Avecto

Defendpoint for Mac Getting Started Guide

Software Version: 4.5.1.0 GA

Document Version: 1.0

Document Date: 30 May 2017

Avecto

Table of Contents

Chapter 1 - Introduction

Defendpoint is the revolutionary endpoint security software that unites IT and end users. With traditional security solutions such as antivirus only effective half of the time, Defendpoint puts you a step ahead. By combining Privilege Management and Application Control, Defendpoint protects your business from advanced targeted attacks.

With Defendpoint for Mac, users are able to run admin tasks and privileged applications without the need for an admin account. You regain control of apps with pragmatic whitelisting, ensuring that only known good applications are able to run, while users have the freedom and flexibility to perform everyday tasks.

1.1 - Features

Achieve least privilege on Mac

There are many functions that require an admin account to run. While most Mac users typically use an admin account to gain the flexibility they need, this represents a large security risk in the enterprise.

Defendpoint for Mac allows users to log on with standard user accounts without compromising productivity or performance, by allowing the execution of approved tasks, applications and installations as required, according to the rules of your policy.

Empower users and gain control

Allow and block the use and installation of specific applications, binaries, packages and bundles. By taking a simple and pragmatic approach to whitelisting, you can gain greater control of applications in use across the business. This immediately improves security by preventing untrusted applications from executing.

Unlock privileged activity

Even privileged applications and tasks that usually require admin rights are able to run under a standard user account. With Defendpoint for Mac, you can unlock approved system preferences such as date and time, printers, network settings and power management without needing admin credentials.

Take a pragmatic approach with broad rules

Broad catch-all rules provide a solid foundation, with exception handling options to handle unknown activity. Define the application and set its identification options such as filename, hash, publisher or URI. Then assign the application to the users who require enhanced rights and set up any additional options such as end user messaging and auditing.

Achieve compliance

You will have the knowledge to discover, monitor and manage user activity from the entire enterprise, drawing upon actionable intelligence to make informed decisions. Graphical dashboards with real-time data will provide a broad range of reports to aid troubleshooting and provide the information you need to proactively manage your policy on an ongoing basis.

Apply corporate branding

You can add your own branding to messages and prompts, with reusable messaging templates that make it easy to improve the end user experience. You have control over text configuration.

Customizable messaging

Working seamlessly with OS X and macOS, Defendpoint for Mac can suppress standard, restrictive messages and allows you to create your own customized authorization prompts to handle exceptions and enable users to request access. Set up access request reasons, challenge/response codes or password protection to add additional security layers, or simply improve prompts to reduce helpdesk enquiries.

Simple, familiar policy design

Firewall-style rules based on application groups make set up and management simple. Using the same Defendpoint interface and client as for Windows, you can create flexible 'Workstyles' based on the requirements of individuals and groups of users.

1.2 - Supported platforms

- OS X 10.10 Yosemite
- OS X 10.11 El Capitan
- macOS 10.12 Sierra

Ensure all operating system updates are applied.

Chapter 2 - Before you start

Before beginning the Defendpoint for Mac evaluation you will need the following:

- A Windows computer or virtual machine, with a local admin account
- A Mac computer or virtual machine, with a local admin account for installation and configuration, and a local standard (non-admin) account for testing.

If you are testing Defendpoint for Mac without using iC3, then you should have a method of copying a configuration XML file from the Windows computer to the Mac. This can be done either by network share, local shared folder or external USB device.

Avecto recommends that this evaluation be carried out on virtual machines. It should not be carried out on production machines.

2.1 - Installation packages

Defendpoint for Mac consists of two installers, downloadable from Avecto Connect:

- A Mac package installer, which will install the Defendpoint Client software
  `DefendpointMacClient.pkg`
- A Windows executable installer, which will install the Defendpoint Management Console
  `DefendpointManagementConsoleMac_x86.exe`
  `DefendpointManagementConsoleMac_x64.exe`

2.2 - Licensing

A Defendpoint for Mac software license has been provided by your Avecto Account Manager.

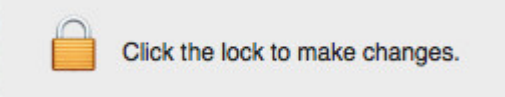
Chapter 3 - Standard user experience without Defendpoint

Before installing Defendpoint, we are going to explore the experience that a standard user would expect to encounter. By performing five common actions, we can illustrate the restrictions and risks a standard user is exposed to. Later in this guide once Defendpoint has been installed and configured, you'll perform the same actions to illustrate how Defendpoint helps to empower standard users with increased productivity, as well as securing the endpoint.

