Avecto defendpoint

Group Policy Editor Sandboxing Guide

Software Version: 5.0.102.0 GA

Document Version: 1.0

Document Date: November 2017

Table of Contents

Chapter 1 - What is Sandboxing?

Sandboxing in Defendpoint isolates the web browser and any content that is accessed such as websites, PDFs and Microsoft Office documents and Microsoft Outlook email attachments. This is achieved using the URL and content rules and groups contained in a Defendpoint configuration.

Sandboxing uses a "sandbox", which is an isolated environment that protects the user and their private documents from anything running inside. If any untrusted or malicious websites or content are opened, the effects of the malware are contained. When the user next logs off, the sandbox, along with any malicious code and unwanted changes, are removed from the endpoint.

Avecto use a unique approach to sandboxing, by using the Windows security model to provide the user with a lightweight and seamless experience, whilst also providing native application support with minimal performance overheads.

1.1 - Sandboxing Contexts

There are three '*contexts*' under which websites and downloaded content can be opened:

'Native/Private' – The website or content is considered completely safe and therefore not isolated.
Websites and applications running in the native/private context have full access to your private documents, but no access to your trusted or untrusted documents.

'Trusted' – The website or content is opened in a sandbox and any downloaded files are considered trusted. If they are opened subsequently they will be opened in a trusted sandbox.
Websites and applications running in the trusted sandbox have read-only access to your private documents, and full access to your trusted documents. They have no access to your untrusted documents.

Untrusted – The website or content is opened in a sandbox any downloaded files are considered untrusted. If they are opened subsequently they will be opened in an untrusted sandbox.
Websites and applications running in the untrusted sandbox have no access to your private or trusted documents. They have full access to your untrusted documents.

When the **Classify email attachments for sandboxing** general rule is enabled all attachments are classified as untrusted.

Chapter 2 - How Does Sandboxing Work?

2.1 - Permissions and Security

Defendpoint sandboxing offers a protective environment to safely open and browse internet content and email attachments. Windows native security ensures that isolated web browsers and applications remain completely isolated from the user's private data. Defendpoint allows content to be saved to the real user's profile in a secure manner so that downloaded content can be persisted after the sandbox has been deleted.

Any content that is saved to the user's profile always opens in the same sandboxed context it originated from, and cannot be accessed by native applications. This helps to protect the user from any malicious code that may be embedded in untrusted content.

Below is a summary of the user's folders that are accessible from a sandbox, and the restrictions that each sandbox context will incur for private content in those folders:

User folder	Trusted browsing access to private content	Untrusted browsing access to private content
Desktop	Read-only	No Access
Documents	Read-only	No Access
Downloads	Read-only	No Access
Pictures	Read-only	No Access
Videos	Read-only	No Access
Music	Read-only	No Access
Personal	Read-only	No Access
Favorites / Links	Full Control	Full Control

Content that is saved to any other user folder will be contained inside the sandbox, and is removed when the sandbox is deleted.

Defendpoint sandboxing also isolates any sandbox browsing history and cookies so that they are separate to the private data of the real user.

2.2 - Contexts

Any website can be set to run in a particular sandbox by configuring groups of website domains called a URL group. URL groups are then assigned rules to control their access to personal data by redirecting websites into one of three contexts. Additionally, any documents you open or download from a website will subsequently open in the same context.

There are three contexts that can be selected for sandboxing:

Context	Description	Recommended Use
None	Websites and documents are opened natively, and have full access to your private data. No sandbox is used.	Local and internal websites, where full access to private documents is required. For example, corporate intranets and web-based document stores.
Trusted Browsing	Websites and documents are granted read-only access to your private data, but are prevented from modifying or deleting your private data. A trusted sandbox is used.	Trusted websites that require regular access to private documents, for example corporate cloud storage solutions and CRM systems.
Untrusted Browsing	Websites and documents are prevented from reading, modifying or deleting your private data. An untrusted sandbox is used.	Ideal for all other web browsing.

2.3 - Tagging and Classification

When a user uses a browser to navigate to a website, Defendpoint uses URL rules to allocate a sandbox context for that website. If a document or content is downloaded from the website, Defendpoint 'tags' the content to track which sandbox it has originated from. Tagging is the process used to identify the classification of content.

Classification defines whether the content is:

- **Private** – Content downloaded from a private browsing session. By default all existing content is also treated as private.
- **Trusted** – Any content that originated from the trusted browsing sandbox.
- **Untrusted** – Any content that originated from the untrusted browsing sandbox.

