Windows Information Protection helps enforce data policy at Microsoft

Windows Information Protection, formerly referred to as Enterprise Data Protection (EDP), helps people separate their work and personal data and keeps data encrypted wherever it's stored. Your employees can safely use both work and personal data on the same device without switching applications. Windows Information Protection helps prevent inadvertent data leaks by blocking data sharing through apps and services that are outside of your control. For example, employees can't send protected work files from a personal email account instead of their work account. They also can't accidently post confidential information from a corporate site into a tweet. Windows Information Protection also helps ensure that they aren't saving company information in a public cloud storage location.

Core Services Engineering (CSE, formerly Microsoft IT) began piloting Windows Information Protection with the release of Windows 10 Anniversary Update. We are moving forward with the Windows 10 Creators Update, and we are working with some of the new features in Windows Information Protection that help prevent an employee's personal applications from accessing corporate data and network resources.

Building information protection into Windows 10

Windows Information Protection can differentiate between personal and work information, determine which apps have access to it, and provide the necessary basic controls to determine what employees can do with work data, including where they can save work files or copy and paste text. Before the Windows 10 Anniversary Update, we relied on capabilities in other applications and platforms to help ensure that work data wasn't shared or leaked inadvertently.

One of the original design goals for Windows Information Protection was to offer basic functionality that helps predict accidental data leaks through the most-used paths, which represent most leak cases (80/20 rule). These paths include copy and paste errors and copying data to removable storage, for example.

Windows Information Protection is designed to coexist with advanced data loss prevention (DLP) capabilities found in Office 365 ProPlus, Azure Information Protection, and Azure Rights Management. Advanced DLP prevents printing, for example, or protects work data that is emailed outside your company. Figure 1 shows how the different tools overlap to provide information protection.

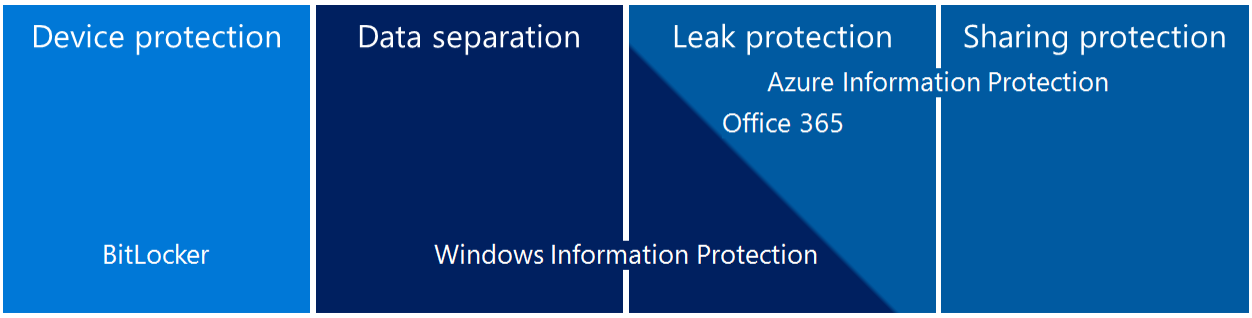

Figure 1. Windows Information Protection is part of a comprehensive information protection strategy

Configuring Windows Information Protection

There isn't anything to install—we simply turned Windows Information Protection on through the Windows Information Protection settings policy in System Center Configuration Manager (Configuration Manager) policy for domain-joined devices, and through Microsoft Intune for non-joined devices.

Using Configuration Manager and Microsoft Intune, it's easy for us to create and deploy Windows Information Protection policies. We can choose protected apps, set our protection mode, and choose how to find work data on the network.

Microsoft employees can sign up for a variety of pilot programs to help us gather feedback and test product usability. We're testing scenarios and configurations that apply Windows Information Protection policies to the personal and work devices of employees who signed up for the pilot deployment program. As we move closer to a broad Windows Information Protection deployment, we're considering rolling out different policies with different protection modes to separate user groups.

