Microsoft

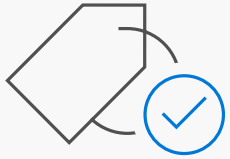
Deploying and managing Windows Information Protection (WIP)

Sophie Chanialaki
Partner Technical Architect, Microsoft 365

Microsoft Information Protection

Protect your sensitive data – wherever it lives or travels

Discover



Classify

Protect

Monitor

Across

Devices

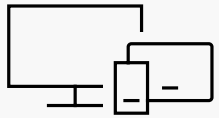
Apps

Cloud services

On-premises

Microsoft Information Protection – the way it was

Office 365 Information Protection

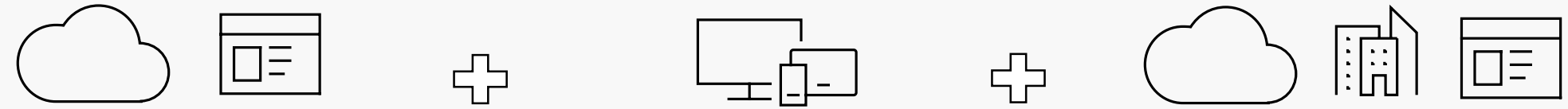


Windows Information Protection

Azure Information Protection

What	Preserve or remediate emails & documents	Protect files and documents	Classify & Protect emails & documents
Where	Office 365 Apps & Services	Windows Clients & Devices	Office Clients, 3rd party Apps & Services, On Premises
How	Office 365 Security Console	Intune Portal	AIP Portal

Microsoft Information Protection – starting today



Office 365 Information Protection + **Windows Information Protection** + **Azure Information Protection**

What	Consistent content detection and classification to protect and preserve sensitive data
Where	Office 365 apps & services, Windows clients & desktops, mobile, on premises + 3rd party apps and services
How	Microsoft 365 Security and Compliance Center

Comprehensive set of capabilities

AZURE INFORMATION PROTECTION

Classify, label & protect files – beyond Office 365, including on-premises & hybrid

MICROSOFT CLOUD APP SECURITY

Visibility into 15k+ cloud apps, data access & usage, potential abuse

OFFICE 365 DATA LOSS PREVENTION

Prevent data loss across Exchange Online, SharePoint Online, OneDrive for Business

OFFICE 365 MESSAGE ENCRYPTION

Send encrypted emails in Office 365 to anyone inside or outside of the company

WINDOWS INFORMATION PROTECTION

Separate personal vs. work data on Windows 10 devices, prevent work data from traveling to non-work locations

OFFICE 365 ADVANCED DATA GOVERNANCE

Apply retention and deletion policies to sensitive and important data in Office 365

MICROSOFT INFORMATION PROTECTION

Discover | Classify | Protect | Monitor

CONDITIONAL ACCESS

Control access to files based on policy, such as identity, machine configuration, geo location

OFFICE APPS

Protect sensitive information while working in Excel, Word, PowerPoint, Outlook

SHAREPOINT & GROUPS

Protect files in libraries and lists

AZURE SECURITY CENTER INFORMATION PROTECTION

Classify & label sensitive structured data in Azure SQL, SQL Server and other Azure repositories

SDK FOR PARTNER ECOSYSTEM & ISVs

Enable ISVs to consume labels, apply protection

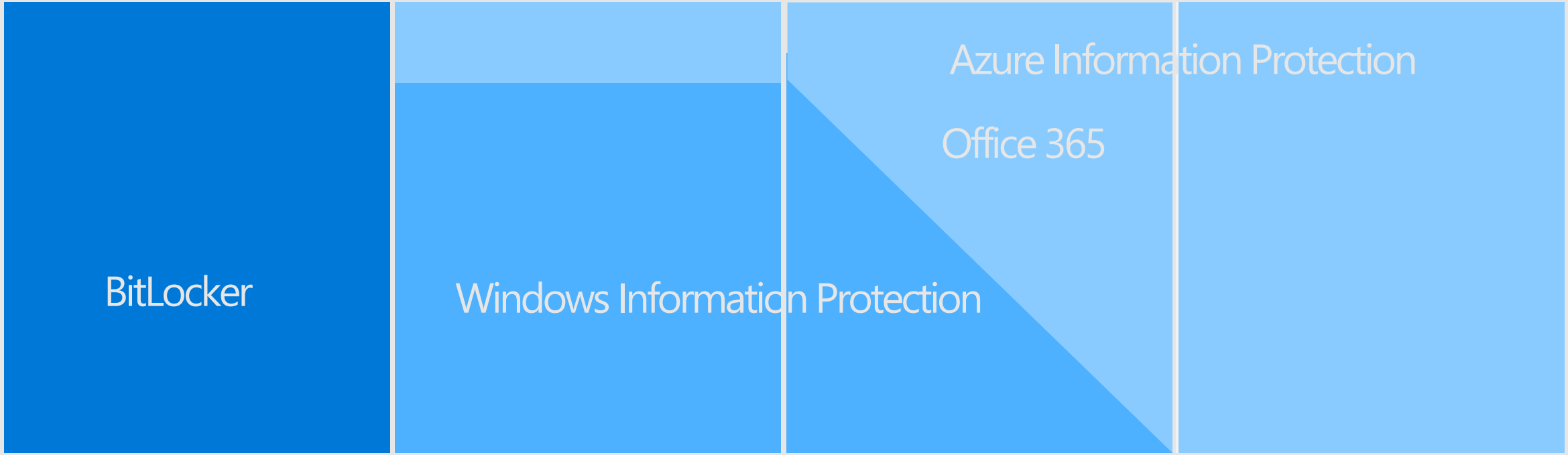
ADOBE PDFs

Natively view and protect PDFs on Adobe Acrobat Reader

YOUR INFORMATION **PROTECTION NEEDS**

DEVICE PROTECTION	DATA SEPARATION	LEAK PROTECTION	SHARING PROTECTION
Protect system and data when device is lost or stolen	Containment Data separation	Prevent unauthorized users and apps from accessing and leaking data	Protect data when shared with others, or shared outside of organizational devices and control

YOUR INFORMATION **PROTECTION NEEDS**



Comprehensive set of capabilities

AZURE INFORMATION PROTECTION
Classify, label & protect files – beyond Office 365, including on-premises & hybrid

MICROSOFT CLOUD APP SECURITY
Visibility into 15k+ cloud apps, data access & usage, potential abuse

OFFICE 365 DATA LOSS PREVENTION
Prevent data loss across Exchange Online, SharePoint Online, OneDrive for Business

OFFICE 365 MESSAGE ENCRYPTION
Send encrypted emails in Office 365 to anyone inside or outside of the company

WINDOWS INFORMATION PROTECTION
Separate personal vs. work data on Windows 10 devices, prevent work data from traveling to non-work locations

OFFICE 365 ADVANCED DATA GOVERNANCE
Apply retention and deletion policies to sensitive and important data in Office 365

MICROSOFT INFORMATION PROTECTION

Discover | Classify | Protect | Monitor

CONDITIONAL ACCESS
Control access to files based on policy, such as identity, machine configuration, geo location

OFFICE APPS
Protect sensitive information while working in Excel, Word, PowerPoint, Outlook

SHAREPOINT & GROUPS
Protect files in libraries and lists

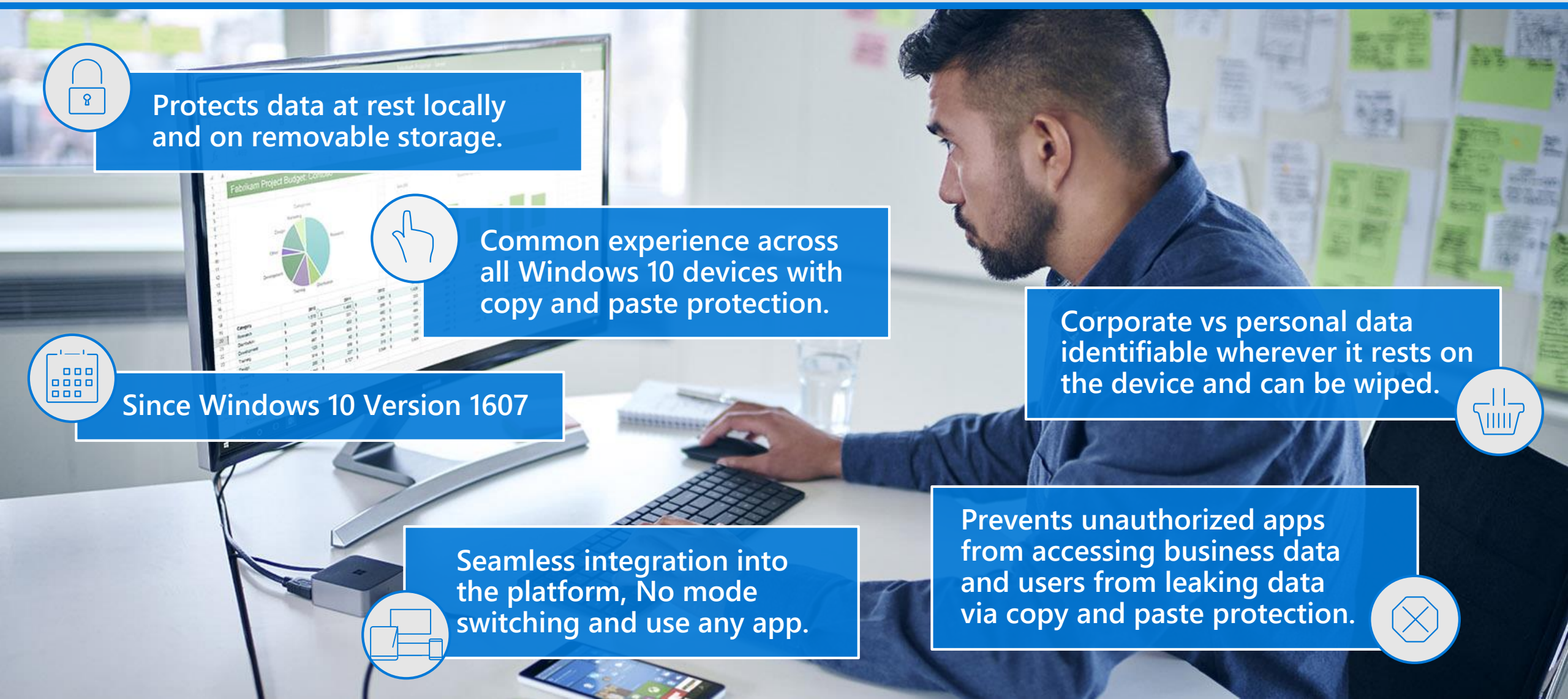
AZURE SECURITY CENTER INFORMATION PROTECTION
Classify & label sensitive structured data in Azure SQL, SQL Server and other Azure repositories

