Copyright Notice

The information contained in this document ("the Material") is believed to be accurate at the time of printing, but no representation or warranty is given (express or implied) as to its accuracy, completeness or correctness. Avecto Ltd, its associated companies and the publisher accept no liability whatsoever for any direct, indirect or consequential loss or damage arising in any way from any use of or reliance placed on this Material for any purpose.

Copyright in the whole and every part of this document belongs to Avecto Ltd ("the Owner") and may not be used, sold, transferred, copied or reproduced in whole or in part in any manner or form or in or on any media to any person other than in accordance with the terms of the Owner’s Agreement or otherwise without the prior written consent of the Owner.

Accessibility Notice

In the event that you are unable to read any of the pages in this document, please contact us and we will arrange to get an accessible version to you.
# Table of Contents

## Installation and Deployment

1. **Introduction** .................................................................................................................. 12
   1.1. About McAfee ePolicy Orchestrator ........................................................................... 13
   1.2. Defendpoint & McAfee .............................................................................................. 13

2. **Planning and Preparation** ............................................................................................... 15
   2.1. Defining User Roles .................................................................................................. 15
   2.2. Implementing Least Privilege ..................................................................................... 15
       2.2.1. Known Applications ......................................................................................... 16
       2.2.2. Unknown Applications ..................................................................................... 16
       2.2.3. Flexible Elevation ............................................................................................. 16

3. **Defendpoint Software Installation** ................................................................................... 17
   3.1. Installing the Defendpoint Server Extension .............................................................. 17
   3.2. Importing the Defendpoint Client Package into ePO .................................................. 18
   3.3. Defendpoint Reporting ............................................................................................. 18

4. **Upgrading Defendpoint from previous versions of Defendpoint or Privilege Guard** 19
   4.1. Planning your deployment ......................................................................................... 19

## Configuring Defendpoint

5. **Defendpoint Modules** .................................................................................................... 21
   5.1. Privilege Management ............................................................................................. 21
   5.2. Application Control .................................................................................................. 23
   5.3. Sandboxing .............................................................................................................. 24

6. **Defendpoint Policies** ...................................................................................................... 26
   6.1.1. Disconnected Users ............................................................................................. 26

7. **Licensing** ........................................................................................................................ 27
   7.1.1. Inserting Licenses ................................................................................................. 27

8. **Workstyles** ........................................................................................................................ 28
   8.1. Workstyle Wizard ..................................................................................................... 28
   8.2. Creating Workstyles ................................................................................................. 29
       8.2.1. Disabling / Enabling Workstyles ......................................................................... 30
8.2.2. Workstyle Precedence ................................................................. 30
8.3. Filtering Workstyles ................................................................. 31
  8.3.1. Account Filters ................................................................. 31
  8.3.2. Computer Filters .............................................................. 32
  8.3.3. Time Range Filter ............................................................. 33
  8.3.4. Expiry Filter .......................................................................... 34
  8.3.5. WMI (Windows Management Information) Filters ..................... 34

9. Managing Applications ............................................................... 36
  9.1. Creating Target Application Groups ......................................... 36
  9.2. Duplicating Target Application Groups ...................................... 36
    9.2.1. Inserting Executables and Scripts ....................................... 36
    9.2.2. Add Application > Executable ............................................ 37
    9.2.3. Inserting ActiveX Controls ................................................. 38
    9.2.4. Inserting Installer Packages ................................................. 39
    9.2.5. Inserting COM Classes ...................................................... 41
    9.2.6. Inserting Windows Store Applications ................................ 43
    9.2.7. Inserting Windows Services ............................................... 44
    9.2.8. Advanced Options ............................................................ 45
  9.3. Inserting Applications from Templates ...................................... 46
  9.4. Inserting Applications from Events ......................................... 46
  9.5. Inserting Applications from Browsing ...................................... 47
  9.6. Remote PowerShell Management ............................................ 48
    9.6.1. Remote PowerShell Scripts ................................................. 48
    9.6.2. Remote PowerShell Commands .......................................... 49
  9.7. Application Rules .................................................................... 50
    9.7.1. Inserting an Application Rule ............................................. 50
  9.8. On Demand Application Rule .................................................. 52
    9.8.1. Managing Languages ........................................................ 52

10. Configuring Sandboxing ............................................................. 54
  10.1. What is Sandboxing ............................................................... 54
  10.2. Sandbox Contexts ................................................................. 54

Sandbox Contexts
Configuring Sandboxing
---

Remote PowerShell Management
Inserting Applications
---

Inserting Applications from Templates
---

Inserting Applications from Events
---

Inserting Applications from Browsing
---

Remote PowerShell Commands
---

Remote PowerShell Scripts
---

WMI (Windows Management Information) Filters
---

On Demand Application Rule
---

Managing Languages
---

Workstyle Precedence
---

Account Filters
---

Computer Filters
---

Time Range Filter
---

Expiry Filter
---

WMI (Windows Management Information) Filters
---

Defendpoint 4.3 ePO Edition
Administration Guide

avecto.com
10.3. URL Groups ........................................................................................................55
10.4. URL Rules and Workstyles ...........................................................................55
  10.4.1. Content Sandboxing ...................................................................................56
  10.4.2. Enabling Internet Zone Mapping ...............................................................57
  10.4.3. Allowing User to Reclassify ......................................................................57
10.5. Printing ............................................................................................................58
10.6. Sandboxing email attachments .....................................................................59
  10.6.1. Enabling sandboxing for Outlook attachments ......................................60
  10.6.2. Opening an attachment from Outlook .....................................................60
  10.6.3. Saving an attachment from Outlook .......................................................60
  10.6.4. Applying Application control rules to email attachments .....................60
  10.6.5. Messaging .................................................................................................61
  10.6.6. Auditing ....................................................................................................61
11. Managing URLs ..................................................................................................62
  11.1. Creating Target URL Groups .......................................................................63
  11.2. Duplicating Target URL Groups .................................................................64
  11.3. Inserting URLs to Target URL Groups .......................................................64
    11.3.1. URL Definitions ......................................................................................64
  11.4. URL Rules .....................................................................................................64
    11.4.1. Inserting a URL Rule ..............................................................................65
12. Content Control ....................................................................................................67
  12.1. Creating Content Groups ............................................................................67
  12.2. Duplicating Content Groups ......................................................................67
  12.3. Inserting Content to Target Content Groups .............................................68
    12.3.1. Target Content Definitions ..................................................................68
  12.4. Content Rules ...............................................................................................68
    12.4.1. Inserting a Content Rule ......................................................................68
13. General Rules .......................................................................................................71
  13.1. Allow User to Unlock a Shared Workstation .............................................71
  13.2. Collect User Information .............................................................................72
  13.3. Collect Host Information .............................................................................72
13.4. Prohibit Privileged Account Management ................................................................. 73
13.5. Windows Remote Management Connections ............................................................ 73
13.6. Allow User to Reclassify Documents ........................................................................... 74
13.7. Classify email attachments for sandboxing ................................................................. 74

14. **End User Messaging** ............................................................................................... 75

14.1. Creating Messages ...................................................................................................... 75
14.2. Message Boxes ........................................................................................................... 76
  14.2.1. Message Design ..................................................................................................... 76
  14.2.2. Message Text ........................................................................................................ 79
  14.2.3. Managing Languages ......................................................................................... 79
  14.2.4. Image Manager ................................................................................................... 81
  14.2.5. Challenge / Response Authorization ................................................................. 82
  14.2.6. Challenge / Response – Designated User Option ............................................... 85
14.3. Message Notifications ............................................................................................... 86
  14.3.1. Setting the Notification Text ................................................................................ 86
14.4. Setting ActiveX Message Text .................................................................................. 86
14.5. Setting Classify Context Text ................................................................................... 87

15. **Custom Tokens** ....................................................................................................... 88

15.1. Creating Custom Tokens ........................................................................................... 88
15.2. Editing Custom Tokens ............................................................................................. 88
  15.2.1. Groups ................................................................................................................ 88
  15.2.2. Privileges ............................................................................................................. 90
  15.2.3. Integrity Level .................................................................................................... 90
  15.2.4. Process Access Rights ....................................................................................... 91

16. **Utilities** .................................................................................................................. 93

16.1. Application Search .................................................................................................... 93
16.2. Importing and Exporting Defendpoint Policy ........................................................... 93
  16.2.1. Import Defendpoint Policy .................................................................................. 93
  16.2.2. Export Defendpoint Policy ................................................................................ 93
16.3. Template Policies ..................................................................................................... 94
16.4. Manage Audit Scripts ............................................................................................... 94
Defendpoint 4.3 ePO Edition
Administration Guide

16.5. Advanced Agent Settings ............................................................................. 94

17. Advanced Configurations Settings ................................................................. 96
  17.1. Privilege Monitoring .................................................................................... 96
  17.2. Workstyle Options .................................................................................... 96
  17.2.1. Events ..................................................................................................... 96
  17.2.2. Privilege Monitoring Log Files ............................................................... 97
  17.3. Advanced Sandboxing Environment .......................................................... 97

Deploying Defendpoint Settings .......................................................................... 98

18. Configuration Precedence ............................................................................... 99

19. Deployment Methods ..................................................................................... 100

20. Avecto End User Utilities ............................................................................... 101
  20.1. Avecto Network Adapter Manager ............................................................... 101
  20.2. Avecto Printer Manager ............................................................................. 102
  20.3. Avecto Programs and Features Manager .................................................... 103
  20.4. Defendpoint Activity Viewer ...................................................................... 103

21. Troubleshooting ............................................................................................ 104
  21.1. Check Defendpoint is Installed and Functioning ....................................... 104
  21.1.1. Check Settings are Deployed ................................................................. 104
  21.1.2. Check Policies are Licensed ................................................................. 104
  21.1.3. Check Workstyle Precedence .............................................................. 104

22. Auditing and Reporting .................................................................................. 105
  22.1. Dashboards ............................................................................................... 105
  22.2. Events ........................................................................................................ 107
  22.2.1. Process Events ...................................................................................... 107
  22.2.2. Configuration Events ............................................................................ 110
  22.2.3. Content Events ..................................................................................... 111
  22.2.4. URL Events .......................................................................................... 112
  22.2.5. User / Computer Events ...................................................................... 112
  22.2.6. McAfee ePO / Avecto Database Events (Threat?) ............................... 113
  22.3. Server Tasks – Avecto Threat Event Purge .............................................. 113
  22.4. Server Tasks – Enterprise Reporting Purge ............................................. 114
22.5. Auditing with Custom Scripts .......................................................... 115

23. Setting up Enterprise Reporting for Defendpoint ePO Edition ......................... 116
   23.1. Defendpoint ePO Edition Reporting Options .............................................. 116
   23.2. Installation Tasks .................................................................................. 117
      23.2.1. Basic level – ePO Queries and Reports Feature (Threat Events) ............... 117
      23.2.2. Advanced level – Avecto Enterprise Reporting in McAfee ePO Extension ....... 117
      23.2.3. Accounts ....................................................................................... 118
   23.3. Database Sizing and Resource Consumption .............................................. 118
      23.3.1. Data Retention Considerations .......................................................... 118
      23.3.2. Database Sizing ................................................................................ 118
   23.4. Defendpoint Reporting Database Installation .............................................. 121
      23.4.1. Installation ....................................................................................... 121
   23.5. Configuring Avecto Reporting for Enterprise Reporting Data ....................... 125
      23.5.1. Configuring access to Reporting Server Charts ...................................... 125
      23.5.2. Configuring access to Reporting Server for ePO Queries ......................... 126
      23.5.3. Server Tasks – Avecto Event Staging ..................................................... 127
      23.5.4. Server Tasks – Avecto Pre-caching Reports (optional) ............................. 129
   23.6. Performance Limitations ........................................................................ 130

24. Reputation Settings ..................................................................................... 132
   24.1. Server Tasks ........................................................................................ 133
   24.2. Reputation in Reporting ......................................................................... 134

Appendices ...................................................................................................... 137

Appendix 1. How Sandboxing Works ................................................................... 138
   A 1.1. Sandbox Permissions and Security ......................................................... 138
   A 1.2. Sandbox Contexts .............................................................................. 139
   A 1.3. Tagging and Classification ..................................................................... 139
   A 1.4. URL Redirection .................................................................................. 140
   A 1.5. Defendpoint Classification .................................................................... 140
   A 1.6. Allow Upload to Internet ..................................................................... 141

Appendix 2. Built-in Groups ............................................................................... 142
   A 2.1. Built-in Groups ..................................................................................... 142
Installation and Deployment

In this section you will find the following chapters:

- Introduction
- Planning and Preparation
- Defendpoint Software Installation
- Upgrading Avecto Software
1. Introduction

Defendpoint, the proactive endpoint security software from Avecto, uniquely combines the technologies of privilege management, application control and sandboxing to protect the operating system, software environment and corporate data from unknown cyber threats.

Defendpoint empowers users to be free without compromising security. Complementing existing patching and anti-malware strategies, it offers strength and depth across both desktops and servers as a holistic solution to endpoint security.

Defendpoint works by firstly enabling the successful removal of admin rights via Privilege Management, which provides a solid foundation to immediately improve overall security.

The Application Control module allows standard users to access only the trusted applications they need through simple yet effective whitelisting techniques.

Sandboxing adds the final layer of defense. Our innovative technology isolates and contains web-based activity, by leveraging the Windows security model, to protect users from online malware.

With Defendpoint, you can apply just the right amount of control to strike an effective balance between security and user freedoms.

Privilege Management

Defendpoint Privilege Management assigns privileges to applications, not users, allowing you to remove admin rights and protect the operating system. With this flexible approach, individuals can still access the applications, tasks and scripts they need to perform their job roles so that they can be productive without compromising security.

Privilege Management provides a solid security foundation, protecting your endpoint from attacks that rely on elevated privileges. It protects the operating system by allowing all users to run with standard accounts, dramatically improving the security posture of the endpoint.

You’ll benefit from all the tools you need to successfully manage an environment without admin rights. With flexible rules and a fully customizable end user experience; employees have just the right amount of access to perform the tasks they require as part of their job roles.

Application Control

Ensuring users are free to access and install the applications they need without compromising security is critical for business. Defendpoint Application Control solves the traditionally difficult challenge of managing business applications.

With its advanced capabilities, you can take a more pragmatic approach to whitelisting without locking down the endpoint, so that users retain the flexibility they need to be productive.

By taking control of your software environment and applying simple rules to manage trusted applications, you automatically reduce risk by blocking the unknown. Application control is so effective that experts analyzing real-world data, including The Council on Cyber Security (in association with SANS), name it the most essential strategy for mitigating cyber threats.
Sandboxing

The Defendpoint Sandboxing module provides an extra level of reassurance to cover the most common entry point for malware and hackers – the internet.

Unlike traditional sandboxing solutions that focus on building barricades, Defendpoint takes a unique approach to isolating content. Leveraging the native Windows security model, all untrusted activity runs inside a secure container. Vulnerabilities in web browsers, plugins and downloaded documents are safely contained and Defendpoint controls the flow of content in and out of the sandbox, resulting in a seamless end user experience.

With Sandboxing, you can safely contain any malicious activity, without restricting your users.

1.1. About McAfee ePolicy Orchestrator

McAfee ePO software, the foundation of the McAfee Security Management solution, unifies management of endpoints, networks, data, and compliance solutions. More than 45,000 organizations use McAfee ePO software on nearly 60 million nodes to manage security, streamline and automate compliance processes, and increase overall visibility across security management activities. With its scalable architecture, fast time to deployment, and ability to support enterprise systems, McAfee ePO software is the most advanced security management software available.

Only McAfee ePO offers:

**End-to-end visibility** — Get a unified view of your security posture. Drillable, drag-and-drop dashboards provide security intelligence across endpoints, data, mobile, and networks for immediate insight and faster response times.

**Simplified security operations** — Streamline workflows for proven efficiencies. Independent studies show ePO software helps organizations of every size streamline administrative tasks, ease audit fatigue, and reduce security management-related hardware costs.

**An open, extensible architecture** — Leverage your existing IT infrastructure. McAfee ePO software connects management of both McAfee and third-party security solutions to your LDAP, IT operations, and configuration management tools. LDAP Servers can be made available via the built-in registered servers in ePO.


1.2. Defendpoint & McAfee

Defendpoint is implemented as a server extension to McAfee ePolicy Orchestrator, enabling workstyles to be managed through the ePO Policy Catalog. Granular auditing and reporting of Defendpoint activity using ePO integrated dashboards and query editor as well as the Avecto own reporting module.

The Defendpoint ePO Edition Enterprise Reporting module uses the Defendpoint Enterprise Reporting database to store Defendpoint audit data for reporting.

The Defendpoint Client package is deployed to endpoints as a Client Task through the ePO System Tree.

If you do not wish to use McAfee ePO for deployment of the Client package, the Defendpoint Client is available as a standalone MSI or Executable package, which can be deployed using any suitable third-party deployment solution.
Avecto client configuration is deployed to endpoints through ePO Policy Assignments, which are automatically applied by the Defendpoint Client.

**Note:** If you do not wish to use McAfee ePO for deployment of the workstyles then you may import/export workstyles as an XML file, and use any suitable deployment solution to deploy the XML file to a set location on each client computer.
2. Planning and Preparation

2.1. Defining User Roles

Defendpoint is an easy solution to deploy, but you will want to spend some time preparing suitable workstyles for your users. Implementing least privilege may require workstyles to be tailored to users’ roles.

The table below shows three typical user roles, but we recommend that you create roles that are tailored to your environment.

<table>
<thead>
<tr>
<th>Role</th>
<th>Requirement for Admin Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Corporate User</td>
<td>Problem applications and simple admin tasks.</td>
</tr>
<tr>
<td>Laptop User</td>
<td>Problem applications, intermediate admin tasks and authorized software installation.</td>
</tr>
<tr>
<td>Technical User</td>
<td>Complex applications, advanced admin tasks and ad hoc software installation.</td>
</tr>
</tbody>
</table>

Defendpoint can cater for all types of users, including the most demanding technical users such as system administrators and developers.

You should also educate users on what they should expect from a least privilege experience, before transferring them to standard user accounts. This ensures that they will report any problems they encounter during the process of moving to least privilege.

*Note:* Contact your solution provider or Avecto to gain access to templates to cater for more complex use case scenarios.

2.2. Implementing Least Privilege

The first step is to identify the applications that require admin privileges for each of the roles you’ve defined. These can fall into one of three categories:

1. **Known Admin Applications** - You already have a definitive list of applications that require admin rights to run.

2. **Unknown Admin Applications** - You are not sure of the applications that require admin rights to run.

3. **Flexible Elevation** - The user will require flexibility and can’t be restricted to a list of applications.
2.2.1. Known Applications

For this category you should simply add the relevant applications to the Defendpoint Application groups for the users, which will automatically elevate these applications when they are launched. You may then remove admin rights from these users. See the Managing Applications section for more information.

2.2.2. Unknown Applications

For this category you have two choices to help you discover the applications that require admin rights:

1. Set up Defendpoint workstyles to monitor privileged application behavior. The Defendpoint audit logs will highlight all of the applications that require admin rights to run. See the Privilege Monitoring section for more information.

2. Set up Defendpoint workstyles to give the user the “on demand” elevation facility, and instruct the user to use this facility for any applications that fail to run once you have taken the user’s admin rights away. The Defendpoint audit logs will highlight all the applications that the user has launched with elevated rights. See the On Demand Application Rule and the Privilege Monitoring sections for more information.

You may now use the audit logs to determine the relevant set of applications that you want to give admin rights to for these users. See the Managing Applications section for more information.

2.2.3. Flexible Elevation

For this category you should set up Defendpoint workstyles that give the user an “on demand” elevation facility, which allows the user to elevate any applications from a standard user account. All elevated applications may be audited, to discourage users from making inappropriate use of this facility. See the On Demand Application Rule section for more information.
3. Defendpoint Software Installation

Defendpoint ePO Edition includes two installation packages:

> Defendpoint_4_1_xxx_0.zip – McAfee ePO Server extension, which includes the workstyle management console and dashboard reports.

> S_AVECPG4100.zip – Defendpoint Client package, which includes both 32-bit and 64-bit versions of the Defendpoint Client.

3.1. Installing the Defendpoint Server Extension

To install the Defendpoint Server Extension:

1. Log in to ePolicy Orchestrator and navigate to Menu > Software > Extensions.

2. In the Extensions screen, click Install Extension in the bottom left corner. The Install Extension dialog will be displayed.

3. Enter or browse to the location of the Defendpoint Server Extension package Defendpoint_4_1_xxx_0.zip and click OK.

4. In the Install Extension summary screen, click OK to proceed with the installation.

5. Once installed, the Defendpoint Server Extension will be displayed under Third Party Extensions.

The Defendpoint server extension requires the following permissions to be enabled for user accounts requiring access to Defendpoint workstyles:

> Avecto Defendpoint Extension Permission (Run Permission for Avecto Defendpoint Extension)

> Avecto Defendpoint Workstyle (View and Change Workstyle Settings)

Additionally, the following McAfee ePO permission must be enabled to assign policy rules:

> Workstyle Assignment Rule (View and Edit Rules)

These permissions can be set in ePO from User Management > Permission Sets.
3.2. Importing the Defendpoint Client Package into ePO

To install the Defendpoint Client Package:

6. Log in to ePolicy Orchestrator and navigate to Menu > Software > Master repository.

7. In the Packages in Master Repository screen, click Check In Package. The Check In Package wizard will be displayed.

8. In the Package screen, select Product or Update (.ZIP) for the Package Type, and enter or browse to the location of the Defendpoint Client Package S_AVECPG4100.zip, and click Open and then click Next at the bottom right of the screen.

9. In the Package Options screen, choose Current for the Branch, then click Save at the bottom right of the screen to save the Client Package to the Master Repository.

The Defendpoint Client Package will be displayed in the Packages in Master Repository list.

Note: Upgrade scenarios may lead you to use branches other than Current to manage two Defendpoint Client packages concurrently.

3.3. Defendpoint Reporting

Defendpoint offers two levels of reporting:

> A basic reporting level that requires no other infrastructure setup and stores ePO thereat events.

> More sophisticated interactive reports using a separate database instance to store events.

For more information please see Setting up Enterprise Reporting for Defendpoint ePO Edition.
4. Upgrading Defendpoint from previous versions of Defendpoint or Privilege Guard

4.1. Planning your deployment

Before upgrading any versions of Defendpoint or Privilege Guard software or existing settings, it is recommended that you test your deployment in a pre-production environment. This will help mitigate any unforeseen compatibility issues, and avoid disruption to the business.

**Note:** In the following sections, all references to Defendpoint, by default also refer to Privilege Guard.

All Defendpoint MSI and Executable installers will automatically remove old versions of Avecto software when installed. Therefore, it is not necessary to manually remove old versions prior to installation of new versions.

The Defendpoint Client guarantees backwards compatibility with previous versions of Defendpoint, but does not guarantee forwards compatibility. Therefore it is recommended that all Defendpoint Clients are upgraded before rolling out new versions of Defendpoint.

**Note:** When upgrading Avecto software, it may be necessary for a reboot to occur in order to complete the installation. When installing in silent mode, a reboot will occur automatically. Therefore it is recommended that upgrades are performed out of core business hours, or during scheduled maintenance windows, to avoid loss of productivity.
Configuring Defendpoint

In this section you will find the following chapters:

- Defendpoint Modules
- Defendpoint Policies
- Licensing
- Workstyles
- Managing Applications
- Configuring Sandboxing
- Managing URLs
- Content Control
- General Rules
- End User Messaging
- Custom Tokens
- Utilities
- Advanced Configuration Settings
5. Defendpoint Modules

The three modules that together comprise Defendpoint are highly integrated systems that operate with one another seamlessly to protect the operating system, software environment and user data from unknown cyber threats.

Privilege Management

The close-knit integration between the Defendpoint Application Control and Privilege Management modules eliminates the potential for conflict or clashes. A single configuration engine and management console, with a single set of rules and common application definitions ensures you maximize productivity.

Application Control

By combining application control with privilege management, all of your corporate applications can be safely elevated without the use of admin rights. The system files and folders are automatically protected and therefore can be whitelisted easily. This allows you to focus on unknown or user applications, greatly reducing complexity. A single policy engine across all three Defendpoint modules means there’s no risk of conflict, and total consistency in reports.

Sandboxing

Tight integration with application control and privilege management enables targeted rules to be defined inside the sandbox. With only a small number of applications needing to run inside a sandbox, such as the web browser and document readers, any executable malware payloads are prevented from ever launching and requests for admin rights can be denied and logged.

5.1. Privilege Management

Privilege Management assigns privileges to applications, not users, allowing you to successfully remove admin rights and protect the operating system. With this flexible approach, individuals can still access the documents, tasks and scripts they need to perform their job roles so that they can be productive without security compromise.

- Eliminate admin rights
- Assign privileges directly to applications
- Protect the endpoint from insider threats

Targeted assignment of privileges

Precision targeting rules mean that admin rights can be assigned securely to individual applications, rather than users, so that all users are able to successfully operate with standard user accounts. Every user is granted just the right level of privilege to suit their specific job role, providing a seamless transition to least privilege.
Broad application support

With support for a broad set of application types, Privilege Management adds the flexibility to cater for the needs of all users, and all privileged tasks. Whether it’s an application, installation, script or COM task, Defendpoint handles all your diverse user requirements.

Works seamlessly with User Account Control

Replace unwanted prompts and specifically target applications that trigger Windows UAC messages. By intercepting and monitoring all exceptions, you can refine policies and provide users with quick and simple ways to request the access they need.

On-demand access to privileges

Grant the ability to elevate applications on-demand, with gated controls such as reason justifications and password verification. Ensure that even advanced users such as sysadmins have the ability to perform their specific roles without compromising security.

Simple to use and manage

Wizard-based workstyles and templates make it faster to get started. A flexible filter engine with targeted control means you can map policies to specific job roles, even web developers and sysadmins in the data center. Simple configuration with clear process flows means less clutter and better visibility, keeping it manageable across thousands of users.

Clear, customizable messaging

You can create an unlimited number of highly personalized messages for managing exceptions that fall outside broader rules. Depending on the level of control you apply, the user can self-approve access with full audit trails, or request a response code from your IT desk. Prompts can be integrated with helpdesk ticketing systems for ease of use.

Layers of in-built security for added protection

Prevent the creation of rogue admin accounts, with unique privileged account protection. Patented anti-tamper ensures Defendpoint cannot be circumvented, safeguarding you from code injection, shatter attacks and token hijacks. The option to digitally sign policies ensures their authenticity from creation until rollout.

Actionable intelligence via advanced reports

Easily identify privileged users and activity with usable data that enables you to keep admin rights to a minimum. Graphical dashboards and reports with drill-down options provide fast access to as much detail as you need. Reports are built on familiar and trusted SQL Server and SQL Reporting Services, which are fully integrated across all three Defendpoint modules (optional for Defendpoint ePO Edition).

Seamless integration with application control

The close-knit integration between Defendpoint’s Application Control and Privilege Management modules eliminates the potential for conflict or clashes. A single configuration engine and management console, with a single set of rules and common application definitions ensures you maximize productivity.
5.2. Application Control

Defendpoint Application Control solves the traditionally difficult challenge of managing business applications. With its advanced capabilities, you take a more pragmatic approach to whitelisting so that users retain the flexibility they need to be productive. Simple yet highly effective management makes it possible to maintain application control across even the largest enterprise.

- Block unauthorized applications
- Handle diverse user needs flexibly
- Defend against zero day and targeted attacks

Take a pragmatic approach

Gone are the days of complex configurations based on hash functions. A simple interface means you set broad rules based on criteria such as software publisher. With these ring-fencing techniques, application whitelisting is finally achievable across thousands of endpoints. Management is also straightforward, with wizard-based workstyles and templates.

Simple to use and manage

Intelligent rules, simple groups and pre-built templates ensure a positive impact from day one. System files and folders are automatically protected for easy whitelisting, allowing the IT team to focus on handling unknown applications.

Clear, customizable messaging

Embrace the exceptions by setting clear, branded messages and prompts to support access to previously unsanctioned software. Tailored options allow you to choose automatic approval for advanced users, protected by full audit trails, or utilize challenge/response codes. Over time, monitor requests and use this insight to fine tune your workstyles.

Combine with privilege management to multiply the security benefit

By combining application control with privilege management, all of your corporate applications can be safely elevated without the use of admin rights. The system files and folders are automatically protected and therefore can be whitelisted easily. This allows you to focus on unknown or user applications, greatly reducing complexity. A single policy engine across all three Defendpoint modules means there’s no risk of conflict, and total consistency in reports.

Overcome challenges with migrations

An operating system migration is the perfect opportunity to regain control over applications across your estate. Use the comprehensive monitoring and reporting capabilities of Defendpoint to identify all of the applications in use across your endpoints, and then use this information to build your workstyles.

Broad set of supported application types

Defendpoint supports a broad set of application types, including the latest Windows 8 store apps. A wide range of criteria ensures accurate identification and simple management, with the ability to validate scripts by hash or certificate.
Patented URL tracking and control

This unique feature allows an application to be identified based on its download source, so you can apply whitelisting rules based on software origin. All downloaded applications are tracked so that rules are applied whenever the software is executed.

Content control

By extending the principles of application control to configuration files and documents, you gain precise control over which configurations, directories and documents are accessible to users or system administrators. When combined with privilege management, access to privileged files can be quickly and easily granted, without needing to assign admin rights to either the user or the application.

Controlled administration

Support advanced use cases such as Windows Services and driver commands as well as remote management through PowerShell. Deliver policies mapped to user or server roles to protect and audit sysadmins and prevent misconfiguration.

5.3. Sandboxing

Defendpoint Sandboxing extends security coverage to the most common entry point for malware and hackers - the internet. Using Windows native security to isolate web-borne threats, your corporate data is protected by a safety net, while the end user experience remains seamless.

> Capture web-borne threats
> Isolate untrusted activity
> Secure your data from malware

Isolate and destroy malware

With the internet representing the greatest window of opportunity for outside threats, malware’s stealthy approach often requires no interaction with the user to gain entry. Even those you consider to be ‘good apps’ can be infected when they open content that originates from the internet. The Defendpoint sandboxing module allows you to contain malware threats that originate online, without restricting user behavior.

Tried and tested security you can rely on

We use the established native security of Windows to create isolated containers for any untrusted tasks. This is the same security model you are already using to secure and control access to the files on your network. With this approach to isolation, the sandbox is extremely lightweight so there’s no need for higher spec PCs and apps just work as expected.

Secure yet usable

Documents downloaded from the internet are automatically merged into the user’s profile, while protecting any private files from being read or overwritten. And when the file is reopened in future it will automatically remain isolated; creating a safe working environment without delays or restrictions. The document can still be edited, saved and printed, meaning the user can function as normal but their personal and corporate data remains protected.
Flexible approach to content control

Defendpoint automatically tracks and classifies documents based on their origin, ensuring that documents will automatically reopen in the isolated environment from where they originated. With added flexibility, the default protection can be overridden by the user if necessary. Users can also grant access to specific private files, allowing them to be uploaded, but not modified.

Seamless integration with Defendpoint modules

Tight integration with application control and privilege management enables targeted rules to be defined inside the sandbox. With only a small number of applications needing to run inside a sandbox, such as the web browser and document readers, any executable malware payloads are prevented from ever launching and requests for admin rights can be denied and logged.
6. Defendpoint Policies

Once you have installed the Defendpoint Server Extension, you can create Defendpoint policies from within the McAfee ePO Policy Catalog.

To create a new Defendpoint policy:

1. Log into ePO Policy Orchestrator and click on **Policy Catalog**.
2. In the **Product** drop-down list, choose **Avecto Defendpoint**.
3. Select the default policy **Avecto Blank Policy** and click **Duplicate**.
4. The **Duplicate Existing Policy** dialog will be displayed. Enter a name in the **Name** field (e.g. **Defendpoint Policy**), and optionally give the policy a description in the **Description** field.
5. Click **OK** to create the new policy.

**Note:** For the purposes of this guide the duplicate policy example above, **Defendpoint Policy**, will be used as the default starting point for relevant instructions.

The new policy will be displayed in the **Policy Catalog**. To edit the policy, click on **Defendpoint Policy**.

The policy summary screen will be displayed, which provides item summaries for the number of Workstyles, Target Application groups, Target URL groups, Target Content groups, Messages, Tokens and Licenses in the policy. As this is a blank policy, all summaries will be ‘zero’.

Each item summary includes an **Edit <Item>** button, which allows you to jump to that section of the policy.

Defendpoint incorporates an Autosave, Autosave Recovery and concurrent edit awareness feature to reduce the risk or impact of data loss and prevent multiple users from overwriting individual policies. For more information please refer to the **Autosave** appendix in this guide.

6.1.1. Disconnected Users

Disconnected users are fully supported by Defendpoint. When receiving policies from McAfee ePO, Defendpoint automatically caches all the information required to work offline, so the settings will still be applied if the client is not connected to the corporate network. Of course, any changes made to the policy will not propagate to the disconnected computer until the McAfee Agent re-establishes a connection to the ePO Server.
7. Licensing

The Defendpoint Client will not function unless it receives a valid license code. If multiple policies are applicable for a computer then as long as a valid license code appears in one of the policies then the Defendpoint client will function. For instance, you may decide to add the Defendpoint licenses to a policy that is applied to all ePO managed endpoints, which will ensure that all computers will receive a valid license (for those computers that have the Defendpoint Client installed). If you are unsure then it is recommended that you always add a valid license when you are creating Defendpoint policies.

7.1.1. Inserting Licenses

1. Log into ePO Policy Orchestrator and click on Policy Catalog.

2. Select the Defendpoint Policy and click on Edit Licenses.

3. Enter a valid license key into the License Key box in the right-hand pane and click Add License.

4. Click Save and then click Exit.

Note: License keys control access to the three Defendpoint modules individually. Confirm the product modules that you are licensed for to avoid unexpected results.
8. Workstyles

The three Defendpoint modules; Privilege Management, Application Control and Sandboxing, are implemented by the use of workstyles.

Workstyles are used to assign rules to applications, websites and content, audit activity and define sandboxing options for a specific user, group or environment. Workstyles are generated by the workstyle wizard and may contain auto-generated groups and rules depending on the type of workstyle you choose to create.

8.1. Workstyle Wizard

The workstyle wizard will guide you through the process of creating a Defendpoint workstyle. The options you select will determine the function of the workstyle.

Workstyle Type

The first choice to make is the type of workstyle you want to create. There are three types of workstyle that can be created in Defendpoint:

- **Controlling workstyle** - allows you to apply rules for access to privileges, applications and to define rules for sandboxing.

- **Monitoring workstyle** - allows you to monitor the use of applications, privileges and user logins.

- **Blank workstyle** - allows you to create an empty workstyle without any predefined elements.

Filtering

The next choice to make is which users the workstyle will be applied to:

- Standard users only

- Everyone, including administrators

The default choice is **Standard users only**. Additional filters can be added to the workstyle after it has been created. For more information on Filtering please refer to the Filtering Workstyles section of this guide.

Workstyle Modules

The Defendpoint suite includes three core modules. Only controlling workstyles incorporate these modules. A controlling workstyle may incorporate one or all of the modules. The three core modules are:

- Privilege Management

- Application Control

- Sandboxing

For more information on the Defendpoint Modules please refer to the Defendpoint Modules section of this guide.
8.2. Creating Workstyles

To create a new Workstyle in ePolicy Orchestrator:

1. From the Policy Catalog click on the Defendpoint Policy and select Edit Workstyles.
2. Select Actions > Create using Wizard.
3. Select a workstyle Type:
   > Controlling - allows you to apply controls for access to applications and privileges and to define sandboxing
   > Monitoring - allows you to monitor the use of privileged applications and privileged accounts.
   > Blank - allows you to create an empty workstyle without any predefined elements.
4. Click Next.
5. Select a filter for the new workstyle. If you wish to apply the new workstyle to standard users only, select Standard users only, or to apply the workstyle to all users (including administrators), select Everyone, including Administrators.
   > If you are creating a Monitoring workstyle you will be asked which versions of Windows are being monitored. Click Next.
6. If you are creating a Controlling workstyle, select one or more Defendpoint Modules and click Next.
7. The workstyle wizard will display pages appropriate to the Defendpoint module(s) you selected in Step 6. Complete the pages relevant to the workstyle type and any modules you have selected.
8. On the final page of the workstyle wizard provide a Name and a Description for the workstyle. If the workstyle has been configured to use a Challenge - Response message you will be asked to enter an authentication key. See Challenge / Response Authorization.
9. Select whether you would like to activate the workstyle now.
10. Click Finish to create the workstyle and exit the wizard.

Depending on the type of workstyle you created and any modules that have been included, Defendpoint will auto-generate certain groups and rules, messages, tokens and filters.

These auto-generated elements are appropriate to the options that are selected in the workstyle wizard and are described in subsequent sections of this guide.
8.2.1. Disabling / Enabling Workstyles

You may disable a workstyle, which will stop it from being processed by the Defendpoint Client.

To disable a workstyle:

1. Select the appropriate workstyle in the left-hand pane.

2. The Workstyle Summary will be displayed in the right-hand pane.

3. Click the Workstyle State to toggle the current state between Enable / Disable.

8.2.2. Workstyle Precedence

If you create multiple workstyles then those that are higher in the list will have a higher precedence. Once an application matches a workstyle, no further workstyles will be processed for that application, so it is important that you order your workstyles correctly if an application could match more than one workstyle.

To change the precedence of a workstyle:

1. Select the Workstyles node in the left-hand pane.

2. In the right-hand pane check the workstyle you wish to move.

3. Select Actions (or use the adjacent buttons) and choose from the available options; Up, Down, Top and Bottom until the workstyle is positioned appropriately.
8.3. Filtering Workstyles

Workstyle filters can be used to refine when a workstyle will actually be applied.

By default a workstyle will apply to all users and computers that receive it. However, you can add one or more filters that will restrict the application of the workstyle:

- **Account Filter** – this filter will restrict the workstyle to specific users or groups of users.
- **Computer Filter** – this filter will restrict the workstyle to specific computers (names or IP addresses), or Remote Desktop clients.
- **Time Filter** – this filter will restrict the workstyle to being applied at particular days of the week and times of the day.
- **Expiry Filter** – this filter will expire a workstyle at a set date and time.
- **WMI Filter** – this filter will restrict the workstyle based on the success or failure of a WMI query.

If you wish to configure a workstyle to apply if *all* filters give a positive outcome, select the option **ALL filters must match**. To configure a workstyle that applies if *any* filter gives a positive outcome, select the option **ANY filter can match**.

Filters can also be configured to apply if there are *no* matches. This is referred to as an ‘exclude’ filter. To set an exclude filter, check the filter and click the **Set NOT** button. (This does not apply to Time and Expiry filters).

**Note:** Time filters and Expiry filters can only be used once in a workstyle.

8.3.1. Account Filters

An account filter specifies the users and groups the workstyle will be applied to.

**Note:** When a new workstyle is created, a default Account filter will be added to target either **Standard Users only** or **Everyone, including administrators**, depending on your selection in the workstyle wizard.

To restrict a workstyle to specific groups or users:

1. Expand the appropriate workstyle in the left-hand pane and click **Filters**.
2. Select **Actions > Add Account Filter**.
3. Click on the new account filter to open the Add/Edit Accounts page.

4. Choose Browse to browse for an account, or select Add Account to add an account manually.

5. Click OK.

Domain and well-known accounts will display a Security Identifier (SID). The SID will be used by the Defendpoint Client, which will avoid account lookup operations. For local accounts the name will be used by the Defendpoint Client, and the SID will be looked up when the policy is loaded by the client. Local Account will appear in the SID column of the accounts list for local accounts.

Note: SIDs must be added if using a group as a filter on a non-domain machine.

By default, an Account filter will apply if any of the User or Group accounts in the list match the user. If you have specified multiple User and Group accounts, and want to apply the workstyle only if ALL entries in the Account filter match, then use the option All items below should match.

You may add more than one Account filter if you want the user to be a member of more than one group of accounts for the workstyle to be applied.

If an Account filter is added, but no User or Group accounts are specified, a warning will be displayed advising No accounts added, and the Account filter will be ignored.

Note: If All items below should match is enabled, and you have more than one User account listed, the workstyle will never apply as the user cannot match two different User accounts.

8.3.2. Computer Filters

A computer filter specifies the computers and IP addresses that the workstyle will be applied to.

To restrict the workstyle to specific computers:

1. Expand the appropriate workstyle in the left-hand pane and click Filters.

2. Select Actions > Add Computer Filter.
3. Click on the new computer filter to open the **Add/Edit Computers** page.

4. Choose **Browse Systems** to select a managed computer from the McAfee ePO System Tree, or select **Add Host Name** to manually enter the computer information.

5. When you have finished adding computers to the filter, click **Finish**.

To restrict the workstyle to specific IP addresses, follow the steps above, but click **Add IP Address** and enter an IP address.

**Note:** You can also use the wildcard * in any octet to include all addresses in that octet range, for example 192.168.*.*. Alternatively, you can specify a particular range for any octet, for example 192.168.0.0-254. Wildcards and ranges can be used in the same IP Address, but not in the same octet.

By default the hostname is matched against the host computer, where the workstyle is being applied. If a user logs on through RDP then you may instruct the computer filter to match against the remote desktop computer by checking the **Match the remote desktop (instead of the local computer)** checkbox. If the user logs on directly to the computer then the remote desktop will be the same as the computer.

You may add more than one computer filter if you want the computer to match more than one computer filter for the workstyle to be applied.

By default, a computer filter will apply if any of the hostnames or IP Addresses in the list match the computer. If you have specified multiple hostnames and IP Addresses, and want to apply the workstyle only if ALL entries in the Computer filter match, then check the option **All items below should match**.

### 8.3.3. Time Range Filter

A time range filter can specify the hours of a day, and days of week that a workstyle will be applied.

To restrict a workstyle to a specific date / time period of activity:

1. Expand the appropriate workstyle in the left-hand pane and click **Filters**.

2. Select **Actions > Add Time Range Filter**.

3. Click on the new time range filter.

4. Click on the 24 x 7 grid squares to toggle when the workstyle should be made **Active** or **Inactive** and click **OK**.

**Note:** Only one Time filter may be added to a workstyle.

The time filter is applied based on the user’s timezone by default. Uncheck the **Use timezone of user for time restrictions (otherwise use UTC)** checkbox to use UTC for the timezone.
8.3.4. Expiry Filter

An expiry filter specifies an expiry date / time for a workstyle.

To restrict a workstyle to an expiry date and time:

1. Expand the appropriate workstyle in the left-hand pane and click **Filters**.
2. Select **Actions > Add Expiry Filter**.
3. Click on the new expiry filter.
4. Set the date and time that you want the workstyle to expire on and click **OK**.

**Note:** Only one Expiry filter may be added to a workstyle.

The expiry time is applied based on the user’s timezone by default. Uncheck the **Use timezone of user for policy expiry (otherwise use UTC)** checkbox to use UTC for the timezone.

8.3.5. WMI (Windows Management Information) Filters

A WMI filter specifies if a workstyle should be applied, based on the outcome of a WMI query.

The filter allows you to specify the following:

- **Description** – Free text to describe the WMI query
- **Namespace** – Set the namespace that the query will execute against. By default, this is `root\CIMV2`.
- **Query** – The WMI Query Language (WQL) statement to execute
- **Timeout** – The time (in seconds) the client will wait for a response before terminating the query. By default, no timeout is specified.

**Note:** Long running WMI queries will result in delayed application launches. Therefore it is recommended that a timeout is specified to ensure that queries are terminated in a timely manner.

When a WMI Query is executed, the client will check if any rows of data are returned. If any data is returned, then the WMI query will be successful. If no data is returned or an error is detected in the execution, the WMI query will be unsuccessful.

It is possible for many rows of data to be returned from a WMI query, in which case you can create more complex WQL statements using WHERE clauses. The more clauses you add to your statement, the fewer rows are likely to return, and the more specific your WMI query will be.

The WMI filter includes several default templates for common WMI queries. To add a new WMI query from a template, click **Add via Template** and use the instant search box to quickly find a template.

WQL statements can include parameterized values which allow you to execute queries including select user, computer and Defendpoint properties. To use parameters, please refer to the Workstyle Parameters Appendix.

**Note:** WMI queries are always run as SYSTEM, and cannot be executed against remote computers or network resources. WMI filters do not support impersonation levels, and can only be used with SELECT queries.
By default, a WMI filter will apply if any of the WMI queries in the list return true. If you have specified multiple WMI queries, and want to apply the workstyle only if ALL queries return true, then check the option **All items below should match**.

If a WMI filter is added, but no WMI queries are specified, a warning will be displayed advising **No queries added**, and the WMI filter will be ignored.
9. Managing Applications

Target Application groups are used to define logical groupings of applications.

Target Application groups are assigned to workstyles, so you must define Target Application groups for all of the applications you wish to assign to a workstyle.

9.1. Creating Target Application Groups

To create a target application group:

1. Log into ePO Policy Orchestrator and click on Policy Catalog.

2. Select Defendpoint Policy and click Edit Target Application Groups.

3. Select Actions > Add (or use the adjacent Add button). In the Add Target Application Group dialog enter a name and optionally a description for the new application group.

4. A new target application group will be created that you can add applications to.

9.2. Duplicating Target Application Groups

You can duplicate a target application group if you need a new target application group that contains the same applications as an existing target application group. You can edit a duplicated target application group independently of the target application group it was duplicated from.

To duplicate a target application group:

1. Log into ePO Policy Orchestrator and click on Policy Catalog.

2. Select Defendpoint Policy and click Edit Target Application Groups.

3. Select Actions > Duplicate. You are asked to confirm the duplication.

A new duplicate application group with an incremental number in brackets appended to the name will be created that you can add applications to.

9.2.1. Inserting Executables and Scripts

To insert any type of application:

1. Select the relevant target application group.

2. In the right-hand pane select Actions > Add Application and then select the application type from the sub-menu.

3. After selecting an application type to add, the Add Application page will be displayed.

4. Enter a description for the application or use the Template… option. For more information about Application Templates please refer to Inserting Applications from Templates.

5. Enter a File or Folder name and configure the Application Definition(s) for the application. See the Target Definitions Appendix.

6. Configure the Advanced Options for the application. See Advanced Options.
7. Click OK. The application will now be added to the Target Application Group.

It is important to select a file for the application type you have chosen, otherwise it will fail to match when the Defendpoint Client processes the application group.

For executable and control panel applets the description will automatically be extracted from the file (if it has a description). You may change the description.

9.2.2. Add Application > Executable

The Insert Application wizard provides various target application 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:

- ActiveX Codebase
- ActiveX Version
- Application Requires Elevation (UAC)
- Command Line
- Drive
- File or Folder Name
- File Hash (SHA-1 Fingerprint)
- File Version
- Parent Process
- Parent Process in Sandbox
- Product Description
- Product Name
- Product Version
- Publisher
- Trusted Ownership
- Sandbox Classification
- Sandbox Content x
- Source URL
9.2.3. Inserting ActiveX Controls

Unlike other application types, Defendpoint only manages the privileges for the installation of ActiveX controls. ActiveX controls usually require administrative rights to install, but once installed they will run with the standard privileges of the web browser.

To insert an ActiveX Control:

1. Select the relevant Target Application Group.

2. In the right-hand pane select **Actions > Add Application** and then select **ActiveX Control** from the sub-menu.

3. After selecting an application type to add, the **Add Application** page will be displayed.

4. Enter a description for the ActiveX Control or use the **Template…** option. For more information about Application Templates please refer to **Inserting Applications from Templates**.

5. Enter a **Codebase (URL)** and configure the **Application Definition(s)** for the application (by default the **ActiveX Codebase** rule will be selected). See the **Target Definitions Appendix**.

6. Configure the **Advanced Options** for the application. See **Advanced Options**.

7. Click **OK**.

The **Insert Application** wizard provides various target application 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:

- **ActiveX Codebase**
- **ActiveX Version**
- **CLSID**
- **Parent Process in Sandbox**
- **Sandbox Classification**
- **Sandbox Context**
9.2.4. Inserting Installer Packages

Defendpoint allows standard users to install and uninstall Windows Installer packages which would normally require local admin rights. Defendpoint supports the following package types:

- Microsoft Software Installers (MSI)
- Microsoft Software Updates (MSU)
- Microsoft Software Patches (MSP)

When a Windows Installer package is added to an application group, and assigned to an Application rule or On Demand Application rule, the action will be applied to both the installation of the file, and also uninstallation via Add/Remove Programs, or Programs and Features.

**Note:** By default, elevation of software uninstalls is disabled in the Defendpoint Client. When this feature is enabled, then the ‘Repair’ option is not available for any installed software package that matches a workstyle. If you wish to grant uninstall privileges to users, and do not require the use of the ‘Repair’ option, you can enable MSI Uninstall support by adding the following registry entry:

```
HKEY_LOCAL_MACHINE\Software\Avecto\Privilege Guard Client\DWORD “MsiUninstallFeatureEnabled” = 1
```

**Note:** The publisher property of an MSx file may sometimes differ to the publisher property once installed in Programs and Features. It is therefore recommended that applications targeted using the Match Publisher validation rule are tested for both installation and uninstallation, prior to deployment, using the Defendpoint Activity Viewer.

Installer Packages typically create child processes as part of the overall installation process. Therefore it is recommended that when elevating MSI, MSU or MSP packages, that the advanced option **Allow child processes will match this application definition** is enabled.

**Note:** If you wish to apply more granular control over Installer Packages and their child processes, use the Child Process validation rule to whitelist or blacklist those processes that will / will not inherit privileges from the parent software installation.

To insert an Installer Package:

1. Select the relevant Target Application Group.
2. In the right-hand pane select **Actions > Add Application** and then select **Installer Package** from the sub-menu.
3. After selecting an application type to add, the **Add Application** page will be displayed.
4. Enter a description for the Installer Package or use the **Template…** option. For more information about Application Templates please refer to **Inserting Applications from Templates**.
5. Enter a **File or Folder** name and configure the **Application Definition(s)** for the application (by default the **Match File or Folder Name** rule will be selected). See the **Target Definitions Appendix**.
6. Configure the **Advanced Options** for the application. See **Advanced Options**.
7. Click **OK**.
The **Insert Application** wizard provides various target application 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:

- Application Requires Elevation (UAC)
- Command Line
- Drive
- File or Folder Name
- File Hash (SHA-1 Fingerprint)
- Parent Process
- Product Code
- Product Name
- Product Version
- Publisher
- Upgrade Code
- Trusted Ownership
- Sandbox Classification
- Sandbox Content
- Source URL
9.2.5. Inserting COM Classes

COM elevations are a form of elevation which are typically initiated from Explorer, when an integrated task requires administrator rights. Explorer will use COM to launch the task with admin rights, without having to elevate explorer. Every COM class has a unique identifier, called a CLSID, used to launch the task.

Normally when a user clicks on a COM task in Explorer it will trigger a UAC prompt which requires access to an administrator account to proceed.

Defendpoint allows you to target specific COM CLSID’s and assign privileges to the task without granting full admin rights to the user. COM based UAC prompts can also be targeted and replaced with custom messaging, where COM classes can be whitelisted and/or audited.

To insert a COM Class:

1. Select the relevant Target Application Group.

2. In the right-hand pane select Actions > Add Application and then select COM Class from the sub-menu.

3. After selecting an application type to add, the Add Application page will be displayed.

4. Enter a description for the COM Class or use the Template... option. For more information about Application Templates please refer to Inserting Applications from Templates.

5. Enter a CLSID (Class ID) name and configure the Application Definition(s) for the application (by default the CLSID rule will be selected). See the Target Definitions Appendix.

6. Configure the Advanced Options for the application. See Advanced Options.

7. Click OK.

The Insert Application wizard provides various target application definitions. The Defendpoint Client must match every definition you configure before it will trigger a match (the rules are combined with a logical AND).

COM Classes are hosted by a COM Server DLL or EXE, so COM Classes can be validated from properties of the hosting COM Server. The following validation options can be used to validate the COM server:

- Application Requires Elevation (UAC)
- AppID
- CLSID
- COM Display Name
- Drive
- File or Folder Name
- File Hash (SHA-1 Fingerprint)
- File Version
Defendpoint 4.3 ePO Edition
Administration Guide

Parent Process in Sandbox
Product Description
Product Name
Product Version
Publisher
Trusted Ownership
Sandbox Classification
Sandbox Context
Source URL

**Note:** Match if Application Requires Elevation (User Account Control) is always enabled, as COM Classes require UAC to elevate.
9.2.6. Inserting Windows Store Applications

The Windows Store Application type allows the installation and execution of Windows Store applications on Windows 8 to be whitelisted, so that users are prevented from installing or using unknown/unauthorized applications within the Windows Application Store.

To insert a Windows Store application:

1. Select the relevant Target Application Group.

2. In the right-hand pane select Actions > Add Application and then select Windows Store Application from the sub-menu.

3. After selecting an application type to add, the Add Application page will be displayed.

4. Enter a description for the Windows Store Application or use the Template… option. For more information about Application Templates please refer to Inserting Applications from Templates.

5. Enter a name and configure the Application Definition(s) for the application (by default the Windows Store Package name rule will be selected).

6. Configure the Advanced Options for the application. See Advanced Options.

7. Click OK.

The Insert Application wizard provides various target application 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:

- Windows Store Application Version
- Windows Store Package Name
- Windows Store Publisher
- Sandbox Classification
- Parent Process in Sandbox
9.2.7. Inserting Windows Services

The Windows Service type allows individual service operations to be whitelisted, so that standard users are able to start, stop and configure services without the need to elevate tools such as the Service Control Manager.

To insert a service:

1. Select the relevant Target Application Group.

2. In the right-hand pane select **Actions > Add Application** and then select **Windows Service** from the sub-menu.

3. After selecting an application type to add, the **Add Application** page will be displayed.

4. Enter a description for the Windows Service or use the **Template…** option. For more information about Application Templates please refer to [Inserting Applications from Templates](#).

5. Enter a Service Name and configure the **Application Definition(s)** for the application (by default the **Service Name** rule will be selected). See the [Target Definitions Appendix](#).

6. Configure the **Advanced Options** for the application. See [Advanced Options](#).

7. Click **OK**.

The Application Wizard provides a number of **Application 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:

- Command Line
- Drive
- File or Folder
- File Hash (SHA-1 Fingerprint)
- File Version
- Parent Process in Sandbox
- Product Description
- Product Name
- Product Version
- Publisher
- Service Actions
- Service Name
- Service Display Name
- Sandbox Classification
9.2.8. Advanced Options

- **Allow child processes will match this application definition** – if this checkbox is enabled then any child processes that are launched from this application (or its children) will also match this rule. The rules are still processed in order, so it’s still possible for a child process to match a higher precedence rule (or workstyle) first. Therefore, this option will prevent a child process from matching a lower precedence rule. It should also be noted that if an application is launched via an On Demand rule and this option is enabled, then its children will be processed against the On Demand rules, and not the Application rules. If this option is not enabled then the children will be processed against the Application rules in the normal way. You can further refine this option by restricting the child processes to a specific application group. The default is to match `<Any Application>`, which will match any child process.

Note: If you wish to exclude specific processes from matching this rule, then click ‘…match…’ to toggle the rule to ‘…does not match…’.

Note: Child Processes are evaluated in the context that the parent was executed. For example, if the parent was executed through On Demand shell elevation, then the Defendpoint Client will first attempt to match On Demand Application rules for any children of the executed application.

- **Force Standard User Rights on File Open/Save Common Dialogs** – if the application allows a user to open or save files using the common Windows open/save dialog then checking this option will ensure that the user does not have admin privileges within these dialogs. These dialogs have explorer like features, and allow a user to rename, delete or overwrite files. If an application is running with elevated rights then the open/save dialogs would allow a user to replace protected system files. By default, Defendpoint will force these dialogs to run with the user’s standard rights, which will prevent the user from tampering with protected system files.
9.3. Inserting Applications from Templates

Application Templates provide a simple way to pick from a list of known applications. A standard set of templates are provided, which cover basic administrative tasks for all supported operating systems, common ActiveX controls, software updaters and Avecto utilities.

To insert an Application Template:

1. Select the relevant Target Application Group.
2. In the right-hand pane select Actions > Add Apps From Template. The All Application Templates page will be displayed.
3. Select the applications you want to add to the Target Application Group. Each application will be highlighted once selected. Use the filter options Filter Text or Type, at the top of the page to refine the number of applications displayed.
4. Select Save.

The application(s) will now be added to the Target Application Group. Click on an application description to modify the settings of the Application Definition(s) and/or the Advanced Options.

Application templates can also be added from within the Insert Application wizard, by clicking the Template… button. When launched from within the Insert Application wizard, the template browser will show only templates for the type of application you have chosen to insert. For more information please refer to the Application Templates Appendix.

9.4. Inserting Applications from Events

The Defendpoint workstyle editor allows you to add applications that have been audited by Defendpoint Clients. Adding applications from events provides a simple and integrated workflow for defining rules based on real application usage.

To add an application from an event:

1. Select the relevant Target Application Group.
2. In the right-hand pane select Actions > Add Apps From Events. The Events page will be displayed.
3. Use the filters and search box to locate an audited application or scroll through the available audited applications.
4. Select an application and click Add Event(s) to Group.
5. Repeat steps 3 and 4 until all desired applications have been added.
6. Click Finish to exit and return to the Target Application Group.

The Events page includes the following filters:

> Preset Edit – Create and edit custom filters that are saved and can be selected from the Preset drop-down menu.
> **Preset** – Select any previously created custom filters in addition to the standard time filters provided.

> **Quick Filter Column** – A selection of default quick filters.

> **Quick Find** – Enter text to find applications. Entered text will match the product description of any audited applications.

> **Use Reporting** – Toggles between searching the Reporting database and the ePO database.

> **Show Unique** – Display unique applications.

> **Hide** – Hide applications already added to the in the current group / any group.

> Once the search criteria has been entered, the page will automatically return a list of unique applications that were audited, matching the criteria you specified. From here you can browse the list.

> Once the applications have been added to the Application Group, you can edit the definitions. All definitions will be pre-populated with values collected from the application.

> **Note**: A unique application is based on the **Product Description** of the application. So if two or more audited applications share the same Product Description, they will be displayed as a single application.

### 9.5. Inserting Applications from Browsing

Applications and services can be added to Target Application groups by browsing the local or remote computer for any of the following:

> Applications on the file system

> Running processes

> Windows Services

Computer browsing utilizes Windows Remote Management (WinRM) and PowerShell, which must be enabled on each target endpoint. For information on configuring WinRM and PowerShell for remote computer browsing, see [Configuring Remote Computer Browsing](#).

By default, the local computer will appear in the **Remote Computer Browser** list. Expand the **Local** computer to display a list of local drive letters, Processes and Services.

Defendpoint allows you to elevate individual PowerShell scripts and commands which are executed from a remote machine. This eliminates the need for users to be logged on with an account which has local admin rights on the target computer. Instead, elevated privileges are assigned to specific commands and scripts which are defined in Application groups, and applied via a workstyle.

PowerShell scripts and commands can be whitelisted to block the use of unauthorized scripts, commands and cmdlets. Granular auditing of all remote PowerShell activity provides an accurate audit trail of remote activity.

PowerShell definitions for scripts and commands are treated as separate application types, which allows you to differentiate between pre-defined scripts authorized by IT, and session based ad-hoc commands.

In order to allow standard users to connect to a remote computer via Windows Remote Management, or WinRM (a privilege normally reserved for local administrator accounts), it is necessary to enable the General Rule **Enable Windows Remote Management Connections**. This rule grants standard users who match the Defendpoint workstyle the ability to connect via WinRM, and can be targeted to specific users, groups of users, or computers using workstyle filters.

Note: In order to allow remote PowerShell management on Windows XP SP3 computers, it is necessary to install the Microsoft Windows Management Core Framework, which include WinRM 2.0 and PowerShell 2.0, which can be downloaded here [http://www.microsoft.com/en-us/download/details.aspx?id=16818](http://www.microsoft.com/en-us/download/details.aspx?id=16818)

End User Messaging

Defendpoint End User Messaging includes limited support for Remote PowerShell sessions; block messages can be assigned to workstyle rules which block remote PowerShell scripts and commands. If a block message is assigned to a workstyle which blocks a script or command, then the Body Message text of an assigned message will be displayed in the remote console session as an error.

9.6.1. Remote PowerShell Scripts

From within a remote PowerShell session, a script (.PS1) can be executed from a remote computer against a target computer. Normally this would require local administrator privileges on the target computer, with little control over the scripts that are executed, or the actions that the script performs. For example:

```
Invoke-Command -ComputerName RemoteServer -FilePath c:\script.ps1 -Credential xxx
```

Defendpoint allows you to target specific PowerShell scripts and assign privileges to the script without granting local admin rights to the user. Scripts can also be blocked if they are not authorized or whitelisted. All Remote PowerShell scripts executed are fully audited for visibility.

Note: When running a Remote PowerShell Script you must use the Invoke-Command cmdlet. Defendpoint will not be able to target PowerShell scripts that are executed from within a remote PowerShell session. Remote PowerShell Scripts must be matched by either a SHA-1 File Hash, or a Publisher (if the script has been digitally signed).

To insert a PowerShell Script:

1. Select the relevant Target Application Group.

2. In the right-hand pane select Actions > Add Application and then select Remote PowerShell Script from the sub-menu.
3. After selecting an application type to add, the Add Application page will be displayed.

4. Enter a description for the Remote PowerShell Script or use the Template... option. For more information about Application Templates please refer to Inserting Applications from Templates.

5. Enter a Publisher and configure the Application Definition(s) for the application (by default the Publisher rule will be selected). See the Target Definitions Appendix.

6. Configure the Advanced Options for the application. See Advanced Options.

7. Click OK.

The Application Wizard provides a number of Application 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 Hash (SHA-1 Fingerprint)
- Parent Process in Sandbox
- Publisher

**Note:** PowerShell scripts that contain only a single line will be interpreted and matched as a command, and will fail to match a PowerShell Script definition. It is therefore recommended that PowerShell scripts contain at least two lines of commands to ensure they are correctly matched as a script. This can be achieved by adding a comment to the script.

9.6.2. Remote PowerShell Commands

From within a remote PowerShell session, a user can execute arbitrary commands from a remote computer against a target computer using cmdlets. Normally this would require local administrator privileges on the target computer, with little control over the commands that are executed, or the cmdlets that are used. For example:

```
Get-service -Name *time* | restart-Service -PassThru
```

Defendpoint allows you to target specific command strings and assign privileges to the command without granting local admin rights to the user. Commands can also be blocked if they are not authorized or whitelisted. All Remote PowerShell commands are fully audited for visibility.

To insert a PowerShell Command:

1. Select the relevant Target Application Group.

2. In the right-hand pane select Actions > Add Application and then select Remote PowerShell Command from the sub-menu.

3. After selecting an application type to add, the Add Application page will be displayed.


5. Enter the command, or if you wish browse for a list of Cmdlets registered on the local computer to help enter the command string, use the Browse Cmdlets... button. If you wish to target any PowerShell command, leave the Command box empty. Click Next.
6. Configure the **Application Definition(s)** for the application (by default the **Publisher** rule will be selected). See the **Target Definitions** Appendix.

7. Configure the **Advanced Options** for the application. See **Advanced Options**.

8. Click **OK**.

The Application Wizard provides a number of Application 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:

- Command Line
- Parent Process in Sandbox
- Sandbox Content

9.7. **Application Rules**

Application rules are applied to Target Application groups. Application rules can be used to enforce whitelisting, monitoring and assigning privileges to groups of applications.

Each rule has a number of elements:

**Rule**

- Target Application Group – the Application Group that the rule is associated with.
- Action – The action that the rule dictates once a match has been made.
- End User Message – Any message that may be displayed to the user.

**Auditing**

- Raise an Event – An event will be logged to the client’s local event log file.
- Run a Script – Allows the creation of script based reports. See **Auditing with Custom Scripts**.
- Privilege Monitoring – Used in Application discovery – Used to monitor and identify which processes are using or require privilege rights.

**McAfee ePO Reporting Options**

- ePO Queries and Reports – Enable ePO Queries and Reports
- Avecto Reporting in (ePO) – Utilize Avecto Reporting

9.7.1. **Inserting an Application Rule**

To insert an application rule:

1. Expand the relevant Workstyle in the left-hand pane.
2. Select the Application Rules node.

3. In the right-hand pane select Actions > Add. The Add Application Rule dialog will be displayed.

4. Select the relevant Target Application Group from the drop-down menu.

   **Note:** The drop-down menu displays a list of groups available. The top of the list displays Built-in and Generated groups. Groups created by the user are displayed below. See Built-in Groups for more information.

5. Select the desired Action, to either Allow Execution or Block Execution.

6. If you wish to prompt the user before the application is executed or blocked then select a message or notification from Show End User Message. The list will show Allow or Block messages depending on your choice in the previous step.

7. If you are allowing the application to execute, select the correct access token from Apply Access Token dependent on the rights you wish to assign to the application group. The token can be set using one of the pre-defined Access Tokens (or you may define any number of Custom Tokens, which will appear at the end of the list of standard options). For more information please refer to the Custom Tokens section of this guide.

   **Note:** This option is only available if you have chosen to Allow the application to execute.

Apply Access Token can be set to one of the following options (or you may 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 applications in the application group without modifying the access token.

- **Enforce User’s Default Rights** – this option will ensure that the applications in the application group are assigned the user’s default rights.

- **Drop Admin Rights** – this option will remove local admin rights from the access token for applications in the application group.

- **Add Admin Rights** – this option will add local admin rights to the access token for applications in the application group.

8. ePO Queries and Reports is checked by default.

9. If you want to utilize Avecto Reporting check Avecto Reporting (in ePO).
10. If you wish to audit the Application Rule being matched then select **On** or **On (Anonymous)** (does not log the username) for **Raise an Event**. This will log events to the local **Application Event Log**.

11. If you wish to run a custom script when the Application Rule has been matched, then select **On** for **Run a Script**. See **Manage Audit Scripts** for more information.

12. If you wish to audit any privileged activity performed by the executed application then select **On** for **Privilege Monitoring**. See **Privilege Monitoring** for more information.

**Auditing**

If you select **On** or **On (Anonymous)** (does not log the username) for **Raise an Event** then an event will be logged to the local application event log every time the application rule is matched.

If you select **On** or **On (Anonymous)** (does not log the username) for **Privilege Monitoring** then an event will be logged to the application event log the first time a process performs a privileged operation (an operation that would fail under a standard user account) for the selected application group. All privileged activity will also be logged to an XML file that can later be viewed with the **Defendpoint Reporting Console** (an MMC snap-in). You may modify the behavior of Privilege Monitoring on the **Privilege Monitoring** tab of the workstyle.

9.8. **On Demand Application Rule**

**On Demand Application Rules** provide the ability for users to launch applications with specific privileges (usually admin rights) on demand.

To enable shell integration:

1. Expand the relevant Workstyle in the left-hand pane.

2. Select the **On Demand Application Rules** node.

3. In the right-hand pane check the **Enable integration with shell context menu** option.

4. You may change the menu option that is displayed, which defaults to **Run with Defendpoint**. The text can include parameterized values which provide a more personalized menu option for users. For more information on parameters, refer to the **Workstyle Parameters** appendix.

5. If you do not wish to hide the standard Windows “**Run As**” menu option then deselect Hide “**Run As**” and “**Run as administrator**” commands in shell context menu.

Insert one or more Shell rules into the list (follow the same procedure outlined in **Inserting an Application Rule**.

**Note:** Unlike Application rules, the On Demand rules list will only receive the assigned privileges if the user launches a relevant application via the shell menu.

9.8.1. **Managing Languages**

The menu option that is displayed can be configured for multiple languages. Defendpoint will detect the regional language of the end user, and if a message in that language has been configured, the correct translation will be displayed.

To add a new menu option translation:
1. In the On Demand Application rules click the **Add Language** button.

2. The **Add Language** dialog is displayed. Select the correct language and then click **OK**.

3. A new text box for the selected language will appear.

4. Enter your own translation for the selected language and click **Save** in the left-hand pane.

**Note:** If a language cannot be matched for the region of the end user, then the Default language will be displayed. To change the default language, select the desired language and click **Set As Default**.
10. Configuring Sandboxing

10.1. What is Sandboxing

The Sandboxing module in Defendpoint isolates the web browser, any internet content that is accessed such as websites, PDF’s and Microsoft Office documents and Microsoft Outlook email attachments. This is achieved easily using the URL and Content rules and groups contained in a Defendpoint configuration.

The sandbox is an isolated environment that protects the user and their private documents from anything running inside, so that if any untrusted or malicious websites or content are opened, then the effects of the malware are contained. When the user next logs off, the sandbox along with any malicious code and unwanted changes are wiped from the endpoint.

Avecto use a unique approach to sandboxing, by leveraging the Windows security model to provide the user with a lightweight and seamless experience, whilst also providing native application support with minimal performance overheads. Sandboxing is fully integrated with the rest of the Defendpoint suite; with a single agent and management console, you can take advantage of advanced Privilege Management and strong Application Control to build an effective defense-in-depth strategy for eliminating the threat of cyber-attacks.

10.2. Sandbox Contexts

There are three ‘contexts’ under which websites and downloaded content can be opened:

- **Private (Local)** – This means no sandbox is used – the website or content is considered completely safe and therefore no sandbox is employed.

  Websites & Applications running in the Private/Native context have full access to your Private documents, but no access to your Trusted or Untrusted documents.

- **Public Trusted (Internet)** – 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 & 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.

- **Public Untrusted (Internet)** – 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 & Applications running in the Untrusted sandbox have no access to your Private or Trusted documents. They have full access to your Untrusted documents.

*Note: When the email attachment general rule is enabled all attachments are classified as Untrusted.*

For more information please refer to the How Sandboxing Works appendix.
10.3. 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 are used to identify whether the website you are navigating to should be opened in a specific sandbox context.

When you create a sandboxing workstyle the wizard auto-generates two URL groups:

- **Private Websites** – this is a group of websites that may contain your company intranet or a website which is considered completely safe and from which you may be regularly downloading and/or uploading private or sensitive documents. The Private Websites URL Group has been configured to open those websites privately, not in a sandbox.

- **Trusted Websites** – this is a group of websites that are deemed to be low risk, and need to be isolated from general browsing activity. Trusted websites are always allowed to read your private documents, but are prevented from editing, overwriting or deleting them. The Trusted Websites URL group has been configured to open those websites in the Trusted Browsing sandbox.

These two groups are empty by default. You determine which websites will be treated as a **Private Website** or a **Trusted Website** by adding URLs to each group. There is a third URL group which is built-in and not visible:

- **Any Website** – this group will automatically match any website that has not been defined in either the **Private** or **Trusted** URL groups. The Any Website URL group has been configured to open those websites in the Untrusted Browsing sandbox.

For more information on built-in groups refer to the **Built-in Groups** appendix.

10.4. 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 you create a sandboxing workstyle the wizard auto-generates three URL rules. These are displayed under the **URL Rules** tab in the details pane for the workstyle.

The auto-generated rules correspond to the auto-generated URL groups:

- **The Private Websites** rule dictates that any website added to the **Private** group will not be subject to sandboxing. It will be opened natively.
The **Trusted Websites** rule dictates that any website added to the **Trusted** group will be opened in a **Trusted** sandbox context.

The **Any Website** rule dictates that any website that is not defined in either the **Trusted** or **Private** groups will be opened in an **Untrusted** sandbox context.

When an internet browser navigates to a website, Defendpoint evaluates each URL rule in the order they are displayed. In this example Defendpoint will first check 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 will proceed 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.

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

Additional URL groups and rules may be added at any time. The order in which each URL rule is evaluated may also be changed by right-clicking a rule and selecting any of the **Move Top**, **Move Up**, **Move Down** or **Move Bottom** options.

For more information please refer to the [How Sandboxing Works](#) appendix.

### 10.4.1. Content Sandboxing

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 tracked. This is achieved using Content rules.

The workstyle wizard offers two modes of operation for handling downloaded content, which is set in the Sandboxing page of the workstyle wizard:

**Mode 1: Sandbox only common documents** – The wizard will create Application and Content rules that only apply to common downloaded content file types, and the applications which typically open those file types. These rules ensure that downloaded files are reopened in their original sandbox context. This mode will create:

- **Sandboxed Content Handlers (Generated)** – This application group will target applications commonly used to open content that is downloaded. This application group is used where an application may open multiple document types.

- **Sandboxed Content (Generated)** – This content group will target content that is commonly downloaded. This content group is used where a document may be opened by multiple applications.

- **Sandboxed Content** – This content rule dictates that any of the file types defined in the associated Sandbox Content group will be sandboxed.

**Mode 2: Sandbox all downloaded content** – The wizard will create Application and Content rules that will apply to all downloaded content file types, except *exclusions*. These rules ensure that all downloaded files are reopened in their original sandbox context. This mode will create:

- **Sandboxed Content Exclusions (Generated)** – This content group will be empty. Content types you wish to be excluded from the sandboxing rule can be added to this group.
> **Sandboxed Content Exclusions (Generated)** – This content rule dictates that any of the file types defined in the associated Sandbox Content group will not be sandboxed.

> **Any Sandboxed Content** – This content rule dictates that all other content types will be sandboxed.

Sandbox enforcement is defined by the **Sandbox** setting in a content rule:

> **Automatic (Use Classification)** – Content originating from a sandbox will be reopened inside the original sandbox context.

> **Do Not Sandbox** – Content will not be sandboxed.

For more information on managing Content rules for sandboxing, see [Content Control](#).

### 10.4.2. Enabling Internet Zone Mapping

Defendpoint Sandboxing includes the ability to map Internet Explorer zones to sandboxes. This feature can be enabled on the Sandboxing page of the Workstyle Wizard by setting the option **Do you want to use internet zones in your configuration** to Yes. When enabled, the Workstyle Wizard will configure create additional URL definitions in the generated URL Groups:

> **Private Websites** – Any domain that matches the Internet Zone Local Computer, or Local Intranet.

> **Trusted Websites** – Any domain that matches the Internet Zone Trusted Sites.

> **Any Website** – Any domain that matches any other Internet Zone, for example Internet and Restricted Sites.

By enabling Internet Zone mapping, you can take advantage of any existing Internet Zone rules you may have deployed on your endpoints. It also provides a flexible alternative to configuring URL definitions, where URLs and the context under which they are accessed can be managed on individual endpoints by configuring the Internet Zone rules in Internet Explorer.

If you wish to define or edit URL definitions based on Internet Zones, refer to [Inserting URLs](#).

For more information please refer to the [How Sandboxing Works](#) appendix.

### 10.4.3. Allowing User to Reclassify

**Note:** This feature is only available to users if it was selected in the workstyle wizard or set using a General Rule.

Users may be given the option of allowing private documents to be uploaded to the internet from the Untrusted browser sandbox. This is achieved via a toggled option that is available from the right-click menu of a particular document.

1. Right-click on a Private file and select **Defendpoint Classification > Allow upload to Internet** from the context menu.
2. Repeat this with a file that has been classified as **Trusted**. Despite their different classifications, both files are now readable from the Untrusted Browsing sandbox, therefore allowing you to upload them to websites running in the Untrusted context.

Users may also be given the option of changing the classification of a document. This is achieved by right-clicking a document and toggling the appropriate classification. The selection will highlight the current classification of the document:

- **Private (Local)** – Document will be opened native.
- **Public (Internet)** – Document will be opened in a sandbox.

### 10.5. Printing

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. This means that you can create a ‘hard copy’ of any content that you require with complete safety.

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 sandboxed applications. This process requires two print dialog boxes. The first print dialog box controls the XPS conversion and is where you can specify the page range. Once **Print** is clicked the XPS file is created. Then the standard Windows print dialog box will be displayed where you can specify all other print options. Once **Print** is clicked in this dialog box the XPS file is sent to any of the printers normally available to the user and is printed in the usual fashion.

When you decide to send content or documents that are sandboxed to print:

1. Select the usual **Print** option for the current application that is displaying the content; regularly **File > Print**.

2. The expected print dialog 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 a sandboxed application:

![Diagram showing user experience](image)

**Notes:** Users on Windows XP will not need to perform Step 3 above. All choices are made in the first print dialog box as for a native (non-sandboxed) application.

Sandbox printing is not supported in Windows Vista.

### 10.6. Sandboxing 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 MS Office documents are crafted to appear genuine and familiar to their target – for example a CV or survey report. Given the volume of email 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 the 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 Application Control, 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 Control 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.

While being a very powerful feature, sandboxing attachments is incredibly easy to implement as described below.
10.6.1. 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 Workstyle wizard offers two modes of operation for handling downloaded content, which is set in the Sandboxing page of the Workstyle wizard:

- **Sandbox only common documents** – common documents include PDF’s, Office documents, Windows media files, Internet Explorer documents etc. and the document handlers that open these files by default. (A document handler is the program that runs by default when you double-click a file, such as Adobe Reader for PDF files, or Microsoft Word for DOCX files).

- **Sandbox all downloaded content** – all attachments, regardless of type, will be sandboxed.

**Note**: Any exclusions that you specify in a Content group will not be sandboxed by either mode.

These modes apply to email attachments as well as downloaded content. For more information see the Content Control and Content Rules sections of this document.

1. Create a sandboxing workstyle using the Workstyle wizard.
2. From the sandbox page of the wizard select one of the sandboxing modes for downloaded content/email attachments. This will automatically configure the workstyle based on your selection.
3. When the workstyle has been created highlight the workstyle and open the General Rules tab.
4. Enable the Classify email attachments for sandboxing general rule.

Outlook attachments will now be sandboxed using the selected sandboxing mode. The types of attachments that are sandboxed can be customized using Content rules and Content groups. For information please see the Content Control section of this document.

10.6.2. Opening an attachment from Outlook

When Content Control has 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.

10.6.3. 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.

10.6.4. Applying Application control rules to email attachments

Application rules have an application control feature that may be also be applied to email attachments. This feature can 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 see the Application Rules section of this document.
10.6.5. 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 see the End User Messaging section of this document.

10.6.6. 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, see the Auditing and Reporting section of this document.
11. Managing URLs

Target 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* are used to identify whether the website you are navigating to should be opened in a specific sandbox.

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

<table>
<thead>
<tr>
<th>Address</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://mail.google.com">https://mail.google.com</a></td>
<td>mail.google.com</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Host name</th>
<th>Will match</th>
</tr>
</thead>
<tbody>
<tr>
<td>google.com</td>
<td><a href="https://www.google.com">https://www.google.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://mail.google.com">https://mail.google.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://drive.google.com">https://drive.google.com</a></td>
</tr>
<tr>
<td>mail.google.com</td>
<td><a href="http://mail.google.com">http://mail.google.com</a></td>
</tr>
</tbody>
</table>

The workstyle wizard auto-generates two URL groups for a workstyle that includes the sandboxing module:

- **Private Websites** – this is a group of websites that may contain your company intranet or a website which is considered completely safe and from which you may be regularly downloading and/or uploading private or sensitive documents. The Private Websites URL Group has been configured to open those websites privately, or not in a sandbox.

- **Trusted Websites** – this is a group of websites that are deemed to be low risk, and need to be isolated from general browsing activity. Trusted websites are always allowed to read your private documents, but are prevented from editing, overwriting or deleting them. The Trusted Websites URL Group has been configured to open those websites in the Trusted Browsing sandbox.

There is a third URL group which is built-in and not visible beneath the URL Groups node:

- **Any Website** – this group will automatically match any website that has not been defined in either the Private or Trusted URL groups. The Any Website URL Group has been configured to open those websites in the Untrusted Browsing sandbox.

For more information on built-in groups please see the Built-in Groups appendix.

The Private and Trusted URL groups are empty by default; these groups are where you determine which websites will be treated as a Private Website or a Trusted Website.

URL groups are then assigned to a URL rule. URL rules dictate which sandbox context is used to open each website in the URL group. The wizard auto-generates three URL rules when a workstyle containing the sandboxing module is created.
When an internet browser navigates to a website, Defendpoint evaluates each URL rule in the order they are displayed. In this example Defendpoint will first check 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 will proceed 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.

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

Additional URL groups and rules may be added at any time. The order in which each URL rule is evaluated may also be changed by selecting **Actions > Top, Up, Down or Bottom** options.

### 11.1. Creating Target URL Groups

To create a Target URL Group:

1. Log into ePO Policy Orchestrator and click on **Policy Catalog**.

2. Select **Defendpoint Policy** and click **Edit Target URL Groups**.

3. Select **Actions > Add** (or use the adjacent **Add** button). In the **Add Target URL Group** dialog enter a name and optionally a description for the new URL group.

4. A new Target URL Group will be created that you can add URLs to.
11.2. Duplicating Target URL Groups

You can duplicate a target URL group if you need a new target URL group that contains the same URLs as an existing target URL group. You can edit a duplicated target URL group independently of the target URL group it was duplicated from.

To duplicate a target application group:

1. Log into ePO Policy Orchestrator and click on Policy Catalog.
2. Select Defendpoint Policy and click Edit Target URL Groups.
3. Select Actions > Duplicate. You are asked to confirm the duplication.

A new duplicate Target URL Group with an incremental number in brackets appended to the name will be created that you can add URLs to.

11.3. Inserting URLs to Target URL Groups

To insert a URL:

1. Select the relevant Target URL group.
2. In the right-hand pane select Actions > Add.
3. The Add Application dialog will be displayed. Enter a description for the URL.
4. Configure the URL definitions (detailed below) for the URL (by default the Host URL rule is selected and cannot be unselected).
5. Click OK to add the URL to the Target URL group.

11.3.1. URL Definitions

The Add URL dialog provides three 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
- Protocol URL
- Zone URL

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.

11.4. URL Rules

URL rules are applied to Target URL groups. These define the sandbox context that is applied to websites navigated to by an internet browser and any documents downloaded from those websites. There are three sandbox contexts available:

- None – Websites and documents are opened natively, and have full access to your private data. No sandbox is used.
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.

Untrusted Browsing – Websites and documents are prevented from reading, modifying or deleting your private data. An Untrusted sandbox is used.

When a controlling workstyle is created that incorporates the sandboxing module, three URL groups and associated rules are created:

Private Website – This group is auto-generated and is empty. The Private rule dictates that any website added to the Private group will not be subject to sandboxing. It will be opened natively.

Trusted Website – This group is auto-generated and is empty. The Trusted rule dictates that any website added to the Trusted group will be opened in a Trusted sandbox context.

Any Website – This group is built-in and is not visible in the tree pane. The Any Website rule dictates that any website that is not defined in either the Trusted or Private groups will be opened in an Untrusted sandbox context.

For more information about URL groups please refer to the Managing URLs section of this guide.

For more information about auto-generated and built-in groups please refer to the Built-in Groups appendix

11.4.1. Inserting a URL Rule

To insert a URL rule:

1. Expand the relevant Workstyle in the left-hand pane.

2. Select the URL Rules node.

3. In the right-hand pane select Actions > Add. The Add URL Rule dialog will be displayed.

4. Select the relevant Target URL Group from the drop-down menu.

Note: The drop-down menu displays a list of groups available. The top of the list displays Built-in and Generated groups. Groups created by the user are displayed beneath a dashed line. See Built-in Groups for more information.

5. Select the desired sandbox context using the Sandbox drop-down menu.

6. Send Events to ePO Reports is checked by default.

7. If you want to utilize Avecto Reporting check the Send Events to Avecto Reports.

8. If you wish to audit the URL Rule being matched then select On for Raise event in local Event Log. This will log events to the local Event Log.

9. If you wish to run a custom script when the URL Rule has been matched, then select On for Run a Script. See Managing Audit Scripts for more information.

10. Click OK to create the URL rule.

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

Content Control allows you to control the accessibility of privileged content, as well as control the behavior for content downloaded from a sandbox. Content groups provide a means of targeting specific types of content, based on file type, location, or which from sandbox they originate, and rules determining the behavior for that content are applied to each content group in a workstyle. There are three 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 may 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.

- To ensure that content originating from a sandbox is always opened in the same sandbox.

  Content groups can be added which specifically target content that has been tagged or classified as either Trusted or Untrusted. This group can then be assigned to a Content rule which will automatically sandbox the content based on its classification. Content that is not classified, or classified as ‘Private’ will open natively.

The Workstyle Wizard will automatically create Content rules and Content groups that ensure content is automatically sandboxed based on classification, if the Sandboxing module is enabled in the workstyle. Defendpoint also includes a built-in content group to target Any Content.

The following sections explain how to create Content groups which include content definitions, and how to assign groups to Content rules to apply the specific Content Control rules that meet your requirements.

12.1. Creating Content Groups

To create a content group:

1. Log into ePO Policy Orchestrator and click on Policy Catalog.

2. Select Defendpoint Policy and click Edit Content URL Groups.

3. Select Actions > Add (or use the adjacent Add button). In the Add Target Content Group dialog enter a name and optionally a description for the new Content group.

4. A new Content Group will be created that you can add content to.

12.2. Duplicating Content Groups

You can duplicate a content group if you need a new content group that contains the same content as an existing content group. You can edit a duplicated content group independently of the content group it was duplicated from.
To duplicate a content group:

1. Log into ePO Policy Orchestrator and click on **Policy Catalog**.
2. Select **Defendpoint Policy** and click **Edit Content URL Groups**.
3. Select **Actions > Duplicate** You are asked to confirm the duplication.
4. A new Content Group will be created that you can add content to.

### 12.3. Inserting Content to Target Content Groups

To insert a content type:

1. Select the relevant Target Content group.
2. In the right-hand pane select **Actions > Add**.
3. The **Add Content** dialog will be displayed. Enter a description for the Content type.
4. Configure the Content definitions (detailed below) for the Content type (by default the **File or Folder Name** rule is selected and cannot be unselected).
5. Click **OK** to add the Content type to the Content group.

#### 12.3.1. Target Content Definitions

The Content dialog 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 or Folder Name
- Drive
- Controlling Process
- Sandbox Classification

#### 12.4. Content Rules

Content rules are applied to Target Content groups. Content rules define the actions Defendpoint will take when content (a file) is opened (double-clicked) by the user. Based on the content’s classification, Defendpoint will open the content in the appropriate sandbox context.

For more information on Sandbox contexts please refer to the **How Sandboxing Works** appendix.

For more information about Content groups please refer to the **Content Control** section of this guide.

#### 12.4.1. Inserting a Content Rule

To insert an application rule:

1. Expand the relevant Workstyle in the left-hand pane.
2. Select the **Content Rules** node.

3. In the right-hand pane select **Actions > Add**. The **Add Content Rule** dialog will be displayed.

4. Select the relevant Target Content group from the drop-down menu.

5. Select the desired **Action**, to either **Allow Modification** or **Block Access**.

6. If you wish to prompt the user before the content is modified or access is blocked then select a message or notification from **Show End User Message**. The list will show **Elevate** or **Block** messages depending on your choice in the previous step.

7. If you are allowing the content to be modified, select the correct access token from **Apply Access Token** dependent on the rights you wish to assign to the application group. The token can be set using one of the pre-defined Access Tokens (or you may define any number of Custom Tokens, which will appear at the end of the list of standard options). For more information please refer to the **Custom Tokens** section of this guide.

8. Select the desired sandbox context using the **Sandbox** drop-down menu.

9. **Send Events to ePO Reports** is checked by default.

10. If you want to utilize Avecto Reporting check the **Send Events to Avecto Reports**.

11. If you wish to audit the Content Rule being matched then select **On** for **Raise event in local Event Log**. This will log events to the local **Event Log**.

12. If you wish to run a custom script when the Application Rule has been matched, then select **On** for **Run a Script**. See **Managing Audit Scripts** for more information.

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

General rules provide additional configuration settings for the features detailed in the following sections.

These rules can be enabled or disabled after a workstyle has been created from General Rules.

13.1. Allow User to Unlock a Shared Workstation

This rule allows (or disallows) a user to unlock a shared workstation on Windows XP. Usually only administrators can unlock a shared workstation, but this rule enables you to override that standard Windows XP behavior.

When a user attempts to use the Ctrl-Alt-Del combination on a locked XP desktop, the Defendpoint Client will attempt to match a workstyle which includes a setting for Allow User to Unlock a Shared Workstation. If a workstyle is matched, then desktop unlock is either granted to the user or revoked from user, and subsequent workstyles will be ignored. If no workstyles are matched, then the user receives default privileges.

This rule provides three options:

- **Not Configured** – This workstyle will be ignored.
- **Enabled** – The user will be granted privileges to unlock the workstation.
- **Disabled** – The user will have any unlock privileges revoked.

*Note:* Use Workstyle Filters to grant or revoke workstation unlock privileges to specific endpoints.
13.2. Collect User Information

This rule, when enabled will raise an audit event each time a user logs on to the client machine. The audit event will collect the following information which is reported through the Avecto Defendpoint Reporting:

- **Logon Time** – The date and time the user logged on.
- **Is Administrator** – The client will check whether the user account has been granted local administrator rights either directly or through group membership.
- **Session Type** – The type of logon session, I.E., Console, RDP, ICA.
- **Session Locale** – The regional settings of the user session / profile
- **Logon Client Session Hostname** – The hostname of the client the user is logging on from. This will either be the local computer (for Console sessions) or the remote device name (for remote sessions).
- **Logon Client Session IP Address** – The IP Address of the client the user is logging on from. This will either be the local computer (for Console sessions) or the remote device name (for remote sessions).

**Note:** For more information on user information reporting, refer to the Avecto Defendpoint Reporting guides.

13.3. Collect Host Information

This rule, when enabled will raise an audit event on computer start-up or when the Defendpoint Client service is started. The audit event will collect the following information which is reported through Enterprise Reporting:

- **Instance ID** – A unique reference identifying a specific service start event.
- **OS Version** – The Name and Version of the Operating System, including Service Pack.
- **Chassis Type** – The type of chassis of the client, I.E., Workstation, Mobile, Server, VM, etc.
- **Language** – The default system language.
- **Location** – The current region and time zone of the device.
- **Client Version** – The version of the Defendpoint Client.
- **Client Settings** – The type of installation and current settings of the Defendpoint Client.
- **System Uptime** – Time since the computer booted.
- **Unexpected Service Start** - Only added if the service has unexpectedly started (IE, a previous start was not proceeded by a service stop).

An additional event will be raised when the computer shuts down, or when the Defendpoint Client service is stopped:

- **Instance ID** – A unique reference identifying the last service start event.
Computer Shutdown – Value identifying whether the service stopped as part of a computer shutdown event.

Note: This option is only available in policies set under the Computer Configuration group policy. For more information on configuring group policy, see Managing Defendpoint Settings without Group Policy.

Note: For more information on computer information reporting, refer to the Avecto Defendpoint Reporting guides.

13.4. Prohibit Privileged Account Management

This rule, when enabled, blocks users from modifying local privileged group memberships. This prevents real administrators, or applications which have been granted administrative rights through Defendpoint, from adding, removing or modifying the memberships of any local privileged group which would grant local administrative rights to member user accounts and groups.

The list of local privileged groups that are prohibited from modification when this rule is enabled is:

- Built-in Administrators
- Power Users
- Account Operators
- Server Operators
- Printer Operators
- Backup Operators
- RAS Servers Group
- Network Configuration Operators

This rule provides three options:

- Not Configured – This workstyle will be ignored.
- Enabled – The user will not be able to add, remove or modify user accounts in local privileged groups.
- Disabled – Default behavior based on the users rights, or those of the application.

13.5. Windows Remote Management Connections

This rule, when enabled, authorizes standard users who match the workstyle to connect to a computer remotely via WinRM, which would normally require local administrator rights. This General Rule supports Remote PowerShell Command management, and must be enabled in order to allow a standard user to execute PowerShell scripts and/or commands.

See Remote PowerShell Management for more information on configuring Remote PowerShell.

Note: In order to allow remote network connections, you may be required to enable the Windows Group Policy setting Access this computer from the network. For more information, see: http://technet.microsoft.com/en-us/library/cc740196(v=WS.10).aspx
13.6. Allow User to Reclassify Documents

This rule, when enabled, authorizes standard users who match the workstyle to change the **Defendpoint Classification** of documents from the context menu. When a user right-clicks on a document the choice to reclassify the document will be available:

- **Private** – A file that was originally *private* and is reclassified *public* will automatically be opened in an **Untrusted** sandbox.

- **Public** – A file that was originally *public* (sandboxed) and is reclassified *private* will **not** be opened in a sandbox.

- **Allow upload to Internet** – Right-click on a file that has been classified as **Private** and **Allow upload to Internet** from the context menu. Repeat this with a file that has been classified as **Trusted**. Despite their different classifications, both files are now available to upload to the internet.

13.7. Classify email attachments for sandboxing

This 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.
14. End User Messaging

You can define any number of end user messages and notifications. Messages and notifications are displayed when a user’s action triggers a rule (application / on-demand or content rule). Rules can be triggered by an application launch or block or when content is modified.

Once defined, a message may be assigned to an individual rule in the workstyle rules tabs by editing the rule.

Depending on the type of workstyle you’ve created, Defendpoint may auto-generate certain messages for you to use.

14.1. Creating Messages

To create a message:

1. Select the Messages node in the relevant workstyle. The right-hand pane displays the All Messages page.

2. In the right-hand pane select Actions > Add. The Add Message dialog will be displayed.

3. Select a message template from either the Use a Message Box template or Use a Notification (balloon) drop-down lists.

   Note: Message Boxes can be interactive (the user may be asked to input information before an action occurs). Notifications are descriptive (displaying information about an action that has occurred).

4. Customize the message (more advanced message configuration can be performed after the message has been created).

5. Click OK.

A new message will be created. You may now further refine the message by selecting it and editing the Design and the Text options available beneath each message.
14.2. Message Boxes

Message boxes provide an effective way of alerting the user before an action is performed. For example, before elevating an application or allowing content to be modified, or advising that an application launch or content modification has been blocked.

Message boxes give the user information about the application or content, the action taken, and can also be used to request information from the user. Messages allow authorization and authentication controls to be enforced before access to an application or content is granted.

Message boxes are fully customizable, with visual styles, corporate branding and display text, so that users are offered a familiar and contextual experience.

Messages can be assigned to both application rules and content rules. A message box will display different properties depending on which of these targets it is assigned to. To view the differences a Preview option allows you to toggle between the Application Preview and the Content Preview. This is available from the Preview drop-down located in the top right corner of the details pane.

Message Name and Description

You may edit a message name or description by clicking on either element:

1. Select the Message (in either the left or right-hand pane).

2. Click the underlined Message Name or Description. The Message Properties dialog will be displayed.

3. Enter the relevant text and click OK.

14.2.1. Message Design

Messages have a wide array of configuration options, which are detailed below.

As you change the various message options the preview message will automatically update. Click the preview message to enlarge (any program information will contain placeholders).

Once you have configured the message options you should configure the Message Text for the message, which includes full multi-lingual support.
**Miscellaneous Settings**

- **Show message on secure desktop** – check this option to show the message on the secure desktop. This is recommended if the message is being used to confirm the elevation of a process, for enhanced security.

**Message Header Settings**

- **Header Style** – select the type of header, which can be No header, Defendpoint, Warning, Question or Error.

- **Show Title Text** – determines whether to show the title text.

- **Text Color** – select the color for the title text (the automatic color is based on the Header Style).

- **Background Type** – set the background of the header, which can be Solid background, Gradient background or Custom image. (The default Background Type is Custom Image making the Color 1 and Color 2 options initially unavailable).

- **Color 1** – select the color for a Solid background or the first color for a Gradient background (the automatic color is based on the Header Style).

- **Color 2** – select the second color for a Gradient background (the automatic color is based on the selected Header Style).

- **Custom Image** – select the image for a Custom image background. This option is only enabled if you have selected Custom Image for the Background Type. Click the “…” button to import, export, modify or delete images using the Image Manager.

**Message Body Settings**

The Message Body Settings display specific information about the program or content. These can be configured on the Message Text tab; they can display Automatic default values or Custom values. The Automatic default values are:

- **Show Line One** – The Program Name or the Content Name

- **Show Line Two** – The Program Publisher or the Content Owner

- **Show Line Three** – The Program Path or the Content Program

Custom values are configured on the Message Text tab.

- **Show reference Hyperlink** – this option determines whether to show a hyperlink in the message below the body settings (the hyperlink is configured on the Message Text tab).

**User Reason Settings**

This option determines whether to prompt the end user to enter a reason before an application launches (Allow Execution message type) or to request a blocked application (Block Execution message type).

- **Show User Reason Prompt** – Select between Text box and Drop-down list. The Text box allows users to write a reason or request. The Drop-down allows users to select a pre-defined reason or request from a drop-down menu. The pre-defined drop-down entries can be configured on the Message Text tab.
Remember User Reasons (per-application) – Reasons are stored per-user in the registry.

**User Authorization**

- Authorization Type – set this option to **User must authorize** to force the user to re-authenticate before proceeding. If you wish to use this option for over the shoulder departmental administration then set this option to **Designated user must authorize**.

- Authentication Method – set this option to **Any** to allow authentication using any method available to the user. If you wish to enforce a specific authentication method, then set to either **Password only** or **Smart card only**. Note that if you select a method that is not available to the user, then the user will be unable to authorize the message.

- Designated Users – if the Authorization Type has been set to **Designated user must authorize** then click the Edit Users button to add one more user accounts or groups of users that will be allowed to authorize.

- Run application as Authorizing User – if the Authorization Type has been set to **Designated user must authorize** then this option determines whether the application runs in the context of the logged on user or in the context of the authorizing user. The default is to run in the context of the logged on user.

**Note:** If **Run application as Authorizing User** is set to **Yes**, then Defendpoint will attempt to match a workstyle of the same type (Application Rule or On Demand Application Rule) for the authorizing user. If no workstyle is matched, then Defendpoint will fall back to the original user workstyle.

**Note:** When **Run application as Authorizing User** is set to **Yes**, and the message is applied to a content rule, the application will never run in a sandbox - even if that selection has been made.

**Challenge / Response Authorization**

- Enabled – set this option to **Yes** to present the user with a challenge code. In order for the user to proceed, they must enter a matching response code. Note that when this option is enabled for the first time, you will be requested to enter an Authorization Key. For more information, see **Challenge / Response Authorization**.

- Authorization Period (per-application) - set this option to determine the length of time a successfully returned challenge code is active for. Choose from:

  - One use Only - A new challenge code will be presented to the user on every attempt to run the application.

  - Entire Session - A new challenge code will be presented to the user on the first attempt to run the application. After a valid response code has been entered, the user will not be presented with a new challenge code for subsequent uses of that application until they next log on.

  - Forever - A new challenge code will be presented to the user on the first attempt to run the application. After a valid response code has been entered, the user will not be presented with a new challenge code again.

  - As defined by helpdesk - A new challenge code will be presented to the user on the first attempt to run the application. After a valid response code has been entered, the user will not receive a new challenge code for the duration of time specified by the helpdesks.
Suppress messages once authorized – If the Authorization Period has not been set to One Use Only the Suppress messages once authorized option is enabled and configurable.

Show Information tip – This option determines whether to show an information tip in the challenge box. To configure the text of the information tip, see Message Text.

Maximum Attempts – This option determines how many attempts the user has to enter a successful response code for each new challenge. Set this option to Three Attempts to restrict the user to three attempts, otherwise set this option to Unlimited.

Note: After the third failure to enter a valid response code, the message will be cancelled and the challenge code will be rejected. The next time the user attempts to run the application, they will be presented with a new challenge code. Failed attempts are accumulated even if the user clicks Cancel between attempts.

Authorization Settings

If Authorization Type has been set to Designated user must authorize this field becomes active. It allows you to choose between either:

- **Yes – Both required** – both the Challenge / Response and the Designated User credentials are required.
- **No – Either one sufficient** – either the Challenge / Response or the Designated User credentials are required.

Email Settings

The email settings are only enabled for blocking messages.

- **Allow user to email an application request** – check this option to allow the user to email a request to run an application (only available for the Block Execution message type).
- **Mail To** – email address to send the request to (separate multiple email addresses with semicolons).
- **Subject** – subject line for the email request.

The Mail To and Subject fields can include parameterized values, which can be used with email based automated helpdesk systems. For help with using parameters, please refer to the Workstyle Parameters appendix.

14.2.2. Message Text

All of the text in the message may be configured in the Message Text tab, which includes support for any number of end user languages.

As you change the message text the preview message can be updated by clicking the Update button (any program or content information will contain placeholders).

14.2.3. Managing Languages

By default, a single language is defined (English) with a set of default text strings. You may add additional languages as follows:

1. Select Message Text below the message.
2. Click the **Add Language** button.

3. The **Add Language** dialog is displayed. Select the correct language and then click **OK**.

4. Select the relevant language (and region) from the drop-down box.

5. Enter your own translations for the selected language and click **Save** in the left-hand pane.

If you have more than one language then you can set the default language. This is the language that will be used if an end user is using a language that has not been defined. The default language is set to English, but you may change the default language:

1. Select the language you want to set as the default language.

2. Click **Set As Default**.

**Note:** If a language cannot be matched for the region of the end user, then the Default language will be displayed. To change the default language, select the desired language and click **Set As Default**.

If you delete a language that has been set to the default language then the language at the top of the language list is set as the default language. You must always have at least one language defined.

### Setting the Message Text

We recommend that you change the default text strings, as many are simply placeholders, all defined in English.

To set the message text strings, select the relevant language in the languages list and simply edit the text values in the text property grid.

The text in any text string can include parameterized values which provide more personalized messages for users. For help with using parameters, refer to the **Workstyle Parameters** appendix.

**Note:** The Body Message text supports multi-line text. The pipe symbol (|) is used to denote a newline, e.g. "line1|line2|line3"

### Information

Message Information fields contain the *character strings* that will be displayed on the message. These fields are editable and there are three different field groups:

- Application
- Content
- Custom (displayed when the **Message Mode** is set to **Custom**)  

The field group that is displayed is determined by the **Message Mode** setting.

### Message Mode

Messages can be assigned to application rules, on-demand application rules and content rules.

In **Automatic** mode the information displayed is dictated by the type of rule the message is assigned to; application rule or content rule.

In **Custom** mode the message will display whatever is entered into the **Custom** fields irrespective of rule type.
Changing the pre-defined Drop-down User Reason List

If you want to change the pre-defined user reasons available from the Message Box drop-down list:

1. Select the User Reason List field.
2. Use the Add, Edit and Delete buttons to edit the available User Reasons.

Changing the Message Text for Buttons

Depending on the message options the message box will have either one or two buttons:

- For a prompt the message box will have OK and Cancel buttons.
- For a blocking message with **Allow user to email an application request** enabled the message box will have OK and Cancel buttons. We recommend you change the OK button text to be “Email”, unless you make it clear in the message text that the OK button will send an email request.
- For a blocking message with **Allow user to email an application request** disabled the message box will only have an OK button.

You may change the OK button and Cancel button text. For instance, you may change it to “Yes” and “No” if you are asking the end user a question.

14.2.4. Image Manager

The Image Manager associated with message creation allows you to Upload Image, Edit, and Delete images that are referenced in message headers.

All images are stored inside the workstyles as compressed and encoded images.

It is strongly recommended that you delete any unused images to minimize the size of the policies, as Defendpoint does not automatically delete unreferenced images.

The Image Manager is accessible from the Message Design tab. Click the Manage Images button next to the Custom Image drop-down menu.

To upload an image:
1. Click **Upload Image**. The **Import Image status** dialog will be displayed. Click **Choose file** and browse to the location of the file.

2. Select the image and enter an **Image Description**. Click **OK**.

3. The image will be uploaded into Image Manager.

**Note:** Images must be *.png format and be sized between 450x50 and 600x100 pixels.

To edit an image:

1. In the **Custom Image** field select Manage Images.

2. Select the image in the list and click **Edit**.

3. The **Image Properties** dialog will appear.

4. Alter the description and click **OK**.

To delete an image:

1. Select the image in the list and click **Delete**.

2. When prompted, click **Yes** to delete the image.

**Note:** If an image is referenced by any messages then you will not be allowed to delete it.

14.2.5. **Challenge / Response Authorization**

Challenge / Response Authorization provides an additional level of control for access to applications and privileges, by presenting users with a 'challenge' code in an End User Message. In order for the user to progress, they must enter a corresponding 'response' code into the message.

Challenge / Response Authorization is configured as part of an End User Message, and can be used in combination with any other authorization and authentication features of Defendpoint messaging.

Authorization is applied per user, per application, meaning that each user will be presented with challenge codes which, when authorized, will only apply to them. Likewise, each unique application requiring Challenge / Response Authorization will present the user with a different, unique challenge code.

Challenge and response codes are presented as an 8 digit number, which is ideal for verbal communication with a telephone helpdesk, and minimizes the chance of incorrect or accidental entry.

When a user is presented with a challenge code, the message may be cancelled without invalidating the code. If the user runs the same application, they will be presented with the same challenge code. This allows users to request a response code from IT helpdesks which may not be immediately available to provide a response.

There are two main configuration options available for how challenge codes are presented to users:

- **Authorization Period (per-application)** - For each application, challenge codes can be optionally presented to a user for **One Use Only, Entire Session, Forever** or **As defined by**
helpdesk, depending on the level of control and flexibility you wish to apply to the user and application.

> **Maximum Attempts** – This option determines how many attempts the user has to enter a successful response code for each new challenge. There are two options available, **Unlimited** which will allow the user to try entering the response code an unlimited number of times, or **Three Attempts** which will only allow a maximum of three attempts to enter a correct response code before the message is cancelled and the challenge code is invalidated.

If a challenge code is invalidated due to excessive failed attempts, the user will be presented with a new challenge code the next time they attempt to run the application. Failed attempts are remembered even if the user clicks **Cancel** between attempts.

It is recommended that **Three Attempts** is enabled, to prevent the user from attempting to guess response codes through brute force retries.

For more information on configuring Challenge / Response Authorization enabled End User Messages, see **Message Design**.

**Authorization Key**

The first time Challenge / Response is enabled, you will be asked to create an Authorization Key. The Authorization Key is then used by the Defendpoint Client to generate challenge codes. The Authorization Key is also required to generate the response code to match a challenge code created with the same key.

Once you have entered an Authorization Key, it will be applied to all End User Messages in the same Defendpoint Settings, for all messages that have Challenge / Response Authorization enabled.

To Change the Authorization Key:

1. Click the Messages node of a workstyle and select **Actions > Set Challenge / Response Authorization Keys**.

2. In the **Challenge / Response Authorization Key** dialog, edit the **Enter Key** and **Confirm Key** with the new Authorization Key.

3. Click **OK** to complete. If the key entered is not exact, you will be presented with a warning message.

**Note**: It is recommended that a complex Authorization Key of at least 15 characters is used, which includes a combination of alphanumeric, symbolic, upper and lowercase characters. As a best practice, the Authorization Key should be changed periodically.
**Generating a Response Code**

Response codes are generated using the PGChallengeResponseUI.exe utility, which is installed as part of the Defendpoint Management Console installation, and is located in the following directory (on a client machine):

```
C:\Program Files\Avecto\Privilege Guard Management Consoles\n```

To generate a response code:

1. Run the program PGChallengeResponseUI.exe.
2. In **Enter shared key**, enter the correct Authorization Key, and in **Enter challenge code**, enter the challenge code presented to the user.
3. The response code will automatically be displayed once both the **Authorization Key** and the 8 character challenge code have been entered.

The **Generated Response** value is then entered into the **End User Message** which presented the corresponding challenge.

**Note:** PGChallengeResponseUI.exe is a standalone utility and can be distributed separately to the ePO extension.

**Generating a Response Code from the command line**

Response codes can also be generated from the command line using the PGChallengeResponse.exe command line utility, which is installed as part of the Defendpoint Management Console installation, and is located in the following directory (on a client machine):

```
C:\Program Files\Avecto\Privilege Guard Management Consoles\n```

To generate a response code from the command line:

1. Open the Command Prompt by clicking the Start Menu and typing `cmd.exe`.
2. In the Command Prompt, type the following command, then press Enter:
   ```
   cd "\program files\avecto\privilege guard management consoles"
   ```
3. Once you have opened the Defendpoint Management Consoles directory, type the following command (where `<challenge>` is the challenge code presented to a user):
   ```
   pgchallengeresponse.exe <challenge>
   ```
4. At the Authorization Key prompt, enter the correct Authorization Key, then press Enter.

**Automating Response Code Generation**

The PGChallengeResponse.exe supports full command line use, allowing it to be easily integrated into any third party workflow that supports the execution of command line executables. The command line is as follows:

```
PgChallengeResponse.exe <challenge code> <authorization key>
```

Where `<challenge code>` is the code presented to the user and `<authorization key>` is the key that was configured within the Defendpoint Settings which presented the End User Message.
The utility will return the response code as an exit code, so it can be captured from within a custom script or wrapper application. Below is an example VBScript:

```vbscript
Dim WshShell, oExec
Dim strChallenge,strKey,strExecutable
strExecutable = "C:\Program Files\Avecto\Privilege Guard Management Consoles\PGChallengeResponse.exe"
strChallenge = InputBox("Enter Challenge Code","Challenge")
strKey = InputBox("Enter Authorization Key","Key")
Set WshShell = WScript.CreateObject("WScript.Shell")
Set oExec = WshShell.Exec(strExecutable & " " & strChallenge & " " & strKey)
Do While oExec.Status = 0
    WScript.Sleep 100
Loop
msgbox "Response Code: " & oExec.ExitCode
Set WshShell = Nothing
Set oExec = Nothing
```

14.2.6. Challenge / Response – Designated User Option

As described, Challenge / Response provides an additional level of control for access to applications and privileges.

An extra aspect of this feature is the Designated User authorization. When this option is enabled a designated user such as a system administrator can authorize the elevation in place of (or in addition to) a Challenge Response code.

<table>
<thead>
<tr>
<th>Input</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Challenge/Response code only is provided</td>
<td>Application runs as logged on user</td>
</tr>
<tr>
<td>Valid Challenge/Response code is provided and valid (but not required) credentials are provided</td>
<td>Application runs as logged on user</td>
</tr>
<tr>
<td>Invalid Challenge/Response code is provided but valid credentials are provided</td>
<td>Application runs as authorizing user</td>
</tr>
<tr>
<td>No Challenge/Response code is provided but valid credentials are provided</td>
<td>Application runs as authorizing user</td>
</tr>
</tbody>
</table>
For more information on Designated User settings see the Authorization Settings section of Message Design.

14.3. Message Notifications

Message notifications allow information about workstyle actions to be communicated to users in an unobtrusive manner. When enabled for a workstyle, actions performed can show a notification, which can be dismissed by the user, or will disappear after a short period.

Message notification text is fully customizable, so that users are given concise, yet relevant information about the action performed. As you change the text properties the preview notification will automatically be updated.

Message Notifications are displayed either as a systray bubble (Windows 7 and older operating systems), or as a Toast notification (Windows 8).

14.3.1. Setting the Notification Text

It is highly recommended that you change the default text strings, as they are simply placeholders, and all are defined in English.

To set the notification text strings, select the relevant language in the languages list and simply edit the text values in the text property grid.

**Note:** Message notifications are not supported for SYSTEM processes.

14.4. Setting ActiveX Message Text

When Defendpoint is configured to elevate the installation of an ActiveX control, a built-in progress dialog of the installation process is displayed.

The following text strings can be set:

- **Title** – The title text of the progress dialog.

- **Download Message** – The text displayed during the download phase.

- **Install Message** – The text displayed during the installation phase.

- **Cancel Button** – the text displayed for the button that cancels the ActiveX installation.

The display text can be configured for multiple languages. Defendpoint will detect the regional language of the end user, and if ActiveX strings in that language have been configured, the correct translation will be displayed.

To set the ActiveX message text:

1. Click the Messages node and select Actions > ActiveX Message Text.

2. The Configure ActiveX Languages dialog will be displayed.

3. Edit the text according to the selected language. To add a new language, click Add in the left-hand pane.

4. Once you have finished editing the ActiveX text strings, click OK to finish.
14.5. Setting Classify Context Text

When Defendpoint is configured to allow the user to change the Defendpoint Classification of documents from the shell menu, a right-click context menu will be displayed.

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. Select the Messages node and select Actions > Classify Content Text.

2. The Configure Languages… dialog will be displayed.

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 Finish.

**Note:** 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.
15. Custom Tokens

Access Tokens (and Custom Tokens) are assigned to an application, or when content is being edited, to modify the privileges of that activity. Within an Access Token is a collection of settings that specify the group memberships, associated Privileges, Integrity level and Process Access Rights. Defendpoint includes a set of built-in Access Tokens that can be used to Add Administrator Rights, Remove Administrator Rights, or enforce the users default privileges. A ‘passive’ Access Token is also available that does not change the privileges of the activity, but still applies Anti-Tamper protection.

Access Tokens are assigned to Applications or Content through rules within a workstyle. For more advanced configurations, Custom Tokens can be created where group memberships, privileges, permissions and integrity can be manually specified. You can optionally define any number of custom tokens.

15.1. Creating Custom Tokens

To create a new custom token:

1. Expand the relevant Workstyle in the left-hand pane.

2. Select the Custom Tokens node. The right-hand pane displays the All Custom Tokens page.

3. In the right-hand pane select Actions > Add Token. The Create New Custom Tokens dialog will be displayed.

4. Select a token type and enter a Name and a Description.

5. Click OK.

The new custom token will be displayed beneath the Custom Tokens node. Click the new token to display the Token Summary.

You may now define the Groups, Privileges, Integrity Level and Process Access Rights for the custom token.

15.2. Editing Custom Tokens

15.2.1. Groups

The Groups section of the custom token specifies the groups that will be added or removed from the token.

To insert a group:

1. Select Groups in the left-hand pane. The Token groups will be displayed in the right-hand pane.

2. In the right-hand pane select Actions > Add.

3. The Add Group to Token dialog is displayed.
4. Enter a Group Name and a Security Identifier (SID). Select whether to Add Account or Remove Account and click OK.

5. By default, when you insert a group the Add Account checkbox is checked, and the group will be added to the custom token. If you wish to remove the group from the custom token then click the Remove Account checkbox for the relevant group.

6. Domain and well known groups will display a Security Identifier (SID). The SID will be used by the Defendpoint Client, which will avoid account lookup operations. For local groups the name will be used by the Defendpoint Client, and the SID will be looked up when the custom token is created by the client. Local Account will appear in the SID column of the groups list for local groups.

Setting the Token Owner

By default, the owner of a custom token that includes the Administrators group will have the owner set to the Administrators group. If the Administrators group is not present in the custom token then the User is set as the owner.

If you wish the User to be the owner, regardless of the presence of the Administrators group, then click the Ensure the User is always the Token Owner checkbox.

Anti-Tamper Protection

By default, Defendpoint prevents elevated processes from tampering with the files, registry and service that make up the Agent installation. It also prevents any elevated process from reading or writing to the local Defendpoint policy cache.

If you wish to disable anti-tamper protection, then uncheck the Enable anti-tamper protection checkbox.

Note: Under normal circumstances, this option should remain enabled, except in certain scenarios where elevated tasks require access to protected areas. For instance, if you are using an elevated logon script to update the local Defendpoint policy.
15.2.2. Privileges

The **Privileges** section of the custom token specifies the privileges that will be added to or removed from the custom token.

If you wish to add a privilege to the custom token then click the **Add** option for the relevant privilege.

If you wish to remove a privilege from the custom token then click the **Remove** option for the relevant privilege.

If you wish to reset the default state of a privilege click the **No Change** option for the relevant privilege.

To reset, add or remove multiple privileges, check the relevant privileges and select **Actions > Set <action>** (or use the adjacent buttons).

To clear all of the privileges in the custom token before applying privileges, check the **Remove all existing privileges in access token before applying privileges** checkbox. If this checkbox is left unchecked then the privileges are added or removed from the user’s default custom token.

Refer to the **Windows Privileges** appendix for further information.

15.2.3. Integrity Level

The **Integrity Level** section of the custom token specifies the integrity level for the custom token. The integrity level is ignored if the Defendpoint Client is running on Windows XP or Windows Server 2003.

To set the integrity level:

1. Select the **Integrity Level** node in the left-hand pane. The integrity levels will be displayed in the right-hand pane as radio buttons.

2. Set the appropriate integrity level.

The integrity level should be set as follows:

<table>
<thead>
<tr>
<th>Integrity Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Included for completion and should not be required</td>
</tr>
<tr>
<td>High</td>
<td>Set the integrity level associated with an administrator</td>
</tr>
<tr>
<td>Medium</td>
<td>Set the integrity level associated with a standard user</td>
</tr>
<tr>
<td>Low</td>
<td>Set the integrity level associated with protected mode (an application may fail to run or function in protected mode)</td>
</tr>
<tr>
<td>Untrusted</td>
<td>Included for completion and should not be required</td>
</tr>
</tbody>
</table>
### 15.2.4. Process Access Rights

The **Process Access Rights** section of a custom token allows you to specify which rights other processes will have over a process launched with that custom token.

Tokens that include the administrators group have a secure set of access rights applied by default, which will prevent code injection attacks on elevated processes initiated by processes running with standard user rights in the same session.

**Enabling or Disabling an Access Right**

Use the **Enable** / **Disable** options to enable or disable a specific access right.

To enable or disable multiple access rights, check the relevant access rights and select **Actions > Set <action>** (or use the adjacent buttons).

The access rights should be set as follows:

<table>
<thead>
<tr>
<th>Access Right</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROCESS_ALL_ACCESS</td>
<td>All possible access rights for a process object.</td>
</tr>
<tr>
<td>PROCESS_CREATE_PROCESS</td>
<td>Required to create a process.</td>
</tr>
<tr>
<td>PROCESS_CREATE_THREAD</td>
<td>Required to create a thread.</td>
</tr>
<tr>
<td>PROCESS_DUP_HANDLE</td>
<td>Required to duplicate a handle using DuplicateHandle.</td>
</tr>
<tr>
<td>PROCESS_QUERY_INFORMATION</td>
<td>Required to retrieve certain information about a process, such as its token, exit code, and priority class</td>
</tr>
<tr>
<td>PROCESS_QUERY_LIMITED_INFORMATION</td>
<td>Required to retrieve certain information about a process</td>
</tr>
<tr>
<td>PROCESS_SET_INFORMATION</td>
<td>Required to set certain information about a process, such as its priority class</td>
</tr>
<tr>
<td>PROCESS_SET_QUOTA</td>
<td>Required to set memory limits using SetProcessWorkingSetSize</td>
</tr>
<tr>
<td>PROCESS_SUSPEND_RESUME</td>
<td>Required to suspend or resume a process</td>
</tr>
<tr>
<td>PROCESS_TERMINATE</td>
<td>Required to terminate a process using TerminateProcess</td>
</tr>
<tr>
<td>Permission</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PROCESS_VM_OPERATION</td>
<td>Required to perform an operation on the address space of a process</td>
</tr>
<tr>
<td>PROCESS_VM_READ</td>
<td>Required to read memory in a process using ReadProcessMemory</td>
</tr>
<tr>
<td>PROCESS_VM_WRITE</td>
<td>Required to write to memory in a process using WriteProcessMemory</td>
</tr>
<tr>
<td>READ_CONTROL</td>
<td>Required to read information in the security descriptor for the object, not including the information in the SACL</td>
</tr>
<tr>
<td>SYNCHRONIZE</td>
<td>Required to wait for the process to terminate using the wait functions</td>
</tr>
</tbody>
</table>
16. Utilities

The utilities comprises of tools and resources to maximise the flexibility of Defendpoint and enhance your working routines.

16.1. Application Search

The Application Search is an interactive list of every application that is included in the current Defendpoint policy. Each Application Group and its applications are listed with clickable links that allow you to drilldown to the Application, its Definition and Advanced Options settings.

16.2. Importing and Exporting Defendpoint Policy

Defendpoint policies may be imported to and exported from McAfee ePO as XML files, in a format common to other editions of Defendpoint such as Defendpoint Group Policy Edition. This allows for policies to be migrated and shared between different deployment mechanisms.

Note: Importing and exporting policies from the Utilities section of a policy differs to importing and exporting policies from the McAfee ePO Policy catalog, as the utility will export an Avecto standard XML file. When exporting from the Policy catalog, the exported XML uses the ePO policy format XML and as such is not suitable for import/export to the MMC.

16.2.1. Import Defendpoint Policy

To import a Defendpoint XML Configuration:

1. Select the Utilities node and click Import Defendpoint Policy.
2. Browse to the location of the XML file to import.
3. If you want to merge the imported settings with the settings already contained within the policy, check Merge imported settings. If you want to overwrite the existing policy with the imported policy, uncheck Merge imported settings.
4. Click Load Configuration to complete the import.

16.2.2. Export Defendpoint Policy

1. Select the Utilities node and select Export Defendpoint Policy.
2. From the Policy Export page right-click on the policy name and select Save Link As... from the context menu. Enter a file name and select a location to save the XML file.
3. Alternatively click on the policy name and from the dialog select Open with or Save File.
4. If you select Save File the file will be saved to the default downloads folder.
16.3. Template Policies

Template Policies are a collection of Policy Templates and Workstyle Templates. Policy Templates are designed to quicken the creation of policies for specific styles of implementation. Workstyle Templates are designed with typical user roles in mind.

Each Template has a description and an explanation.

**Note:** Importing a Policy Template will overwrite any and all current settings in the policy. Please ensure you have exported or duplicated any required settings before loading a Policy Template.

16.4. Manage Audit Scripts

When an application is allowed, elevated or blocked or when content modification is allowed or blocked, Defendpoint will log an event to McAfee ePO to record details of the action. If you wish to record the action in a bespoke or third party tracking system that supports PowerShell, VBScript or Jscript based submissions, you can use the Run a Script setting within an Application, On Demand Application or Content Rule.

To add a new auditing script:

1. Select the **Utilities** node and click **Manage Audit Scripts**.
2. In the left-hand pane select **Action > Add**. The **Add Script** dialog will be displayed.
3. Enter a **Script Name**.
4. Select either **PowerShell**, **VB Script** or **Javascript** from the **Script Language** drop-down list.

**Note:** PowerShell audit scripts can only be run in the System context.

5. Select how long the script will be allowed to execute, before it is terminated from the **Timeout** drop-down list. By default, this will be set to **Infinite**.
6. Select whether the script should be executed in the **System** context or the current **User** context, from the **Script Context** drop-down list.
7. Enter your script code either manually or by copy/paste. Alternatively you can import a script by selecting **Action > Import** at step 2 and browsing to the location of the relevant script.
8. Click **OK** to finish.

16.5. Advanced Agent Settings

The Advanced Agent Settings utility allows you to configure and deploy additional registry based settings to Defendpoint Clients. Advanced Agent Settings are available under the **Utilities** node.

To add a new value:

1. Select the **Utilities** node and click **Advanced Agent Settings**.
2. Select either **32-bit Agent Values** if you wish to configure a 32-bit registry setting, or **64-bit Agent Values** for a 64-bit registry setting.
3. In the right-hand pane select **Actions > Add Value**. The **Add Registry Value** dialog will be displayed.

4. Enter a **Value Name** for the new setting.

5. Choose the correct type, either **DWORD**, **String** or **Multi-String**.

6. Enter the value data. For **DWORD** values, you can choose between Hexadecimal and Decimal.

7. Click **OK** when finished.

**Warning:** Advanced Agent Settings should only be used when instructed to do so by Avecto Technical Hotline Support.
17. **Advanced Configurations Settings**

17.1. **Privilege Monitoring**

Defendpoint includes the ability to monitor the behavior of specific privileged applications and processes – a feature called Privilege Monitoring. Privilege Monitoring is enabled as an auditing option in the properties of an application or the On Demand application rule. When enabled, Defendpoint will record all privileged operations performed by the application or process that would fail under a standard user account. These include file operations, registry operations, and any interactions with other components such as Windows services.

The application must be running under a privileged account, such as an administrator or power user. Alternatively an application could be running with elevated privileges because you have added it to the Application Rules or On Demand Application Rules section of the workstyle and assigned it to run with admin rights.

Privilege Monitoring logs are recorded on each endpoint, and the logs can be accessed using the Defendpoint Reporting MMC snap-in. The configuration of Privilege Monitoring logs is applied to each Workstyle.

For more information about Privilege Monitoring contact your Avecto consultant.

17.2. **Workstyle Options**

To edit the advanced options for a workstyle:

1. Expand the Workstyles node and select the relevant workstyle.
2. In Workstyle Summary page (right-hand pane) click on the Workstyle name. The Workstyle Properties dialog will be displayed.

3. Configure the Monitoring options (see below).
4. Click OK.

17.2.1. **Events**

> **Log Event to Application Event Log** – this option will log an event to the application event log, the first time an application performs a privileged operation.
Log Cancel Events (when user cancels message) – this option will raise an event when a user cancels an End User Message, either by clicking the Cancel button, Email button, or clicking a Hyperlink. The action performed by the user is available as a Policy Parameter [PG_ACTION], which can be used by the script to perform different audit actions based on the user interaction.

17.2.2. Privilege Monitoring Log Files

The following Privilege Monitoring options are available:

Log Application Activity to Log Files – this option will enable logging of privileged activity to log files. The activity level can be set with the activity slider:

Application Summary – this option only logs information about the application.

Application Summary and Activity – this option logs information about the application and unique privileged activity (Default option).

Application Summary and Detailed Activity – this option logs information about the application and all privileged activity.

Maximum Activity Records Per Process – this option determines the maximum number of records that will be recorded per process (Default 100).

Keep Application Activity Logs for – this option determines how long activity logs are kept before they will be purged (Default 14).

17.3. Advanced Sandboxing Environment

The Advanced Sandboxing Environment 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.
Deploying Defendpoint Settings

In this section you will find the following chapters:

› Configuration Precedence
› Deployment Methods
› Avecto End User Utilities
› Troubleshooting
› Auditing and Reporting
› Setting up Enterprise Reporting for Defendpoint ePO Edition
› Reputation Settings
18. Configuration Precedence

Defendpoint supports a variety of deployment methods, and can accept multiple simultaneous configurations from any combination of the following:

- **Group Policy** – Configurations that are stored in Group Policy Objects, configured via GPMC (Active Directory Group Policy) and GPEdit (Local Group Policy). Group Policy based configurations are evaluated according to GPO precedence rules.

- **Local Policy** – A standalone configuration which is stored locally, configured via MMC.

- **Webserver Policy** – A configuration located on a web server, accessible via HTTP(s), FTP or FILE.

- **McAfee ePO Policy** - A configuration that is stored within McAfee ePO, configured via the ePO Policy catalog.

Defendpoint uses a logical precedence to evaluate each configuration for matching rules. By default the client will apply the following precedence:

```
ePO Policy > Group Policy > Local Policy
```

Configuration precedence settings can be configured either as part of the client installation, or via the Windows Registry once the client has been installed.

To modify configuration precedence at client installation:

Use one of the following command lines to install the Defendpoint Client with a specific configuration precedence:

```
msiexec /i DefendpointClient_x(XX).msi
POLICYPRECEDENCE="EPO,WEBSERVER,GPO,LOCAL"
```

```
DefendpointClient_x(XX).exe /s /v
POLICYPRECEDENCE="EPO,WEBSERVER,GPO,LOCAL"
```

Where (XX) represents 86 or 64 in relation to the 32-bit or 64-bit installation respectively.

To modify configuration precedence via the Registry:

Run Regedit.exe with elevated privileges (ensuring you are using a Defendpoint token with anti-tamper disabled) and navigate to the following key:

```
HKEY_LOCAL_MACHINE\Software\Avecto\Privilege Guard Client
```

```
REG_SZ PolicyPrecedence = "EPO,WEBSERVER,GPO,LOCAL"
```

19. Deployment Methods

Certain types of deployment method may be enabled or disabled. By default, all deployment types are enabled. To include or exclude a method of deployment from evaluation, edit the entries in the registry value below. If this key does not already exist, then the default behavior is to include all methods:

```
HKEY_LOCAL_MACHINE\Software\Avecto\Privilege Guard Client
REG_SZ PolicyEnabled = "EPO,WEBSERVER,GPO,LOCAL"
```

Where "EPO,WEBSERVER,GPO,LOCAL" are the available deployment methods.

Note: Registry settings may be deployed via the Advanced Agent Settings feature. For more information, see Advanced Agent Settings. In order to apply a configuration deployment method via Advanced Agent Settings, the setting must be applied to a type of configuration that is already part of the Configuration Precedence order.
20. Avecto End User Utilities

Defendpoint includes three end user utilities to enable users to manage advanced network adapter settings, printer settings, and software installations, as many of these capabilities would usually be hosted in the explorer shell, making it difficult to give these tasks elevated rights.

20.1. Avecto Network Adapter Manager

The network adapter manager presents the network adapters to the end user in a familiar format.

From this utility a user may modify the properties of a network adapter, rename an adapter or disable an adapter.

In order to make the network adapter manager available to a user you must perform the following steps:

1. Add the Avecto Network Adapter Utility to the Defendpoint Settings and assign Admin Rights to this application for the relevant users (the utility is included in the Application Templates).

2. Create a shortcut on the users’ desktop to the network adapter manager, PGNetworkAdapterUtil.exe, which can be found in the Defendpoint Client installation directory (usually C:\Program Files\Avecto\Privilege Guard Client).

20.2. Avecto Printer Manager

The printer manager utility presents the printers to the end user in a familiar format.

From this utility a user may add and delete printers, access printer properties and preferences, view the printer queue, access Print server properties and print a test page.

In order to make the printer manager available to a user you must perform the following steps:

1. Add the Avecto Printer Management Utility to the Defendpoint Settings and assign Admin Rights to this application for the relevant users (the utility is included in the Application Templates).

2. Create a shortcut on the user’s desktop to the printer manager, PGPinterUtil.exe, which can be found in the Privilege Guard client installation directory (usually C:\Program Files\Avecto\Privilege Guard Client).
20.3. Avecto Programs and Features Manager

The programs and features manager presents the installed software to the end user in a familiar format.

From this utility a user may uninstall, change and repair software that is installed on their computer.

In order to make the programs and features manager available to a user you must perform the following steps:

1. Add the Avecto Programs and Features Manager to the Defendpoint Settings and assign Admin Rights to this application for the relevant users (the utility is included in the Application Templates).

2. Create a shortcut on the users desktop to the programs and features manager, PGProgramsUtil.exe, which can be found in the Defendpoint client installation directory (usually C:\Program Files\Avecto\Privilege Guard Client).

By default, the PGProgramsUtil will not display Windows Updates. To enable the option to show updates (via a toggle button), use the following command line switch:

```
PGProgramsUtil.exe /showupdates
```

20.4. Defendpoint Activity Viewer

The Defendpoint Activity Viewer is an advanced diagnostics tool designed to help identify improvements in Defendpoint Policies. It allows IT administrators to remotely connect to any Defendpoint Client on the network, and view all recent activity on the desktop.

The Activity Viewer will collect a complete audit of every application that was run on the desktop, and provide a detailed summary of how the Defendpoint client interacted with those applications, what actions it applied, and the rules that it used to determine that action.

The activity is displayed in a rich, detailed, yet simple to use interface that provides every snippet of information required to better understand the policies deployed to endpoints, how they affect the applications being run, and rapidly identify unexpected outcomes.

For more information and help with using the Defendpoint Activity Viewer, refer to the Activity Viewer Help from within the Activity Viewer Management Console.
21. Troubleshooting

21.1. Check Defendpoint is Installed and Functioning

If you are having problems the first step is to check that you have installed the client and that the client is functioning.

The easiest way to determine that the client is installed and functioning is to check for the existence of the Avecto Defendpoint Service in the services management console. Ensure that this service is both present and started. The Defendpoint service is installed by the Defendpoint Client and should start automatically.

**Note:** On Windows XP SP2 and Windows Server 2003 ensure that you have installed the client with the executable installer, which includes MSXML6. Alternatively you may use the MSI package, but you must also install Microsoft MSXML6 or ensure that it is already installed.

The Defendpoint service requires MSXML6 in order to load the Defendpoint settings, but the service will still run even if MSXML6 is not present.


21.1.1. Check Settings are Deployed

Assuming the Defendpoint Client is installed and functioning, the next step is to check that you have deployed policies to the ePO managed endpoint.

ePO policies are stored by the Privilege Guard Client as an xml file in the following location:

```
%ProgramData%\Avecto\Privilege Guard\ePO Cache\Machine\PrivilegeGuardConfig.xml
```

21.1.2. Check Policies are Licensed

One of the most common reasons for Defendpoint not functioning is the omission of a valid license from the Defendpoint Policy. If you are creating multiple policies, then you must ensure that the computer or user receives at least one policy that contains a valid license. To avoid problems it is simpler to add a valid license to every set of Defendpoint Policies that you create.

21.1.3. Check Workstyle Precedence

Assuming that Defendpoint is functioning and licensed, most other problems are caused by configuration problems or workstyle precedence problems. Please be aware that if you have multiple policies, these will be evaluated in alphanumeric order.

Once an application matches an application group entry in the Application Rules or the On Demand Application Rules, then processing will not continue for that application. Therefore, it is vital that you order your entries correctly:

- If you create multiple workstyles then workstyles higher in the list have a higher precedence.
- If you have multiple rules in the Application Rules and the On Demand Application Rules sections of a workstyle then entries higher in the list have a higher precedence.

**Application Rules** are applied to applications that are launched either directly by the user or by a running process. **On Demand Application Rules** are only applied to applications that are launched from the Defendpoint shell menu (if enabled).
22. Auditing and Reporting

The Defendpoint McAfee ePO Integration Pack includes a set of rich preconfigured dashboards, built in ePO Queries and Reports, which summarize Defendpoint event data collected from McAfee ePO managed computers.

Avecto also provide an enterprise level, scalable reporting solution in Defendpoint Enterprise Reporting. Defendpoint Enterprise Reporting (ER) includes a rich set of dashboards and reports designed to simplify the centralized management and auditing of Defendpoint activity throughout the desktop and server estate. Each dashboard provides detailed and summarized information regarding Application, User, Host and Workstyle usage. For more information contact Avecto.

22.1. Dashboards

The McAfee ePO integration includes the following dashboards:

- Avecto Privilege Guard: Blocked
- Avecto Privilege Guard: Elevated
- Avecto Privilege Guard: Executed
- Avecto Privilege Guard: Monitoring

To access the dashboards, click on the Dashboards icon and then select one of the Defendpoint dashboards from the Dashboard drop down menu.

Defendpoint: Executed

The Avecto Defendpoint: Executed dashboard contains all events raised by Defendpoint relating to applications which were allowed to execute under Defendpoint control. These events include:

- **Auto-Elevated** – Applications elevated by Application Privileges policy.
- **User-Elevated** – Applications elevated by ‘On-Demand’ shell elevation policy.
- **Passive** – Applications granted a passive access token.
- **Drop-Admin** – Applications which have had admin rights removed.
- **Default-Rights** – Applications which have had standard user rights enforced.
- **Custom-Token** – Applications granted a custom created access token.
- **Admin-required** – Applications which require admin rights to run (Privilege Monitoring).

The Avecto Defendpoint: Executed dashboard includes the following monitors:

- Avecto Defendpoint: Top 10 Executed Apps
- Avecto Defendpoint: Top 10 Executed by Publisher
- Avecto Defendpoint: Executed over Last 7 Days
Each chart element in the monitors can be hovered over to display a count of how many executed applications make up that element. To view the details of executed applications for a particular element, simply click on the element to drill down.

**Note:** If you wish to add, remove or amend any of the default monitors, you can do so within McAfee ePO Queries and Reports. It is recommended that this is done only by advanced McAfee ePO administrators. Please refer to McAfee ePO documentation for details on managing dashboards, queries and reports.

**Avecto Defendpoint: Elevated**

The Avecto Defendpoint: Elevated dashboard contains all events raised by Defendpoint relating to applications which were elevated by Defendpoint policy. These events include:

- Auto-Elevated – Applications elevated by Application Privileges policy.
- User-Elevated – Applications elevated by ‘On-Demand’ shell elevation policy.

The Avecto Defendpoint: Elevated dashboard includes the following monitors:

- Avecto Defendpoint: Top 10 Elevated Apps
- Avecto Defendpoint: Top 10 Elevated by Publisher
- Avecto Defendpoint: Elevated over Last 7 Days

Each chart element in the monitors can be hovered over to display a count of how many elevated applications make up that element. To view the details of elevated applications for a particular element, simply click on the element to drill down.

**Note:** If you wish to add, remove or amend any of the default monitors, you can do so within McAfee ePO Queries and Reports. It is recommended that this is done only by advanced McAfee ePO administrators. Please refer to McAfee ePO documentation for details on managing dashboards, queries and reports.

**Avecto Defendpoint: Blocked**

The Avecto Defendpoint: Blocked dashboard contains all events raised by Defendpoint relating to applications which were blocked by Defendpoint policy.

The Avecto Defendpoint: Blocked dashboard includes the following monitors:

- Avecto Defendpoint: Top 10 Blocked Apps
- Avecto Defendpoint: Top 10 Blocked by Publisher
- Avecto Defendpoint: Blocked over Last 7 Days

Each chart element in the monitors can be hovered over to display a count of how many blocked applications make up that element. To view the details of blocked applications for a particular element, simply click on the element to drill down.

**Note:** If you wish to add, remove or amend any of the default monitors, you can do so within McAfee ePO Queries and Reports. It is recommended that this is done only by advanced McAfee ePO administrators. Please refer to McAfee ePO documentation for details on managing dashboards, queries and reports.
Avecto Defendpoint: Monitoring

The Avecto Defendpoint: Monitoring dashboard contains all events raised by Defendpoint, relating to applications detected by Defendpoint, requiring elevated rights to run.

The Avecto Defendpoint: Monitoring dashboard includes the following monitors:

- Avecto Defendpoint: Top 10 Apps Requiring Elevated Rights
- Avecto Defendpoint: Top 10 Requiring Elevated Rights by Publisher
- Avecto Defendpoint: Elevated Rights over Last 7 Days

Each chart element in the monitors can be hovered over to display a count of how many monitored applications make up that element. To view the details of monitored applications for a particular element, simply click on the element to drill down.

**Note:** If you wish to add, remove or amend any of the default monitors, you can do so within McAfee ePO Queries and Reports. It is recommended that this is done only by advanced McAfee ePO administrators. Please refer to McAfee ePO documentation for details on managing dashboards, queries and reports.

### 22.2. Events

The Defendpoint client sends events to ePO via the McAfee Agent, and also to the local application event log, dependent on the audit and privilege monitoring settings within the Defendpoint policy.

The following events are logged by the Defendpoint client:

#### 22.2.1. Process Events

<table>
<thead>
<tr>
<th>ePO ID (Event ID)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>202250 (100)</td>
<td>process has started with admin rights added to token.</td>
</tr>
<tr>
<td>202251 (101)</td>
<td>process has been started from the shell context menu with admin rights added to token.</td>
</tr>
<tr>
<td>202253 (103)</td>
<td>process has started with admin rights dropped from token.</td>
</tr>
<tr>
<td>202254 (104)</td>
<td>process has been started from the shell context menu with admin rights dropped from token.</td>
</tr>
<tr>
<td>202256 (106)</td>
<td>process has started with no change to the access token (passive mode).</td>
</tr>
<tr>
<td>202257 (107)</td>
<td>process has been started from the shell context menu with no change to the access token (passive mode).</td>
</tr>
<tr>
<td>202259 (109)</td>
<td>process has started with user’s default rights enforced.</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>202260</td>
<td>process has started from the shell context menu with user’s default rights enforced.</td>
</tr>
<tr>
<td>202262</td>
<td>process requires elevated rights to run.</td>
</tr>
<tr>
<td>202263</td>
<td>process has started with custom token applied.</td>
</tr>
<tr>
<td>202264</td>
<td>process has started from the shell context menu with user’s custom token applied.</td>
</tr>
<tr>
<td>202266</td>
<td>process execution was blocked.</td>
</tr>
<tr>
<td>202267</td>
<td>process has stopped (deprecated)</td>
</tr>
<tr>
<td>202268</td>
<td>process started in the context of the authorizing user</td>
</tr>
<tr>
<td>202269</td>
<td>process started from the shell menu in the context of the authorizing user</td>
</tr>
<tr>
<td>202270</td>
<td>Process execution was cancelled by the user</td>
</tr>
<tr>
<td>202275</td>
<td>Defendpoint handled service control start action</td>
</tr>
<tr>
<td>202276</td>
<td>Defendpoint handled service control stop action</td>
</tr>
<tr>
<td>202277</td>
<td>Defendpoint handled service control pause/resume action</td>
</tr>
<tr>
<td>202278</td>
<td>Defendpoint handled service control configuration action</td>
</tr>
<tr>
<td>202279</td>
<td>Defendpoint blocked a service control start action</td>
</tr>
<tr>
<td>202280</td>
<td>Defendpoint blocked a service control stop action</td>
</tr>
<tr>
<td>202281</td>
<td>Defendpoint blocked a service control pause/resume action</td>
</tr>
<tr>
<td>202282</td>
<td>Defendpoint blocked a service control configuration action</td>
</tr>
<tr>
<td>202283</td>
<td>Defendpoint service control action run in the context of the authorizing user</td>
</tr>
<tr>
<td>Event ID</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>202284 (159)</td>
<td>Defendpoint service control start action cancelled</td>
</tr>
<tr>
<td>202285 (160)</td>
<td>Defendpoint service control stop action cancelled</td>
</tr>
<tr>
<td>202286 (161)</td>
<td>Defendpoint service control pause/resume action cancelled</td>
</tr>
<tr>
<td>202287 (162)</td>
<td>Defendpoint service control configuration action cancelled</td>
</tr>
<tr>
<td>202296 (198)</td>
<td>Privileged group modification blocked</td>
</tr>
<tr>
<td>202297 (199)</td>
<td>Process execution was blocked, the maximum number of challenge/response failures was exceeded</td>
</tr>
<tr>
<td>202299 (1)</td>
<td>Service Error - unlicensed.</td>
</tr>
</tbody>
</table>

Each process event contains the following information:

- Command line for the process
- Process ID for the process (if applicable)
- Parent process ID of the process
- Policy that applied
- Application Group that contained the process
- End user reason (if applicable)
- Custom access token (if applicable)
- File hash
- Certificate (if applicable)

**Note:** Each process event also contains Product properties, where applicable, but these can only be viewed in the Defendpoint Reporting Console.
22.2.2. Configuration Events

All events with a value of 200 - 299 ID are not sent to ePO Dashboards.

<table>
<thead>
<tr>
<th>ePO ID (Event ID)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>Successfully loaded Defendpoint configuration (information)</td>
</tr>
<tr>
<td>201</td>
<td>Loaded Defendpoint configuration but encountered non-critical problem (warning)</td>
</tr>
<tr>
<td>202</td>
<td>Failed to load Defendpoint configuration (error)</td>
</tr>
<tr>
<td>210</td>
<td>Successfully downloaded Defendpoint configuration</td>
</tr>
<tr>
<td>211</td>
<td>Failed to download Defendpoint configuration</td>
</tr>
</tbody>
</table>

Each configuration event contains the following information:

- File Name (Cached XML file)
- Configuration Source (Group Policy or Local Computer)
- Configuration Security (Plain Text XML or Signed XML)
- Security Information (Subject DN of Signed Certificate)
- GPO Name
- GPO display Name
- GPO Version
- GPO Active Directory Path
- GPO File System Path
- GPO Link Information
22.2.3. Content Events

All events with a value equal or greater than 600 have the same ePO Event ID.

<table>
<thead>
<tr>
<th>ePO ID (Event ID)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>600</td>
<td>Content has been updated with Add Admin Rights token</td>
</tr>
<tr>
<td>601</td>
<td>Content has been updated with a custom token</td>
</tr>
<tr>
<td>602</td>
<td>Content has been updated with Drop Admin Rights token</td>
</tr>
<tr>
<td>603</td>
<td>Content has been updated with Passive token</td>
</tr>
<tr>
<td>604</td>
<td>Content has been updated with Enforce User's Default Rights token</td>
</tr>
<tr>
<td>605</td>
<td>Content access was blocked</td>
</tr>
<tr>
<td>606</td>
<td>Content access was cancelled by the user</td>
</tr>
<tr>
<td>607</td>
<td>Content has been sandboxed</td>
</tr>
</tbody>
</table>

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
22.2.4. URL Events

<table>
<thead>
<tr>
<th>ePO ID (Event ID)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>650</td>
<td>Defendpoint redirected a user’s web browser navigation</td>
</tr>
</tbody>
</table>

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

22.2.5. User / Computer Events

These events are not sent to ePO Dashboards.

<table>
<thead>
<tr>
<th>ePO ID (Event ID)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>300</td>
<td>Detected user logon (information)</td>
</tr>
<tr>
<td>400</td>
<td>Defendpoint Service started (information)</td>
</tr>
</tbody>
</table>

**Note:** Health events are audited on the endpoint, and are visible in the Application Event Log using the Windows Event Viewer.
22.2.6. McAfee ePO / Avecto Database Events (Threat?)

Table Column Descriptions

<table>
<thead>
<tr>
<th>Table Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EventID</td>
<td>The Defendpoint ID for the event type.</td>
</tr>
<tr>
<td>ProcessStartTimeMS</td>
<td>Time that the process referenced in the event started.</td>
</tr>
<tr>
<td>ProductDescription</td>
<td>Product Description assigned by the vendor to the process referenced in the event.</td>
</tr>
</tbody>
</table>

For a full list of table column descriptions please refer to App16 McAfee ePO / Avecto Database Events.

22.3. Server Tasks – Avecto Threat Event Purge

The standard ePO tasks allow for the purging of Threat Events. As Avecto ePO Events are coupled to these, when deleted the Avecto events are also deleted. However in some cases it is desired that the Avecto portion of the event is more aggressively purged to save space. This task enables this by deleting these events older than a specified age whilst keeping the main Threat Event.

Note, these events are the ones held in the ePO database and hence Reporting Server events are in no way affected by this task.


2. On the Description page enter an appropriate name e.g. Avecto Event Purge and click Next.

3. On the Actions page, from the Actions drop-down menu, scroll up and select Avecto Defendpoint ePO Event Purge.
4. Depending on your data size and requirements enter the number of days after which events should be purged and click Next.

5. On the Schedule page adjust the options to suit your requirements and click Next.

6. Select Save from the Summary page.

22.4. Server Tasks – Enterprise Reporting Purge

You can purge Enterprise Reporting database events that are older than a defined period in order to manage the size of your database.


2. On the Description page enter an appropriate name e.g. Avecto ER Purge and click Next.

3. On the Actions page, from the Actions drop-down menu, scroll up and select Avecto Defendpoint Enterprise Reporting Purge
4. Choose the number of months that you will purge events older than.

5. On the Schedule page adjust the options to suit your requirements and click Next.

6. Select Save from the Summary page.

22.5. Auditing with Custom Scripts

When an application is allowed, elevated or blocked, Defendpoint will log an event to the application event log to record details of the action. If you wish to record the action in a bespoke or third party tracking system that supports PowerShell, VBScript or Jscript based submissions, you can use the Run a Script setting within an application rule. For more information see Managing Custom Scripts in the Utilities Section.
23. Setting up Enterprise Reporting for Defendpoint ePO Edition

This chapter explains how to install and configure Avecto Defendpoint Enterprise Reporting, which enables organizations to monitor and report on activity from Windows desktops and servers.

Defendpoint is implemented as a server extension to McAfee ePolicy Orchestrator, enabling agent deployment, policy management through the ePO Policy Catalog, and granular auditing and reporting of Defendpoint activity using the ePO integrated dashboards and query editor as well as the Avecto reporting module.

Reporting event centralization is supported via the ePO server. These events can be displayed using the reports module built into the Defendpoint Extension or via custom queries using the standard ePO reporting facilities.

Also provided are Threat Event linked audit events which are stored in the ePO database and displayed via the built in dashboards and queries.

The Defendpoint ePO Edition Enterprise Reporting module uses the Defendpoint Enterprise Reporting database to store Defendpoint audit data for reporting.

23.1. Defendpoint ePO Edition Reporting Options

Defendpoint offers two reporting levels when using the McAfee ePO edition. The options may be used individually or together to gain the required functionality:

**Basic level – ePO Queries and Reports Feature (Threat Events)**

- No prerequisites required
- Data is stored in the McAfee ePO Server database or Defendpoint MSFT SQL Server database
- Highly configurable dashboards, charts and tabular reports that can incorporate data from other ePO Server products in ePO
- Supports custom reporting
- Access to audit data from Defendpoint policy editor

**Advanced level – Avecto Enterprise Reporting in McAfee ePO Extension**

**Additional Prerequisites:**
MSFT SQL Server 2008 R2 or later

- Data is stored in a dedicated MSFT SQL Server database that can be hosted in, or separately from McAfee ePO Server’s database.
- Highly detailed dashboards and drill through reports in ePO.
- Direct addition of applications from reports into application groups.
- Access to audit data from Defendpoint policy editor
- Support for application reputation via integration with Intel Security Threat Intelligence Exchange (TIE) using Data Exchange Layer (DXL) and VirusTotal.
Access to audit data from Defendpoint policy editor.

Note: Times on reports are shown using the time zone of the ePO server. All events are stored in the database in UTC.

There are two main considerations with regard to Enterprise Reporting – where is the data stored and where are reports presented.

Note: If you have any queries during the installation process please contact an Avecto consultant.

23.2. Installation Tasks

23.2.1. Basic level – ePO Queries and Reports Feature (Threat Events)

➢ No additional setup required – access the dashboards through the queries and reports feature in the McAfee ePO server web application interface.

➢ If the second option below is also chosen, you will still have access to application audit data using the ePO Queries and Reports feature.

23.2.2. Advanced level – Avecto Enterprise Reporting in McAfee ePO Extension

1. Provision accounts required for installation and runtime

➢ Refer to the Accounts section for the accounts required.

➢ Please note that you will need access to the ePO Server Host as well as the MSFT SQL Server host where the Avecto Enterprise Reporting is located.

2. Install Defendpoint database as described in Defendpoint Reporting Database Installation.

3. McAfee ePO Registered Servers for Avecto Enterprise Reporting

➢ Execute the ePO configuration steps in Configuring access to Reporting Server Charts & Configuring access to Reporting Server for ePO Queries.

4. McAfee ePO Server Tasks for Avecto Enterprise Reporting

➢ Execute the configuration steps in Server Tasks – Avecto Event Staging & Server Tasks – Avecto Pre-caching Reports (Optional).
23.2.3. Accounts

Before commencing with the installation of the Enterprise Reporting components, it is recommended that the following accounts are created.

Accounts Required for Installation

<table>
<thead>
<tr>
<th>Name</th>
<th>Details</th>
<th>Account Type</th>
<th>Permissions / Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>DatabaseCreator</td>
<td>Used by the Reporting Database installer to create the Defendpoint database</td>
<td>Windows account or SQL Authentication account</td>
<td>SQL Server permission – sysadmin</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note: The database must be installed by a user whose default schema is DBO. For more information, refer to: <a href="http://technet.microsoft.com/en-us/library/ms190387(v=sql.105).aspx">http://technet.microsoft.com/en-us/library/ms190387(v=sql.105).aspx</a></td>
</tr>
</tbody>
</table>

23.3. Database Sizing and Resource Consumption

23.3.1. Data Retention Considerations

The Audit Event database and Microsoft SQL Server Reporting Services database used to support Avecto Defendpoint Enterprise Reporting may be hosted and scaled independently.

It's important to identify the length of time that Defendpoint audit event data must be retained in the Defendpoint database as it drives resource utilization projections, and initial allocation.

Defendpoint Enterprise Reporting is designed to report on activity in recent time, not as a long term archival data storage solution.

In order to facilitate your decision making regarding retention time in the Defendpoint database, please refer to the following sections in our standard documentation:

- Description of the views of data exposed in Defendpoint Enterprise Reporting - the Reporting Dashboard Guide.
- Description of the events audited by Defendpoint Auditing and Reporting – Events.
- Description of the Workstyle parameters. You may consider these as the fields that are collected in the audit events, eventually stored in the Defendpoint Audit Events database. Please refer to the Workstyle Parameters appendix.

23.3.2. Database Sizing

The Audit Event database has to be sized to accommodate substantial data volume, matching the number of clients generating audit data and the desired retention period.

Database storage requirements may be estimated roughly using the following calculation:

\[
\text{Number of hosts} \times \text{Number of events per host per day}
\]
For example, an organization of 10,000 hosts, with each host generating an average of 15 events per day, requiring a 30 day retention would require a database capacity of:

\[ 10,000 \times 15 \times 5 \times 30 = 22,500,000 \text{Kb}, \text{or} 21.5 \text{Gb} \]

A typical event volume would be 10-20 events per host per day and varies based on Defendpoint auditing configuration, user job function (role/workstyle) and user activity patterns.

**Note:** Please refer to the Defendpoint Database sizing calculator to further explore database sizing and growth expectations.

**Database resource utilization (CPU, Memory) is highly variable depending on the hardware platform.**

**Example Use Case Volumes**

Based on an organization of 10,000 hosts requiring a 42 day (six weeks) retention.

**Discovery:** Between 40 – 60 events per machine per day

(4.6K per event (based on real world data))

**Average total:** 67.06 GB

**Production:** Between 2 – 10 events per machine per day

(4.6K per event (based on real world data))

**Average total:** 5.66 GB

**Note:** If the number of events ‘per machine per day’ is raised to 15 then the Average total increases to **16.99 GB**

**Key considerations:**

**Volume of inbound audit event records**

As seen above, the number of events per hour may be estimated following simple calculations.

The audit event records are bulk inserted (no integrity checks, transactions) in batches of 100 by the Event Parser, and post-processed by a scheduled job that normalizes the audit event records into the Audit Event database schema.

**Queries triggered from MSFT SQL Reporting Services Reports**

As the database grows in size, the resource impact of the reporting platform queries becomes important.

The volume of data maintained in the audit event database will affect the duration and resource cost of these queries.

Finer-grained audit data management and clean-up is possible using the ER Database Administration Dashboard. The Database Administration Dashboard allows the purging of audits related to specific applications and suppression of incoming audit items related to those applications. For more
information please refer to the Database Administration description in the *Reporting Dashboard Guide*.

For more information about the database purge utility please refer to the *Database Maintenance* chapter in the *Enterprise Reporting Setup Guide*.

**Important**: Prior to purging large sets of data, please ensure your SQL Transaction logs are able to grow to accommodate. It may be necessary to delete data in stages when setting this up for the first time.
23.4. Defendpoint Reporting Database Installation

As part of the install, you will specify the database connection details, and the installer will create the Defendpoint database (if it doesn’t already exist).

**Important:** The Defendpoint Reporting Database installer creates a database and database permissions through embedded SQL scripts. If your database administration team does not allow the creation of databases, or database permissions by installers, please contact Avecto support for assistance with an alternative approach.

23.4.1. Installation

To install Defendpoint Reporting Database, run the appropriate installation package with an account that has *DatabaseCreator* privileges:

- If you are running the installer on the database machine use
  `DefendpointReportingDatabase.msi`

- If you are running the installer on a client machine use
  `DefendpointReportingDatabase.exe`

1. Run the appropriate installation package.

2. Click **Next** to continue. The **License Agreement** dialog will appear.
3. After reading the license agreement, select **I accept the terms in the license agreement** and click **Next** to continue. The **Database Server** dialog will appear.

4. Enter the name of the database catalog for Defendpoint audit data. Click **Next** to continue. The **Configure Event Parser Database User** dialog will appear.
5. Create or configure a user in the database for the Event Parser service to use. Click **Next** to continue. The **Configure Reporting Services Database User** dialog will appear.

6. Create or configure a user in the database to read data for the reports (choose the same Windows account as used in the previous step).

Note: This is the user that will be used for configuring the registered servers.
7. Click **Next** to continue. The **Ready to Install the Program** dialog will appear.

8. Click **Install** to complete the installation.

9. The status bar will display the progress of the installation.
10. The **InstallShield Wizard Completed** dialog will be displayed.

**Note:** The Avecto Defendpoint Enterprise Reporting MSFT SQL Database must be configured as a registered server in McAfee ePO.

For Database Sizing and Resource Consumption information please refer to the Database Sizing and Resource Consumption appendix of this guide.

### 23.5. Configuring Avecto Reporting for Enterprise Reporting Data

#### 23.5.1. Configuring access to Reporting Server Charts

1. Log in to ePolicy Orchestrator and navigate to **Menu > Registered Servers** and select **New Server**.

2. On the next page select **Avecto Reporting** from the **Server type** drop-down list and enter an appropriate name e.g. **ER**. Click **Next**.
3. Complete the configuration page and click **Test Connection**. On successful connection click **Save**.

**Note**: Avecto recommends you have a user account that should have **db_owner** access to the Avecto database or alternatively should be a member of the **Event Parser** role and the **Reporting Services Database** role if these were created during the Reporting Database installation.

23.5.2. Configuring access to Reporting Server for ePO Queries

1. Select **Menu > Registered Servers** and select **New Server**.

2. On the next page select **Database Server** from the **Server type** drop-down list and enter an appropriate name e.g. **Avecto Reporting Queries**. Click **Next**.
3. Complete the configuration page and click **Test Connection**. On successful connection click **Save**.

23.5.3. Server Tasks – Avecto Event Staging

Configure **Event Staging** to push the data to the Enterprise Reporting database:

2. On the **Description** page enter an appropriate name e.g. **Avecto Event Staging** and click **Next**.

3. On the **Actions** page, from the **Actions** drop-down menu, scroll up and select **Avecto Defendpoint Reporting Event Staging**.

4. Adjust the **Time in minutes to check for staging events** to 55. Ensure **Verbose logging** is not selected and click **Next**.

5. On the **Schedule** page adjust the **Schedule type** to **Hourly** and click **Next**.

6. Select **Save** from the **Summary** page.
7. From Menu > Server Tasks select and check the Avecto Event Staging box.

8. Select Actions > Enable Tasks.

Note: It is possible to create and run multiple Event Staging tasks as per above if required.

23.5.4. Server Tasks – Avecto Pre-caching Reports (optional)

This optional step allows top level Reporting Charts to be generated during non-business hours so that they are immediately available subsequently.

1. Select Menu > Server Tasks and from the Actions menu select New Task.

2. On the Description page enter an appropriate name e.g. Avecto Pre-caching Reports and click Next.

3. On the Actions page, from the Actions drop-down menu, scroll up and select Avecto Defendpoint Reporting Pre-Caching.

4. Depending on your data size and requirements select the appropriate Interval Queries options and click Next.
5. On the **Schedule** page adjust the options to suit your requirements and click **Next**.

**Note**: Avecto recommends you run this task through the night so that reports are available at the earliest convenience. Reports caches are re-set at 24:00 hours (local time zone). Therefore the pre-caching server task should be set to run after this time.

6. Select **Save** from the **Summary** page.

### 23.6. Performance Limitations

The default configuration of the ePO server is to only allow 2 concurrent tasks that can only share a single processor core. For larger systems this may not be adequate for performance. ePO can be reconfigured to make better use of the processor cores for scheduled tasks as described below.

More information can be in the McAfee Knowledge Base article KB83698
https://kc.mcafee.com/corporate/index?page=content&id=KB83698&snspd-0115

1. Select **Menu > Server Settings** and click on **Scheduler Tasks**.

2. Click **Edit**.
3. From Total maximum tasks select Absolute maximum calculation.

This ensures you are not restricted to using only one core for calculations.

Note: The server must be restarted for these changes to take effect.
24. Reputation Settings

Intel Security’s Reputation feature can be configured from:

Menu > Server Settings > Avecto Reputation Settings

Click **Edit** to change the options.

**Note:** Threat Intelligence Exchange (TIE) via the Data Exchange Layer (DXL) and Virus Total are supported.

Use the radio buttons to enable each source. If the required DXL extensions are not installed then a warning message will be displayed indicating that TIE is not available.

Once added the screen should look like this:

**Note:** If using a public (non-commercial) Virus Total key, the rate of queries is limited to 4 per minute. These keys should only be used for evaluation. API keys are available to purchase directly from Virus Total.
TIE does not have this restriction so using “0” for an unlimited query rate is recommended.

24.1. Server Tasks

A server task for updating reputations in the background is available:

1. Select Menu > Server Tasks > New Task

2. Enter a name for the task such as “Reputation Update” and click Next.

3. Select “Avecto Reputation Update” from the Actions drop down menu.

4. Enable the check box for the reputation type you wish to update. It is possible to update both types using the same task, however that means they will be carried out sequentially which may not be desirable.

5. The task can either look for reputations of applications that do not yet have a reputation or it can search for reputations older than a specified number of days and then update them.

6. Schedule the task(s) as per other Server Tasks.
24.2 Reputation in Reporting

Reputations are displayed in various Avecto reports where they can be updated on-demand.

They are shown in the following reports:

- Discovery
- Applications
- Application Details
- Requests
- Events
- Event Details

Using the Applications report as an example, the screen shot shows all the reputation states of:

- Pending (no reputation has been checked)
- Unknown (the sources do not have a reputation)
- Good (at least one source knows this application and it is good and no sources say it is poor)
- Poor (any source indicates it has a poor reputation)

The threshold between Poor and Good is on the Server Settings page.

A detailed breakdown of the application can be accessed by clicking on it:
Reputations can be updated from **Actions > Update Reputations**.

**Note**: The speed of update via this method will be constrained by the rate of the slowest source. When using a public API based Virus Total update, this can be very slow but the update may be cancelled at any time.

Reputation is also displayed on the detailed **Application Report** and **Event Report**. Reputation can also be updated from here.
Appendices

In this section you will find the following appendices:

> **Appendix 1** – How Sandboxing Works
> **Appendix 2** – Built-in Groups
> **Appendix 3** – Target Definitions
> **Appendix 4** – Application Templates
> **Appendix 5** – Configuring Remote Computer Browsing
> **Appendix 6** – Environment Variables
> **Appendix 7** – Regular Expressions Syntax
> **Appendix 8** – Workstyle Parameters
> **Appendix 9** – Windows Privileges
> **Appendix 10** – Example PowerShell Configurations
> **Appendix 11** – Manual Deployment of the Defendpoint Client
> **Appendix 12** – Using Defendpoint Events to Build Queries
> **Appendix 13** – Rule Precedence
> **Appendix 14** – Autosave Function
> **Appendix 15** – Database Sizing and Resource Consumption
> **Appendix 16** – McAfee ePO / Avecto Database Events
Appendix 1. How Sandboxing Works

A 1.1. Sandbox Permissions and Security

Defendpoint Sandboxing offers a protective environment to safely open and browse internet content and email attachments, and Windows native security ensures that sandboxed 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 may be persisted after the sandbox has been destroyed.

Any content that is saved to the real user’s profile always opens in the same sandbox 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:

<table>
<thead>
<tr>
<th>User Folder</th>
<th>Trusted Browsing access to private content</th>
<th>Untrusted Browsing access to private content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop</td>
<td>Read-only</td>
<td>No Access</td>
</tr>
<tr>
<td>Documents</td>
<td>Read-only</td>
<td>No Access</td>
</tr>
<tr>
<td>Downloads</td>
<td>Read-only</td>
<td>No Access</td>
</tr>
<tr>
<td>Pictures</td>
<td>Read-only</td>
<td>No Access</td>
</tr>
<tr>
<td>Videos</td>
<td>Read-only</td>
<td>No Access</td>
</tr>
<tr>
<td>Music</td>
<td>Read-only</td>
<td>No Access</td>
</tr>
<tr>
<td>Personal</td>
<td>Read-only</td>
<td>No Access</td>
</tr>
<tr>
<td>Favourites / Links</td>
<td>Full Control</td>
<td>Full Control</td>
</tr>
</tbody>
</table>

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

Note: Defendpoint sandboxing also isolates any sandbox browsing history and cookies so that they are available between sandbox sessions. Each sandbox will persist only its version of browsing history and cookies, separate to the private data of the real user.
A 1.2. Sandbox 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 open in the same context.

There are three contexts that can be selected in the Defendpoint Sandboxing module:

<table>
<thead>
<tr>
<th>Context</th>
<th>Description</th>
<th>Recommended Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Websites and documents are opened natively, and have full access to your private data.</td>
<td>Local and internal websites, where full access to private documents is required. For example, corporate intranets and web based document stores.</td>
</tr>
<tr>
<td>Trusted Browsing</td>
<td>Websites and documents are granted read-only access to your private data, but are prevented from modifying or deleting your private data.</td>
<td>Trusted internet based websites that require regular access to private documents, for example corporate cloud storage solutions, CRM systems, etc.</td>
</tr>
<tr>
<td>Untrusted Browsing</td>
<td>Websites and documents are prevented from reading, modifying or deleting your private data.</td>
<td>Ideal for all other web browsing.</td>
</tr>
</tbody>
</table>

A 1.3. Tagging and Classification

When an internet browser navigates 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 will also be 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.
A 1.4. URL Redirection

When an internet browsing session first begins, Defendpoint will open the web browser in the appropriate sandbox context. This may 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 sandbox context, then a new instance of the web browser will be created. If an instance of the web browser already exists for that context, then a new tab will be 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.

**Note:** In order for sandboxing to successfully redirect web addresses, third-party Browser Helper Objects (BHO’s) – specifically PGBHO - must be enabled.

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

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

A 1.5. Defendpoint Classification

**Note:** This feature is only available to users if it was selected in the workstyle wizard.

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

A document 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.

When Defendpoint Classification is enabled, a user can toggle the classification of a file between Private and Public.

- A file that was originally private and is reclassified public will automatically be opened in an Untrusted sandbox.

- A file that was originally public (sandboxed) and is reclassified private will not be opened in a sandbox.

- A file 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 i.e. Trusted or Untrusted.
A 1.6. Allow Upload to Internet

**Note:** This feature is only available to users if it was selected in the workstyle wizard.

Users may be given the option of allowing *Read* access to individual private documents, from within the Untrusted Browsing sandbox. This is achieved via a toggled option that is available from the right-click menu of a particular document.

1. Right-click on a Private file and select Defendpoint Classification > Allow upload to Internet from the context menu.

2. Repeat this with a file that has been classified as **Trusted**. Despite their different classifications, both files are now readable from the Untrusted Browsing sandbox, therefore allowing you to upload them to websites running in the Untrusted context.
Appendix 2. Built-in Groups

Further technical information regarding Groups created automatically by Defendpoint.

A 2.1. Built-in Groups

Avecto includes a number of built-in groups that may be used in any Application Rule, URL Rule or Content Rule. These groups provide a simple and convenient way of applying broad rules to applications, websites and content, in particular when defining ‘catch-all’ rules. Built-in groups also help to simplify your configurations by reducing the amount of groups.

<table>
<thead>
<tr>
<th>Group</th>
<th>Criteria</th>
<th>Valid Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any Website</td>
<td>Matches any website navigated to in Internet Explorer.</td>
<td>URLs</td>
</tr>
<tr>
<td>Any Sandboxed Content</td>
<td>Matches any trusted or untrusted file content double-clicked.</td>
<td>Non-application file types</td>
</tr>
<tr>
<td>Any Application</td>
<td>Matches any application that executed. Will also match any child applications.</td>
<td>Executables</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Control Panel Applets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Installer Packages</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Management Consoles</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Scripts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PowerShell Scripts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Batch Scripts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Registry Scripts</td>
</tr>
<tr>
<td>Any Signed Application</td>
<td>Matches any application that executed which has been signed by a publisher. Will also match any child applications of signed applications.</td>
<td>Executables</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Control Panel Applets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Installer Packages</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Management Consoles</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Scripts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PowerShell Scripts</td>
</tr>
<tr>
<td>Any UAC Prompt</td>
<td>Matches any application that triggers a Windows UAC prompt. Will also match any child applications.</td>
<td>Executables</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Installer Packages</td>
</tr>
<tr>
<td></td>
<td></td>
<td>COM Classes</td>
</tr>
</tbody>
</table>
| Any Signed UAC Prompt | Matches any application that triggers a Windows UAC Prompt, which has been signed by a publisher. Will also match any child applications. | Executables  
Installer Packages  
COM Classes |
|---|---|---|
| Any Sandboxed UAC Prompt | Matches any sandboxed process that triggers a Windows UAC Prompt. | Executables  
Installer Packages  
COM Classes |
Appendix 3. Target Definitions

Defendpoint Targets are elements that can be added to groups. Defendpoint has three types of groups; Application groups, URL groups and Content groups. Therefore three targets exist that can be added to these groups; Applications, URLs and Content.

Target Definitions are used to define exactly what constitutes a valid Target. It is these definitions that a Target rule will match against. 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 list describes all of the available Target definitions:

**ActiveX Codebase**

When inserting ActiveX controls this is enabled by default and it is recommended that you should use this option in most circumstances. You must enter the URL to the codebase for the ActiveX control. You may choose to match based on the following options (wildcard characters ? and * may be used):

- Exact Match
- Starts With
- Ends With
- Contains
- Regular Expressions

Although you may enter a relative codebase name, it is strongly recommended that you enter the full URL to the codebase, as it is more secure.

**ActiveX Version**

If the ActiveX control you entered has a version property then you can choose **Check Min Version** and/or **Check Max Version** and edit the respective version number fields.

**AppId**

This option allows you to match the App ID of the COM Class, which is a GUID used by windows to set properties for a CLSID. AppId’s can be used by 1 or more CLSID’s.

The available operators are identical to the File or Folder Name definition.

If you wish 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.

**Application Requires Elevation (UAC)**

This option can be used to check if an application requires elevated rights to run and would cause User Account Control (UAC) to be triggered. This is a useful way to replace inappropriate UAC prompts with Defendpoint End User Messages to either block or prompt the user for elevation. As Windows XP on Windows Server 2003 do not support UAC, processes running on those systems will never match this rule.
CLSID

This option allows you to match the class ID of the ActiveX control or COM Class, which is a unique GUID stored in the registry.

COM Display Name

If the class you entered has a Display Name then it will automatically be extracted and you can choose to match on this property. By default a substring match is attempted (Contains). Alternatively, you may choose to pattern match based on either a Wildcard match (? and *) or a Regular Expression. The available operators are identical to File or Folder Name definition.

Command Line

If the filename is not specific enough you may match the command line, by checking this option and entering the command line to match. By default a substring match is attempted (Contains). Alternatively, you may choose to pattern match based on either a Wildcard match (? and *) or a Regular Expression. The available operators are identical to File or Folder Name definition.

If you wish 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.

Note: PowerShell removes double quotes from command strings prior to them being transmitted to the target. Therefore it is not recommended that Command Line definitions include double quotes, as they will fail to match the command.

Controlling Process

This option allows you to target content based on the process (application) that will be used to open the content file. The application must have been added to an application group. You may also define whether any parent of the application will match the definition.

Drive

This option can be used to check the type of disk drive the file is located. Choose from one of the following options:

- **Fixed Disk** - Any drive that is identified as being an internal hard disk.
- **Network** - Any drive that is identified as a network share.
- **RAM Disk** - Any drive that is identified as a RAM drive.
- **Any Removable drive or media** - If you wish to target any removable drive or media, but are unsure of the specific drive type, choose this option which will match any of the removable media types below. Alternatively, if you wish to target a specific type, choose from one of the following removable media types:
  - **Removable Media** - Any drive that is identified as Removable Media.
  - **USB** - Any drive that is identified as a disk connected via USB.
  - **CD/DVD** - Any drive that is identified as a CD or DVD drive.
  - **eSATA Drive** - Any drive that is identified as a disk connected via eSATA.
If you wish 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.

**File or Folder Name**

Applications are validated by matching the file or folder name. You may choose to match based on the following options (wildcard characters ? and * may be used):

- Exact Match
- Starts With
- Ends With
- Contains
- Regular Expressions

Although you may enter relative filenames, it is strongly recommended that you enter the full path to a file or the COM Server. Environment Variables are also supported.

If you wish 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.

**Note:** It is not recommended that the definition File or Folder Name does NOT Match is used in isolation for executable types, as it will result in matching every application, including hosted types such as Installer packages, scripts, batch files, registry files, management consoles and Control Panel Applets.

**Important:** When creating blocking rules for Applications or Content, and the File or Folder Name is used as matching criteria against paths which exist on network shares, this should be done using the UNC network path and not by the mapped drive letter.

**File Hash**

If the filename is not considered secure and the file has not been signed then a file hash should be considered. Ensure that you have entered a file that exists on the system where the console is running, as this will cause the SHA-1 hash to be calculated automatically. Although you can edit this field, it is strongly recommended that you don’t unless you are typing in a hash that you have retrieved from another system. Although this validation option is the most secure, as it will validate the contents of the file, you must remember to update the file hash if the application file is changed. For this reason, file hashes should be a last resort, and other rules should be used to identify the application where possible.

If you wish 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.

**File Hash (SHA-1 fingerprint)**

If a reference file was entered, then an SHA-1 hash of the PowerShell script will be generated. This definition ensures that the contents or the script file (which can normally be edited by any user) remain unchanged, as changing a single character in the script will cause the SHA-1 Hash to change.

If you wish 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.

**File Version**
If the file, service executable or COM Server you entered has a File Version property then it will automatically be extracted and you can choose Check Min Version and/or Check Max Version and edit the respective version number fields.

**Parent Process**

This option can be used to check if an application’s parent process matches a specific application group. You must create an application group for this purpose or specify an existing application group in the Parent Process Group. Setting match all parents in tree to **True** will traverse the complete parent/child hierarchy for the application, looking for any matching parent process, whereas setting this option to **False** will only check the application’s direct parent process.

If you wish 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**.

**Parent Process in Sandbox**

This option can be used to check if an application’s parent process is running in a Sandbox. Choose from one of the following options:

- Any
- Trusted Browsing
- Untrusted Browsing

If you wish 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**.

**Product Code**

If the file you entered has a Product Code then it will automatically be extracted and you can choose to check this code.

**Product Description**

If the file you entered has a Product Description property then it will automatically be extracted and you can choose to match on this property. By default a substring match is attempted (**Contains**). Alternatively, you may choose to pattern match based on either a Wildcard match (?) and *) or a **Regular Expression**. The available operators are identical to the **File or Folder Name** definition.

If you wish 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**.

**Product Name**

If the file, COM Server or service executable you entered has a Product Name property then it will automatically be extracted and you can choose to match on this property. By default a substring match is attempted (**Contains**). Alternatively, you may choose to pattern match based on either a Wildcard match (?) and *) or a **Regular Expression**. The available operators are identical to the **File or Folder Name** definition.

If you wish 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**.

**Product Version**
If the file or COM Server or Service executable you entered has a Product Version property then it will automatically be extracted and you can choose Check Min Version and/or Check Max Version and edit the respective version number fields.

Publisher

This option can be used to check for the existence of a valid publisher. If you have browsed for an application, then the certificate subject name will automatically be retrieved, if the application has been signed. For Windows system files the Windows security catalog is searched, and if a match is found then the certificate for the security catalog is retrieved. Publisher checks are supported on Executables, Control Panel Applets, Installer Packages, Windows Scripts and PowerShell Scripts. By default a substring match is attempted (Contains). Alternatively, you may choose to pattern match based on either a Wildcard match (\? and \*) or a Regular Expression. The available operators are identical to the File or Folder Name definition.

If you wish 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.

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 wish 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.

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 wish 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.

Service Action

This option allows you to define the actions which are allowed. Choose from:

- Service Stop - Grants permission to stop the service.
- Service Start - Grants permission to start the service.
- Service Pause / Resume - Grants permission to pause and resume the service.
- Service Configure - grants permission to edit the properties of the service.

Service Name - This option allows you to match the name of the Windows service, for example "W32Time". You may choose to match based on the following options (wildcard characters \? and \* may be used):

- Exact Match
- Starts With
- Ends With
Contains

Regular Expressions

If you wish to reverse the outcome of this definition, to target applications which DO NOT match the definition, then click the definition to toggle between \textit{matches} and \textit{does NOT match}.

Service Display Name

This option allows you to match the name of the Windows service, for example "W32Time". You may choose to match based on the following options (wildcard characters ? and * may be used):

- Exact Match
- Starts With
- Ends With
- Contains
- Regular Expressions

If you wish to reverse the outcome of this definition, to target applications which DO NOT match the definition, then click the definition to toggle between \textit{matches} and \textit{does NOT match}.

Source URL

If an application was downloaded using a web browser, this option can be used to check where the application or installer was originally downloaded from. The application is tracked by Defendpoint at the point it is downloaded, so that if a user decided to run the application or installer at a later date, the source URL can still be verified. By default a substring match is attempted (\textit{Contains}). Alternatively, you may choose to pattern match based on either a Wildcard match (?) and * or a \textit{Regular Expression}. The available operators are identical to the File or Folder Name definition.

If you wish to reverse the outcome of this definition, to target applications which DO NOT match the definition, then click the definition to toggle between \textit{matches} and \textit{does NOT match}.

Trusted Ownership

This option can be used to check if an application's file is owned by a trusted owner (the trusted owner accounts are SYSTEM, Administrators or Trusted Installer).

If you wish to reverse the outcome of this definition, to target applications which DO NOT match the definition, then click the definition to toggle between \textit{matches} and \textit{does NOT match}.

Upgrade Code

If the file you entered has an Upgrade Code then it will automatically be extracted and you can choose to check this code.

A 3.1. Windows Store Application Definitions

Windows Store Application Version

This option allows you to match the version of the Windows Store Application, for example "16.4.4204.712". You can choose Check Min Version and/or Check Max Version and edit the respective version number fields.
If you wish 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.

**Windows Store Package Name**

This option allows you to match the name of the Windows Store Application, for example "microsoft.microsoftskydrive". By default a substring match is attempted (Contains). Alternatively, you may choose to pattern match based on either a Wildcard match (?) and *) or a Regular Expression. The other available operators are:

- Exact Match
- Starts With
- Ends With

If you wish 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.

**Windows Store Publisher**

This option allows you to match the publisher name of the Windows Store Application, for example "Microsoft Corporation". By default a substring match is attempted (Contains). Alternatively, you may choose to pattern match based on either a Wildcard match (?) and *) or a Regular Expression. The other available operators are:

If you wish 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.

*Note:* The Browse File and Browse Apps... options can only be used if configuring Defendpoint Settings from a Windows 8 client.

**A 3.2. URL Definitions**

**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 wish to match any hostname, an asterisk (*) is allowed.

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.

Multiple domains may be added to the same URL definition by using a comma (,). For example, you may 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.

*Note:* 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.

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.
Zone URL

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

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.
Appendix 4. Application Templates

Defendpoint ships with some standard application templates to simplify the definition of applications that are part of the operating system, common ActiveX controls and software updaters.

The standard application templates are split into convenient categories:

- Avecto Utilities
- Common ActiveX Controls
- Common Printer Driver Manufacturers
- Software Updaters
- Tools and utilities for administrators and developers
- Windows 7 and Windows Server 2008 R2
- Windows Vista and Windows Server 2008
- Windows XP and Windows Server 2003
- COM Classes for third party software
- COM Classes for file, folder and drive operations
- COM Classes for general Windows operations
- COM Classes for security features and configurations
- COM Classes for software installation, uninstallation and updates
- COM Classes for network device settings, sharing options and configuration

Each category then has a list of applications for that category. Picking an application will cause the Application or ActiveX control dialogs to be pre-populated with the appropriate information.
Appendix 5. Configuring Remote Computer Browsing

The Defendpoint Workstyle Editor allows you to browse computers on the network for executables, Windows services and running processes, which can be added to Target Application groups. This provides a convenient alternative to manual entry.

Remote computer browsing leverages Windows Remote Management (WinRM) and PowerShell, which must be configured on each target endpoint in advance of using the computer browser feature to access the remote computer.

WinRM and Powershell are components of the Windows Management Framework, and are part of Windows 7 and Windows Server 2008 R2. For older versions of Windows, the Windows Management Framework can be downloaded and installed as an optional update at:


To configure the ePO Server.

1. Configure WinRM trusted hosts:
   a) Open PowerShell (elevated).
   b) Type
      
      ```
      winrm s winrm/config/client '@{TrustedHosts="<endpoint>"}'
      ```
      where `<endpoint>` should be replaced with the hostname or IPAddress of the network computer to be trusted (a wildcard "*" can also be used).
      and press Enter.

To configure a network computer.

1. Verify that PS-Remoting is enabled:
   a) Open PowerShell (elevated).
   b) Type
      ```
      Enable-PSRemoting
      A
      ```
      and then type A to accept all defaults (this can also be enabled via AD Group Policy).

2. Configure WinRM to allow remote connections:
   a) In the same PowerShell window, type
      ```
      winrm qc
      ```
      and press Enter.
   b) Type
      ```
      winrm set winrm/config/service @{AllowUnencrypted="true"}
      ```
      and press Enter.

To test for a successful connection

Run this command from the ePO server:

```
```

where `<endpoint>` should be replaced with the hostname or IPAddress of the network computer, `<username>` and `<password>` replaced with administrator credentials on the network computer.
If the connection is unsuccessful

Fix the local security policy to enable classic mode authentication for network logons.

4. Set to classic

Mixed environments

1. Open PowerShell (elevated).
2. Type
   `new-itemproperty -name LocalAccountTokenFilterPolicy -path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -propertyType DWord -value 1`
   and press Enter.
Appendix 6. Environment Variables

Defendpoint supports the use of the following environment variables within file path and command line application definitions:

**System Variables**

- %ALLUSERSPROFILE%
- %COMMONPROGRAMFILES(x86)%
- %COMMONPROGRAMFILES%
- %PROGRAMDATA%
- %PROGRAMFILES(\x86)%
- %PROGRAMFILES%
- %SYSTEMROOT%
- %SYSTEMDRIVE%

**User Variables**

- %APPDATA%
- %USERPROFILE%
- %HOMEPATH%
- %HOMESHARE%
- %LOCALAPPDATA%
- %LOGONSERVER%

To use any of the environment variables above, simply enter the variable, including the % characters, into a file path or command line. The Defendpoint Client will expand the environment variable prior to attempting a file path or command line match.
## Appendix 7. Regular Expressions Syntax

Defendpoint can control applications at a granular level by utilizing regular expression syntax. Defendpoint utilizes the ATL regular expression library **CAtlRegExp**. Below is a summary of the regular expression syntax used by this library.

<table>
<thead>
<tr>
<th>Meta character</th>
<th>Meaning</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any character except [^$.</td>
<td>?+()]</td>
<td>All characters except the listed special characters match a single instance of themselves. To match one of these listed characters use a backslash escape character (see below)</td>
</tr>
<tr>
<td>\ (backslash)</td>
<td>Escape character: interpret the next character literally.</td>
<td>“a+b” matches “a+b”</td>
</tr>
<tr>
<td>. (dot)</td>
<td>Matches any single character</td>
<td>“a.b” matches “aab”, “abb” or “acb”, etc.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Indicates a character class. Matches any character inside the brackets.</td>
<td>“[abc]” matches “a”, “b”, or “c”</td>
</tr>
<tr>
<td>^ (caret)</td>
<td>Negates the character class. A negated character class matches any character except those inside the brackets.</td>
<td>“[^abc]” matches all characters except “a”, “b”, and “c”</td>
</tr>
<tr>
<td>- (minus character)</td>
<td>In a character class, indicates a range of characters</td>
<td>“[0-9]” matches any of the digits “0” through “9”</td>
</tr>
<tr>
<td>?</td>
<td>Indicates that the preceding expression is optional: it matches once or not at all.</td>
<td>“ab?c” matches “ac” or “abc”</td>
</tr>
<tr>
<td>+</td>
<td>Indicates that the preceding expression matches one or more times</td>
<td>“ab+c” matches “abc” and “abbc”, “abbcc”, etc.</td>
</tr>
<tr>
<td>* (asterisk)</td>
<td>Indicates that the preceding expression matches zero or more times</td>
<td>“ab*c” matches “ac” and “abc”, “abbc”, etc.</td>
</tr>
<tr>
<td></td>
<td>(vertical pipe)</td>
<td>Alternation operator: separates two expressions, exactly one of which matches.</td>
</tr>
<tr>
<td>??, +?, *?</td>
<td>Non-greedy versions of ?, +, and *. These match as little as possible, unlike the greedy versions which match as much as possible.</td>
<td>Given the input “&lt;abc&gt;&lt;def&gt;”, “.?” matches “&lt;abc&gt;” while “.” matches “&lt;abc&gt;&lt;def&gt;.”</td>
</tr>
<tr>
<td>()</td>
<td>Grouping operator</td>
<td>“(One)</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>{}</td>
<td>Indicates a match group. The actual text in the input that matches the expression inside the braces can be retrieved through the CAtlREMatchContext object.</td>
<td></td>
</tr>
<tr>
<td>\</td>
<td>Escape character: interpret the next character literally (for example, [0-9]+ matches one or more digits, but [0-9]+ matches a digit followed by a plus character). Also used for abbreviations (such as \a for any alphanumeric character; see table below). If \ is followed by a number n, it matches the nth match group (starting from 0). Note that in C++ string literals, two backslashes must be used: &quot;\a&quot;, &quot;\b&quot;, &quot;{.<em>?}.</em>?&lt;/\0&gt;&quot;.</td>
<td>{.<em>?}.</em>?&lt;/\0&gt; matches &quot;&lt;head&gt;Contents&lt;/head&gt;&quot;</td>
</tr>
<tr>
<td>$</td>
<td>At the end of a regular expression, this character matches the end of the input.</td>
<td>[0-9]$ matches a digit at the end of the input</td>
</tr>
<tr>
<td></td>
<td>Alternation operator: separates two expressions, exactly one of which matches.</td>
<td>T</td>
</tr>
<tr>
<td></td>
<td>Negation operator: the expression following ! does not match the input.</td>
<td>a!b matches &quot;a&quot; not followed by &quot;b&quot;</td>
</tr>
</tbody>
</table>

Appendix 8. Appendix – Workstyle Parameters

The Defendpoint Settings include a number of features that allow customization of text and strings that are used for end user messaging and auditing. If you wish to include properties that relate to the settings applied, the application being used, the user or the installation of the Defendpoint Client, then parameters may be used that expand when the text is used.

Parameters are identified as any string surrounded by [square parentheses], and if detected, the agent will attempt to expand the parameter. If successful, the parameter will be replaced with the expanded property. If unsuccessful, the parameter will remain part of the string. The table below shows a summary of all available parameters and where they are supported.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[PG_ACTION]</td>
<td>The action which the user performed from an End User Message</td>
</tr>
<tr>
<td>[PG_AGENT_VERSION]</td>
<td>The version of the Defendpoint Client</td>
</tr>
<tr>
<td>[PG_APP_DEF]</td>
<td>The name of the Application Rule that matched the application</td>
</tr>
<tr>
<td>[PG_APP_GROUP]</td>
<td>The name of the Application Group that contained a matching Application Rule</td>
</tr>
<tr>
<td>[PG_AUTH_USER_DOMAIN]</td>
<td>The domain of the designated user who authorized the application</td>
</tr>
<tr>
<td>[PG_AUTH_USER_NAME]</td>
<td>The account name of the designated user who authorized the application</td>
</tr>
<tr>
<td>[PG_COM_APPID]</td>
<td>The APPID of the COM component being run</td>
</tr>
<tr>
<td>[PG_COM_CLSID]</td>
<td>The CLSID of the COM component being run</td>
</tr>
<tr>
<td>[PG_COM_NAME]</td>
<td>The name of the COM component being run</td>
</tr>
<tr>
<td>[PG_COMPUTER_DOMAIN]</td>
<td>The name of the domain that the host computer is a member of</td>
</tr>
<tr>
<td>[PG_COMPUTER_NAME]</td>
<td>The NetBIOS name of the host computer</td>
</tr>
<tr>
<td>[PG_CONTENT_DEF]</td>
<td>The definition name of the matching content</td>
</tr>
<tr>
<td>[PG_CONTENT_FILE_CLASSIFICATION]</td>
<td>The sandbox classification of a matching content</td>
</tr>
<tr>
<td><strong>[PG_CONTENT_FILE_DRIVE_TYPE]</strong></td>
<td>The drive type of a matching content</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td><strong>[PG_CONTENT_FILE_HASH]</strong></td>
<td>The Sha-1 hash of a matching content</td>
</tr>
<tr>
<td><strong>[PG_CONTENT_FILE_IE_ZONE]</strong></td>
<td>The Internet Zone of a matching content</td>
</tr>
<tr>
<td><strong>[PG_CONTENT_FILE_NAME]</strong></td>
<td>The file name of a matching content</td>
</tr>
<tr>
<td><strong>[PG_CONTENT_FILE_OWNER]</strong></td>
<td>The owner of a matching content</td>
</tr>
<tr>
<td><strong>[PG_CONTENT_FILE_PATH]</strong></td>
<td>The full path of a matching content</td>
</tr>
<tr>
<td><strong>[PG_CONTENT_GROUP]</strong></td>
<td>The group name of a matching content definition</td>
</tr>
<tr>
<td><strong>[PG_DOWNLOAD_URL]</strong></td>
<td>The full URL from which an application was downloaded</td>
</tr>
<tr>
<td><strong>[PG_DOWNLOAD_URL_DOMAIN]</strong></td>
<td>The domain from which an application was downloaded</td>
</tr>
<tr>
<td><strong>[PG_EVENT_TIME]</strong></td>
<td>The date / time that the Policy matched</td>
</tr>
<tr>
<td><strong>[PG_EXEC_TYPE]</strong></td>
<td>The type of execution method – Application Rule or Shell Rule</td>
</tr>
<tr>
<td><strong>[PG_GPO_DISPLAY_NAME]</strong></td>
<td>The display name of the GPO</td>
</tr>
<tr>
<td><strong>[PG_GPO_NAME]</strong></td>
<td>The name of the Group Policy Object which contained the matching Policy</td>
</tr>
<tr>
<td><strong>[PG_GPO_VERSION]</strong></td>
<td>The version number of the Group Policy Object which contained the matching Policy</td>
</tr>
<tr>
<td><strong>[PG_MESSAGE_NAME]</strong></td>
<td>The name of the Custom Message that was applied</td>
</tr>
<tr>
<td><strong>[PG_MSG_CHALLENGE]</strong></td>
<td>The 8 digit challenge code presented to the user</td>
</tr>
<tr>
<td><strong>[PG_MSG_RESPONSE]</strong></td>
<td>The 8 digit response code entered by the user</td>
</tr>
<tr>
<td><strong>[PG_POLICY_NAME]</strong></td>
<td>The name of the policy</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td><strong>[PG_PROG_CLASSID]</strong></td>
<td>The ClassID of the ActiveX control</td>
</tr>
<tr>
<td><strong>[PG_PROG_CMD_LINE]</strong></td>
<td>The command line of the application being run</td>
</tr>
<tr>
<td><strong>[PG_PROG_DRIVE_TYPE]</strong></td>
<td>The type of drive where application is being executed</td>
</tr>
<tr>
<td><strong>[PG_PROG_FILE_VERSION]</strong></td>
<td>The file version of the application being run</td>
</tr>
<tr>
<td><strong>[PG_PROG_HASH]</strong></td>
<td>The SHA-1 hash of the application being run</td>
</tr>
<tr>
<td><strong>[PG_PROG_NAME]</strong></td>
<td>The Program Name of the application</td>
</tr>
<tr>
<td><strong>[PG_PROG_PARENT_NAME]</strong></td>
<td>The file name of the parent application</td>
</tr>
<tr>
<td><strong>[PG_PROG_PARENT_PID]</strong></td>
<td>The Process Identifier of the parent of the application</td>
</tr>
<tr>
<td><strong>[PG_PROG_PATH]</strong></td>
<td>The full path of the application file</td>
</tr>
<tr>
<td><strong>[PG_PROG_PID]</strong></td>
<td>The Process Identifier of the application</td>
</tr>
<tr>
<td><strong>[PG_PROG_PROD_VERSION]</strong></td>
<td>The Product version of the application being run</td>
</tr>
<tr>
<td><strong>[PG_PROG_PUBLISHER]</strong></td>
<td>The Publisher of the application</td>
</tr>
<tr>
<td><strong>[PG_PROG_TYPE]</strong></td>
<td>The type of application being run</td>
</tr>
<tr>
<td><strong>[PG_PROG_URL]</strong></td>
<td>The URL of the ActiveX control</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>[PG_SANDBOX_NAME]</td>
<td>The name of the sandbox</td>
</tr>
<tr>
<td>[PG_SANDBOX_USER_NAME]</td>
<td>The Username of the sandboxed user account</td>
</tr>
<tr>
<td>[PG_SANDBOX_USER_SID]</td>
<td>The SID of the sandboxed user account</td>
</tr>
<tr>
<td>[PG_SERVICE_ACTION]</td>
<td>The action performed on the matching service</td>
</tr>
<tr>
<td>[PG_SERVICE_DISPLAY_NAME]</td>
<td>The display name of the Windows service</td>
</tr>
<tr>
<td>[PG_SERVICE_NAME]</td>
<td>The name of the Windows service</td>
</tr>
<tr>
<td>[PG_STORE_PACKAGE_NAME]</td>
<td>The package name of the Windows Store App</td>
</tr>
<tr>
<td>[PG_STORE_PUBLISHER]</td>
<td>The package publisher of the Windows Store App</td>
</tr>
<tr>
<td>[PG_STORE_VERSION]</td>
<td>The package version of the Windows Store App</td>
</tr>
<tr>
<td>[PG_TOKEN_NAME]</td>
<td>The name of the built-in Token or Custom Token that was applied</td>
</tr>
<tr>
<td>[PG_URL_ADDRESS]</td>
<td>The full address of the matching URL</td>
</tr>
<tr>
<td>[PG_URL_DEF]</td>
<td>The Definition name of the matching URL</td>
</tr>
<tr>
<td>[PG_URL_GROUP]</td>
<td>The URL Group Name of the matching URL</td>
</tr>
<tr>
<td>[PG_URL_HOST]</td>
<td>The Hostname of the matching URL</td>
</tr>
<tr>
<td>[PG_URL_IE_ZONE]</td>
<td>The Internet Zone of the matching URL</td>
</tr>
<tr>
<td>[PG_URL_PROTOCOL]</td>
<td>The Protocol of the matching URL</td>
</tr>
<tr>
<td>[PG_USER_DISPLAY_NAME]</td>
<td>The display name of the user</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>[PG_USER_DOMAIN]</td>
<td>The name of the domain that the user is a member of</td>
</tr>
<tr>
<td>[PG_USER_NAME]</td>
<td>The account name of the user</td>
</tr>
<tr>
<td>[PG_USER_REASON]</td>
<td>The reason entered by the user</td>
</tr>
<tr>
<td>[PG_USER_SID]</td>
<td>The SID of the user</td>
</tr>
<tr>
<td>[PG_WORKSTYLE_NAME]</td>
<td>The name of the Workstyle</td>
</tr>
</tbody>
</table>
Appendix 9.  Appendix – Windows Privileges

A 9.1.  Standard User Privileges

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SeChangeNotifyPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeIncreaseWorkingSetPrivilege</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>SeShutdownPrivilege</td>
<td>Desktop Only</td>
<td>Desktop Only</td>
</tr>
<tr>
<td>SeTimeZonePrivilege</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>SeUndockPrivilege</td>
<td>Desktop Only</td>
<td>Desktop Only</td>
</tr>
</tbody>
</table>

A 9.2.  Administrator Privileges

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SeBackupPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeCreateGlobalPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeCreatePagefilePrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeCreateSymbolicLinkPrivilege</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SeDebugPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeEnableDelegationPrivilege</td>
<td>Server Only</td>
<td>Server Only</td>
</tr>
<tr>
<td>SeImpersonatePrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Administrator Privileges cont.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SeIncreaseBasePriorityPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeIncreaseQuotaPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeLoadDriverPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeMachineAccountPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeManageVolumePrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeProfileSingleProcessPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeRemoteShutdownPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeRestorePrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeSecurityPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeShutdownPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeSystemEnvironmentPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeSystemProfilePrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeSystemTimePrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeTakeOwnershipPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### System Privileges

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SeAssignPrivilegeTokenPrivilege</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SeAuditPrivilege</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SeCreatePermanentPrivilege</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SeCreateTokenPrivilege</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SeLockMemoryPrivilege</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SeRelabelPrivilege</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td>Server 2008 R2 Only</td>
<td></td>
</tr>
<tr>
<td>SeSyncAgentPrivilege</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SeTcbPrivilege</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SeTrustedCredManAccessPrivilege</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td>Server 2008 R2 Only</td>
<td></td>
</tr>
<tr>
<td>SeUnsolicitedInputPrivilege</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td>Server 2008 R2 Only</td>
<td></td>
</tr>
</tbody>
</table>
Appendix 10. Appendix – Example PowerShell Configurations

A 10.1. Create New Configuration, Save to Local File

```powershell
# Import both Defendpoint cmdlet module
Import-Module 'C:\Program Files\Avecto\Privilege Guard\Client\PowerShell\Avecto.Defendpoint.Cmdlets\Avecto.Defendpoint.Cmdlets.dll'

# Create a new variable containing a new Defendpoint Configuration Object

## Add License ##
# Create a new license object
$PGLicence = New-Object Avecto.Defendpoint.Settings.License
# Define license value
$PGLicence.Code = "5461E0D0-DE30-F282-7D67-A7C6-B011-2200"
# Add the License object to the local PG Config file
$PGConfig.Licenses.Add($PGLicence)

## Add Application Group ##
# Create an Application Group object
# Define the value of the Application Group name
$AppGroup.name = "New App Group"
# Add the Application Group object to the local PG Config file
$PGConfig.ApplicationGroups.Add($AppGroup)

## Add Application ##
# Create an application object
$PGApplication = Get-DefendpointFileInformation -Path C:\windows\system32\calc.exe
# Add the application to the Application group
$PGConfig.ApplicationGroups[0].Applications.AddRange($PGApplication)
```
## Add Message ##

# Create a new message object

```powershell
$PGMessage = New-Object Avecto.Defendpoint.Settings.message $PGConfig
```

# Define the message Name, Description and OK action and the type of message

```powershell
$PGMessage.Name = "Elevation Prompt"
$PGMessage.Description = "An elevation message"
$PGMessage.OKAction = [Avecto.Defendpoint.Settings.Message+ActionType]::Proceed
$PGMessage.Notification = 0
```

# Define whether the message is displayed on a secure desktop

```powershell
$PGMessage.ShowOnIsolatedDesktop = 1
```

# Define How the message contains

```powershell
$PGMessage.HeaderText = [Avecto.Defendpoint.Settings.message+MsgHeaderType]::Default
$PGMessage.HideHeaderMessage = 0
$PGMessage.ShowLineOne = 1
$PGMessage.ShowLineTwo = 1
$PGMessage.ShowLineThree = 1
$PGMessage.ShowReferLink = 0
$PGMessage.ShowCancel = 1
$PGMessage.ShowCRInfoTip = 0
```

# Define whether a reason settings

```powershell
$PGMessage.Reason = [Avecto.Defendpoint.Settings.message+ReasonType]::None
$PGMessage.CacheUserReasons = 0
```

# Define authorisation settings

```powershell
$PGMessage.PasswordCheck = [Avecto.Defendpoint.Settings.message+AuthenticationPolicy]::None
$PGMessage.AuthenticationType = [Avecto.Defendpoint.Settings.message+MsgAuthenticationType]::Any
$PGMessage.RunAsAuthUser = 0
```

# Define Message strings

```powershell
$PGMessage.MessageStrings.Caption = "This is an elevation message"
```
$PGMessage.MessageStrings.Header = "This is an elevation message header"

$PGMessage.MessageStrings.Body = "This is an elevation message body"

$PGMessage.MessageStrings.ReferURL = "http:\\www.bbc.co.uk"

$PGMessage.MessageStrings.ReferText = "This is an elevation message refer"

$PGMessage.MessageStrings.ProgramName = "This is a test Program Name"

$PGMessage.MessageStrings.ProgramPublisher = "This is a test Program Publisher"

$PGMessage.MessageStrings.PublisherUnknown = "This is a test Publisher Unknown"

$PGMessage.MessageStrings.ProgramPath = "This is a test Path"

$PGMessage.MessageStrings.ProgramPublisherNotVerifiedAppend = "This is a test verification failure"

$PGMessage.MessageStrings.RequestReason = "This is a test Request Reason"

$PGMessage.MessageStrings.ReasonError = "This is a test Reason Error"

$PGMessage.MessageStrings.Username = "This is a test Username"

$PGMessage.MessageStrings.Password = "This is a test Password"

$PGMessage.MessageStrings.Domain = "This is a test Domain"

$PGMessage.MessageStrings.InvalidCredentials = "This is a test Invalid Creds"

$PGMessage.MessageStrings.OKButton = "OK"

$PGMessage.MessageStrings.CancelButton = "Cancel"

# Add the PG Message to the PG Configuration

$PGConfig.Messages.Add($PGMessage)

## Add custom Token ##

# Create a new custom Token object

$PGToken = New-Object Avecto.Defendpoint.Settings.Token

# Define the Custom Token settings

$PGToken.Name = "Custom Token 1"

$PGToken.Description = "Custom Token 1"

$PGToken.ClearInheritedPrivileges = 0

$PGToken.SetAdminOwner = 1

$PGToken.EnableAntiTamper = 0
$PGToken.IntegrityLevel = [Avecto.Defendpoint.Settings.Token+IntegrityLevelType]::High

# Add the custom token to the PG Configuration
$PGConfig.Tokens.Add($PGToken)

## Add Policy ##

### Add Policy ###

# Create new policy object

# Define policy details
$PGPolicy.Disabled = 0
$PGPolicy.Name = "Policy 1"
$PGPolicy.Description = "Policy 1"

# Add the policy to the PG Configurations
$PGConfig.Policies.Add($PGPolicy)

### Add Policy Rule ###

# Create a new policy rule

# Define the Application rule settings
$PGPolicyRule.ApplicationGroup = $PGConfig.ApplicationGroups[0]
$PGPolicyRule.BlockExecution = 0
$PGPolicyRule.ShowMessage = 1
$PGPolicyRule.Message = $PGConfig.Messages[0]
$PGPolicyRule.TokenType = [Avecto.Defendpoint.Settings.Assignment+TokenTypeType]::AddAdmin
$PGPolicyRule.ForwardEPO = 0
$PGConfig.Policies[0].ApplicationAssignments.Add($PGPolicyRule)

## Set the Defendpoint configuration to a local file and prompt for user confirmation ##

Set-DefendpointSettings -SettingsObject $PGConfig -Localfile -Confirm
A 10.2. Open Local User Policy, Modify then Save

# Import the Defendpoint cmdlet module

Import-Module 'C:\Program Files\Avecto\Privilege Guard Client\PowerShell\Avecto.Defendpoint.Cmdlets\Avecto.Defendpoint.Cmdlets.dll'

# Get the local file policy Defendpoint Settings

$PGConfig = Get-DefendpointSettings -LocalFile

# Disable a policy

$PGPolicy = $PGConfig.Policies[0]

$PGPolicy.Disabled = 1

$PGConfig.Policies[0] = $PGPolicy

# Remove the PG License

$TargetLicense = $PGConfig.Licenses[0]

$PGConfig.Licenses.Remove($TargetLicense)

# Update an existing application definition to match on Filehash

$UpdateApp = $PGConfig.ApplicationGroups[0].Applications[0]

$UpdateApp.CheckFileHash = 1

$PGConfig.ApplicationGroups[0].Applications[0] = $UpdateApp

# Set the Defendpoint configuration to the local file policy and prompt for user confirmation

Set-DefendpointSettings -SettingsObject $PGConfig -LocalFile -Confirm

A 10.3. Open Local Configuration and Save to Domain GPO

# Import the Defendpoint cmdlet module

Import-Module 'C:\Program Files\Avecto\Privilege Guard Client\PowerShell\Avecto.Defendpoint.Cmdlets\Avecto.Defendpoint.Cmdlets.dll'

# Get the local Defendpoint configuration and set this to the domain computer policy, ensuring the user is prompted to confirm the change

Appendix 11. Manual Deployment of Defendpoint Client

The Defendpoint Client can optionally be deployed manually using any Windows Installer compatible third party deployment system. The Defendpoint Client package is available as both an MSI package and self-installing executable package, from the Avecto product archive.

Pre-requisites

The Defendpoint Client must be installed in ePO Mode, either by selecting the McAfee ePolicy Orchestrator Integration option when installing the Defendpoint Client, or by using a command-line option if installing the client via a deployment system. This will install additional components required to communicate with the McAfee Agent.

To install the client MSI package silently in ePO Mode, use the following command line:

```
MSIEXEC.exe DefendpointClient_x(XX).msi -qn EPOMODE=1
```

(# being 86 or 64 for each system type)

To install the client executable silently in ePO Mode, use the following command line (the double quotes are required):

```
DefendpointClient_x(XX).exe /s /v"/qn EPOMODE=1"
```

Where (XX) represents 86 or 64 in relation to the 32-bit or 64-bit installation respectively.

**Important**: The syntax above must be copied exactly for the install to work as designed, including all spacing.

**Note**: If you are deploying Defendpoint using McAfee ePO, then ePO Mode is automatically enabled.

Disabling ePO Mode

Once installed in ePO Mode, the Defendpoint Client will send events to the McAfee Agent, as well as raising events to the Application Log. If you wish to disable ePO mode at any time, set the following registry key:

```
HKEY_LOCAL_MACHINE\Software\Avecto\Privilege Guard Agent\n
DWORD "EPOMode"=0
```

To re-enable ePO Mode, set the above DWORD value to 1.
Appendix 12. Using Defendpoint Events to Build Queries

Defendpoint collects and stores a broad set of information about every executed application, which is stored in the McAfee ePO Database. This information may then be used in the McAfee ePO Queries & Reports console to create custom dashboard widgets.

Below is a table showing all event properties that are available, and a description of their purpose.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Group</td>
<td>The name of the application group for the matched application definition</td>
</tr>
<tr>
<td>Application Hash</td>
<td>The SHA-1 Hash of the file executed</td>
</tr>
<tr>
<td>Application Type</td>
<td>The type of application:</td>
</tr>
<tr>
<td></td>
<td>APPX</td>
</tr>
<tr>
<td></td>
<td>BAT</td>
</tr>
<tr>
<td></td>
<td>COM</td>
</tr>
<tr>
<td></td>
<td>CPL</td>
</tr>
<tr>
<td></td>
<td>EXE</td>
</tr>
<tr>
<td></td>
<td>MSC</td>
</tr>
<tr>
<td></td>
<td>MSI</td>
</tr>
<tr>
<td></td>
<td>OCX</td>
</tr>
<tr>
<td></td>
<td>PS1</td>
</tr>
<tr>
<td></td>
<td>REG</td>
</tr>
<tr>
<td>Authorization Challenge</td>
<td>If Challenge / Response Authorization is enabled, the Challenge Code presented to the user will be collected. Otherwise this property will remain blank.</td>
</tr>
<tr>
<td>Authorization Response</td>
<td>If Challenge / Response Authorization is enabled, the valid Authorization Code entered user will be collected. Otherwise this property will remain blank.</td>
</tr>
<tr>
<td>Authorizing Domain User</td>
<td>If Run As Other User is enabled, the domain name of the authorizing user will be collected.</td>
</tr>
<tr>
<td>Authorizing User SID</td>
<td>If Run As Other User is enabled, the Secure Identifier (SID) of the authorizing user will be collected.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Client IP Address</td>
<td>If the user was logged on via a remote session to the computer where Defendpoint performed an action, the IPV4 Address of the remote computer will be collected.</td>
</tr>
<tr>
<td>Client Name</td>
<td>If the user was logged on via a remote session to the computer where Defendpoint performed an action, the name of the remote computer will be collected.</td>
</tr>
<tr>
<td>COM Application ID</td>
<td>The AppID of the COM elevated application.</td>
</tr>
<tr>
<td>COM Class ID</td>
<td>The CLSID of the COM elevated application.</td>
</tr>
<tr>
<td>COM Display Name</td>
<td>The common name of the COM elevated application.</td>
</tr>
<tr>
<td>Command Line</td>
<td>The command line of the executed application.</td>
</tr>
<tr>
<td>Computer Name</td>
<td>The name of the computer where Defendpoint performed an action.</td>
</tr>
<tr>
<td>File Name</td>
<td>The full path of the file executed.</td>
</tr>
<tr>
<td>File Owner Domain User</td>
<td>The name of the account which owns the executed application.</td>
</tr>
<tr>
<td>File Owner User SID</td>
<td>The Secure Identifier (SID) of the account which owns the executed application.</td>
</tr>
<tr>
<td>File Version</td>
<td>The file version of the executed application.</td>
</tr>
<tr>
<td>Group Description</td>
<td>The description of the Application Group for the matched application definition.</td>
</tr>
<tr>
<td>Host SID</td>
<td>The Secure Identifier (SID) of the computer where Defendpoint performed an action.</td>
</tr>
<tr>
<td>Is Shell</td>
<td>Determines if the application was launched from an On Demand shell menu option. If blank, then a shell menu was not used.</td>
</tr>
<tr>
<td>Message Description</td>
<td>The description for the End User Message displayed to the user.</td>
</tr>
<tr>
<td>Message Name</td>
<td>The name of the End User Message displayed to the user.</td>
</tr>
<tr>
<td>Parent Process File Name</td>
<td>The full path of the parent process which spawned the audited application.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Parent Process ID</td>
<td>The Process Identifier (PID) of the parent process which spawned the audited application.</td>
</tr>
<tr>
<td>Parent Process Unique ID</td>
<td>A GUID used to uniquely identify a Process relationships.</td>
</tr>
<tr>
<td>PG Event ID</td>
<td>Defendpoint Event Log Event ID. See Process Events.</td>
</tr>
<tr>
<td>Policy Description</td>
<td>The description of the Defendpoint policy that matched the executed application.</td>
</tr>
<tr>
<td>Policy Name</td>
<td>The name of the Defendpoint policy that matched the executed application.</td>
</tr>
<tr>
<td>Process ID</td>
<td>The Process Identifier (PID) of the executed application.</td>
</tr>
<tr>
<td>Product Code</td>
<td>The Product Code for an executed MSI, MSU or MSP package.</td>
</tr>
<tr>
<td>Product Description</td>
<td>A friendly description for the executed application.</td>
</tr>
<tr>
<td>Product Name</td>
<td>The Product Name of the executed application.</td>
</tr>
<tr>
<td>Product Version</td>
<td>The product version of the executed application.</td>
</tr>
<tr>
<td>Reason</td>
<td>If End User reason was enabled for an End User Message, the reason entered by the user will be collected. If blank, then End User Reason was disabled in the message.</td>
</tr>
<tr>
<td>Source URL</td>
<td>If the application was downloaded, then the full URL of where the application was downloaded from will be collected.</td>
</tr>
<tr>
<td>Start Time</td>
<td>The time the process was started.</td>
</tr>
<tr>
<td>Stop Time</td>
<td>This is a deprecated filed and no longer used.</td>
</tr>
<tr>
<td>Token Description</td>
<td>The description of the Access Token applied to the executed application.</td>
</tr>
<tr>
<td>Token Name</td>
<td>The name of the Access Token applied to the executed application.</td>
</tr>
<tr>
<td>UAC Triggered</td>
<td>Determines if the application triggered User Account Control (UAC). If blank, then UAC was not triggered.</td>
</tr>
<tr>
<td>Upgrade Code</td>
<td>The Upgrade Code for an executed MSI, MSU or MSP package.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>User Name</strong></td>
<td>The name of the user who executed an application.</td>
</tr>
<tr>
<td><strong>User SID</strong></td>
<td>The Secure Identifier (SID) of the user who executed an application.</td>
</tr>
<tr>
<td><strong>Vendor</strong></td>
<td>The Display Name of the Publisher Certificate who signed the application.</td>
</tr>
<tr>
<td><strong>Windows Store App Name</strong></td>
<td>The common name of the Windows Store Application.</td>
</tr>
<tr>
<td><strong>Windows Store App Publisher</strong></td>
<td>The Display Name of the Publisher Certificate who signed the Windows Store Application.</td>
</tr>
<tr>
<td><strong>Windows Store App Version</strong></td>
<td>The version number of the Windows Store Application.</td>
</tr>
</tbody>
</table>

In addition to the event properties relating to Defendpoint, there are also a number of Threat Event properties set as part of a Defendpoint event:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action Taken</strong></td>
<td>Friendly name used to identify the type of action performed by Privilege Guard:</td>
</tr>
<tr>
<td></td>
<td>Auto-Elevated</td>
</tr>
<tr>
<td></td>
<td>User-Elevated</td>
</tr>
<tr>
<td></td>
<td>Drop-Admin</td>
</tr>
<tr>
<td></td>
<td>Passive</td>
</tr>
<tr>
<td></td>
<td>Discovery</td>
</tr>
<tr>
<td></td>
<td>Default-Rights</td>
</tr>
<tr>
<td></td>
<td>Admin-Required</td>
</tr>
<tr>
<td></td>
<td>Custom-Token</td>
</tr>
<tr>
<td></td>
<td>Blocked</td>
</tr>
<tr>
<td><strong>Event ID</strong></td>
<td>McAfee ePO standardized Privilege Guard Event ID. See Process Events.</td>
</tr>
<tr>
<td><strong>Threat Name</strong></td>
<td>Internal name used to identify the type of action performed by Privilege Guard:</td>
</tr>
<tr>
<td></td>
<td>ADD_ADMIN</td>
</tr>
<tr>
<td>SHELL_ADD_ADIM</td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td></td>
</tr>
<tr>
<td>DROP_ADMIN</td>
<td></td>
</tr>
<tr>
<td>PASSIVE</td>
<td></td>
</tr>
<tr>
<td>DEFAULT_RIGHTS</td>
<td></td>
</tr>
<tr>
<td>APPLICATION_RIGHTS</td>
<td></td>
</tr>
<tr>
<td>CUSTOM</td>
<td></td>
</tr>
<tr>
<td>PROCESS_BLOCKED</td>
<td></td>
</tr>
</tbody>
</table>
Appendix 13. Rule Precedence

If you add more than one Application Rule, Content Rule or URL Rule to a workstyle then entries that are higher in the list will have a higher precedence. Once a target matches a rule, no further rules or workstyles will be processed for that target. If a target could match more than one workstyle or rule then it is important that you order both your workstyles and rules correctly.

To give a rule a higher precedence within a workstyle:

1. Expand the relevant Workstyle and then select the rule type; Application, On Demand, Content or URL.
2. Check the rule and select Actions > Up (or use the adjacent buttons).
3. Repeat step 2 until you have the Rule positioned correctly.

To give a rule a lower precedence, follow the procedure above, but click Move Down. You may also click Move Top or Move Bottom to move a rule to the top or bottom of the list.
Appendix 14. Autosave Function

A 14.1. Autosave

If a policy has pending edits then these are retained initially in memory and then on session timeout to permanent storage.

This can occur when the session has expired, when you have selected Log Off or the browser has been closed while Avecto policies were being edited.

If the server can determine that the session has ended, e.g. via log out, then the permanent storage autosave is always used.

The in-memory version is only used when the browser has been closed and the session has not yet timed out.

A 14.2. Autosave Recovery

When the policy is edited next you will receive a prompt that there is an existing edit available. You will be given the option to discard or recover the change.

**Note:** The autosave will not be removed until the policy has been saved.

When saved then autosave policy will be automatically removed. This is the case for both recovery and discard. The choice simply affects which data is loaded into the policy.

The autosaved policy has the same name as the current policy but with (autosave) appended to the name. It is possible to duplicate this policy if the user wishes to retain the changes in different policy.

The in-memory storage recovery is covered as part of the locking workflows below.

A 14.3. Policy locking

When a policy is being edited then it is locked to prevent other users making conflicting changes which could override their edits. The policy is locked *after* the summary screen. If another user attempts to edit the same policy they will be shown the name and ID of the user making the edit. They are then presented with three options:

- Break lock and take current changes
- Break lock and use last save
- Open in read only mode

They can also use the standard ePO options of Duplicate/Save/Cancel (lower right).

**Note:** The Save/Cancel options both actually cancel in this case.

The Duplicate option will use the last save.

**Note:** Anyone with write access to the policy can break the lock.
The original user will get a warning that the lock on their policy has been broken. When select **Save** they will be prompted for a new policy name – default of the current name with their username appended. Options for cancel and discard changes will be available.

When the browser is closed during an edit the returning login is treated as a new user. Therefore it is possible to be prompted with an option to break the lock for yourself. As ePO permits multiple logins from the same user this is possible in normal use in addition to the browser close scenario e.g. using two different browsers or via a private browsing window.

A new feature to import directly from another ePO policy has been added. This is to allow recovery and switching of policy contents without having to change the policy assignments.

This is available via **Utilities > Import Defendpoint Policy**.
Appendix 15. Database Sizing and Resource Consumption

A 15.1. Data Retention Considerations

The Audit Event and Microsoft SQL Server Reporting Services databases used to support Avecto Defendpoint Enterprise Reporting may be hosted and scaled independently.

It's important to identify the length of time that Defendpoint audit event data must be retained in the Defendpoint database as it drives resource utilization projections, and initial allocation.

Defendpoint Enterprise Reporting is designed to report on activity in recent time, not as a long term archival data storage solution.

- Avecto provides a database purge utility that may be used to purge data manually, or automatically on a configured period to ensure database growth is capped.

- Unlimited database growth inevitably reduces query execution performance, and increases resource utilization for queries.

Important: Prior to purging large sets of data, please ensure your SQL Transaction logs are able to grow to accommodate. It may be necessary to delete data in stages when setting this up for the first time.

In order to facilitate your decision making regarding retention time in the Defendpoint database, please refer to the following sections in our standard documentation:

- Description of the views of data exposed in Defendpoint Enterprise Reporting - the Reporting Dashboard Guide.

- Description of the events audited by Defendpoint in the Administration Guide: Chapter 27 – Auditing and Reporting – Events.

- Description of the Workstyle parameters. You may consider these as the fields that are collected in the audit events, eventually stored in the Defendpoint Audit Events database. Defendpoint Administration Guide: Workstyle Parameters – Appendix D.

A 15.2. Database Sizing

The Audit Event database has to be sized to accommodate substantial data volume, matching the number of clients generating audit data and the desired retention period.

Database storage requirements may be estimated roughly using the following calculation:

\[
\text{Number of hosts} \times \text{Number of events per host per day} \times 5\text{Kb per event} \times \text{Number of retention days}
\]

For example, an organization of 10,000 hosts, with each host generating an average of 15 events per day, requiring a 30 day retention would require a database capacity of:

\[10,000 \times 15 \times 5 \times 30 = 22,500,000\text{Kb}, \text{ or } 21.5\text{Gb}\]

A typical event volume would be 10-20 events per host per day and varies based on Defendpoint auditing configuration, user job function (role/workstyle) and user activity patterns.
Note: Please refer to the Defendpoint Database sizing calculator to further explore database sizing and growth expectations.

Database resource utilization (CPU, Memory) is highly variable depending on the hardware platform.

Example Use Case Volumes

Based on an organization of 10,000 hosts requiring a 42 day (six weeks) retention.

**Discovery:** Between 40 – 60 events per machine per day

(4.6K per event (based on real world data))

**Average total:** 67.06 GB

**Production:** Between 2 – 10 events per machine per day

(4.6K per event (based on real world data))

**Average total:** 5.66 GB

*Note:* If the number of events ‘per machine per day’ is raised to 15 then the Average total increases to 16.99 GB

Key considerations:

**Volume of inbound audit event records**

As seen above, the number of events per hour may be estimated following simple calculations.

**Queries triggered from MSFT SQL Reporting Services Reports**

As the database grows in size, the resource impact of the reporting platform queries becomes important.

The volume of data maintained in the audit event database will affect the duration and resource cost of these queries.

To maintain good performance, it is recommended that the **ER Purge Utility** is used to limit the timespan of audit event data retained in the database.

Finer-grained audit data management and clean-up is possible using the ER Database Administration Dashboard. The Database Administration Dashboard allows the purging of audits related to specific applications and suppression of incoming audit items related to those applications. For more information please refer to the Database Administration description in the *Reporting Dashboard Guide.*

*Important:* Prior to purging large sets of data, please ensure your SQL Transaction logs are able to grow to accommodate. It may be necessary to delete data in stages when setting this up for the first time.

---

Appendix 16. McAfee ePO / Avecto Database Events
<table>
<thead>
<tr>
<th>Table Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppGroupDescription</td>
<td>Description of the Defendpoint application group that matched the process referenced in the event.</td>
</tr>
<tr>
<td>AppGroupName</td>
<td>Name of the Defendpoint application group that matched the process referenced in the event.</td>
</tr>
<tr>
<td>ApplicationHash</td>
<td>The SHA-1 hash of the process referenced in the event.</td>
</tr>
<tr>
<td>ApplicaitonType</td>
<td>File extension of the process referenced in the event.</td>
</tr>
<tr>
<td>ApplicationPolicyDescription</td>
<td>Description of the Application Rule which matched the process referenced in the event.</td>
</tr>
<tr>
<td>ApplicationPolicyId</td>
<td>Unique identifier of the Application Rule which matched the process referenced in the event.</td>
</tr>
<tr>
<td>AppxName</td>
<td>Name of the Windows Store application referenced in the event.</td>
</tr>
<tr>
<td>AppxPublisher</td>
<td>Digital signature of the Windows Store application referenced in the event.</td>
</tr>
<tr>
<td>AppxVersion</td>
<td>Vendor assigned version number assigned to the Windows Store application referenced in the event.</td>
</tr>
<tr>
<td>AuthorizationChallenge</td>
<td>If available, the 8 digit challenge code presented to the user.</td>
</tr>
<tr>
<td>AuthorizationResponse</td>
<td>Deprecated.</td>
</tr>
<tr>
<td>AuthorizingDomainUser</td>
<td>The name of the user that satisfied the Designated User requirement of the event.</td>
</tr>
<tr>
<td>AuthorizingUserSID</td>
<td>The Security Identifier (SID) of the user that satisfied the Designated User requirement of the event.</td>
</tr>
<tr>
<td>AutoID</td>
<td>Unique reference assigned to the event entry in the table.</td>
</tr>
<tr>
<td>ChallengeResponseStatus</td>
<td>Deprecated.</td>
</tr>
<tr>
<td>ClientName</td>
<td>Name of endpoint which connected using a remote session.</td>
</tr>
<tr>
<td><strong>Column</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ClientPV4</td>
<td>V4 IP address of client who connected using a remote session.</td>
</tr>
<tr>
<td>CommandLine</td>
<td>The command line of the process referenced in the event.</td>
</tr>
<tr>
<td>COMAppID</td>
<td>The unique identifier of the application associated to the COM CLSID.</td>
</tr>
<tr>
<td>COMCLSID</td>
<td>The unique identifier of the COM class object referenced in the event.</td>
</tr>
<tr>
<td>COMDisplayName</td>
<td>The name of the COM class object referenced in the event.</td>
</tr>
<tr>
<td>DomainUser</td>
<td>The username of the user session who started the process.</td>
</tr>
<tr>
<td>DriveType</td>
<td>The type of drive from which the process was being executed.</td>
</tr>
<tr>
<td>EventID</td>
<td>The Defendpoint ID for the event type.</td>
</tr>
<tr>
<td>FileName</td>
<td>The filename of the process referenced in the event.</td>
</tr>
<tr>
<td>FileOwnerDomainUser</td>
<td>The name of the user that is the NTFS owner of the process referenced in the event.</td>
</tr>
<tr>
<td>FileOwnerUserSID</td>
<td>The Security Identifier (SID) of the user that is the NTFS owner of the process referenced in the event.</td>
</tr>
<tr>
<td>FileVersion</td>
<td>File version of the process referenced in the event.</td>
</tr>
<tr>
<td>HostName</td>
<td>The name of the host upon which the process referenced in the event executed.</td>
</tr>
<tr>
<td>HostID</td>
<td>The Security Identifier (SID) of the host upon which the process referenced in the event executed.</td>
</tr>
<tr>
<td>MessageDescription</td>
<td>Description of the Defendpoint message that matched the process referenced in the event.</td>
</tr>
<tr>
<td>MessageName</td>
<td>Name of the Defendpoint message that matched the process referenced in the event.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ParentID</td>
<td>Unique ID assigned by Windows to the parent process of the process referenced in the event.</td>
</tr>
<tr>
<td>ParentProcessFileName</td>
<td>Name of the parent process of the process referenced in the event.</td>
</tr>
<tr>
<td>ParentProcessGUID</td>
<td>Unique reference assigned by Defendpoint to the parent process of the process referenced in the event.</td>
</tr>
<tr>
<td>PID</td>
<td>Unique ID assigned by Windows to the process referenced in the event.</td>
</tr>
<tr>
<td>PolicyDescription</td>
<td>Description of the Defendpoint policy that matched the process referenced in the event.</td>
</tr>
<tr>
<td>PolicyName</td>
<td>Name of the Defendpoint policy that matched the process referenced in the event.</td>
</tr>
<tr>
<td>PowerShellCommand</td>
<td>If available, the PowerShell cmdlet referenced in the event.</td>
</tr>
<tr>
<td>ProcessGUID</td>
<td>Unique reference assigned by Defendpoint to the process referenced in the event.</td>
</tr>
<tr>
<td>ProcessStartTime</td>
<td>Time that the process referenced in the event started.</td>
</tr>
<tr>
<td>ProcessStartTimeMS</td>
<td>Deprecated.</td>
</tr>
<tr>
<td>ProcessStopTime</td>
<td>Deprecated.</td>
</tr>
<tr>
<td>ProcessStopTimeMS</td>
<td>Deprecated.</td>
</tr>
<tr>
<td>ProductCode</td>
<td>Product Code assigned to the process referenced in the event.</td>
</tr>
<tr>
<td>ProductDescription</td>
<td>Product Description assigned by the vendor to the process referenced in the event.</td>
</tr>
<tr>
<td>ProductName</td>
<td>Product Name assigned by the vendor to the process referenced in the event.</td>
</tr>
<tr>
<td>ProductVersion</td>
<td>Product Version assigned by the vendor to the process referenced in the event.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Publisher</td>
<td>Digital signature assigned by the vendor to the process referenced in the event.</td>
</tr>
<tr>
<td>Reason</td>
<td>Details of the reason provided by the user for using the process referenced in the event.</td>
</tr>
<tr>
<td>ServiceDisplayName</td>
<td>The Display name of the Windows service referenced in the event.</td>
</tr>
<tr>
<td>ServiceName</td>
<td>The Service name of the Windows service referenced in the event.</td>
</tr>
<tr>
<td>SourceURL</td>
<td>If available, the URL from which the process referenced in the event was downloaded.</td>
</tr>
<tr>
<td>TokenAssignmentIsShell</td>
<td>Binary flag to indicate if the process was launched using the shell integration feature.</td>
</tr>
<tr>
<td>TokenDescription</td>
<td>Description of the token applied by Defendpoint to the process referenced in the event.</td>
</tr>
<tr>
<td>TokenName</td>
<td>Name of the token applied by Defendpoint to the process referenced in the event.</td>
</tr>
<tr>
<td>UACTriggered</td>
<td>Flag to indicate if the process matched on a UACTriggered rule.</td>
</tr>
<tr>
<td>UpgradeCode</td>
<td>Upgrade Code assigned to process referenced in the event.</td>
</tr>
<tr>
<td>UserSID</td>
<td>The Security Identifier (SID) of the user who started the process.</td>
</tr>
</tbody>
</table>

**Note:** No individual event will return values in all fields, so it is expected behavior to have NULL values in task specific columns.
Avecto + You...

UK
Hobart House
Cheadle Royal Business Park
Cheadle, Cheshire, SK8 3SR
Phone +44 (0)845 519 0114
Fax +44 (0)845 519 0115

Americas
125 Cambridge Park Drive
Suite 301, Cambridge, MA 02140
USA
Phone 978-703-4169
Fax 978 910 0448

Australia
Level 8
390 Collins Street, Melbourne,
Victoria 3000, Australia
Phone +613 8605 4822
Fax +613 8601 1180

avecto.com
info@avecto.com