Defendpoint for Windows Getting Started Guide

Software Version: 5.2.21.0 GA

Document Version: 1.0

Document Date: August 2018

Table of Contents

Chapter 1 - Introduction

Defendpoint combines privilege management and application control technology in a single lightweight agent. This scalable solution allows global organizations to eliminate admin rights across the entire business – across Windows and Mac desktops and even in the data center.

Actionable intelligence is provided by Enterprise Reporting, an insights solution with endpoint analysis, dashboards and trend data for auditing and compliance.

This guide talks about the aims of an evaluation and the options available to you. It also takes you through setting up your environment using the Avecto Virtual Lab (AVL) and the high level Policy Editor features on the interface. The final part of the guide takes you through setting up the QuickStart policy, which is built into Defendpoint, and our recommendations about using it as a starting point for your Defendpoint configuration.

Chapter 2 - Aims of an Evaluation

Before you embark on any testing whether it be a short evaluation or a full Proof of Concept (PoC), it is important to understand what success looks like for your organization. The aim of this technical evaluation is to allow your organization to take a look at the technology to ensure that it meets your requirements.

Following this initial evaluation we recommend that you engage directly with an Avecto Account Manager or Channel Partner (if used) to fully scope out next steps in your Avecto Journey. This is detailed further in **What's Next?** detailed on page 21.

2.1 - What do you want to achieve?

Typically, in order to help you identify your initial requirements for the evaluation, you will need to engage the different business units and capture their requirements. We have included a sample set of questions below which can be used as a starting point.

- What applications require admin rights to run within your department?
- What percentage of your users have admin rights?
- Do you have users that need to install printers?
- Do you have users that need to install ActiveX Controls?
- Do you have users that need to run built-in Windows features or functions that require the user to be a local administrator?
- Do you have a list of applications that you want to prohibit from running?
- Do you want to allow your users to install software?
- Do you want to create an approved list of applications that users can run?
- Do you have a list of trusted URLs?

During the evaluation, you should work through a series of use-cases that highlight how to secure your endpoints whilst providing users with the flexibility they need to do their job. This will provide an overview of Defendpoint, illustrating its features that couple security with the right balance of user freedoms.

2.2 - How does it work?

This innovative solution allows organizations to balance security and usability, ensuring user experience is never compromised. Defendpoint combines privilege management and application control technology in a single lightweight agent. This scalable solution allows global organizations to eliminate admin rights across the entire business – across Windows and Mac desktops and even in the data center.

With privileges assigned to applications, not users, Defendpoint allows you to successfully remove admin rights and protect the operating system. Individuals can still access the applications and tasks they need to perform their job role, so they can be productive without security compromise. Least privilege mitigates the risk of privilege escalation and removes the potential for rootkit infections, protecting the integrity of the OS.

Defendpoint allows you to take a more pragmatic approach to whitelisting, so that users retain the flexibility they need to be productive. Simple yet highly effective rules make it possible to maintain application control across even the largest enterprises without relying on signatures or hashes. A trust-based model working seamlessly with privilege management stops malware payloads from running or gaining a foothold on the endpoint.

Chapter 3 - Evaluation Options

This Defendpoint evaluation can be completed by using the following methods:

- The Avecto Virtual Lab (AVL) environment – test lab provided by Avecto.
- A full Defendpoint installation – test lab provided by client.

3.1 - Avecto Virtual Lab

All of these Virtual Machines are connected and configured, providing a secure, isolated test environment that can be tailored to suit your requirements. You'll be provided with a URL link, password and license key from Avecto. Connect to the AVL using the URL link and password provided and then follow the steps in **Introduction to the Avecto Virtual Lab (AVL)** detailed on page 7. You can then start configuring Defendpoint and discover how to achieve a Defense in Depth strategy.

3.2 - Defendpoint Installation in your Environment

The installation of Defendpoint for evaluation purposes can be performed on a single machine with both an administrator and a standard user account. Once Defendpoint is installed you can begin to use the QuickStart Policy.

Fore more information on installing Defendpoint see the Defendpoint Administration Guide.