SDK FOR PARTNER ECOSYSTEM & ISVs
Enable ISVs to consume labels, apply protection

ADOBE PDFs
Natively view and protect PDFs on Adobe Acrobat Reader

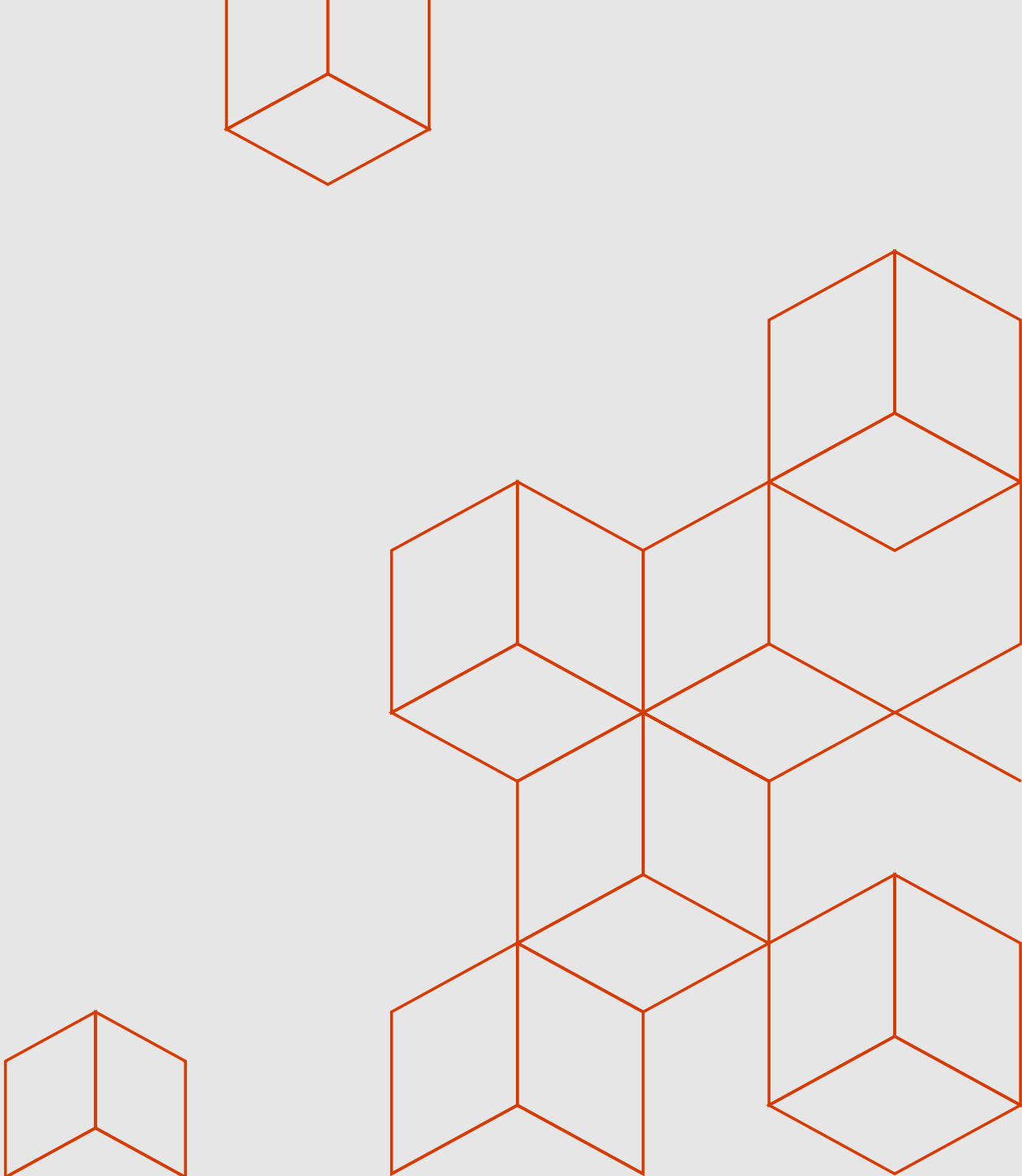
WINDOWS INFORMATION PROTECTION

Integrated protection against accidental data leaks

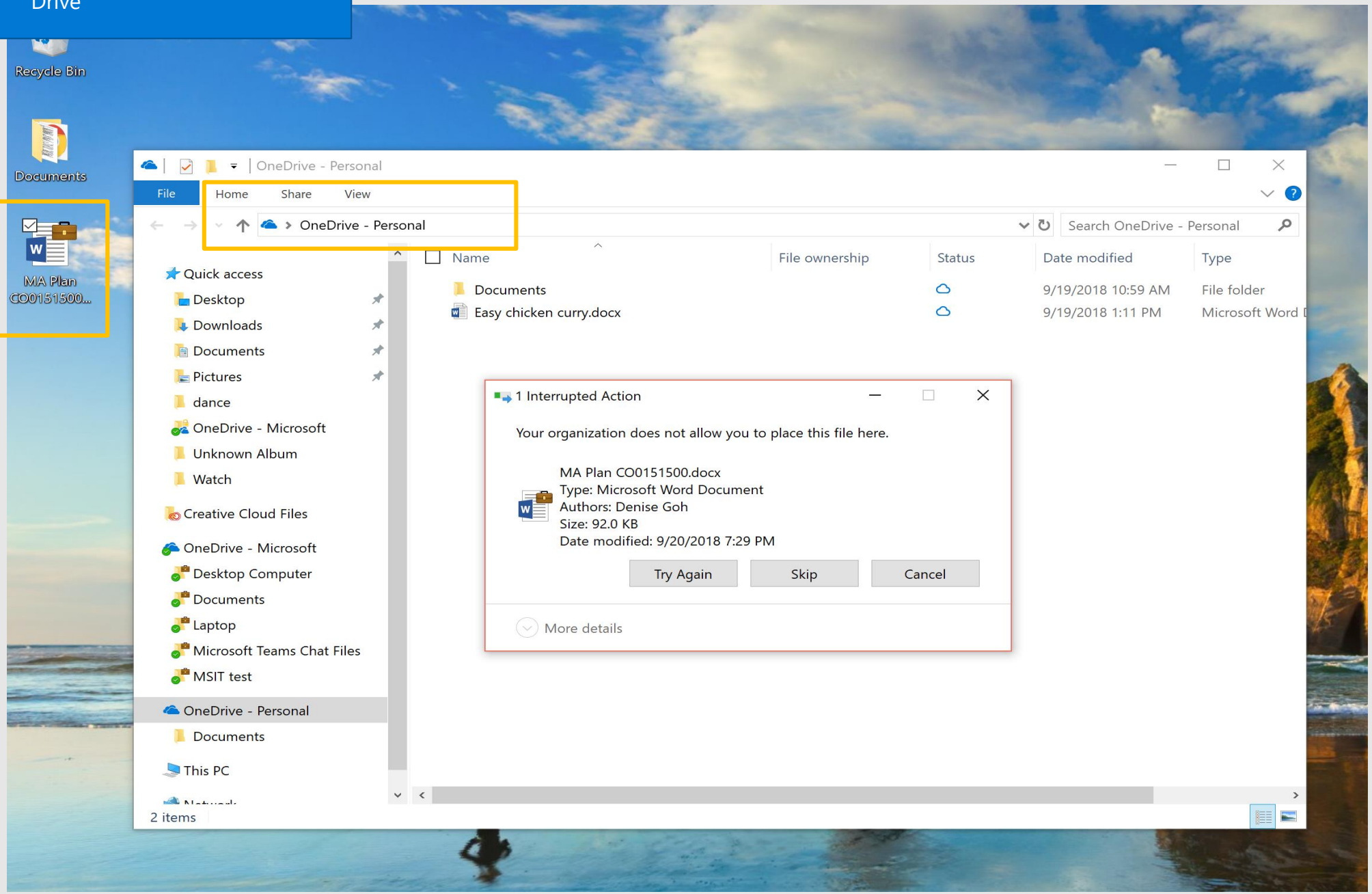


Demo

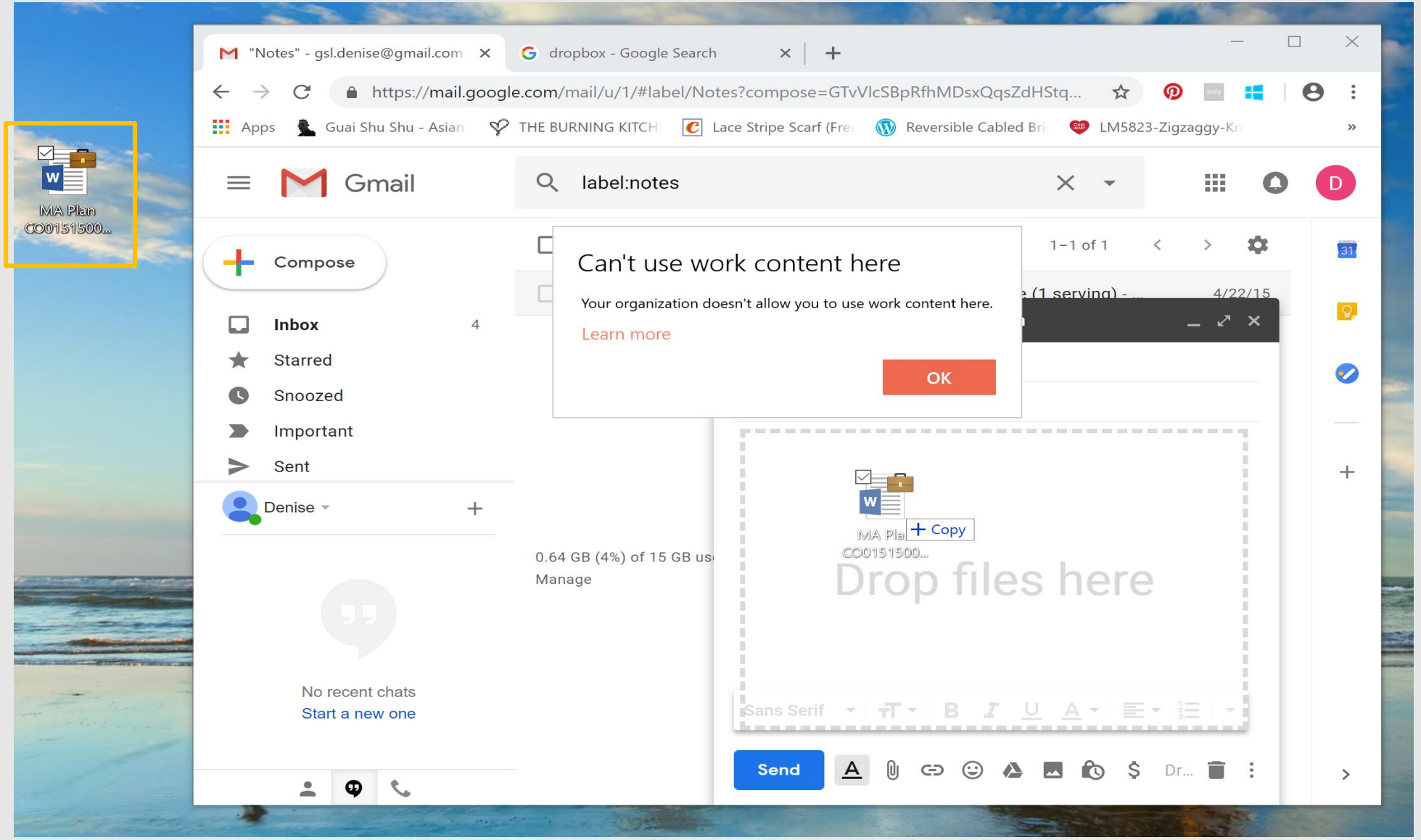
Windows Information Protection Client



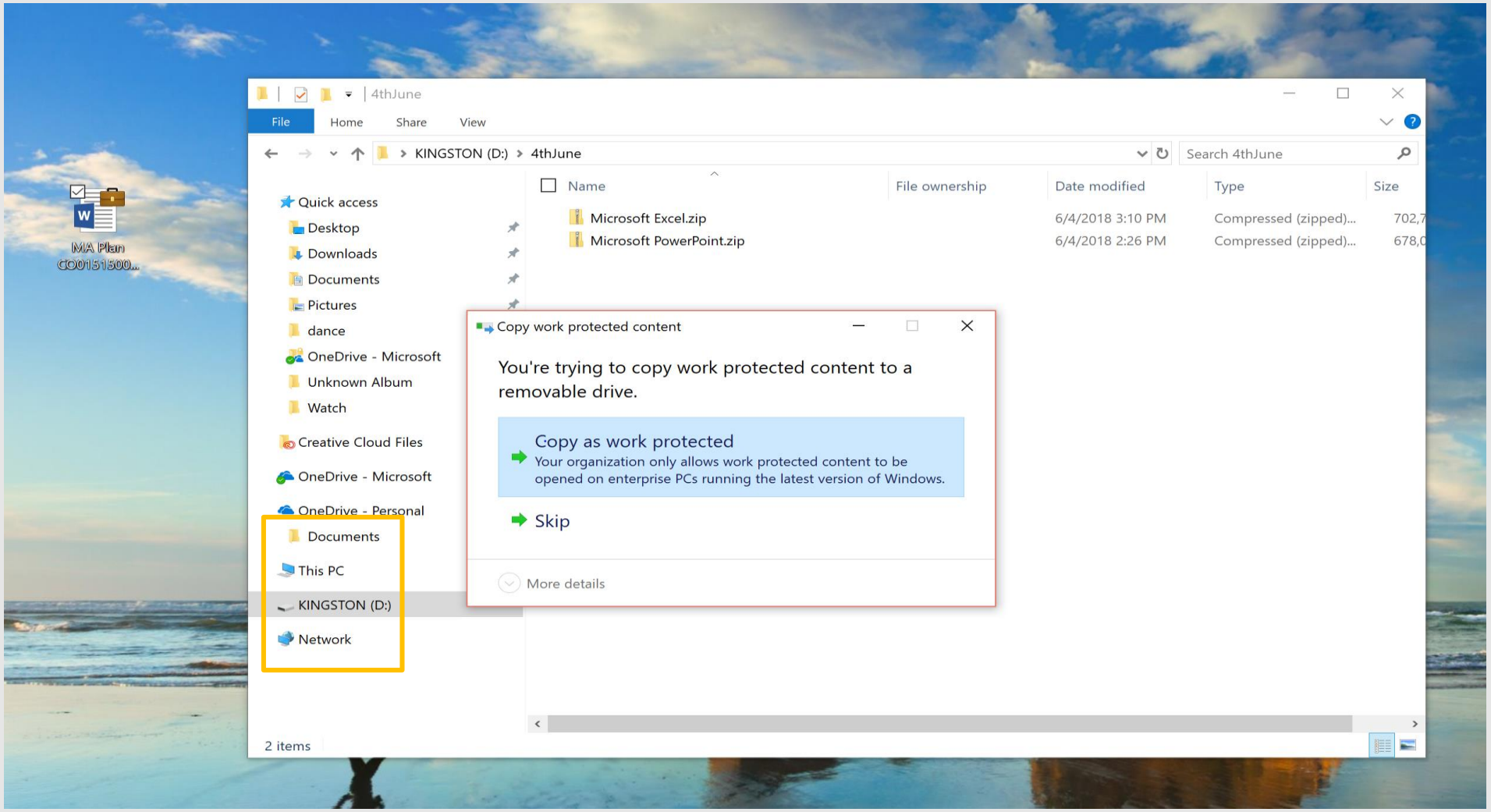
WIP – Copying Highly Confidential file to Personal One Drive