Understanding enlightened and unenlightened applications

Apps can be enlightened (also referred to as Windows Information Protection-aware) or unenlightened (also referred to as Windows Information Protection-unaware). The difference between the two is:

- Enlightened apps can differentiate between work and personal data and correctly determine which to protect, based on our policies.
- Unenlightened apps treat all data as work data and encrypt everything.

Several enlightened applications give employees the choice of handling their data as work or personal. Many of the Microsoft productivity applications—including Microsoft Edge; Internet Explorer 11; Office Mobile apps, including Word, Excel, PowerPoint, and Outlook Mail and Calendar; Microsoft Photos; Notepad; and Microsoft Paint—have the option to save a file as work or personal.

> *Note: In Windows 10, app developers can use a new set of APIs to create enlightened apps that can use and edit both work and personal data.*

Adding applications to a Windows Information Protection policy

Within our Windows Information Protection policy, we can add almost any application to the protected application list—even applications that are unenlightened. This list of apps tells Windows which apps can access Windows Information Protection-protected data, so the list doesn't have to be modified to open work data.

Enlightened apps are used to prevent work data from being moved to unprotected network locations and to avoid encrypting personal data. Unenlightened apps that are included in the Windows Information Protection protected application list will encrypt all files they create or modify. This means that Windows Information Protection could encrypt personal data and cause data loss when the data is retrieved. It is important that any unenlightened applications we add to the policy are used only to handle work data.

During our policy-creation process in Configuration Manager and Microsoft Intune, we chose out-of-the-box enlightened applications, including Microsoft Edge and Notepad, and internal line-of-business applications.

Configuration Manager includes a Create Configuration Item Wizard for Windows Information Protection that walks us through the process of configuring settings, which is shown in Figure 2.

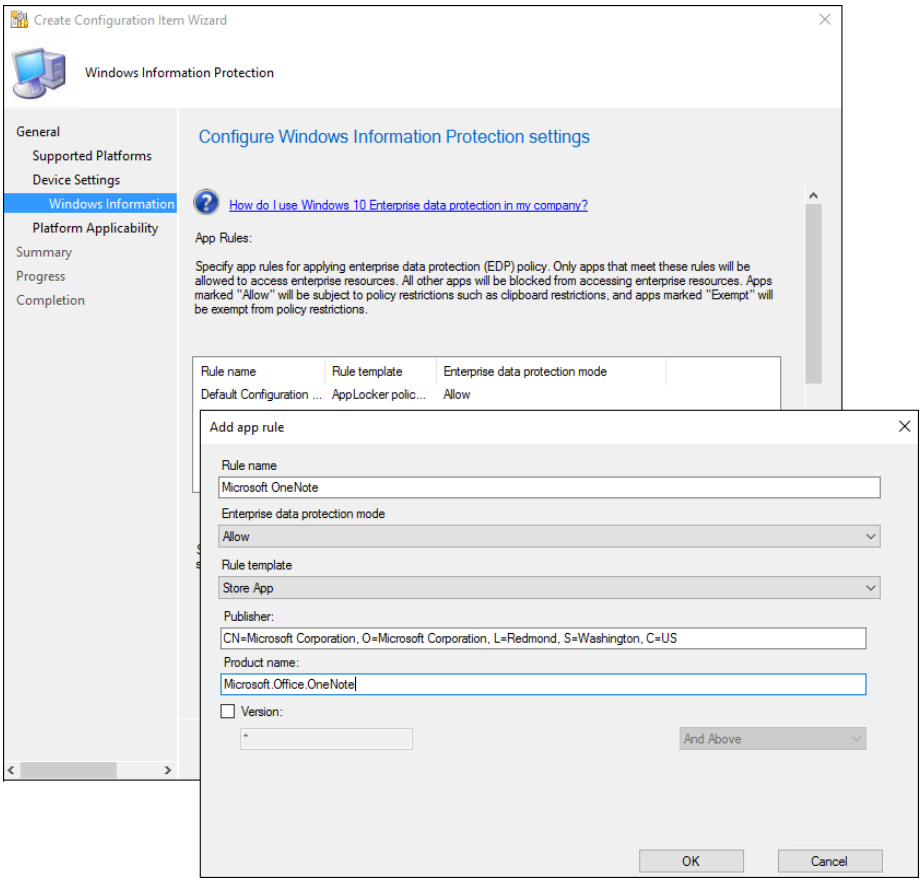

Figure 2. Using the System Center Configuration Manager wizard to add an application to a Windows Information Protection policy