The tag persists so that Defendpoint can consistently apply the correct sandbox context, even if it is edited, renamed or duplicated.

2.4 - URL Redirection

When an internet browsing session starts, Defendpoint opens the web browser in the appropriate sandbox context. This can result in the web browser closing and re-opening. Subsequent websites that are visited will also be opened in the appropriate sandbox context. In the event that a website needs to be redirected to a different context, a new instance of the web browser will be created. If an instance of the web browser already exists for that context, a new tab is created within the existing web browser instance. This ensures that websites under different contexts remain completely isolated. This transition between the different sandbox contexts happens automatically without any interaction required by the user.

In order for sandboxing to successfully redirect web addresses in Internet Explorer, third-party BHOs (Browser Helper Objects) specifically PGBHO must be enabled.

On certain operating systems, such as Windows Servers, BHOs are disabled by default. The Microsoft KB article below documents how to disable BHOs. Follow the instructions but at Step 4 verify that third-party browser extensions are enabled.

http://support.microsoft.com/kb/298931

Chapter 3 - Implementing Sandboxing

You can implement sandboxing by creating rules within your workstyles that target websites and content, and by defining sandboxing options for a specific user, group or environment.

3.1 - Configuring Sandboxing Settings

Sandboxing settings are always available for you to configure if your policy has sandboxing in it. If you would like to configure sandboxing for your policy but it doesn't yet contain sandboxing, please follow these instructions.

To configure sandboxing settings in your Defendpoint policy:

1. Right-click on the **Windows** node and click **Advanced Policy Editor Settings**. The **Advanced Policy Editor Settings** dialog box appears.
2. Click the **Show Sandboxing Settings** check box. This allows you to subsequently configure sandboxing in Defendpoint.

All of the sandboxing settings, such as URL groups, are now visible in the interface. Features relating to Sandboxing are documented in the Sandboxing Guide for ease of use.

3.2 - URL Groups

URL groups are used to define a list of URL hostnames (websites) so that URL rules can be assigned to each group based on their potential risk. The list of URL hostnames is used to identify whether the website you are navigating to should be opened in a specific sandbox context.

The hostname is the part of the website address preceded by a double slash, and before the single slash. For example:

Address	Hostname
https://www.avecto.com	www.avecto.com
https://mail.google.com	mail.google.com

The hostname can also be used to match specific subdomains of a website. For example:

Hostname	Will match
google.com	https://www.google.com https://mail.google.com https://drive.google.com
mail.google.com	http://mail.google.com

3.2.1 - Creating URL Groups

To create a URL group:

1. Expand the **Defendpoint Settings** node and then expand the **Windows** node.
2. Select the **URL Groups** node.
3. Right-click the **URL Groups** node and then click **New URL Group**.

A new URL group will be created and it will be highlighted so that you can rename it. Press **Enter** once you have renamed the URL group. You can now add URLs to the URL group you have created.

Create a URL group for each of the three sandboxing contexts:

- Private websites – websites that you don't want to sandbox
- Trusted websites – websites that you want to open in a trusted sandbox
- Any websites – all websites that haven't been defined in the other two groups that should be opened an untrusted sandbox.

For more information on sandboxing contexts see **Sandboxing Contexts** detailed on page 4.

3.2.2 - URL Group Description

You can set a description for a URL group by accessing the URL group properties:

1. Select the **URL Group** in the tree pane.
2. Right-click the **URL Group** and then click **Properties**.
3. Set the **Description** in the **Properties** dialog box.
4. Click **OK**.

3.2.3 - Inserting URLs

To insert a URL:

1. Select the relevant URL group.
2. Right-click the URL list in the details pane and select **Insert URL**. The **Insert URL** wizard appears.
3. Enter a URL or domain hostname and click **Next**.
4. On the **Description** page of the wizard add a valid description and click **Next**.
5. Configure the **URL Criteria** (detailed below) for the URL (by default the **Host URL** and **Protocol URL** rules will be selected and the **Host URL** rule cannot be cleared).
6. Click **Finish** to add the URL to the URL group.

3.2.4 - URL Definitions

The **Insert URL** wizard provides various URL definitions. The Defendpoint Client must match every definition you configure before it will trigger a match (the rules are combined with a logical AND). The following definitions are available:

Host URL

Matches the website based on the hostname. The hostname is an explicit match, and does not allow partial matches or wildcards. However, if you want to match any hostname, an asterisk (*) is allowed.