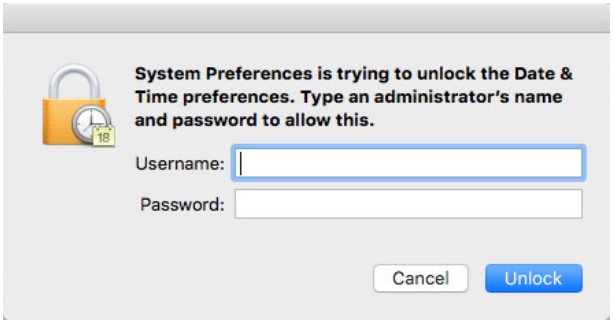
If you are already familiar with the limitations of a standard user on a Mac, you can skip this section.

3.1 - Using administrative preference panes

Preference panes allow the user to set preferences for specific applications or the system. Many of these are 'padlocked' as shown below.



1. As a standard user open the **Date & Time** preference pane.
2. Click the padlock to unlock the preference pane. You will be presented with an Apple authorization dialog as displayed below. A standard user cannot authorize this dialog, and so cannot alter the **Date & Time** settings.



Standard users cannot unlock preference panes that have a padlock without knowledge of an admin's password. Later in the evaluation we will demonstrate how any padlocked preference panes that are considered necessary for the standard user to access can be made available using Defendpoint whilst preventing the user from unlocking any other preference panes.

3.2 - Installing software packages

Packages are used to install applications or files and execute scripts. To do this test, you will need to copy a package (.pkg) to the standard user's desktop.

1. As a standard user run the package installer by double clicking it.
2. Progress through the installation dialog until you reach the **Install** button. Note that when **Install** is clicked, the user is presented with an authorization dialog, which they cannot authorize.

Standard users cannot install packages. Using Defendpoint, standard users can be empowered to install packages without requiring an administrator account. This can eliminate unnecessary support calls and IT intervention. However, packages that have not been authorized can be intercepted, and controls can be applied that allow IT teams to dictate which packages can or cannot be installed by a standard user.

3.3 - Running application bundles from untrusted locations

Application bundles are the most common type of application on Macs. The majority of pre-installed applications, as well as apps installed from the Apple App Store, are application bundles. Application bundles can also be downloaded from any internet site, and run from any location on the system. Because of this, application bundles that are potentially malicious can easily be introduced by standard users, and represent a significant risk to the business.

To do this test, you will need to copy an application bundle (.app) to the standard users desktop.

1. As a standard user download and run an application bundle.
2. Even though the application has not been installed to the trusted /Applications folder, you can see that the application still runs.

Standard users can download and run application bundles without requiring an admin account. Using Defendpoint, untrusted application bundles can automatically be blocked from running.

3.4 - Using application bundles installed with OS X and macOS

Many of the built-in tools and applications that make up OS X and macOS are also application bundles. Some may require an administrator account to run, and others (which you may not want users accessing) do not.

1. As a standard user, try running the application *iTunes*. This may not be an application you would want users to access, as it can be configured to synchronize documents (including documents and IP that may be business sensitive) to iCloud.
2. Standard users are able to run built-in applications such as iCloud, and can also install applications from the Apple Store, and these applications may not be desirable in a well-managed environment.
3. As a standard user, try running the application *Keychain*. This application will run successfully as a standard user, but there are features such as the System Keychain that are padlocked. Try unlocking the padlock, and you will receive an authorization message which you cannot authorize.

3.5 - Running binaries using the command line

Binaries are typically executed from the Terminal command line application. Many binary commands can be executed by standard users, without requiring an admin account or root. As an IT admin, you may want to restrict the use of, or even block access to certain binaries that are executed by your users.

One example is the '`curl`' binary, which allows users to transfer data from or to a server. It is commonly used to download from a website without using a web browser.