Windows Information Protection helps protect the information handled by applications on the protected applications list by restricting functions such as copying or moving work data to personal apps or non-work locations, including websites, social media apps, personal email, personal cloud, and so on.

Protection and management modes

There are four different protection and management modes to choose from when creating a Windows Information Protection policy.

- **Hide Overrides.** Windows Information Protection looks for inappropriate data sharing practices and blocks employees from completing the action. This can include sharing work data with non-protected apps, sharing work data between apps, or trying to share data outside of our network. Hide Overrides mode is best in IT environments that are very structured or have stringent controls over the applications and websites that can be used to do work on employee devices.
- **Allow Overrides.** Windows Information Protection looks for inappropriate data sharing. It warns employees if they do something that is potentially unsafe; however, this mode lets the employee override the policy and share the data. Windows Information Protection then logs the event to an audit log that we can access through the reporting configuration service provider. Allow Overrides is good for structured IT environments, where you need to allow some exceptions. For example, an employee in marketing or PR may need to cut and paste information

into a social media site, which would normally be a blocked action. Allow Overrides is a good choice for IT environments that are trying out more stringent settings before moving to Hide Overrides mode.

- **Silent.** Windows Information Protection runs silently. It logs inappropriate data sharing without blocking anything that would've prompted employee interaction in Allow Overrides mode. Unallowed actions, like apps trying to access a network resource or Windows Information Protection-protected data, are allowed but audited. Silent mode is good choice for more open IT environments or where large groups of users, like testers or application developers, have legitimate reasons to perform actions that might be blocked under other circumstances. Silent mode is also good to use when an organization is thinking about implementing Allow Overrides or Hide Overrides mode, because the event log will offer information about the number of overridden or blocked events that implementing Windows Information Protection will cause.
- **Off.** Windows Information Protection is turned off and doesn't help to protect or audit data.

Our CSE pilot configuration for Windows Information Protection is Silent mode, but we also have pilot groups that are using Allow Overrides and Hide Overrides modes. As we move forward and plan to roll out Windows Information Protection across the broader environment, we are also looking at the effects of rolling out more than one protection mode. Using Windows Information Protection, we can create different policies for different user groups to create a more customized protection plan.

Identifying personal and work data

To protect data at the device level, we needed to identify personal data versus work data. Data is considered work data if it's copied from a known corporate location or written by a known corporate application. Protected apps can access work data and will prevent that data from being shared in non-protected or personal apps. For example, an employee can copy and paste protected information with other protected apps, but not with their personal apps. Windows Information Protection automatically identifies work data based on its origin. Data that is downloaded from a protected location—like SharePoint, a network file share, or a company website—is recognized as work data.

Encryption

Work data is automatically encrypted after it's saved on a device from an enlightened application or source, or if an employee identifies it as work data. Then, when the work data is written to disk, Windows Information Protection uses the Windows-provided Encrypting File System to protect it with an encryption key and associate it with the employee.

In an enlightened application, by default, documents are identified as personal unless information from a Windows Information Protection-protected source was copied or included in the file. From an unenlightened application that's configured as a work application in the Windows Information Protection policy, files are only saved as work files. Other unenlightened applications will only save files as personal files.

With Windows Information Protection, employees can use Windows File Explorer to see the protection status of a file and change it from work to personal or from personal to work. File protection states can't be changed by users that are piloting in Hide Overrides mode. For users that are piloting Allow Overrides and Silent modes, changing a file's protection status from personal to work is logged as an audit event.

If an employee opens Windows Information Protection-encrypted content from Word, edits the content, and then tries to save the edited version with a different name, Word, by default, applies Windows Information Protection to the new document. Also, if an employee saves it as a new document and deliberately chooses to save it without protection, they can do that in Allow Overrides mode (with a prompt) or Silent mode, and it's logged in a Windows Information Protection audit log.

Cloud storage and backup

Our policies specify that employees should use OneDrive for Business and/or SharePoint Online for storing and sharing work data in the cloud. If an employee tries to save Windows Information Protection-protected work files to their personal OneDrive or another unallowed cloud storage location, depending on the mode, one of the following actions will occur:

- **Hide Overrides** mode. The Windows Information Protection-protected work files will not sync, and the employee will see an error message.
- **Silent** mode. The Windows Information Protection-protected work files can be moved or copied to the user's personal local OneDrive sync folder, the files will sync without issue, and an audit log event will be generated.
- **Allow Overrides** mode. The user will receive a prompt that they can't place protected work files in that location. The user has to change their content from work protected to personal, and then the Windows Information Protection-protected work files can be moved or copied to the user's personal local OneDrive sync folder. The files will sync without issue and an audit log event will be generated.

Removable media

Windows Information Protection-protected work files can be saved to removable media, such as an external hard drive or a USB flash drive, for local storage or temporary backup. In Silent mode, the employee isn't notified, the file is saved without encryption, and it's logged in a Windows Information Protection audit log. If Windows Information Protection is in Allow Overrides mode, the employee is notified that the file will be unprotected, and they can choose to continue or cancel. If they continue, the file is unencrypted so it can be opened on other devices, and it's logged in a Windows Information Protection audit log.

There is another option that we are piloting and will be deploying broadly—the option to allow users to copy work files, providing they are a supported file type, such as an Azure Rights Management Services (RMS)-protected file.

Removing access to work data

Using Windows Information Protection, we can revoke access to work data from devices that are managed through Microsoft Intune, and leave personal data alone. This is a benefit when an employee leaves the company or when a device is lost or stolen. After determining that data access needs to be removed, we can use Microsoft Intune to unenroll the device so that when it connects to the network, the employee's encryption key for the device is revoked and the work data becomes unreadable.

On phones, after the encryption key is revoked, work data can't be recovered from the device. For computers running Windows 10, it's possible for us to recover that data.

Event logging

Silent and Allow Overrides modes allow the user to share data at their discretion, such as changing file ownership from work to personal, or moving work files to a removable drive or personal cloud. These events are logged on local devices in the Windows event log. To see logged events, you can use one of the available options, such as forwarding events to a Windows Event Collector server that collects and stores the Windows Information Protection events in a database where they can be analyzed if necessary.

Challenges

Windows Information Protection is useful in helping prevent unintentional information sharing. As with other methods that we use to protect information, malicious users can always find ways to deliberately leak data, including taking pictures of information on their screen or retyping protected text. Fortunately, most employees don't have malicious intent. Typically, inappropriate information sharing results from a of lack of training or through misidentification of a safe application or website. We can review event logs and audit reports to look for behaviors that might indicate intentional mishandling of data.

Conclusion

Windows Information Protection provides an obvious separation between personal and work data—employees can work with either, without switching environments. That separation of personal and work data supports BYOD at Microsoft. It enhances employee mobility and productivity, while helping to keep work data safe from inadvertent

disclosure. We can use Windows Information Protection to wipe work data off a corporate-owned device and leave the personal data alone. Event logging makes it easy to track issues and take remedial actions.

With Windows Information Protection, we have device-level data protection for our line-of-business apps without updating the apps. Windows Information Protection integrates with our existing management systems, Microsoft Intune and System Center Configuration Manager. It also integrates with many third-party mobile device management systems.

For more information

Microsoft IT Showcase

microsoft.com/itshowcase

Create a Windows Information Protection (WIP) policy using Microsoft Intune

Mobile, collaborative, and secure—Using Windows Information Protection to protect corporate data