Multiple domains can be added to the same URL definition by using a comma (,). For example, you can create a single definition for both google.com and google.co.uk by entering "google.com,google.co.uk" in the domain name property of a URL definition.

For domains that contain commas, you will need to 'escape' the comma be entering ",,"

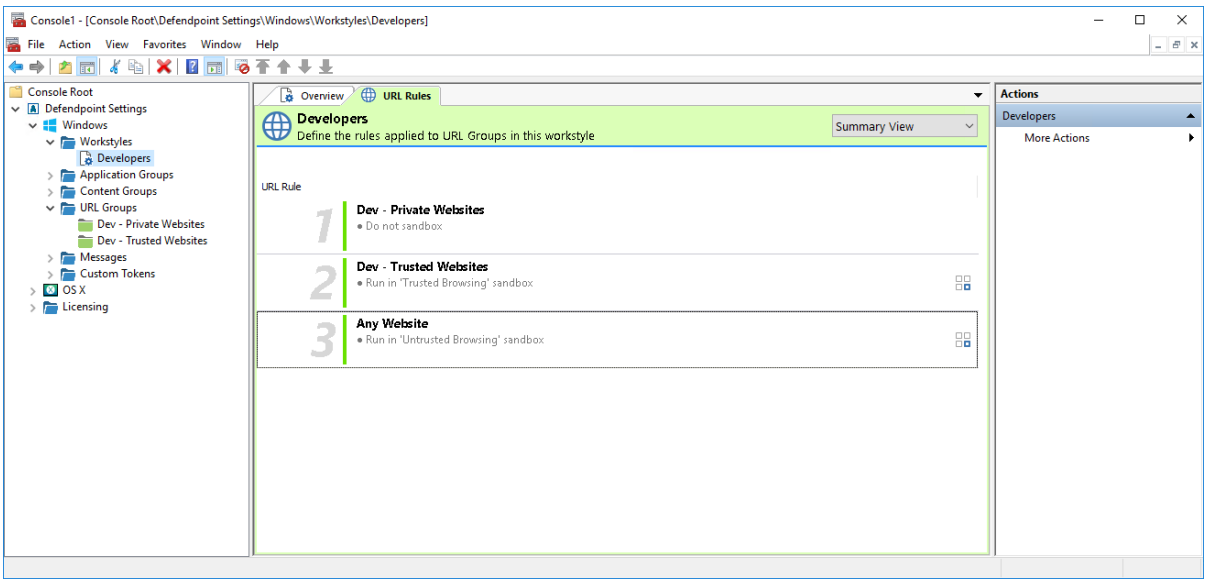
Protocol URL
Matches the website based on the protocol. There are two URL protocols available: HTTP and HTTPS. This criteria is optional, and if disabled the definition will match both HTTP and HTTPS protocols.

Zone URL
Matches the website based on the zone as configured in Internet Explorer Zones. For more information on configuring Internet Zones, see http://support.microsoft.com/kb/174360.

For each of the three criteria you can change the matching logic between '**URL matches**' or '**URL does NOT match**'. To do this, click on the blue definition name to toggle the matching logic.

3.3 - URL Rules and Workstyles

URL groups are then assigned to a URL rule on the **URL Rules** tab of a workstyle. URL rules dictate which sandbox context is used to open each website in the URL group.



When a user uses a browser to navigate to a website, Defendpoint evaluates each URL rule in the order they are displayed. In the example shown in the image above, Defendpoint first checks if there are any matches against URLs that have been added to the **Private Websites** group and redirect the website to a native web browser.

If no match is found, Defendpoint proceeds to check for matches in the **Trusted Websites** group, redirecting any matching website to a web browser in the trusted browsing sandbox.

If no match is found in the preceding groups, the **Any Website** group ensures that all other websites are automatically redirected to a web browser in the untrusted browsing sandbox.

The example shown above is recommended best practice. It offers the highest level of protection from unknown or compromised websites containing malicious code exploits.

The order in which each URL rule is evaluated can be changed by right-clicking a rule and selecting any of the **Move Top**, **Move Up**, **Move Down** or **Move Bottom** options.