WIP – Copying Highly Confidential file to Gmail



WIP – Copying Highly Confidential file to USB Drive



Business/Personal

One experience

Business/Personal

One experience

Data is isolated

Data is encrypted at rest

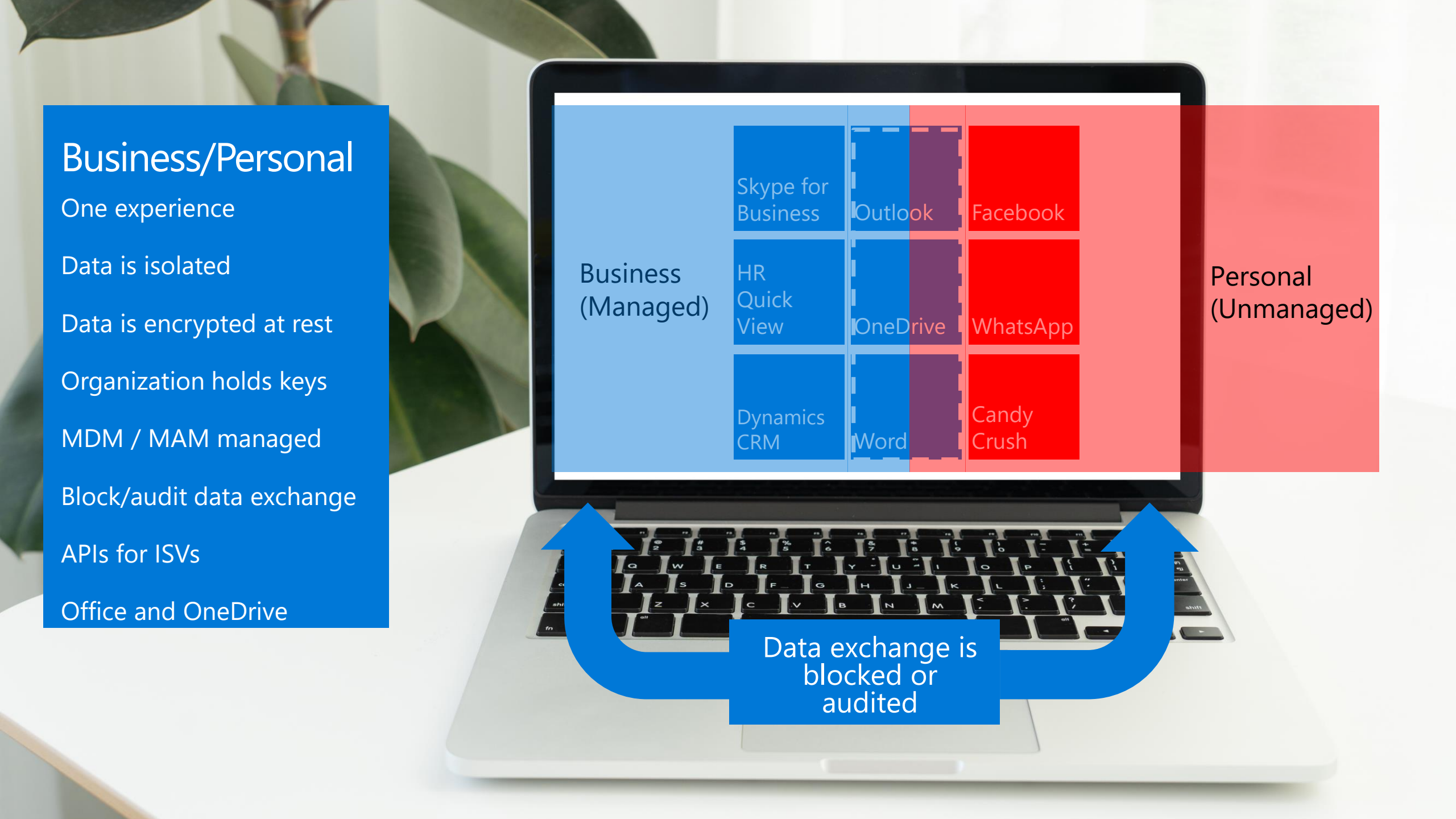
Organization holds keys

MDM / MAM managed

Block/audit data exchange

APIs for ISVs

Office and OneDrive

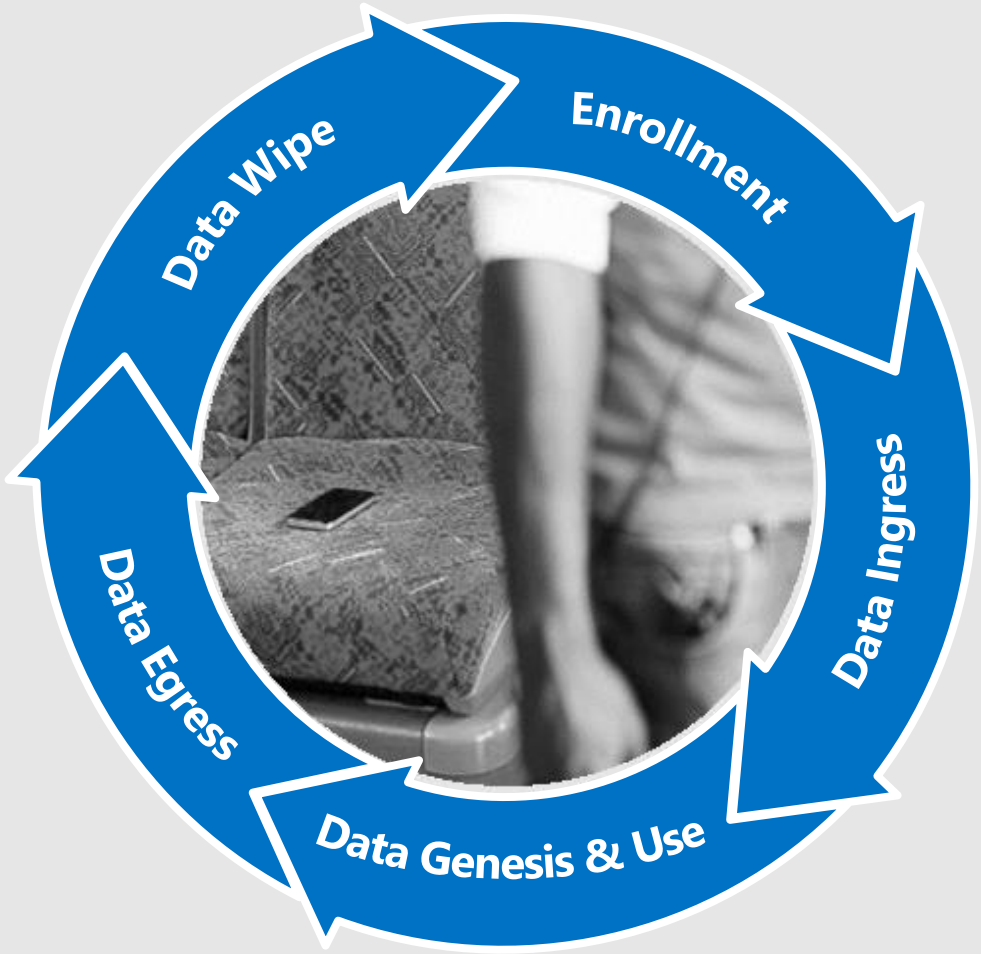


Enlightened Applications

Unenlightened Applications – How to manage

- Option 1: Use Allow policy
  - *Caution:* Auto-encrypts all files touched
  - Intended for Line of Business (LOB) apps
  - Can include in policy for fully managed devices
- Option 2: Use Exempt policy
  - WIP rules don't apply to the app
  - Access work without impacting personal data
- Option 3: Enlighten the app
  - See: http://aka.ms/wip-dev-guide

WINDOWS INFORMATION PROTECTION **LIFECYCLE**



Policy and keys provisioned to device

Data coming from corporate network location automatically protected by WIP

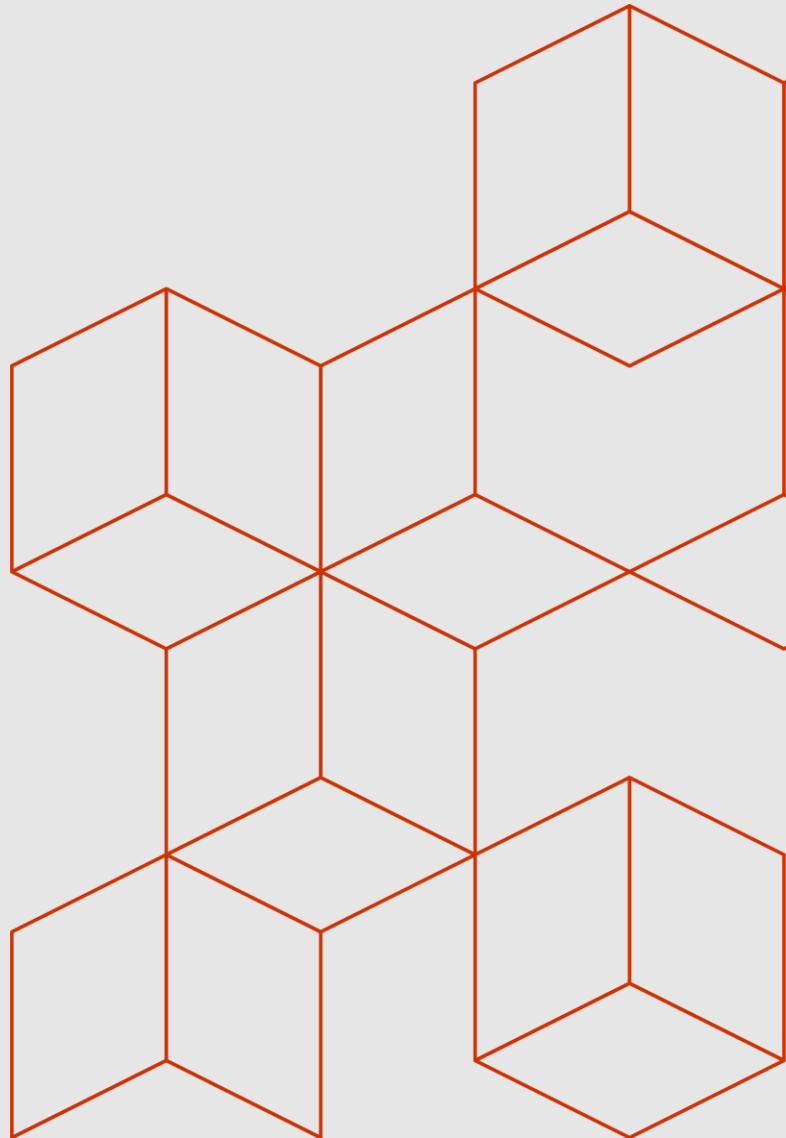
App can automatically protect data or users
can define data as personal or corporate

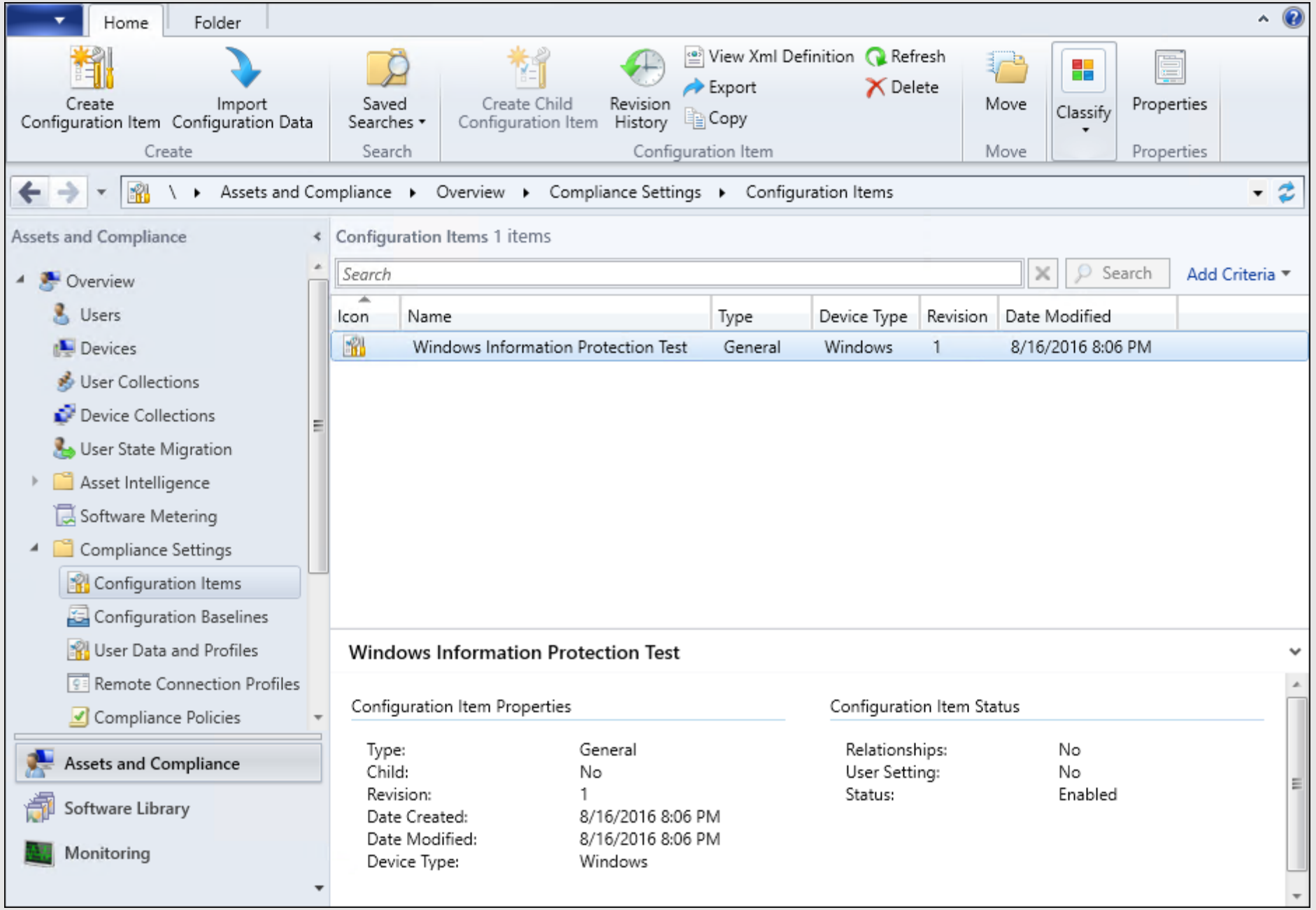
Protection can be maintained anywhere on the device or when data moves to removable storage. Azure Information Services can be used maintain protection in B2B scenarios.

Selectively wipe corporate data on demand
or when device is unenrolled

Demo – Intune

Demo – SCCM




Home
Folder
Create Configuration Item
Import Configuration Data
Create
Saved Searches
Search
Create Child Configuration Item
Revision History
View Xml Definition
Export
Copy
Refresh
Delete
Configuration Item
Move
Move
Classify
Properties
Properties
\ ▸ Assets and Compliance ▸ Overview ▸ Compliance Settings ▸ Configuration Items
Assets and Compliance
Overview
Users
Devices
User Collections
Device Collections
User State Migration
Asset Intelligence
Software Metering
Compliance Settings
Configuration Items
Configuration Baselines
User Data and Profiles
Remote Connection Profiles
Compliance Policies
Assets and Compliance
Software Library
Monitoring
Configuration Items 1 items
Search
Search
Add Criteria
Icon
Name
Type
Device Type
Revision
Date Modified
Windows Information Protection Test
General
Windows
1
8/16/2016 8:06 PM
Windows Information Protection Test
Configuration Item Properties
Type: General
Child: No
Revision: 1
Date Created: 8/16/2016 8:06 PM
Date Modified: 8/16/2016 8:06 PM
Device Type: Windows
Configuration Item Status
Relationships: No
User Setting: No
Status: Enabled

Create Configuration Item Wizard

General

- General
  - Supported Platforms
  - Device Settings
  - Platform Applicability
- Summary
- Progress
- Completion

Specify general information about this configuration item

Configuration items define a configuration and associated validation criteria to be assessed for compliance on client devices.

Name: Windows Information Protection Example

Description: Sample policy for WIP documentation purposes.

Specify the type of configuration item that you want to create:

Settings for devices managed with the Configuration Manager client

- (•) Windows 10
- ( ) Mac OS X (custom)
- ( ) Windows Desktops and Servers (custom)
  - [ ] This configuration item contains application settings

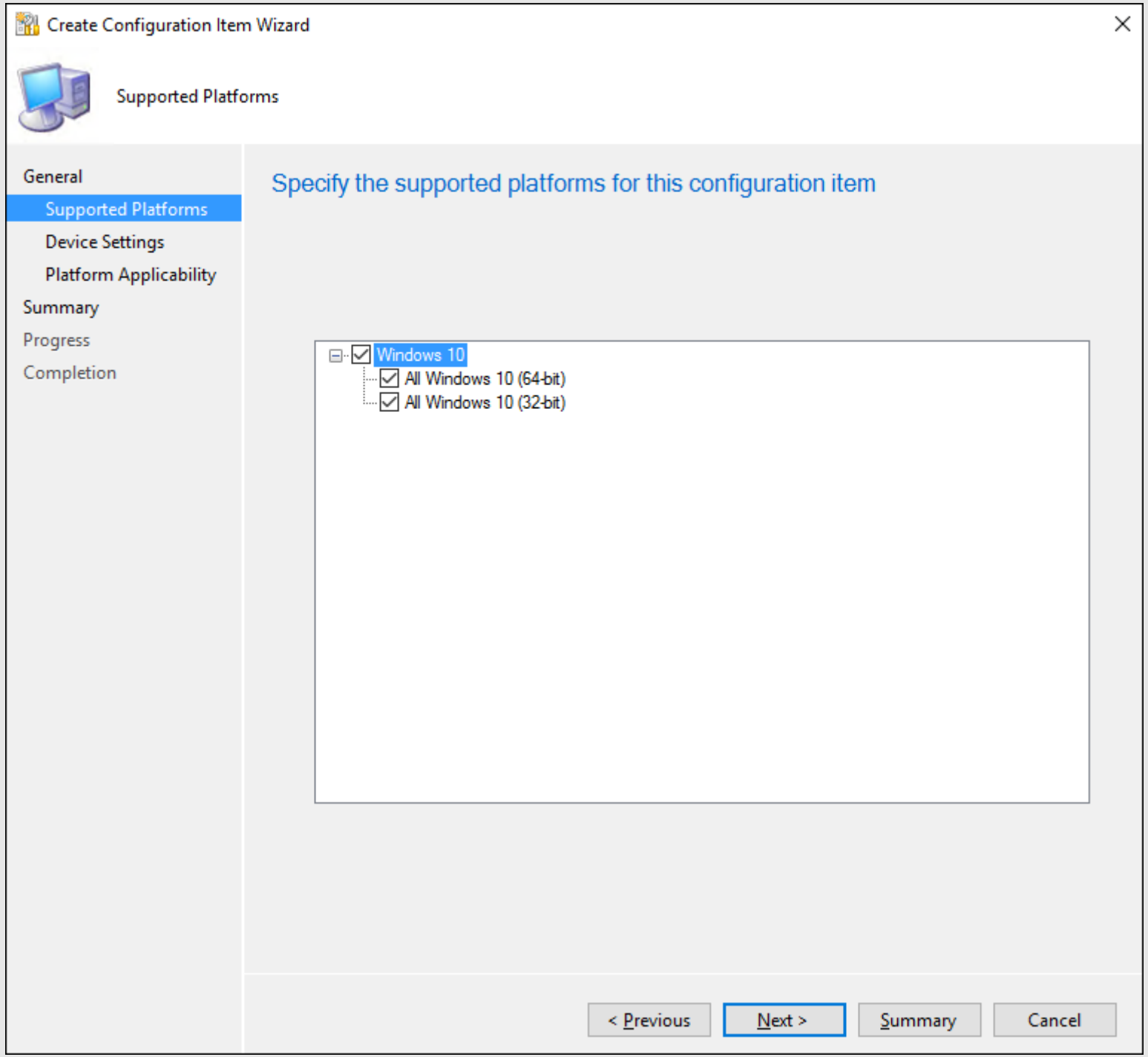
Settings for devices managed without the Configuration Manager client

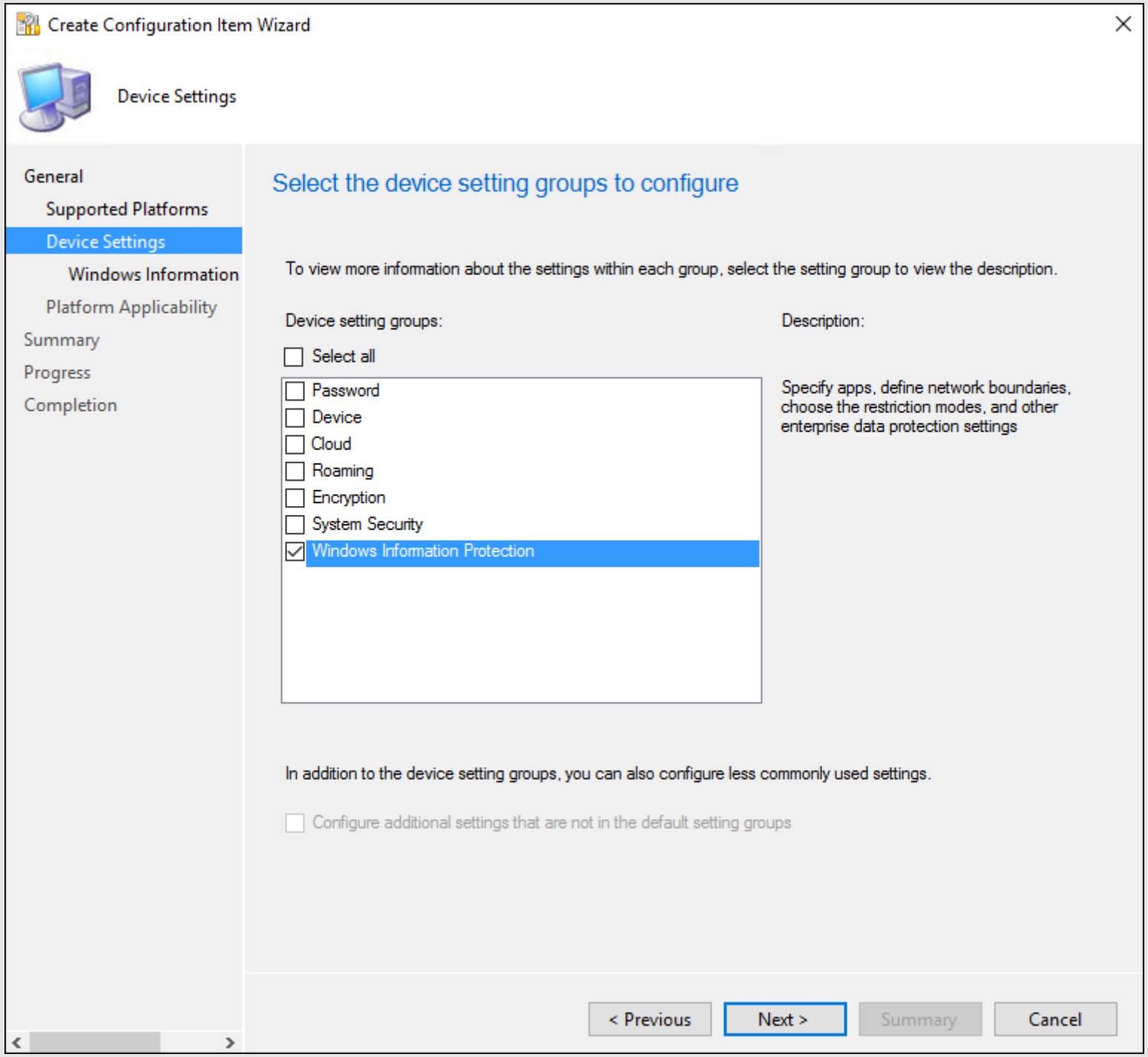
- ( ) Windows 8.1 and Windows 10
- ( ) Windows Phone
- ( ) iOS and Mac OS X
- ( ) Android and Samsung KNOX