1. As a standard user, open the Terminal and type:
   `curl` <the server/website and file name of the file you want to download> `-o ~/Desktop/`<filename>

   For example, if you wanted to download the *Defendpoint for Mac* PDF from the Avecto website and call it *downloaded.pdf* you would type:
   ```
   curl https://avectoweb.blob.core.windows.net/cms/1465/datasheet-defendpoint-for-mac.pdf -o ~/Desktop/downloaded.pdf
   ```

2. Press **Enter**. The '`curl`' command will be executed. As a standard user you have accessed the Terminal and downloaded the file to the desktop.

Using Defendpoint, you can apply Application Control rules to binaries so that only authorized users are able to use certain whitelisted commands.

3.6 - Running sudo commands using the command line

Sudo allows authorized standard users to run commands as the root user or another user. To determine whether a user is authorized to run a particular command, sudo uses the sudo configuration (sudoers) file.

1. As a standard user, open the Terminal and enter:
   ```
   sudo cat /etc/sudoers
   ```

2. When prompted, enter your password.
3. As, by default, standard users don't have the abillity to run sudo commands, the following message appears in the terminal:
   <user name> `is not in the sudoers file. This incident will be reported.`

To allow standard users to use sudo, or to prevent administrators from performing certain actions using sudo, you have to edit the sudoers file. However, there is no easy way to centrally manage sudo and the syntax in the sudoers file can be difficult to learn and understand. Using Defendpoint, you can allow users to run specific sudo commands without changing the sudoers file.

You have now completed this section. You have been introduced to some of the problems standard users experience, and also the security risks that cannot be mitigated by removing a user's admin rights. In the next section, you will install Defendpoint for Mac and build a configuration that solves these problems.

Chapter 4 - Defendpoint Software Installation

The Defendpoint installation is performed in two stages; the Defendpoint Management Console is installed on to a Windows computer and the Defendpoint Client is installed on to Mac computers.

4.1 - Installing the Defendpoint Management Console

The Defendpoint Management Console is used to create and edit Defendpoint Settings that are applied to Mac computers. The Defendpoint Management Console is an MMC extension snap-in.

Using an administrator account, log on to the Windows computer you would like to manage Defendpoint from.

To install Defendpoint, run the appropriate installation package:

- For 32-bit (x86) systems run *DefendpointManagementConsoles_x86.exe*
- For 64-bit (x64) systems run *DefendpointManagementConsoles_x64.exe*

1. The installation will detect if any prerequisites are needed. Click **Install** to install any missing prerequisites. This may take a few minutes.
2. Once the prerequisites have been installed, the **Welcome** dialog appears. Click **Next** to continue.
3. After reading the license agreement, select **I accept the terms in the license agreement** and click **Next**.
4. Enter your name and the name of your organization and click **Next** .
5. If you want to change the default installation directory then click the **Change** button and select a different installation directory. Click **Next**
6. Leave the **McAfee ePolicy Orchestrator Integration** check box cleared and click **Next**.
7. Click **Install** to start installing the Defendpoint Console.
8. Once installed, click **Finish**. The Defendpoint Console has now been successfully installed.

In order to use the Event Import Wizard, you will need to install the Microsoft SQL Server 2008 R2 Native Client. For installation instructions and to download this component, visit https://www.microsoft.com/en-gb/download/details.aspx?id=16978

4.2 - Installing the Defendpoint Client on the Mac

If you are installing on to OS X 10.10 Yosemite or OS X 10.11 El Capitan and you want Defendpoint to control commands run with sudo, you need to make sure that sudo 1.8 is installed before installing the Defendpoint Client.

The Defendpoint for Mac Client allows Defendpoint Settings to be applied to the Mac computer.

1. Log on to the Mac using a local administrator account and copy the client installer package *DefendpointMacClient.pkg* onto your desktop.
2. Double-click the installation package.

The padlock icon in the top right-hand corner of the installer screen means that the package is signed by Avecto. You can view the certificate by clicking on the padlock. You should not install Defendpoint for Mac Client if the certificate is missing from the installer package.

3. Click **Continue** to start the installer.
4. Click **Continue** to accept the **End User License Agreement**. When the verification prompt appears, click **Agree** to continue.
5. Leave the default installation destination and click **Install** to being the installation.

We recommend that you install Defendpoint for Mac Client to the default location.

6. Once complete, the **Summary** dialog appears. Click **Close** to complete the installation of the Defendpoint for Mac Client.