3.3.1 - Inserting a URL Rule

To insert an URL rule:

1. Select the relevant workstyle in the tree pane.
2. Select the **URL Rules** tab in the details pane.
3. Right-click in the **URL Rules** tab and click **Insert URL Rule**.
4. The **Create URL Rule** dialog box appears.
5. Select the relevant URL group using the **Target URL Group > Click to select** drop-down menu.
6. Select the desired sandbox context using the **Sandbox** drop-down menu. See **Contexts** detailed on page 5 for information on the different contexts.
7. If you want to audit the URL rule being matched then select **On** for **Raise an Event**. This will log events to the local **Event Log** as well as your configured event audit location (ERP).
8. If you want to run a custom script when the URL rule has been matched, then select **On** for **Run a Script**. See the Policy Editor Admin Guide for more information on auditing with custom scripts.
9. Click **OK** to create the URL rule.

If you select **On** or **On (Anonymous)** (does not log the username) for **Raise an Event** then an event will be logged to the Application Event Log every time that a website is redirected to, from or between a sandbox.

The **Summary View** and **Detail View** can be used to show information about your URL group entries in either graphical form or in table form.

For more information please see **How Does Sandboxing Work?** detailed on page 5.

3.3.2 - Determining Browsers to Sandbox

URL rules control whether a website accessed using Internet Explorer or Google Chrome is opened natively, in a trusted sandbox, or in an untrusted sandbox.

To *limit* browser sandboxing to only one of these browsers, use an Advanced Agent Setting.

Type	Value Name	Value Data	Result
DWORD	BrowserSandboxingEnabled	0	No browsers are enabled for sandboxing
DWORD	BrowserSandboxingEnabled	1	Only Chrome is enabled for sandboxing
DWORD	BrowserSandboxingEnabled	2	Only Internet Explorer is enabled for sandboxing
DWORD	BrowserSandboxingEnabled	3	Chrome and Internet Explorer are enabled for sandboxing

Unless one of the Advanced Agent Settings to disable Chrome sandboxing has been set prior to installation, a Defendpoint extension will be automatically added to Google Chrome when the Defendpoint Client is installed.

If you decide you do not want to use sandboxing for Google Chrome and want the extension to be removed, disable Chrome sandboxing using an Advanced Agent Settings. The extension will automatically be removed when the machine is next restarted.

3.4 - Sandboxing Content

Once you have defined URL groups and assigned those groups to URL rules in your workstyle, the next step is to define how downloaded content will be managed. This is achieved using content rules.

3.4.1 - Content Control

Content control allows you to control the accessibility of privileged content. Content groups provide a means of targeting specific types of content, based on file/folder, drive, or controlling process. Rules determining the behavior for that content are applied to each content group in a workstyle.

There are two main use cases for applying content control:

To allow standard users to modify privileged content, without having to assign admin rights to either the user, or the application used to modify the content.

- Content groups can be added to content rules where the content can be assigned admin rights. When this is done, any user who receives the workstyle can modify matching content without requiring an administrator account.

To block access to content or directories.

- Content groups can be added to content rules where the ability to open the content can be controlled with a *Block* action. When this is done, any user who would normally be able to open and read the content would be blocked from opening the content.

The following sections explain how to create content groups including content definitions, and how to assign groups to content rules to apply the specific content control rules that meet your requirements.

3.4.2 - Creating Content Groups

To create a content group:

1. Expand the **Defendpoint Settings** node.
2. Select the **Content Groups** node.
3. Right-click the **Content Groups** node and then click **New Content Group**.

A new content group will be created and it will be highlighted so that you can rename it. Press **Enter** once you have renamed the content group. You can now add content to the content group.

Content Group Description

You can set a description for a content group by accessing the content group properties:

1. Select the **Content Group** in the tree pane.
2. Right-click the **Content Group** and then click **Properties**.
3. Set the **Description** in the **Properties** dialog box.
4. Click **OK**.

Inserting Content

To insert a content type:

1. Select the relevant content group.
2. Right-click the content list in the details pane and select **Insert File**. The **Insert Content** wizard appears.
3. Enter a file or folder name that you wish to insert. Alternatively, you can browse for a file or folder using the **Browse File** and **Browse Folder** buttons.
4. After selecting a content / file type to insert, click **Next**.
5. Enter a description for the content and then click **Next**.
6. Configure the **Content Criteria** (detailed below) for the content (by default the **Match File or Folder Name** rule will be selected).
7. Click **Finish**.