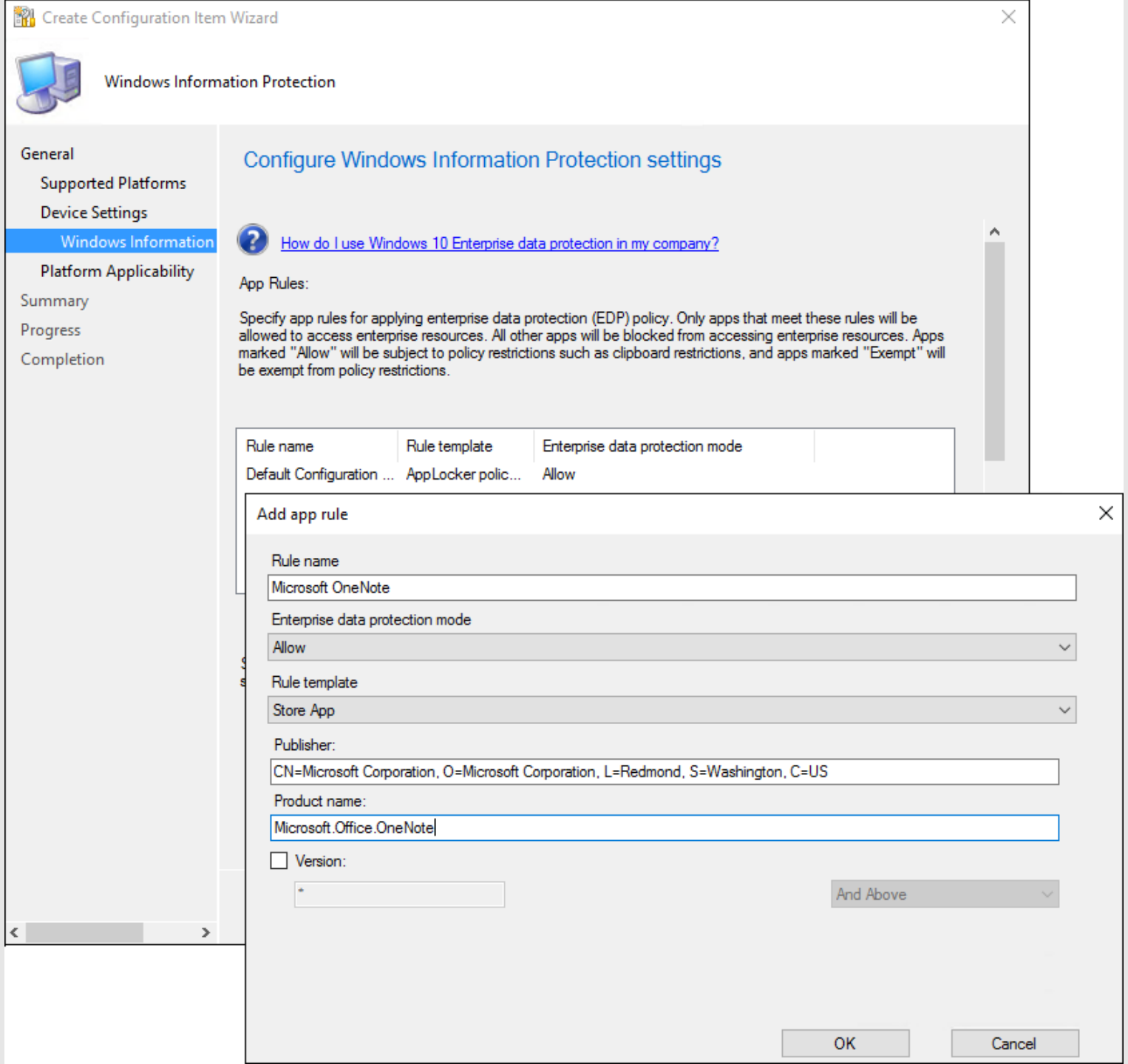
Assigned categories to improve searching and filtering:

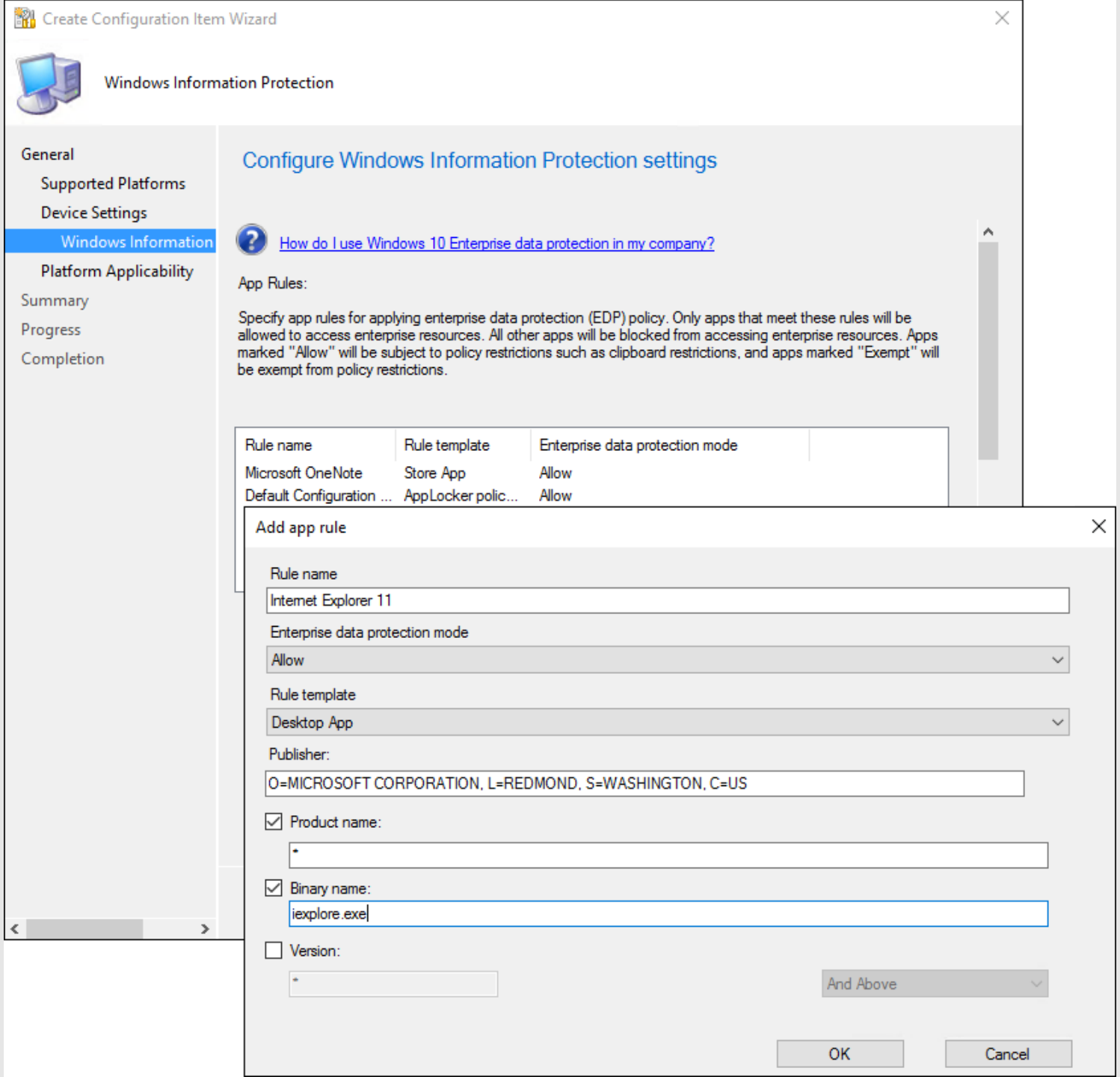
Categories...

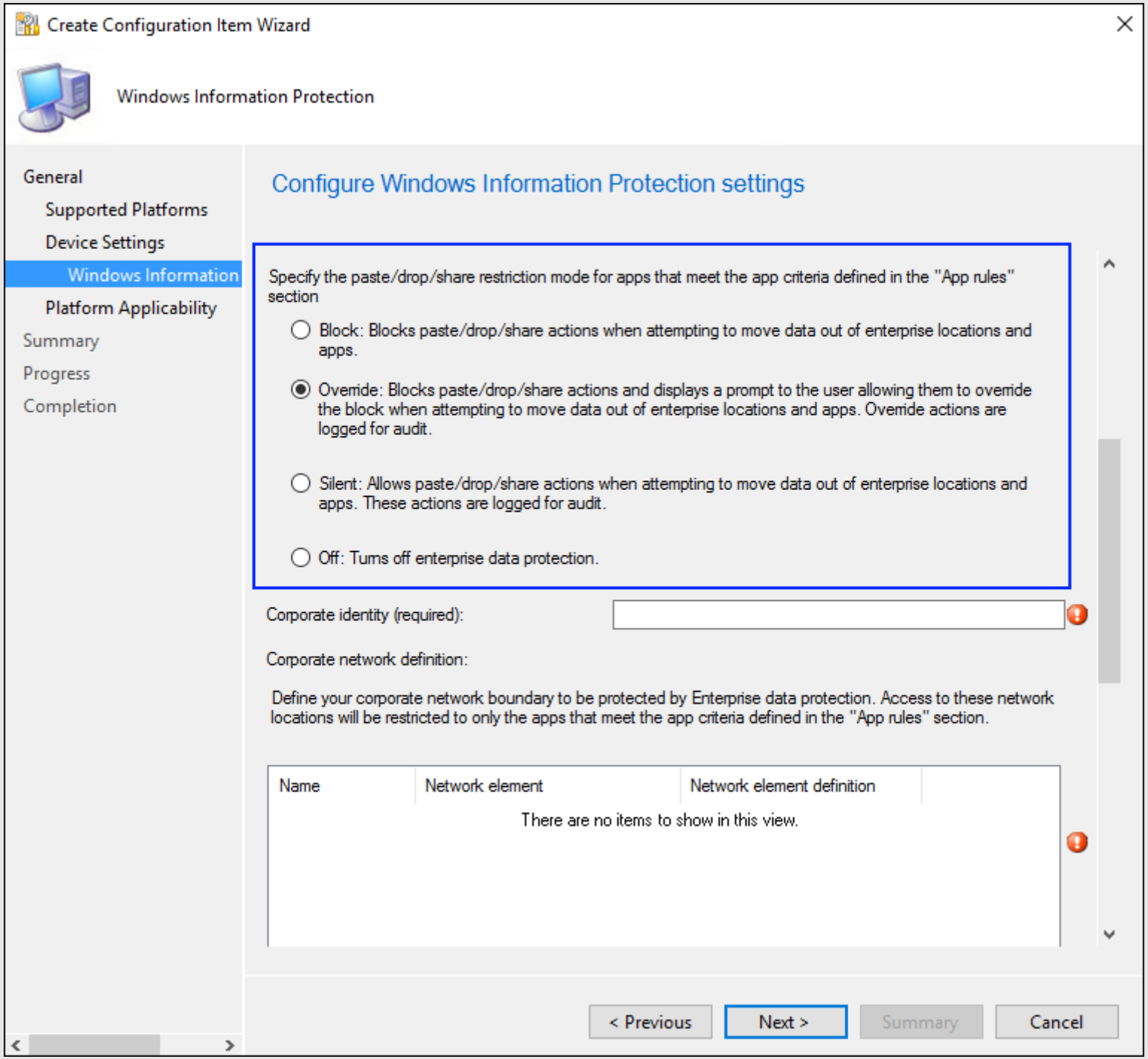
< Previous | Next > | Summary | Cancel

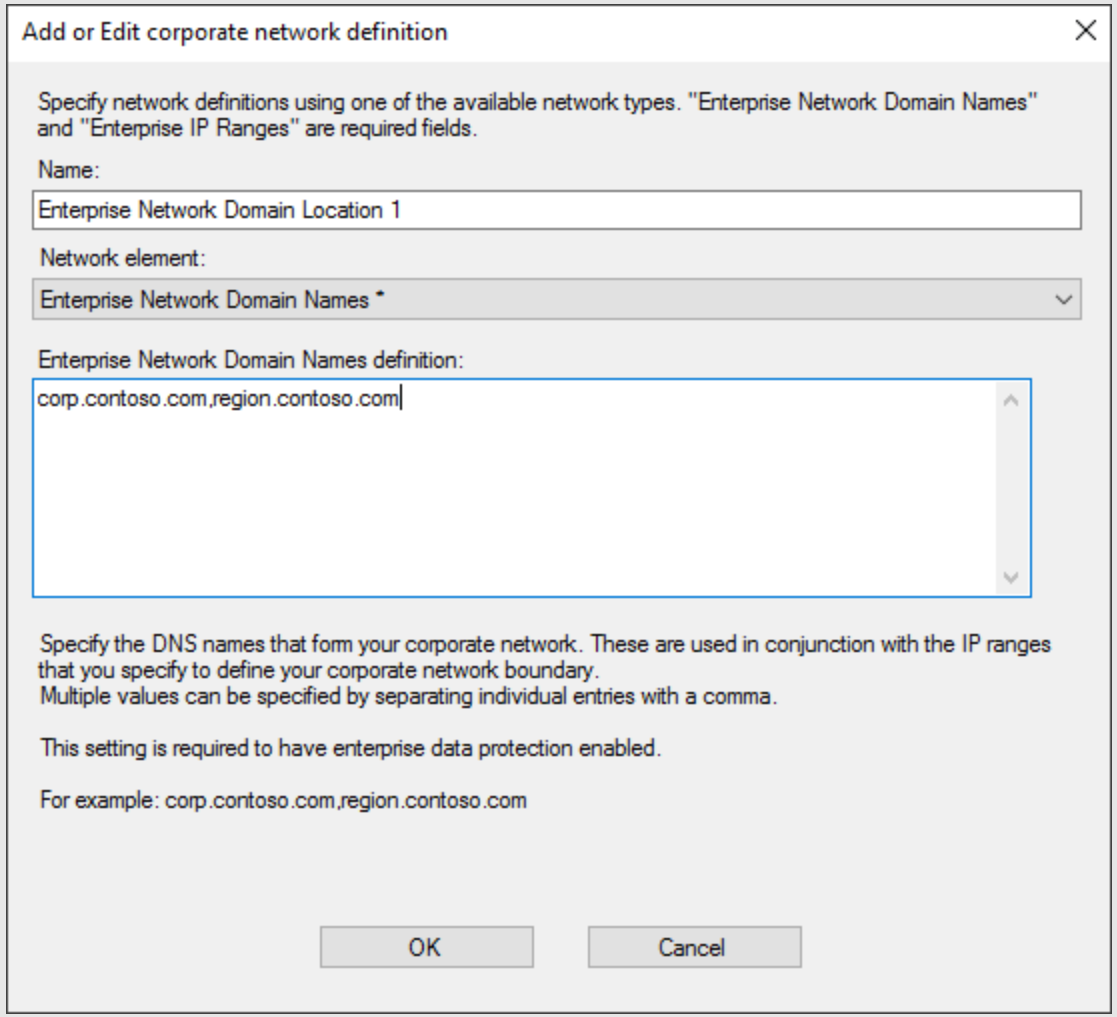

Create Configuration Item Wizard
Supported Platforms
General
Supported Platforms
Device Settings
Platform Applicability
Summary
Progress
Completion
Specify the supported platforms for this configuration item
Windows 10
All Windows 10 (64-bit)
All Windows 10 (32-bit)
< Previous
Next >
Summary
Cancel


Create Configuration Item Wizard
Device Settings
General
Supported Platforms
Device Settings
Windows Information
Platform Applicability
Summary
Progress
Completion
Select the device setting groups to configure
To view more information about the settings within each group, select the setting group to view the description.
Device setting groups:
Description:
Select all
Password
Device
Cloud
Roaming
Encryption
System Security
Windows Information Protection
Specify apps, define network boundaries, choose the restriction modes, and other enterprise data protection settings
In addition to the device setting groups, you can also configure less commonly used settings.
Configure additional settings that are not in the default setting groups
< Previous
Next >
Summary
Cancel


Create Configuration Item Wizard
Windows Information Protection
General
Supported Platforms
Device Settings
Windows Information
Platform Applicability
Summary
Progress
Completion
Configure Windows Information Protection settings
How do I use Windows 10 Enterprise data protection in my company?
App Rules:
Specify app rules for applying enterprise data protection (EDP) policy. Only apps that meet these rules will be allowed to access enterprise resources. All other apps will be blocked from accessing enterprise resources. Apps marked "Allow" will be subject to policy restrictions such as clipboard restrictions, and apps marked "Exempt" will be exempt from policy restrictions.
Rule name
Rule template
Enterprise data protection mode
Default Configuration ...
AppLocker polic...
Allow
Add app rule
Rule name
Microsoft OneNote
Enterprise data protection mode
Allow
Rule template
Store App
Publisher:
CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Product name:
Microsoft.Office.OneNote
Version:
*
And Above
OK
Cancel

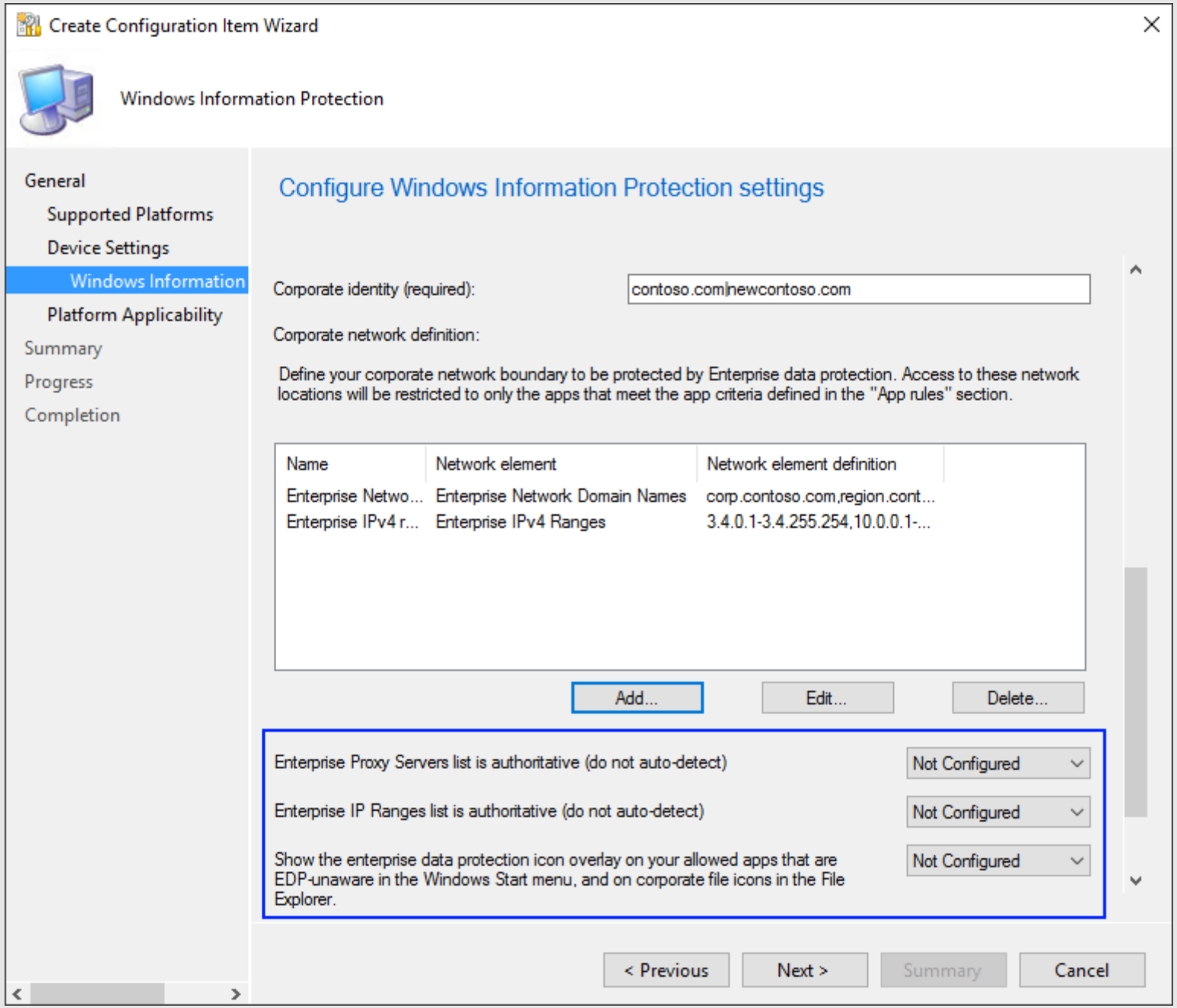

Create Configuration Item Wizard
Windows Information Protection
General
Supported Platforms
Device Settings
Windows Information
Platform Applicability
Summary
Progress
Completion
Configure Windows Information Protection settings
How do I use Windows 10 Enterprise data protection in my company?
App Rules:
Specify app rules for applying enterprise data protection (EDP) policy. Only apps that meet these rules will be allowed to access enterprise resources. All other apps will be blocked from accessing enterprise resources. Apps marked "Allow" will be subject to policy restrictions such as clipboard restrictions, and apps marked "Exempt" will be exempt from policy restrictions.
Rule name
Rule template
Enterprise data protection mode
Microsoft OneNote
Store App
Allow
Default Configuration ...
AppLocker polic...
Allow
Add app rule
Rule name
Internet Explorer 11
Enterprise data protection mode
Allow
Rule template
Desktop App
Publisher:
O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US
Product name:
*
Binary name:
iexplore.exe
Version:
*
And Above
OK
Cancel

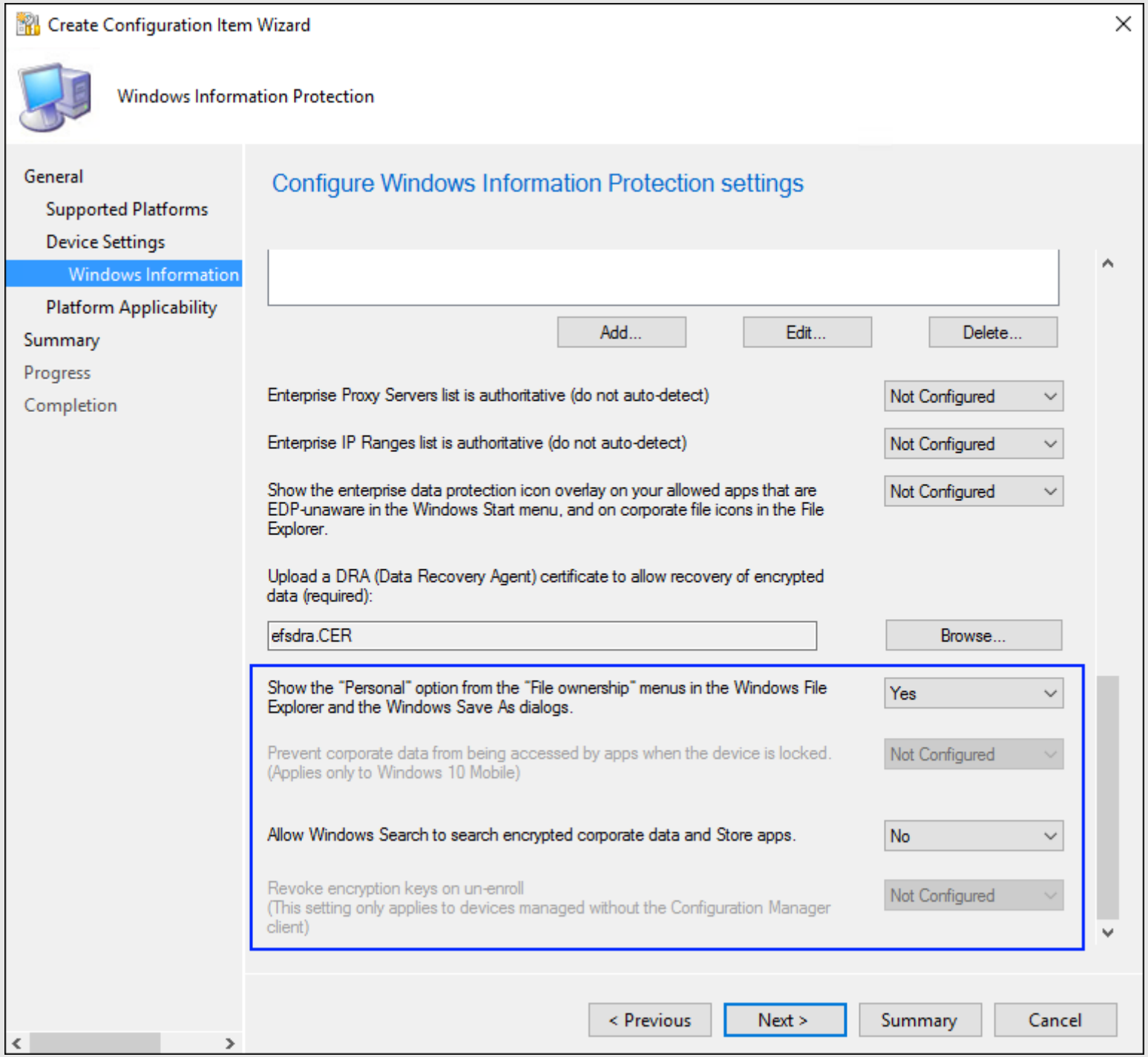

Create Configuration Item Wizard
Windows Information Protection
General
Supported Platforms
Device Settings
Windows Information
Platform Applicability
Summary
Progress
Completion
Configure Windows Information Protection settings
Specify the paste/drop/share restriction mode for apps that meet the app criteria defined in the "App rules" section
Block: Blocks paste/drop/share actions when attempting to move data out of enterprise locations and apps.
Override: Blocks paste/drop/share actions and displays a prompt to the user allowing them to override the block when attempting to move data out of enterprise locations and apps. Override actions are logged for audit.
Silent: Allows paste/drop/share actions when attempting to move data out of enterprise locations and apps. These actions are logged for audit.
Off: Turns off enterprise data protection.
Corporate identity (required):
Corporate network definition:
Define your corporate network boundary to be protected by Enterprise data protection. Access to these network locations will be restricted to only the apps that meet the app criteria defined in the "App rules" section.
Name
Network element
Network element definition
There are no items to show in this view.
< Previous
Next >
Summary
Cancel