Chapter 5 - Creating and deploying a configuration

This section will describe the steps to create your first configuration, using the Defendpoint Management Console. These steps are performed on the Windows computer where you installed the Management Console. This section includes the following steps:

1. Launching MMC and adding the Management Console Snap-in.
2. Creating and licensing a new configuration.
3. Using the Workstyle Wizard to build the rules for the configuration.
4. Exporting the configuration to an XML file.

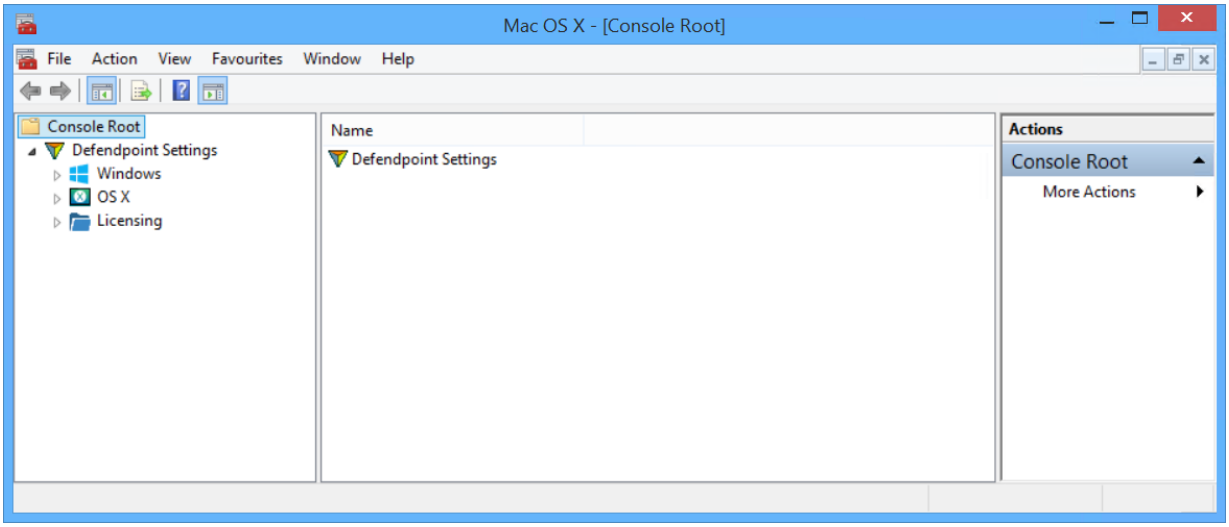
5.1 - Launching the Defendpoint Management Console

The Defendpoint Management Console is accessed as a snap-in to the Microsoft Management Console.

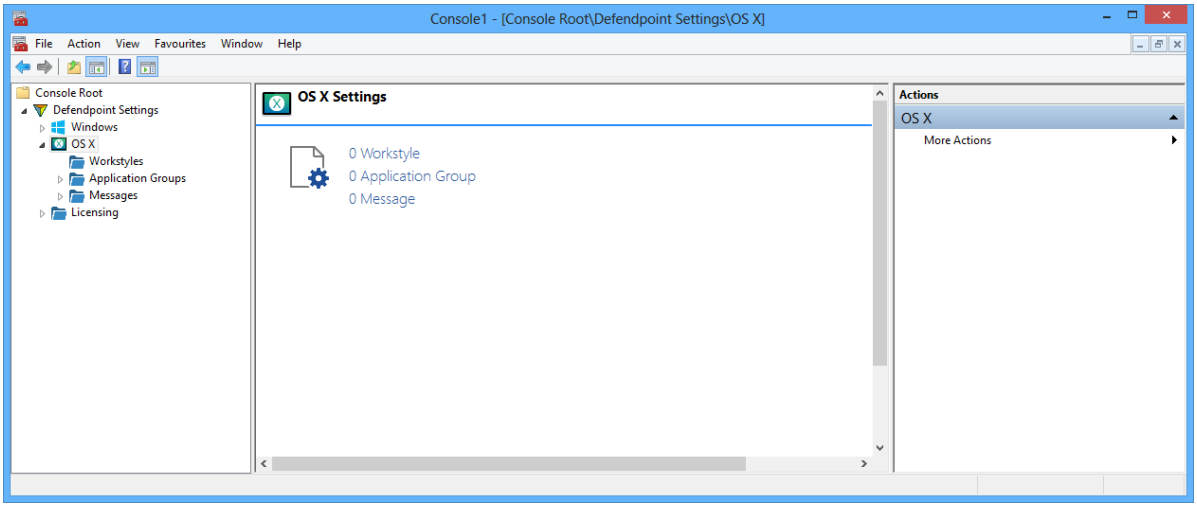
From your administrator account launch the Microsoft Management Console (MMC.exe). Type 'MMC' into the **Search Box** from the **Start Menu** and press the **Enter** key.