Target Content Definitions

The **Insert Content** wizard provides various content definitions. The Defendpoint client must match every definition you configure before it will trigger a match (the rules are combined with a logical AND).

The following definitions are available:

- File/Folder
- Drive
- Controlling Process
- Sandboxing Classification

3.4.3 - Content Rules

The **Content Rules** tab of the workstyle is where content rules are applied to content groups.

Content rules define the actions Defendpoint will take when content (a file) is opened (double-clicked) by the user.

For more information about content groups, see **Creating Content Groups** detailed above.

Inserting a Content Rule

To insert a content rule:

1. Select the relevant workstyle in the tree pane.
2. Select the **Content Rules** tab in the details pane.
3. Right-click in the **Content Rules** tab and click **Insert Content Rule**.
4. The **Create Content Rule** dialog box appears.
5. Select the relevant content group from the **Target Content Group > Click to select** drop-down menu.
6. Select the desired **Action** from either **Allow Modification** or **Block Access**.

If you have selected the action **Block Access**, the **Apply Access Token** option will be disabled.

7. If you want to prompt the user before the content is modified or blocked then select a message or notification from the **Show End User Message** drop-down menu.
8. You must define one or more messages or notifications before you can assign an end user message. If you do not want to prompt the user with a message or notification, then select **Off**. For more information see **End User Messaging** detailed on page 1.
9. If you are allowing the content in the selected content group to be modified, select the correct access token from the **Apply Access Token** drop-down menu.

   Apply Access Token can be set to one of the following options (or you can define any number of custom access tokens, which will appear at the end of the list of standard options):

   - **Passive (No Change)** – This option allows you to audit the file types in the content group without modifying the access token.
   - **Enforce User's Default Rights** – This option ensures that the file types in the content group are assigned the user's default rights.
   - **Drop Admin Rights** – This option removes local admin rights from the access token for file types in the content group.
   - **Add Admin Rights** – This option adds local admin rights to the access token for file types in the content group.

10. If you want to audit the content rule being matched then select **On** for **Raise an Event**. This logs events to the local **Event Log**.
11. If you want to run a custom script when the content rule has been matched, then select **On** for **Run a Script**. For more information on audting and reporting, see the Defendpoint for Windows Administration Guidesee **Auditing and Reporting** detailed on page 18.

If you select **On** or **On (Anonymous)** (does not log the username) for **Raise an Event** then an event will be logged to the event log every time a process launches for the selected content group.

The **Summary View** and **Detail View** can be used to show information about your content group entries in either graphical form or in table form.

3.5 - Allow Users to Reclassify Documents

A document that already exists locally on your system is classified as *private*. Therefore, it will not be opened in a sandbox.

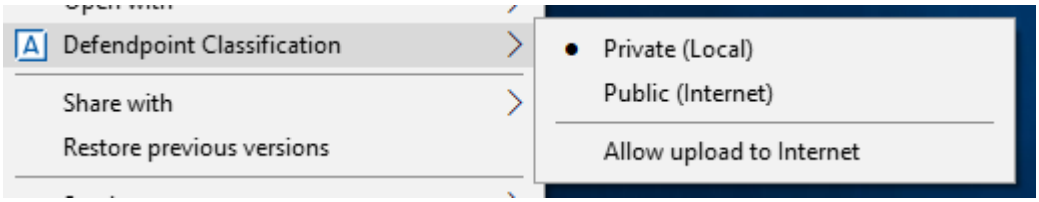
A file downloaded to your system from either a trusted or untrusted sandbox is classified as *public* and will be opened in either a trusted or untrusted sandbox, depending on which sandbox the document originated from.

If you want users to be able to reclassify documents, set the **Allow user to reclassify documents** general rule to **Enabled** on the relevant workstyle. When this rule is enabled, a user can toggle the classification of a document between *private* and *public*:

- A document that was originally *private* and is reclassified *public* will automatically be opened in an **Untrusted** sandbox.
- A document that was originally *public* (sandboxed) and is reclassified private will **not** be opened in a sandbox.
- A document that was originally *public* (sandboxed), has been reclassified *private*, and then subsequently reclassified back to *public*, will be opened in a sandbox context appropriate to its original status: **Trusted** or **Untrusted**.

Enabling this rule also gives users the option of allowing private documents to be uploaded to the internet from an untrusted sandbox. This is achieved via a toggled option that is available from the context menu of a particular document.