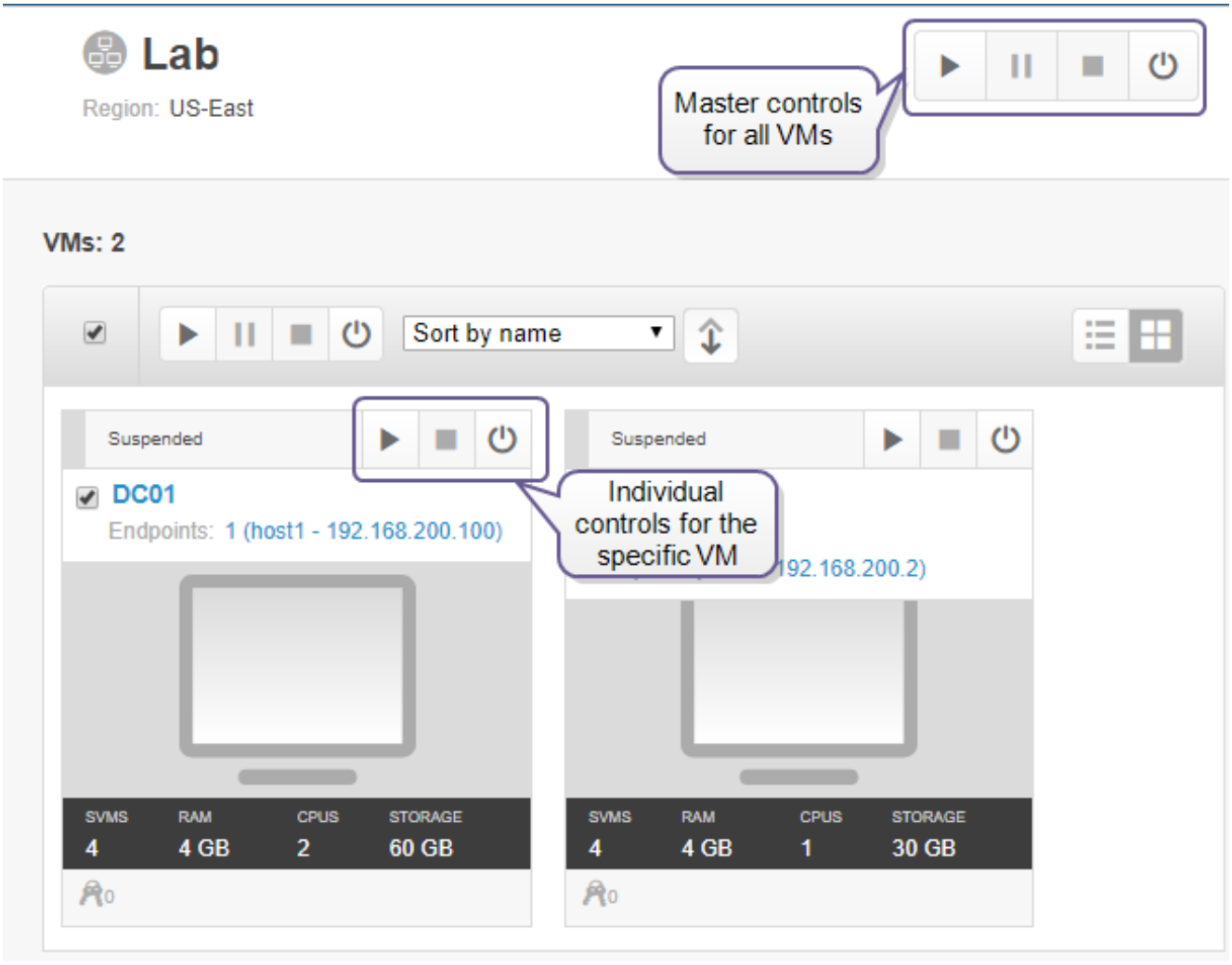
Chapter 4 - Introduction to the Avecto Virtual Lab (AVL)

The Avecto Virtual Lab (AVL) is a complete, working environment providing access to every aspect of Defendpoint Group Policy and ePO Edition. The AVL includes a Domain Controller and a Windows 10 endpoint client preloaded with all Avecto's latest releases ready for testing. Additional clients can be added upon request.

These virtual machines are connected and configured, providing a secure, isolated test environment that can be tailored to suit your requirements.

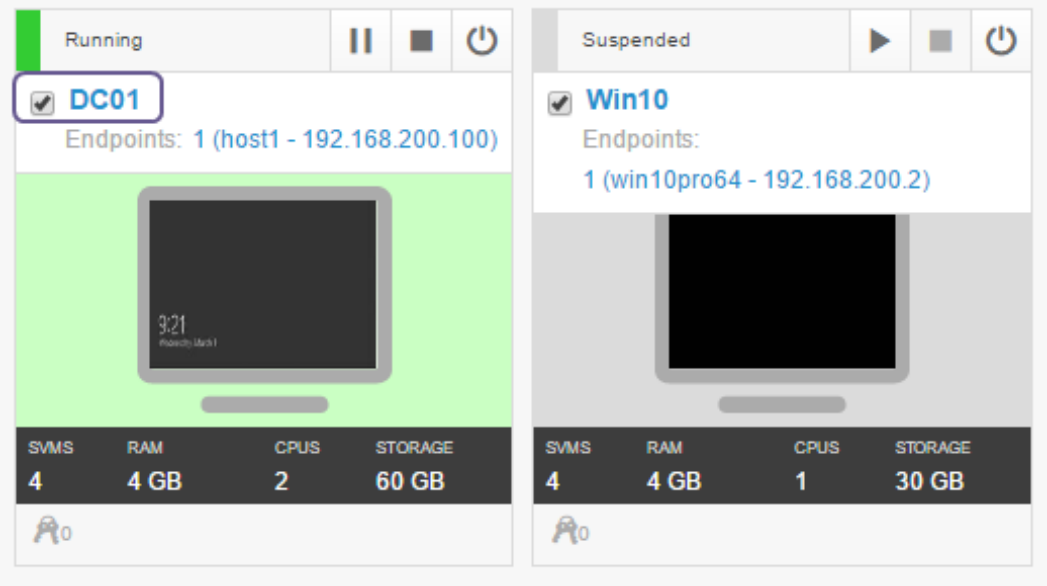
To log in and configure the AVL:

1. Connect to the AVL using the URL link and password provided .
2. All virtual machines are suspended to start with. You can either switch all machines on at once, using the master transport controls in the top right-hand corner of the screen, or individually using the control for each specific machine:



The AVL is pre-configured with the latest Defendpoint version including the Enterprise Reporting Pack, McAfee ePO and Activity Viewer tools.

1. Turn the VM DC01 on.
2. Click the machine name to connect to it:



There are two domain user accounts in the AVL:

- AVECTOLAB\Administrator
- AVECTOLAB\StandardUser

The password for both accounts is '1234' (without quotes).