We will now add Defendpoint as a snap-in to the console.

1. Select **File** from the menu bar and select **Add/Remove Snap-in**.
2. Scroll down the list and select the **Defendpoint Settings** snap-in. Click **Add** and then click **OK**.
3. Optionally select **File > Save as** and save a shortcut for the snap-in to the desktop as Defendpoint.



4. Expand the **Defendpoint Settings** node in the left-hand pane and select the **OS X** node to display the main screen in the details pane.



5.2 - Licensing

The Defendpoint Client will not function unless it receives a valid license code, which needs to be added in the Defendpoint Console.

5.2.1 - Inserting licenses

To insert a license:

1. Expand the **Defendpoint Settings** node.
2. Select the **Licensing** node.
3. Type the license code into the edit box at the top of the licensing page. The edit box will turn from red to green, once you have entered a valid license code. A description of the license code will be displayed and the **Add** button will be enabled.
4. Click **Add** to add the license to the list of current licenses.

5.3 - Using the Workstyle Wizard to build rules for the configuration

Defendpoint for Mac settings are configured under the **OS X** node. Expand this node to show the following sub-nodes:

- **Workstyles**
  Workstyles are used to assign application rules (such as auto-enhancing or blocking rules) to specific users or groups of users. Multiple workstyles can be created, so that different types of user can be managed according to the level of control and flexibility you want to apply to them.

  Each Workstyle can contain one or more Rules, where an Application Group can have a default action applied to it.
- **Application groups**
  Application Groups are containers which include one or more applications. Application Groups allow you to group similar applications together based on what action you want to apply to them, for example an application you want to auto-enhance, or application you want to block. Each application rule within a workstyle has an assigned application group, which can be selected from the application groups you create.

  Application Groups can be used in multiple workstyles, allowing you to auto-enhance specific applications for some users, but block them for other users.
- **Messages**
  Messages are where you configure the customizable message dialogs that can be presented to users when they attempt to run an application that has matched a particular workstyle. Each application rule within a workstyle can optionally have a message you have created assigned to it.

  Each message lets you add certain controls such as password verification, justification boxes or Challenge/Response codes, which the user must obey before being allowed to OK the message dialog.

  Multiple messages can be created, allowing you to show specific information based on the user or application or action you assign.

Defendpoint for Mac includes a Workstyle Wizard, which will quickly create workstyles, application groups and messages based on Avecto best practices for managing enterprise Mac endpoints. We recommend that for your first configuration, you use the Workstyle Wizard. Once completed, the settings can be tailored and further customized based on your own requirements.

To use the Workstyle Wizard:

1. Expand the **Defendpoint Settings** node, then expand the **OS X** node.
2. Expand and select the **Workstyles** node.
3. Right-click the **Workstyles** node and then click **Create Workstyle**. The workstyle wizard will be displayed.
4. Select a workstyle *Type*:
    - **Controlling** - allows you to apply controls for access to applications and privileges.
    - **Blank** - allows you to create an empty workstyle without any predefined elements.
5. Choose **Controlling**, and click **Next**.
6. Select a filter for the new workstyle. The default choice is **Standard users only**. Click **Next**.
7. The **Module Selection** page allows you to create a workstyle with Privilege Management rules, Application Control rules, or both. Select both modules and click **Next**.
8. The Privilege Management page lets you define the behavior when an unexpected authorization dialog is detected. To ensure that users have the best experience, Defendpoint can suppress these messages and replace them with a default action. In the drop-down box, choose from the following options to define the default action, and click **Next**:
    - Block, and show a message
    - Present users with a challenge code
    - A warning, but allow them to proceed
9. The Application Control page lets you define the type of application control you want to apply. Based on your selection, you can then pick the default action for when an unknown or blacklisted application is run by a user. Choose from the following options:
    - **As a whitelist (recommended)** – A workstyle will be created where trusted applications are automatically allowed, as well as any specific application you allow. If you choose this option, the default actions for non-whitelisted applications are:
        - Do nothing, just audit
        - Warn, but allow the user to proceed
        - Present users with a challenge code
        - Block, and show a message
    - **As a blacklist** – A workstyle will be created where all applications will be automatically allowed, except for applications that you specifically choose to block. If you choose this option, the default actions for blacklisted applications are:
        - Block, and show a message
        - Present users with a challenge code
10. Once you have picked the preferred type of application control and the preferred default behavior, click **Next**.
11. On the final page of the workstyle wizard provide a **Name** and a **Description** for the workstyle. If you select 'Present users with a challenge code' in step 8, you will be asked to enter an authentication key. For more information on challenge codes, see the Mac Console Admin Guide.
12. Select whether you would like to activate the workstyle now, and then click **Finish** to create the workstyle and exit the wizard.