Add or Edit corporate network definition
Specify network definitions using one of the available network types. "Enterprise Network Domain Names" and "Enterprise IP Ranges" are required fields.
Name:
Enterprise Network Domain Location 1
Network element:
Enterprise Network Domain Names *
Enterprise Network Domain Names definition:
corp.contoso.com,region.contoso.com
Specify the DNS names that form your corporate network. These are used in conjunction with the IP ranges that you specify to define your corporate network boundary.
Multiple values can be specified by separating individual entries with a comma.
This setting is required to have enterprise data protection enabled.
For example: corp.contoso.com,region.contoso.com
OK
Cancel

Network location type	Format	Description
Enterprise Cloud Resources	**With proxy:** contoso.sharepoint.com,contoso.internalproxy1.com| contoso.visualstudio.com,contoso.internalproxy2.com **Without proxy:** contoso.sharepoint.com|contoso.visualstudio.com	Specify the cloud resources to be treated as corporate and protected by WIP. For each cloud resource, you may also optionally specify a proxy server from your Internal proxy servers list to route traffic for this cloud resource. Be aware that all traffic routed through your Internal proxy servers is considered enterprise. If you have multiple resources, you must separate them using the "|" delimiter. If you don't use proxy servers, you must also include the "," delimiter just before the "|". For example: `URL <,proxy>|URL <,proxy>`. **Important** In some cases, such as when an app connects directly to a cloud resource through an IP address, Windows can't tell whether it's attempting to connect to an enterprise cloud resource or to a personal site. In this case, Windows blocks the connection by default. To stop Windows from automatically blocking these connections, you can add the `/*AppCompat*/` string to the setting. For example: `URL <,proxy>|URL <,proxy>|/*AppCompat*/`.
Enterprise Network Domain Names (Required)	corp.contoso.com,region.contoso.com	Specify the DNS suffixes used in your environment. All traffic to the fully-qualified domains appearing in this list will be protected. This setting works with the IP ranges settings to detect whether a network endpoint is enterprise or personal on private networks. If you have multiple resources, you must separate them using the "," delimiter.
Proxy servers	proxy.contoso.com:80;proxy2.contoso.com:443	Specify the proxy servers your devices will go through to reach your cloud resources. Using this server type indicates that the cloud resources you're connecting to are enterprise resources. This list shouldn't include any servers listed in your Internal proxy servers list. Internal proxy servers must be used only for WIP-protected (enterprise) traffic.

Internal proxy servers	contoso.internalproxy1.com;contoso.internalproxy2.com	Specify the internal proxy servers your devices will go through to reach your cloud resources. Using this server type indicates that the cloud resources you're connecting to are enterprise resources. This list shouldn't include any servers listed in your Proxy servers list. Proxy servers must be used only for non-WIP-protected (non-enterprise) traffic. If you have multiple resources, you must separate them using the ";" delimiter.
Enterprise IPv4 Range (Required)	**Starting IPv4 Address:** 3.4.0.1 **Ending IPv4 Address:** 3.4.255.254 **Custom URI:** 3.4.0.1-3.4.255.254, 10.0.0.1-10.255.255.254	Specify the addresses for a valid IPv4 value range within your intranet. These addresses, used with your Enterprise Network Domain Names, define your corporate network boundaries. If you have multiple ranges, you must separate them using the "," delimiter.
Enterprise IPv6 Range	**Starting IPv6 Address:** 2a01:110:: **Ending IPv6 Address:** 2a01:110:7fff:ffff:ffff:ffff:ffff:ffff **Custom URI:** 2a01:110:7fff:ffff:ffff:ffff:ffff:ffff, fd00::-fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	Specify the addresses for a valid IPv6 value range within your intranet. These addresses, used with your Enterprise Network Domain Names, define your corporate network boundaries. If you have multiple ranges, you must separate them using the "," delimiter.
Neutral Resources	sts.contoso.com,sts.contoso2.com	Specify your authentication redirection endpoints for your company. These locations are considered enterprise or personal, based on the context of the connection before the redirection. If you have multiple resources, you must separate them using the "," delimiter.


Create Configuration Item Wizard
Windows Information Protection
General
Supported Platforms
Device Settings
Windows Information
Platform Applicability
Summary
Progress
Completion
Configure Windows Information Protection settings
Corporate identity (required):
contoso.com|newcontoso.com
Corporate network definition:
Define your corporate network boundary to be protected by Enterprise data protection. Access to these network locations will be restricted to only the apps that meet the app criteria defined in the "App rules" section.
Name
Network element
Network element definition
Enterprise Netwo...
Enterprise Network Domain Names
corp.contoso.com,region.cont...
Enterprise IPv4 r...
Enterprise IPv4 Ranges
3.4.0.1-3.4.255.254,10.0.0.1-...
Add...
Edit...
Delete...
Enterprise Proxy Servers list is authoritative (do not auto-detect)
Not Configured
Enterprise IP Ranges list is authoritative (do not auto-detect)
Not Configured
Show the enterprise data protection icon overlay on your allowed apps that are EDP-unaware in the Windows Start menu, and on corporate file icons in the File Explorer.
Not Configured
< Previous
Next >
Summary
Cancel


Create Configuration Item Wizard
Windows Information Protection
General
Supported Platforms
Device Settings
Windows Information
Platform Applicability
Summary
Progress
Completion
Configure Windows Information Protection settings
Add...
Edit...
Delete...
Enterprise Proxy Servers list is authoritative (do not auto-detect)
Not Configured
Enterprise IP Ranges list is authoritative (do not auto-detect)
Not Configured
Show the enterprise data protection icon overlay on your allowed apps that are EDP-unaware in the Windows Start menu, and on corporate file icons in the File Explorer.
Not Configured
Upload a DRA (Data Recovery Agent) certificate to allow recovery of encrypted data (required):
efsdra.CER
Browse...
Show the "Personal" option from the "File ownership" menus in the Windows File Explorer and the Windows Save As dialogs.
Yes
Prevent corporate data from being accessed by apps when the device is locked. (Applies only to Windows 10 Mobile)
Not Configured
Allow Windows Search to search encrypted corporate data and Store apps.
No
Revoke encryption keys on un-enroll
(This setting only applies to devices managed without the Configuration Manager client)
Not Configured
< Previous
Next >
Summary
Cancel

Create Configuration Item Wizard

Summary

- General
  - Supported Platforms
  - Device Settings
    - Windows Information
  - Platform Applicability
- Summary
- Progress
- Completion

The wizard will create a device configuration item with the following settings

Details:

The wizard will create a device configuration item with the following settings:

New device configuration item will be saved as:
- Name: Windows Information Protection Example
- Description: Sample policy for WIP documentation purposes.
- Categories:

The following compliance rules are added:
- EDP App Management Mode
- Allowed desktop apps
- Allowed universal apps
- Enterprise IP ranges
- Enterprise network domains
- Enterprise protected domains
- Data Recovery Certificate
- Block the user from decrypting data that was created or edited by the apps configured above
- Allow encrypted data and store apps to appear in Windows search

The following settings are added:

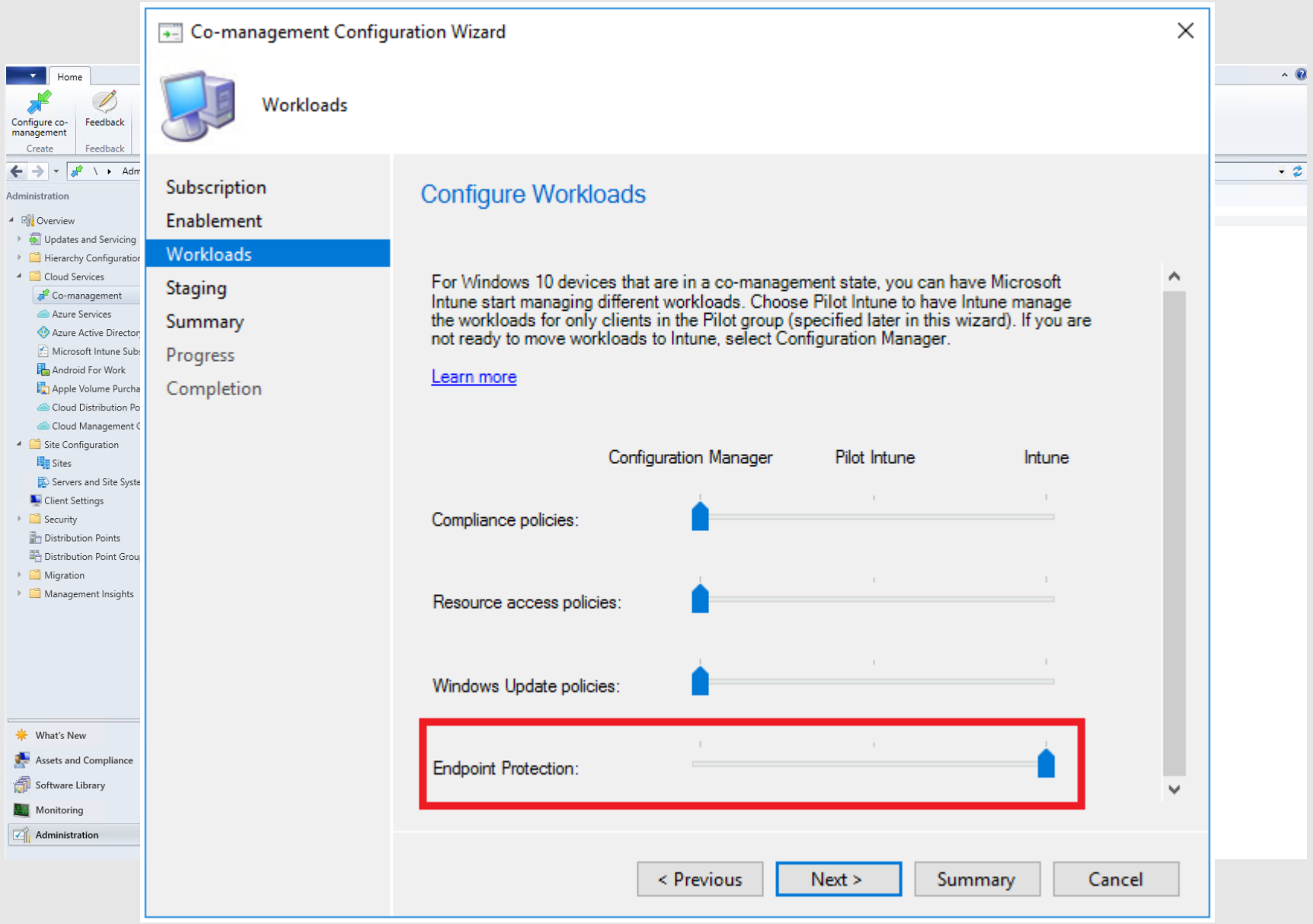
The following applicability criteria are added:
- All Windows 10 (64-bit)
- All Windows 10 (32-bit)

To change these settings, click Previous. To apply the settings, click Next.

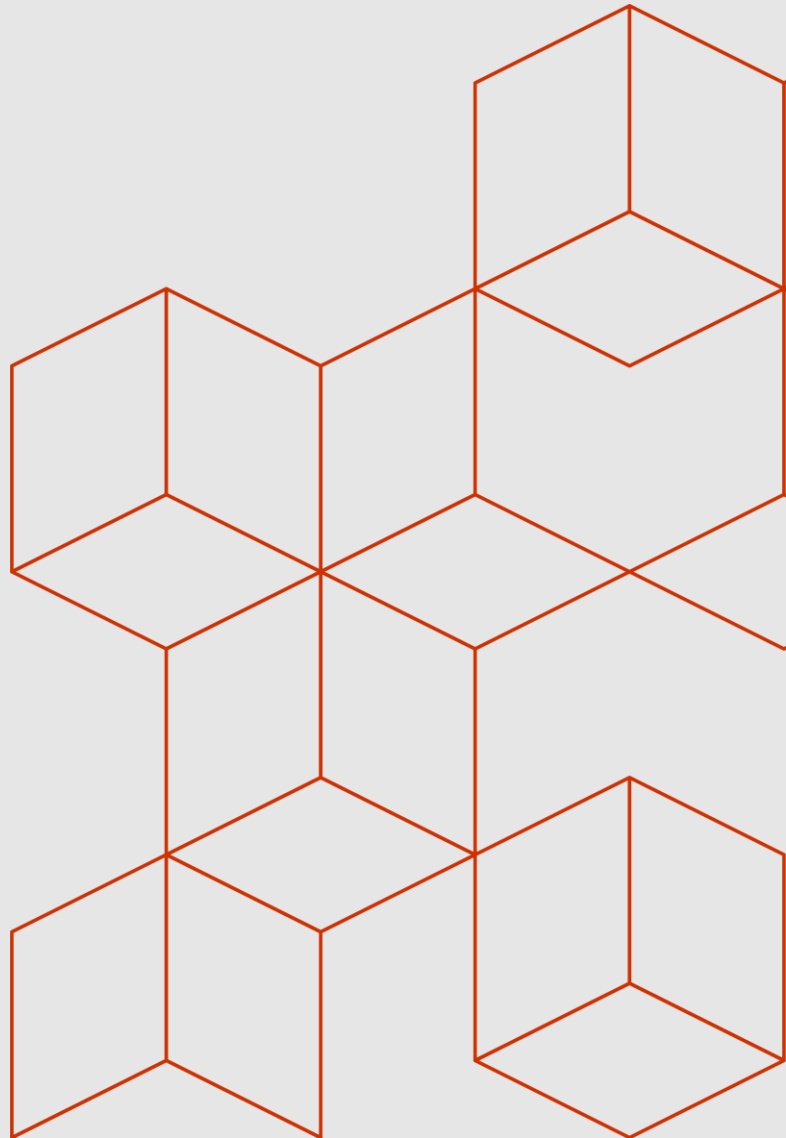
< Previous | Next > | Summary | Cancel

SCCM 1802

Co-management with Intune



Windows Information Protection
+
Azure Information Protection



WIP & AIP – v1607: Side by side

WIP

- Basic, context-aware protection
- User action not needed for protection
- Clipboard, etc., is seamless Work ←→Work
- Protected sharing via corp servers

AIP

- Granular, app-level, policy-based protection
- Requires user action

Side-by-side technologies, different keys, complementary scenarios

WIP & AIP – v1703: USB roaming

What you get

- WIP uses Azure RMS key on removable storage
- Auth to Azure RMS, opens on v1703 and later PCs
- Tenant-wide user access by default
  - Can adjust access with RMS templates

What you need

- Configure WIP to use AIP for removable media (E3 subscription)
- Creators Update (v1703) or later client

WIP & AIP – v1809: WIP as label outcome

What you get

- WIP applied to labeled files on create/modify/arrival
- Set via Office/M365 Security & Compliance Center (SCC)

What you need

- Office/M365 Security & Compliance Center
- Windows 10 v1809 client
- Windows Defender Advanced Threat Protection (E5 subscription)

MAM Without enrollment (1703)

- MAM without enrollment limits policy scope
  - Does not turn on device-wide policies
- WIP is “app management” part of MAM-only
- Only enlightened* apps can be managed
- Requires AAD integration
- Home/Pro/Enterprise

WIP Learning (1703)

- Detects unknown apps accessing work
- Intune stores learning data for two weeks
- Azure Log Analytics stores data up to a year
- Works in all enforcement levels
- Gives deployment confidence
  - Know when rules are complete
  - Can stay up to date with changes

Overview - Microsoft O|

windows-analytics-demo.portal.mms.microsoft.com/#Workspace/overview/solutions/details/index?_timeInterval.intervalDuration=604800&solutionId=DeviceHealthProd

Microsoft Operations Management Suite

Data based on last 7 days | Data Plan: Free | Windows-Analytics-Demo

Overview ▸ Device Health (Preview)

Time: Last 7 days

DEVICE RELIABILITY

Device Reliability

More info

Overview

These reports provide you with insights into operating system kernel crashes (blue screens) in your organization so that you can take actions to reduce them.

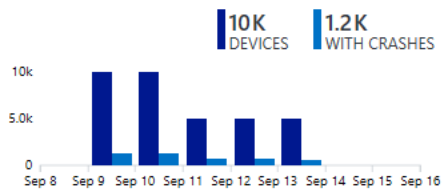
Frequently crashing devices

See which devices are crashing the most; flattening or replacing outliers may help increase average device reliability. The chart at the top shows daily counts of devices with at least one crash in the prior two weeks. The list at the bottom shows devices with the most crashes in the last week.

Driver-induced OS crashes

See which drivers have caused the most devices to crash in

FREQUENTLY CRASHING DEVICES



DEVICE	CRASH COUNT
BarbaraGr-Win.Contoso	87
AndreaLo-Win.Contoso	5
HectorSp-Laptop.Contoso	3
HaGabriel-Dsk.Contoso	3
VilmaGu-Work.Contoso	3
KoDsktp-Office.Contoso	3
SamuelRo-Book.Contoso	3
JamesJe-Box.Contoso	3
KevinCr-Dsk.Contoso	3
Brian-Win-162.Contoso	2

See all...

DRIVER-INDUCED OS CRASHES

Devices crashed by drivers

542

DRIVER	DEVICES CRASHED
igdkmd64.sys	349
netwbw02.sys	44
nvlddmkm.sys	41
iacamera64.sys	23
csi2hostcontrollerdriver.sys	20
mrvlpcie8897.sys	17
intcdaud.sys	17
iaprecisetouch.sys	13
netwtw04.sys	6
usbhub3.sys	3

See all...

WINDOWS INFORMATION PROTECTION

WIP App Learning

More info

Overview

Windows Information Protection (WIP) helps protect work data from accidental sharing.

Your IT department configures which apps are allowed to access work data, and controls the level of protection.

App Learning

Display details about all unconfigured apps on managed devices that try to access work data, and reduce disruptive prompts by adding rules to allow data sharing from approved apps.

APP LEARNING

115
Apps with WIP access events

279
Devices reporting WIP access events

APP	DEVICES
GOOGLE CHROME (CHROME.E...	99
SURFACE (SURFACEDTX.EXE)	41
MICROSOFT OFFICE 2016 (LYN...	28
LENOVO PLATFORM SERVICE (...	17
MICROSOFT.MICROSOFTEDGE	14
NOTEPAD++ (NOTEPAD++.EXE)	14
MICROSOFT.SKYPEAPP	14
SKYPE (SKYPE.EXE)	14
MICROSOFT OFFICE 2016 (UC...	12
MICROSOFT® SILVERLIGHT	9

See all...

Ask me anything

10:08 PM
9/15/2017

Log Search - Microsoft | New tab

windows-analytics-demo.portal.mms.microsoft.com/#Workspace/search/index?_timeInterval.intervalDuration=604800&q=DHWipAppLearning%20%7C%20where%20AppName%20%3D%3D%20%22SKYPE%20(SKYPE.EXE)%22%20%7C%20summarize%20

Microsoft Operations Management Suite | Data Plan: Free | Windows-Analytics-Demo

Log Search

Export | PowerBI | Alert | Save | Favorites | History | Analytics

Data based on last 7 days

1 bar = 6hrs

12:00:00 AM
Sep 9, 2017

TYPE (1)

DHWipAppLearning	23

COMPUTER (14)

BeverlyHe-Work.Contoso	4
KarlyBook179.Contoso	3
Theresa-Wkst.Contoso	3
HowardCo-Office.Contoso	2
StCorey-Office.Contoso	2

[+] More

APPNAME (1)

SKYPE (SKYPE.EXE)	23

WIPACTIONTYPE (2)

FILEREAD	20
NETWORKACCESS	3

+Add

Show legacy language converter

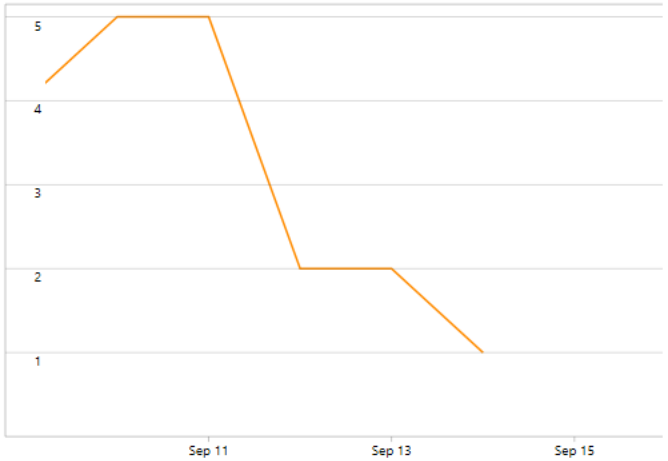
```
DHWipAppLearning | where AppName == "SKYPE (SKYPE.EXE)" | summarize DeviceCount = dcount(ComputerID) by WipAppId
```

Advanced Analytics

00:00:00.359

8 Results | Chart | Table | Windows Information Protection

HITS BY APP NAME - TRENDING



HITS BY APP ID

APP ID	DEVICE COUNT
O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US\SKYPE\SKYPE.EXE\7.40.0.103	8
O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US\SKYPE\SKYPE.EXE\7.39.0.102	3
O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US\SKYPE\SKYPE.EXE\7.28.0.101	1
O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US\SKYPE\SKYPE.EXE	3

Ask me anything

11:08 PM
9/15/2017

Automatic Recovery (1709)

- If you revoke the wrong device …
- …User just re-enrolls to restore access
- PC backs up key to AAD user account

Office, Intune, and SCCM

- WIP support in Office 365 ProPlus
- Intune enhancements
  - MAM “without enrollment” support
  - One click to allow all recommended apps
  - Auto-populates SharePoint sites to cloud resources
- SCCM 1706 enables WIP USB roaming
- SCCM 1802 enables WIP co-management
- Office 365 MIP label support

Example Deployment Options

Quick Start: No prompts, Selective Wipe only

What you get…

- All apps still “just work” – no blocks or copy/paste prompts
- SharePoint, OneDrive, and Outlook email are encrypted
- Encryption retained on copy to USB
- Learn which apps are used for work
- Audit file decryption & Edge uploads outside SPO
- Data is revoked on BYOD unenroll / retire

Quick Start: No prompts, Selective Wipe only

How to configure…

- Apps: Allow Recommended apps
- Enforcement: Silent
- Network: SharePoint online sites (preconfigured by Intune)
  Email address domains (primary pre-added by Intune)
  Recommended Neutral Sites (i.e. MS logon sites)
- Azure RMS: On (no template needed)
- Other: Defaults
  (If Windows 10 <1709, include DRA)

Light enforcement: Only enforce some apps

What you get…

- Selected apps prompt for disclosure, rest “just work”
- More data auto-encrypted: LOB apps’ files & LAN d/l
- Encryption kept by default on USB copy
- Audit: Decryption, Edge uploads, and paste disclosures
- Revoke data on unenroll for BYOD

Light enforcement: Only enforce some apps

How to configure…

- Apps: Allow Recommended apps, plus LOBs
  Explicitly Deny social media apps
  Deny Exemption to your Allowed & Denied apps
  Exempt everything else
- Enforcement: Allow Overrides
- Network: As Quick Start + LAN config
- Azure RMS: On
- Other: As Quick Start
  (Optional: Define file types to encrypt from LAN)

Strict enforcement: Fully managed, work only

What you get…

- Only your apps open work files and LAN file shares
- Most data auto-encrypted: Files in user profile
- Encryption kept on USB copy

Strict enforcement: Fully managed, work only

Configure in SCCM…

- Apps: Allow Recommended apps, plus LOBs
  Exempt apps as needed
- Enforcement: Hide Overrides (a.k.a. “Block”)
- Network: (As Light Enforcement)
- Azure RMS: On
- Other: (As Quick Start)

- Non-WIP: Deploy Known Folders redirection to OneDrive for Business