1. Right-click on a private document and select **Defendpoint Classification > Allow upload to Internet**.



2. Repeat this with a document that has been classified as **Public** and that was downloaded from a trusted sandbox. Despite their different classifications, both files are now readable from the untrusted sandbox, therefore allowing you to upload them to websites running in the untrusted context.

3.5.1 - Setting Classify Context Text

When Defendpoint is configured to allow the user to change the Defendpoint classification of documents, a context menu is accessible by right-clicking on a document. You can configure the text that is displayed for each option available on the context menu.

The following text strings can be set:

- **Title** – The title text of the context menu.
- **Private** – The description for *Private* classification.
- **Public** – The description for *Public* classification.
- **Allow upload to Internet** – The description for the *Upload to Internet* option

The display text can be configured for multiple languages.

To set the classify context menu text:

1. Right-click the **Messages** node and select **Manage Classify Content text**.
2. The **Configure Languages** dialog box appears.
3. To edit the text for an existing language, double-click the text under **Text to display**. To add a new language, click **Add language**.
4. Once you have finished editing the ActiveX text strings, click **OK** to finish.

If language settings for the region of the end user have not been configured, then the default language text will be displayed. To change the default language, select the desired language and click **Set Default**.

3.6 - Sandboxing Definitions

Two sandboxing specific definitions are available when sandboxing is enabled:

- **Sandbox Classification** – This option allows you to target an application based on the application's sandbox classification. This is a useful way of applying privilege management or application control rules to applications that were downloaded from either inside or outside of a sandbox.

  If you want to reverse the outcome of this definition, to target applications which do not match the definition, then click the definition to toggle between **matches** and **does NOT match**.

  This definition is available on content types and on all application types except Remote PowerShell Script and Remote PowerShell Command.

- **Sandbox Context** – This option allows you to target an application based on the application's sandbox context. This is a useful way of applying privilege management or application control rules to applications launching either inside or outside of a sandbox.

  If you want to reverse the outcome of this definition, to target applications which do not match the definition, then click the definition to toggle between **matches** and **does NOT match**.

  This definition is available on content types and all application types.

3.7 - Advanced Sandboxing Environment

The Advanced Sandboxing Environment feature allows for customization of the sandbox setup configuration. Use of this feature is reserved for troubleshooting application compatibility issues, and should not be used except under strict instruction from Avecto Technical Support.

Chapter 4 - Email Attachments

Email poses another significant risk to organizations, as targeted attacks on organizations frequently leverage unsolicited emails to breach network defenses. Malicious documents such as PDFs and Microsoft Office documents are crafted to appear genuine and familiar to their target, for example a CV or survey report. Given the volume of email in a typical organization and each user receives on a daily basis, coupled with the advanced subversion techniques used by email scammers, it is extremely difficult to filter malicious attachments from genuine content.

Defendpoint sandboxing can mitigate Outlook email-based malware by ensuring that attachments are opened within a sandbox, isolating and containing any potential threats that are encountered by users without impacting their productivity. If a malicious document is opened, the effects are contained, protecting the user and their data. Documents can still be opened and edited, and users can still save attachments to their own workspace, and Defendpoint ensures that saved attachments always open back inside the sandbox.

Defendpoint sandboxing is a very effective way of protecting the organization from Outlook email-based threats, and preventing user data and endpoints from being compromised by targeted or spam attacks. Coupled with other Defendpoint settings, you can ensure that any malicious processes or payloads from email attachments are blocked and audited, preventing exploits from ever running and informing Security Response teams of the event. Combined with application rules anything can be stopped from running including scripts, applications and system commands.

With Defendpoint sandboxing, your users can continue to use Outlook email and open attachments seamlessly, whilst keeping the organization free from malware infections originating from email.

4.1 - Enabling Sandboxing for Outlook Attachments

In order for attachments to be sandboxed, Defendpoint uses a general rule to classify the attachment file and content rules are used to control how the file is handled.

The **Classify email attachments for sandboxing** general rule, when enabled, ensures that all email attachments will be isolated as untrusted items in the untrusted sandbox. This will occur when the attachment is opened from within Outlook, or when the attachment is saved to disk and later opened from Windows Explorer.

To enable sandboxing for Outlook attachments:

1. Create a content rule for the types of attachment that you want to control. See **Creating Content Groups** detailed on page 12 and **Inserting a Content Rule** detailed on page 13 for more information on creating content groups and rules.
2. Highlight the workstyle that contains the content rule and open the **General Rules** tab.
3. Enable the **Classify email attachments for sandboxing** general rule.