The configuration will now be populated with a workstyle, application groups and messages, and is ready to deploy to your endpoints for testing. The final step is to export the configuration to XML.

5.4 - What's in the Defendpoint Settings?

Defendpoint for Mac Settings consist of four main areas; Workstyles, Application Groups, Messages and Licensing.

5.4.1 - Workstyles

Using the Workstyle Wizard, you have created a configuration that includes one workstyle that is filtered to apply only to non-administrator users i.e., standard users. Defendpoint uses workstyles to apply application rules, based on the criteria of the user and group filters in the **Filters** tab of the workstyle.

By adding more workstyles to the configuration, you can apply different rules to different users and groups of users. You can do this either by running the Workstyle Wizard again, or you can manually create new workstyles and define your own rules and filters.

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, then Defendpoint will not apply any rule to the user. The order in which workstyles are evaluated can be changed by left clicking them and using the up/down buttons in the toolbar.

For more information on configuring workstyles, refer to the Administration Guide.

5.4.2 - Application Rules

Each workstyle can include one or more Application Rules which, assuming the Workstyle applies to the user, will be used to match the application or task. The Workstyle Wizard automatically creates a number of Application Rules, each one designed to apply an action to different types of application, based on their properties. If a match is made, then a resultant action will be applied.

For each Application Rule, a specific Application Group is assigned (see below), and lets you determine the outcome (i.e., allow, passive or block) of any applications or tasks run by the user, if they match the application group. Application Rules also let you configure whether a matching application should be audited, and whether to show the user a customizable message.

Application Rules are applied in precedence order, meaning that when a user runs an application or task and the workstyle filters match, it is the Application Rule at the top of the list that gets evaluated first. If no match is made, then the next rule is evaluated, and so on. If no rules match the application, then Defendpoint will not apply any rule in that workstyle, and will move onto the next workstyle. The order in which rules are evaluated can be changed by left clicking them and using the up/down buttons in the toolbar.

For more information on configuring Application Rules, refer to the Administration Guide.

5.4.3 - Application Groups

Application Groups are used to build collections of applications or tasks that share common properties, making it easy to apply a common action to them. Each Application Group can contain one or more definitions, which determine which properties of an application should be used to match them. Definitions can be created for any of the following application types:

- **Binaries** – Nearly all commands executed on the command-line (such as from within Terminal) are binaries.
- **Bundles** – This is the most common application type, with many built-in apps and tools, as well as apps from the Apple App Store, being bundles.
- **Preference Panes** – Typically found in System Preferences, this type lets you target preference panes that have a padlock.
- **Packages** – The most common type of installation package, and the typical method of installation for enterprise software.
- **Sudo Commands** – Commands (binaries) being run with sudo, which enables authorized users to run those commands as the root user.

The Application Groups created by the Workstyle Wizard are as follows, and fall into two categories; generated groups that are shared between multiple workstyles, and unique groups (tagged with the group workstyle name) that are specific to a particular workstyle, in the order that they are applied in the workstyle:

1. **[Workstyle name] - Apps that are blocked** – Applications or tasks matching this group will always be blocked.
2. **[Workstyle name] – Apps that are automatically authorized** – Applications or tasks in this group will be automatically authorized, should they trigger an authorization request.
3. **[Workstyle name] – Apps that are allowed** – Applications or tasks in this group will always be allowed to run. This group should be used to allow applications or tasks that would normally be blocked if you have a generic block all application rule at the bottom of your configuration.
4. **Apps in system locations (Generated)** – This group comprises all system directories such as the operating system, and installed approved applications, that require administrator privileges to manage. In a least-privilege deployment, these directories can automatically be trusted, and so any application or task in a system location is allowed to run.

If you are using application control it is not recommended that you modify this group. It is important that this group always has a higher precedence than any catch-all rules, such as Any other apps (Generated) below.

5. **Apps in system locations that request authorization (Generated)** – This group will match all applications or tasks in system directories (see above) that trigger an authorization request.

It is not recommended that you modify this group, as it may result in users receiving authorization prompts from the operating system.

6. **Any other apps (Generated)** – This group will match any other application or task that does not match another Application Group above. This group is referred to as a Catch-All group, and lets you apply a default action to any application that is not trusted, or has not already been assigned to a unique group for that workstyle.

It is not recommended that you modify this group, as it may result in untrusted applications being allowed to run.

For more information on configuring Application Groups, refer to the Administration Guide.

5.4.4 - Messages

Messages can be presented to users when they try to run an application or task. They can be presented before something is allowed to run, or when something has been blocked, or as a replacement for authorization requests. They can be fully customized to display any text you want, and can be stylized with your own brand and logo. They can also include additional controls such as Challenge / Response codes and password verifications as a way of controlling what they can run, and when they can run it. You can create as many messages as you want, and can reuse them in multiple workstyles.

Text-only versions of any configured messages are displayed in the Terminal when you run sudo commands.

The Workstyle Wizard automatically creates a number of messages based on the options you chose, and all of these messages can be customized.

For more information on configuring End User Messages, refer to the Administration Guide.

5.5 - Adding applications to the configuration

Now that you have created a configuration you may want to add some application rules that would allow users to run applications, sudo commands, install packages or unlock System Preferences. You may also want to block applications to prevent them from being used. In this section, you will add new applications to the Application Groups that were created by the Workstyle Wizard.

Later you will test these rules, once the configuration has been applied to the Mac.

In the following sections, [Workstyle] represents the name you give the workstyle in step 11 of the previous section **Using the Workstyle Wizard to build rules for the configuration** detailed on page 14.

5.5.1 - Add a preference pane so that it can be unlocked

In this section, you will add the Date & Time preference pane to the configuration that will allow standard users to automatically unlock it.

1. Expand **Defendpoint Settings > OS X > Application Groups** and select the node *[Workstyle] – Apps that are automatically authorized*.
2. Right-click anywhere in the right-hand pane, and choose **Insert Application > System Preference Pane…**.
3. In the **Insert Application** wizard, click the **Template…** button.
4. Locate *Date and Time* in the list of available templates, or begin typing "*date and time*" in the search box to quickly find it. Select it, and click the **Insert** button.
5. In the Insert Application wizard, accept the pre-populated settings by clicking the **Next >** button, and at the end of the wizard, click **Finish**.

The *Date and Time* preference pane has now been added to the application group, and will automatically allow standard users to unlock it.

5.5.2 - Add a package so that it can be installed

In this section, you will add the package (.pkg) that you tried to install earlier in Section 2.3.2 - Installing software packages, see **Installing software packages** detailed on page 8.

Packages may require two rules; one rule to allow the package to be run (Application Control) and one rule to automatically authorize it (Privilege Management).

To allow the package to run:

1. Expand **Defendpoint Settings > OS X > Application Groups** and select the node *[Workstyle] – Apps that are allowed*.
2. Right-click anywhere in the right-hand pane, and choose **Insert Application > Package…**.
3. In the **Insert Application** wizard, enter the name of the package in the **File or Folder Name…** edit box, ensuring that the letter case matches that exactly of the .pkg. Click **Next**.
4. Optionally give this application rule a description, or accept the default. Click **Next**.
5. In the **Application Definition** page, accept the default settings and click **Finish**.

To automatically authorize the package:

1. Expand **Defendpoint Settings > OS X > Application Groups** and select the node *[Workstyle] – Apps that are automatically authorized*.
2. Right-click anywhere in the right-hand pane, and choose **Insert Application > Package…**.
3. In the **Insert Application** wizard, enter the name of the package in the **File or Folder Name…** edit box, ensuring that the letter case matches that exactly of the .pkg. Click **Next**.
4. Optionally give this application rule a description, or accept the default. Click **Next**.
5. In the **Application Definition** page, check the option **Application requests authorization**, then click **Finish**.