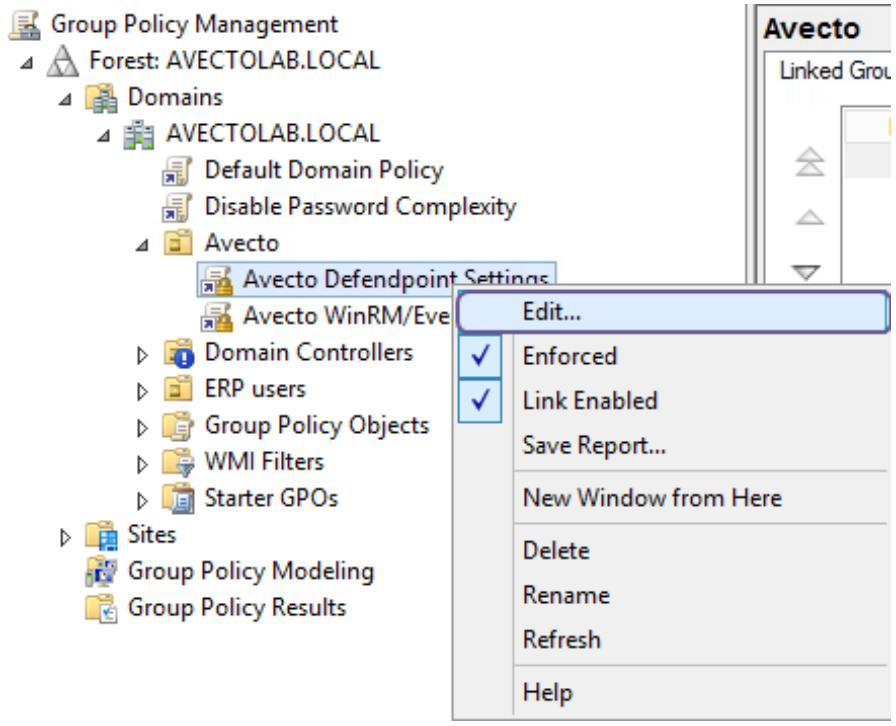
3. Log in using the Administrator account.
   - Username: AVECTOLAB\Administrator
   - Password: 1234
4. Click on the image of the desktop and an HTML5 or Java session will open in a new window or tab on your browser.

From applet at the top of each VM, it is possible to suspend, shutdown or power off the VM. Send control, alt and delete, copy and paste and resize the window.

4.1 - Setting up Defendpoint Configuration in the AVL

For this example, we are going to use Active Directory Group Policy to deliver the workstyle to our target endpoint (s) although Defendpoint workstyles can be deployed in a variety of ways including McAfee ePolicy Orchestrator. For more information on administering Defendpoint with McAfee ePolicy Orchestrator, see the ePO Getting Started Guide.

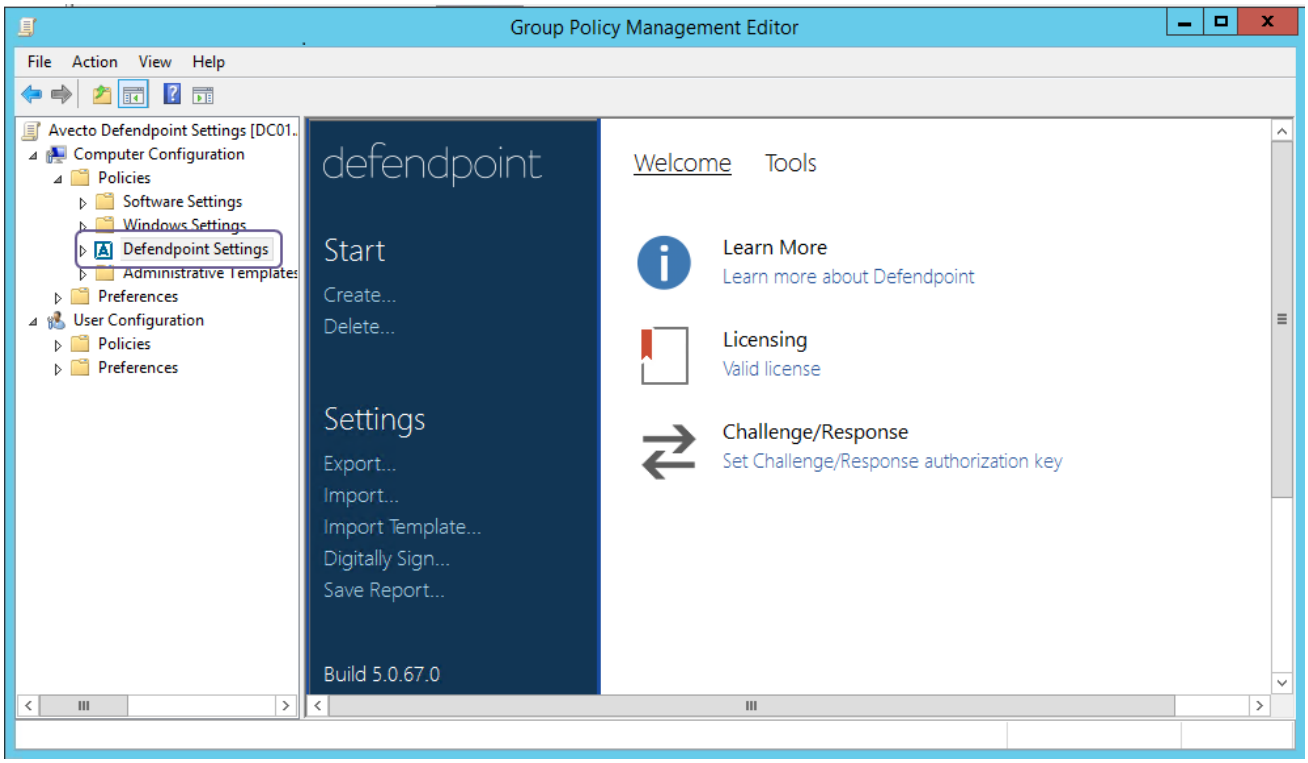
1. On the Domain Controller (DC01), click the **Start** menu and type in 'gpmc.msc' (without quotes). Click **Enter**. This opens the Active Directory Group Policy.
2. Navigate to the Avecto OU (organizational unit). Right-click on 'Avecto Defendpoint Settings' and click **Edit** . Alternatively, there is a shortcut on the desktop.



Defendpoint supports policy deployment using **Computer Configuration** and **User Configuration**. Om this guide, we will be using computer-based policies.

Computer configurations in Group Policy are applied to computers, regardless of who logs on to the computers. User configurations in Group Policy are applied to users, regardless of which computer they log on to. Defendpoint compliments this further with a powerful filtering engine allowing for detailed, granular control and deployment of workstyles.

3. Navigate to Computer Configuration > **Policies** > **Defendpoint Settings** to start the workstyle configuration.



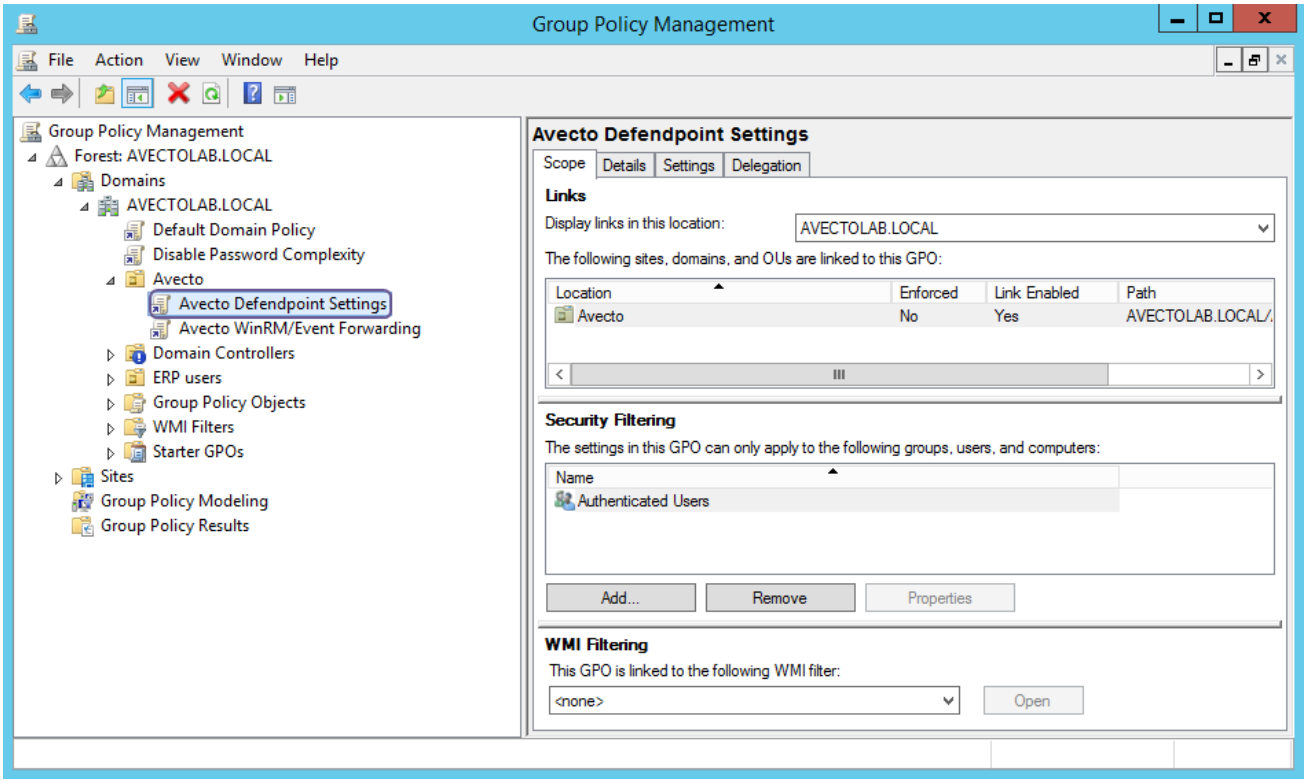
3. You are now prompted to enter a valid license key. Enter the license key provided by Avecto and click **Add**. See the next section **Insert License** detailed below for more information.

4.1.1 - Insert License

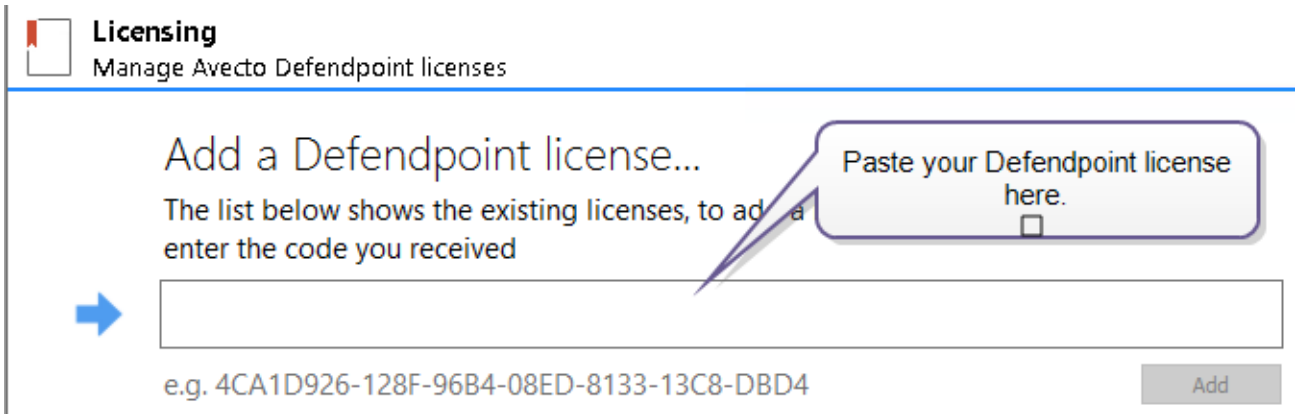
Before you can build any functionality, you need to provide a valid license. This will have been provided by your Avecto Consultant.

To insert a license into Microsoft ePO:

1. Double-click the Group Policy shortcut on the desktop.
2. Navigate to the **Avecto Defendpoint Settings** node.



3. Right click on Avecto Defendpoint Settings and select **Edit**.
4. In the left-hand pane navigate to **Computer Configuration** > **Policies** > **Defendpoint Settings** > **Licensing**.



3. Paste the license in the box and click **Add**.

You are now ready to begin working with Defendpoint.

Chapter 5 - The Policy Editor

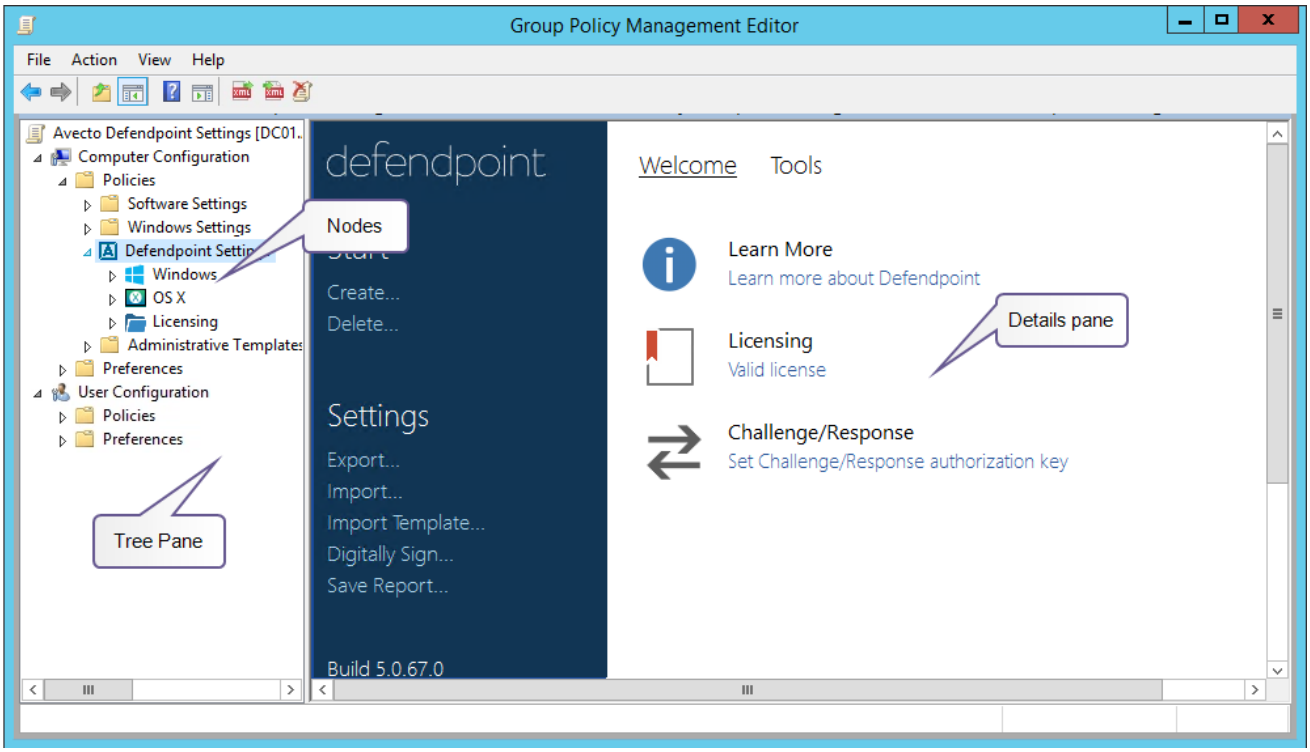
The Policy Editor is used to develop your Defendpoint security policies so that they can be distributed to users in your organization.

5.1 - Defendpoint Naming Conventions

The left-hand pane containing the Defendpoint Settings is the **Tree pane**.

The folders beneath Defendpoint Settings in the tree pane are the **Nodes**.

The middle pane, which displays content relevant to the selected node, is the **Details pane**.

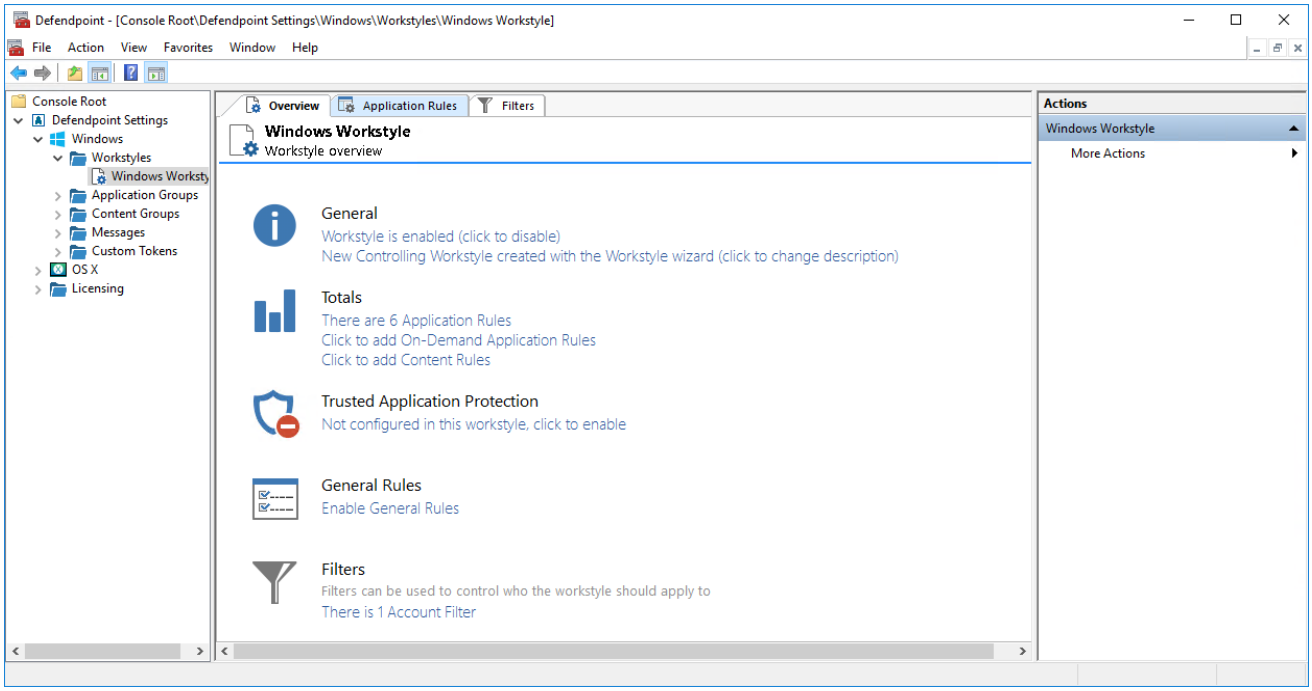


5.2 - Defendpoint Settings

If you expand the **Windows** node you will see five nodes:

- **Workstyles** – Contains rules that assign privileges to applications. By adding more workstyles to your configuration, you can apply different rules to different users and groups of users.
  Workstyles are applied in precedence order, meaning that when a user runs an application or task, it is the workstyle at the top of the list that gets evaluated first. If the filters don't match the user, then the next workstyle is evaluated, and so on. If no workstyle matches the user or action, then Defendpoint will not apply any rules to the user.
- **Application Groups** – Define logical groupings of applications so that you can apply a common action to them in a workstyle. Each application group can contain one or more application definitions, that determine which properties of an application should be used when matching rules.
- **Content Groups** – Define groups of specific file types and file content. These can then be used in content rules within your workstyles to define how Defendpoint will handle files when opened by the user.
- **Messages** – Define end user messages. Messages can be set on rules within your workstyle and will be presented to users when they try to run an application or task that matches a rule. They can be presented before something is allowed to run, when something has been blocked, or as a replacement for authorization requests.
- **Custom Tokens** – Define custom access tokens. For more advanced configurations, Custom Tokens can be created where group memberships, privileges and permissions can be manually specified. These can then be applied to your rules in the same way as the built-in Defendpoint access tokens.

Once a workstyle has been created and selected in the tree pane, the workstyle tabs is displayed in the details pane:



There are six tabs but each workstyle is unlikely to use all of them. You can toggle individual tab displays on and off from the tab drop-down menu at the top right of the details pane.

- **Overview** – Provides a general overview of the workstyle contents.
- **Application Rules** – Allows you to insert, edit or remove application rules.
- **Filters** – Allows you to add or delete filters.

Tabs that contain active settings cannot be toggled off.

5.3 - Automatic Saving

By default the Defendpoint Settings editor will automatically save any changes back to the appropriate GPO (or local XML file if you are using the standalone console).

Automatic saving can be disabled, by clearing the **Auto Commit Settings** option on right-click context menu of the **Defendpoint Settings** node, but this is not recommended unless you are having performance issues. If you clear the **Auto Commit Settings** option then you must select the **Commit Settings** menu option to manually save any changes back to the GPO. The **Auto Commit Settings** option is linked to your user profile, so it will be set for all future editing of Defendpoint Settings.

Chapter 6 - QuickStart Policy

You need to have completed the steps to install your Defendpoint license before you proceed.

The QuickStart policy has been designed from Avecto's experiences of implementing the Defendpoint solution across thousands of customers and millions of endpoints, and is intended to balance security with user freedom.

Starting with the QuickStart policy allows you to transition users to the standard user rights immediately, rather than waiting until the end of your implementation project. This allows you to quickly improve your organization's security by benefiting from operating with standard user rights, whilst allowing users to self-authorize or request authorization for exceptions.

Users will be asked for varying levels of justification or authorization based on the flexibility group you assign to them. Unknown or untrusted applications can be blocked or the user can be prompted to gain authorization first.

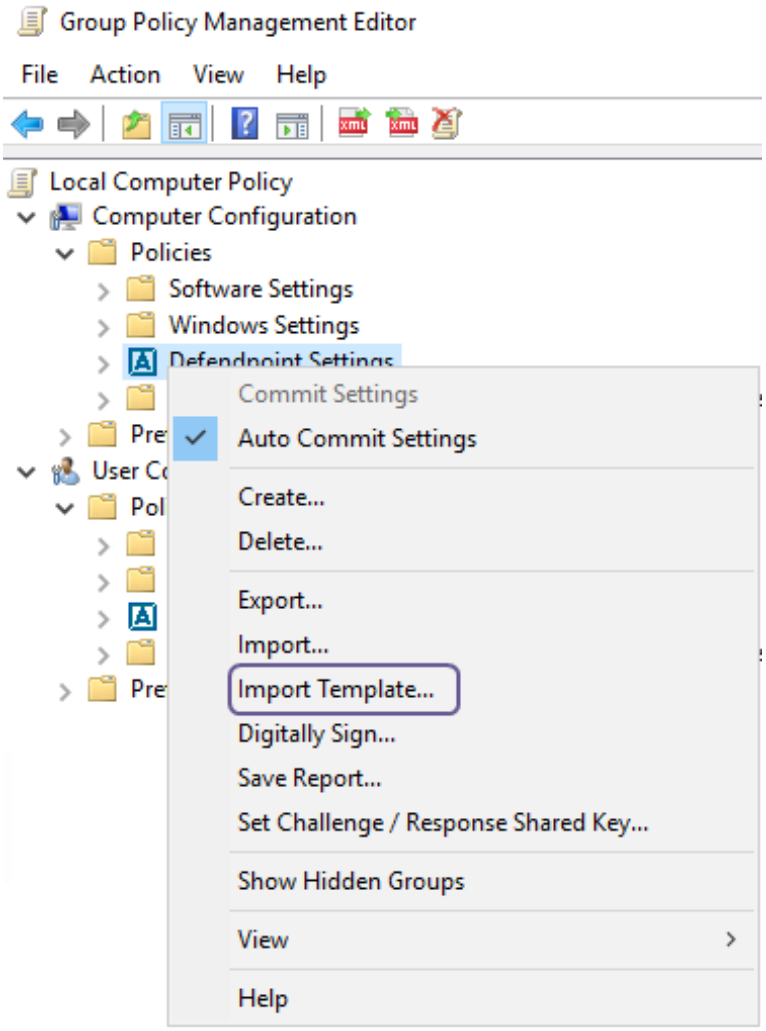
After deploying the policy, you can monitor the events that have been generated to identify applications and processes that are being used and see if any need to be specifically defined in your policy for blocking or elevation.

The QuickStart policy is built into Defendpoint and can be created from the **Welcome** page, which is displayed when you click on the **Defendpoint Settings** node.

6.1 - Importing the QuickStart Policy

To import the QuickStart policy:

1. Right-click on the **Defendpoint Settings** node and click **Import Template**.



2. The **Import Advanced Template** dialog box appears. The default option is QuickStart.
3. Click **Create**. You can choose to either merge this policy with your existing configuration or replace it.

6.2 - QuickStart Policy Settings

The QuickStart Policy Settings contains pre-configured workstyles, applications groups, messages and a custom token that provide a basis for your Defendpoint configuration.

6.2.1 - Workstyles

The QuickStart policy contains four workstyles that should be used together to manage all users in your organization.

General Rules

This workstyle contains a set of default rules that apply to all standard users regardless of what level of flexibility they need.

The General Rules workstyle contains rules to:

- Block any applications that are in the **Block – Blacklisted Apps** group
- Allow Avecto Support tools.
- Allow standard Windows functions, business applications, and applications installed through trusted deployment tools to run with admin rights
- Allow approved standard user applications to run passively

High Flexibility

This workstyle is designed for users that require a lot of flexibility such as developers.

The High Flexibility workstyle contains rules to:

- Allow known white-listed business applications and operating system functions to run
- Allow users to run signed applications with admin rights
- Allow users to run unknown applications with admin rights once they have confirmed that the application should be elevated
- Allow applications that are in the **Add Admin – High Flexibility** group to run with admin rights
- Allow unknown business application and operating system functions to run on-demand

Medium Flexibility

This workstyle is designed for users that require some flexibility such as sales engineers.

The Medium Flexibility workstyle contains rules to:

- Allow known white-listed business applications and operating system functions to run
- Allow users to run signed applications with admin rights once they have confirmed that the application should be elevated
- Prompt users to provide a reason before they can run unknown applications with admin rights
- Allow applications that are in the **Add Admin – Medium Flexibility** group to run with admin rights
- Allow unknown business application and operating system functions to run on-demand
- Restricted OS functions that require admin rights are prevented and require support interaction

Low Flexibility

This workstyle is designed for users that don't require much flexibility such as helpdesk operators. The **Low Flexibility** workstyle contains rules to:

- Prompt users to contact support if a trusted or untrusted application requests admin rights
- Prompt users to contact support if an unknown application tries to run
- Allow known approved business applications and operating system functions to run

6.2.2 - Application Groups

The application groups that are prefixed with "(Default)" or "(Recommended)" are hidden by default and do not need to be altered.

Add Admin – General (Business Apps) – Contains applications that are approved for elevation for all users, regardless of their flexibility level.

Add Admin – General (Windows Functions) – Contains operating system functions that are approved for elevation for all users.

Add Admin – High Flexibility – Contains the applications that require admin rights that should only be provided to the high flexibility users.

Add Admin – Medium Flexibility – Contains the applications that require admin rights that should only be provided to the medium flexibility users.

Allow – Approved Standard User Apps – Contains applications that are approved for all users.

Block – Blacklisted Apps – This group contains applications that are blocked for all users.

(Default) Any Application – Contains all application types and is used as a catch-all for unknown applications.

(Default) Any Trusted UAC Prompt – Contains signed (trusted ownership) application types that request admin rights.

(Default) Any UAC Prompt – This group contains applications types that request admin rights.

(Default) Avecto Tools – This group is used to provide access to an Avecto executable that collects Defendpoint troubleshooting information.

(Default) Controlled OS Functions – Contains operating system applications and consoles that are used for system administration.

(Default) Software Deployment Tool Installs – Contains applications that can be installed by deployment tools such as SCCM (System Center Configuration Manager).

(Default) Whitelisted Functions & Apps – Contains trusted applications, tasks and scripts that should execute as a standard user.

(Recommended) Restricted Functions - This group contains OS applications and consoles that are used for system administration and trigger UAC when they are executed.

(Recommended) Restricted Functions (On Demand) - This group contains OS applications and consoles that are used for system administration.

6.2.3 - Messages

The following messages are created as part of the QuickStart policy and are used by some of the application rules:

Allow Message (Authentication) – Asks the user to provide a reason and enter their password before the application runs with admin rights.

Allow Message (Select Reason) – Asks the user to select a reason from a drop-down menu before the application runs with admin rights.

Allow Message (Support Desk) – Presents the user with a challenge code and asks them to obtain authorization from the support desk. Support can either provide a response code or a designated, authorized user can enter their login details to approve the request.

Allow Message (Yes / No) – Asks the user to confirm that they want to proceed to run an application with admin rights.

Block Message – Warns the user that an application has been blocked.

Block Notification – Notifies the user that an application has been blocked and submitted for analysis.

Notification (Trusted) – Notifies the user that an application has been trusted.

6.2.4 - Custom Token

A custom token is created as part of the QuickStart policy. The custom token is called **Avecto Support Token** and is only used to ensure that an authorized user can gain access to Defendpoint troubleshooting information.

We do not recommend using the **Avecto Support Token** for any other application rules in your workstyles.

6.3 - Customizing the QuickStart Policy

Before deploying the QuickStart policy to your users, you need to make some company-specific customizations to the standard template.

As a minimum you need to:

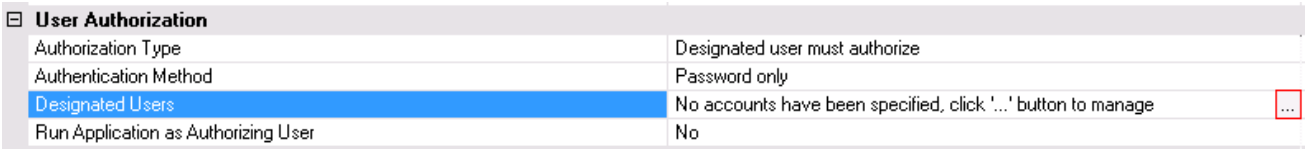
- Configure the users or groups that can authorize requests that trigger messages.
- Assign users and groups to the high, medium and low flexibility workstyles.
- Populate the 'Block Blacklist Apps' application group with any applications that you want to block for all users.

6.3.1 - Configure the Support Message

Instead of having to generate a response code when a user is presented with a challenge code, there is also an option for an authorized user to enter their credentials to approve the request. To enable this functionality you must first designate the users that are able to approve the requests that generate the support message.

To configure the support message:

1. Expand the **Messages** node and select **Allow Message (Support Desk)**.
2. On the **Message Design** tab, select the **Designated Users** option and click **Browse** from the right-hand side of the row. The **Manage users** dialog box appears.



3. Click **Add**. The **Select Users or Groups** dialog box appears.
4. Enter the relevant group or user accounts and click **Check Names** to validate the names or alternatively click **Advanced** to browse for groups and users. Click **OK**.
5. Click **OK** on the **Manage users** dialog box.

6.3.2 - Apply User Filters to Workstyles

To assign relevant users to the High workstyle:

1. Expand the **Workstyles** node and select the **High Flexibility** workstyle.
2. In the details pane, click the **Filters** tab.
3. Click **Add an Account Filter**.
4. Click **Add a new account**. The **Select Users or Groups** dialog box appears.
5. Enter the relevant group or user accounts that should have the high flexibility workstyle applied to them and click **Check Names** to validate the names. Alternatively, click **Advanced** to browse for groups and users. Click **OK**.

Repeat this process for the Medium flexibility workstyles, assigning the relevant users to each one. The Low flexibility workstyle should remain as the default (not administrators).

6.3.3 - Add Applications to the Blacklist

In your organization, there may be applications or processes that you want to block all users from running. To do this you need to add the application to the **Block – Blacklisted Apps** application group.

To add applications or processes to the blacklist:

1. Expand the **Application Groups** node and click **Block – Blacklisted Apps**.
2. Right-click in the **Details** pane and select the type of application that you want to block from the **Insert Application** sub-menu.
3. Using the wizard, enter a description and application definition for the application that you want to block. See the Defendpoint for Windows Administration Guide for more information on the different application types.

6.4 - QuickStart Policy Summary

By using and building on the QuickStart policy, you can quickly improve your organization's security without having to monitor and analyze your users' behavior first and then design and create your Defendpoint configuration.

After the QuickStart policy has been deployed to groups within your organization, you can start to gather information on your users' behavior. This will provide you with a better understanding of the applications being used within your organization, and whether they require admin rights, need to be blocked, or need authorizing for specific users.

This data can then be used to further refine the QuickStart policy to provide more a tailored Defendpoint solution for your organization.

Chapter 7 - What's Next?

Once you are satisfied with your testing and evaluation of Defendpoint, it's time to discuss the next steps on your Avecto journey. Avecto offer a wide range of consultancy packages which can be tailored to suit your organization, making sure that you get the best of the technology and achieve your objectives.

For example, Avecto offers advice and workshops which are aimed at establishing your objectives, requirements, acceptance criteria (use cases), thus assessing the impact on your business. The workshops will provide an insight into the scope of any subsequent consultancy effort, for both Proof of Concepts (PoCs) and production deployment.

In addition, Avecto and its partner offer a number of consultancy packages including Health Checks, Discovery Audits, and Defendpoint training courses.

Whichever option you choose, Avecto and its partners do not just sell software, we focus on project success and have an established and well respected implementation methodology. For contact information refer to the Contact page on our website.