Outlook attachments will now be sandboxed using the rules defined in your workstyle. The types of attachments that are isolation can be customized using content rules and content groups.

4.2 - Opening an Attachment from Outlook

When content rules have been configured, if a user opens an attachment from Outlook, Defendpoint launches the default document handler inside the untrusted sandbox, so that the attachment is opened in an isolated environment.

4.3 - Saving an Attachment from Outlook

When a user saves an email attachment to disk, the content is automatically classified ensuring that when opened, it will open in the sandbox.

4.4 - Applying Application Rules to Email Attachments

Application rules can also be applied to email attachments to apply restrictions to the applications that are allowed to run when an attachment is opened. Applying strict rules that only allow specific applications (such as Adobe Reader, Microsoft Office Apps, etc.) is a very effective way of blocking any unknown processes, scripts or malicious payloads from executing, thereby providing effective and proactive defense against exploits. For more information on application rules see the Defendpoint for Windows Administration Guide.

4.5 - Messaging

Information can be displayed to users via the Defendpoint end user messaging feature. This feature allows users to be presented with relevant information when Defendpoint intervenes, for instance with an application blocking message or when a user's action will have a specific result e.g. warning a user that they are about to open a PDF using an outdated version of Adobe Reader. Messages can also warn the user that something has run, or attempted to run, allowing them to contact the IT Help desk. Messages can be configured for application rules, content rules and URL rules. For more information on end user messaging see the Defendpoint for Windows Administration Guide.

4.6 - Auditing

Defendpoint can be configured to audit the opening of Outlook email attachments, and the execution of any applications that run as a result of opening an attachment. Auditing can be enabled or disabled within each workstyle rule, and can be configured to audit all activity, or just a subset of activity based on the application or type of content being opened.

For more information on the types of events that are generated for sandboxing, see **Auditing and Reporting** detailed on page 18

For more information on auditing and reporting, see the Defendpoint for Windows Administration Guide.

Chapter 5 - Auditing and Reporting

The Defendpoint Client sends events to the local application event log, dependent on the audit and privilege monitoring settings within the Defendpoint Settings.

5.1 - URL Events

The Defendpoint client sends events to the local syslog. Defendpoint events can be viewed from the console application by navigating to `/var/log/Defendpoint/audit.log`.

Event ID	Description
650	Defendpoint redirected a user's web browser navigation

Each URL event contains the following information:

- Origin URL
- Origin URL Domain
- Origin URL Protocol
- Origin Sandbox
- Origin Internet Zone
- Target URL
- Target URL Domain
- Target URL Protocol
- Target Sandbox
- Target Internet Zone
- Command Line

5.2 - Content Events

Event ID	Description
600	Content has been updated with add admin rights token.
601	Content has been updated with a custom token.
602	Content has been updated with drop admin rights token.
603	Content has been updated with passive token.
604	Content has been updated with enforce user's default rights token.
605	Content access was blocked.
606	Content access was canceled by the user.
706	A Trusted Application Protection event was passively audited.
716	A Trusted Application Protection event was blocked.
720	A Trusted Application Protection event was canceled by the user.

Each content event contains the following information:

- Content File Name
- Content File Description
- Content File Version
- Content Owner SID
- Content Owner Name
- Content Owner Domain SID
- Content Owner Domain Name
- Content Owner Domain Name NetBIOS
- Controlling Process Command Line
- Controlling Process ID

Chapter 6 - Printing from a Sandbox

When a website or application is opened within a sandbox the content displayed can be sent to a printer safely without any danger of compromising the local computer or wider network.

The way this is achieved is by converting the content or document into an XPS file (which is a form of print file). The XPS format cannot contain scripts or active content, therefore providing a safe format for printing documents from isolated applications. This process requires two print dialog boxes.

When you send content or documents that are classified as public to print:

1. Select the usual **Print** option for the current application that is displaying the content; usually **File > Print**.
2. The expected **Print** dialog box for the application will display your usual printers, ensuring a familiar printing experience. Define any page range parameters you require and select **Print**. The file will then be converted into an XPS file.
3. There will be a very short delay and then the standard Windows **Print** dialog box will display. Here you can adjust any of the available options and choose one of your usual printers. Click **Print** and the file will be sent to the appropriate printer for output.

The diagram below shows the user experience when printing from an isolated application: