador local. O SIL não altera o acesso necessário para as APIs do UAL.

Os dados coletados não são enviados à Microsoft.

Uso das informações

Os provedores WMI de SIL agregam dados fornecidos por outras APIs já existentes no sistema. Os dados podem ser transmitidos para um servidor para agregação adicional pela rede, caso isso tenha sido configurado por um administrador. Por padrão, nada é coletado, processado ou transmitido. No caso da classe MsftSil_UalAccess e do cmdlet Get-SilUalAccess, os dados processados fornecem uma contagem do total de usuários e dispositivos exclusivos de cada função ou produto registrado no recurso UAL (Log de Acesso do Usuário) a partir de dois dias antes da coleta, mas não geram dados de identificação de usuário ou dispositivo. E, embora essa classe WMI e o cmdlet existam no sistema, eles não fazem parte do conteúdo SIL coletado e encaminhado a um agregador por hora quando o SIL é configurado para fazer isso por um administrador do sistema.

Faça suas escolhas e controle

A tarefa por hora do SIL está desabilitada por padrão. Todas as APIs do SIL estão disponíveis para consulta por padrão por administradores do sistema local. A tarefa por hora do SIL pode ser iniciada e interrompida enquanto o servidor está em execução com os cmdlets Start-SilLogging e Stop-SilLogging. O uso do cmdlet Set-SilLogging permite que os administradores do servidor definam a data e a hora do dia do início da tarefa por hora (o padrão é às 3h do sistema local), o URI (Uniform Resource Identifier) de um servidor de agregação de destino e a impressão digital de certificado necessários para garantir uma transmissão confiável dos dados.

Todas as definições de configuração do SIL, incluindo o início e a

interrupção da tarefa por hora, podem ser alteradas no Registro, o que deve ser feito somente quando o sistema é uma máquina virtual e apenas antes da primeira inicialização do sistema.

Início da página