The package has now been added to two application groups, so it will be allowed to run, and when it triggers an authorization, will automatically be authorized.

Package rules for allowing and authorizing are different, so that you can independently control the behavior. This grants you the ability to optionally use different restrictions and messaging for when packages are run, and when they trigger an authorization.

5.5.3 - Add a bundle to block it from being used

In this section, you will add the application bundle *iTunes.app* to the configuration that will block standard users from executing it.

1. Expand **Defendpoint Settings > OS X > Application Groups** and select the node *[Workstyle] – Apps that are blocked*.
2. Right-click anywhere in the right-hand pane, and choose **Insert Application > Bundle…**.
3. In the **Insert Application** wizard, click the **Template…** button.
4. Locate *iTunes* in the list of available templates, or begin typing "*itunes*" in the search box to quickly find it. Select it, and click the **Insert** button.
5. In the **Insert Application** wizard, accept the pre-populated settings by clicking the **Next >** button, and at the end of the wizard, click **Finish**.

The *iTunes* bundle pane has now been added to the application group, and will automatically block standard users from running it.

5.5.4 - Add a binary to block it from being used

In this section, you will add the binary `curl` to the configuration that will block standard users from executing it.

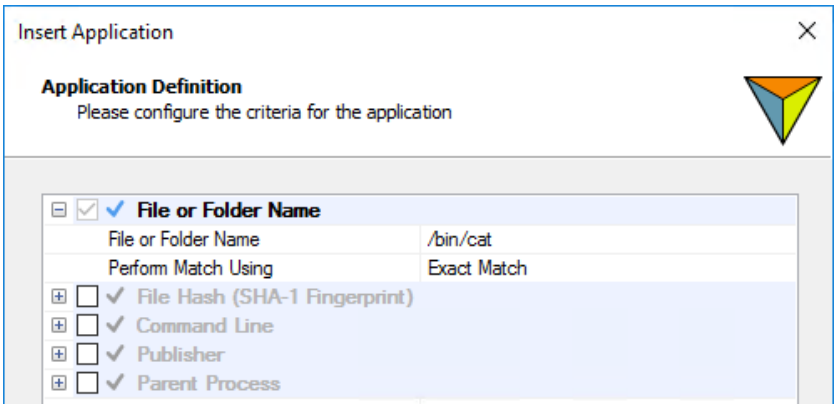
1. Expand **Defendpoint Settings > OS X > Application Groups** and select the node *[Workstyle] – Apps that are blocked*.
2. Right-click anywhere in the right-hand pane, and choose **Insert Application > Binary…**.
3. In the **Insert Application** wizard, enter *curl* in **File or Folder Name…**. Click **Next**.
4. Optionally give this application rule a description, or accept the default. Click **Next**.
5. In the **Application Definition** page, accept the default settings and click **Finish**.

The `curl` binary has now been added to the application group, and will automatically block standard users from running it.

5.5.5 - Add a sudo command so that it can be run

In this section, you will add the sudo command `cat` to the configuration so that standard users can run it using sudo.

1. Expand **Defendpoint Settings > OS X > Application Groups** and select the node *[Workstyle] – Apps that are automatically authorized*.
2. Right-click anywhere in the right-hand pane, and choose **Insert Application > Sudo Command…**.
3. In the **Insert Application** wizard, enter `/bin/cat` in **File or Folder Name…**. Click **Next**.
4. Optionally give this application rule a description, or accept the default. Click **Next**.
5. In the **Application Definition** page, accept the default settings and click **Finish**.



The `cat` command has now been added to the application group and will allow standard users to run this command with sudo.

5.6 - Exporting the Defendpoint settings

To export the Defendpoint settings as an XML file, from the Defendpoint Console:

1. Select the **Defendpoint Settings** node.
2. Right-click and select **Export…**.
3. Choose a location to save the XML, and name the file `pguard.xml`. then click **Save**.

5.7 - Applying the Defendpoint settings to a Mac

Once you have exported your settings to an XML file, the next step is to apply the settings to a Mac. To do this, you will first need to copy the XML file onto Mac; this can be done using a network of virtual machine share, or by using an external USB drive. To apply the settings, you will need to use an account with sudo access.

If you are using iC3, then any settings are automatically deployed to Macs that are managed by iC3.

To apply the Defendpoint settings to a Mac:

1. Log onto the Mac with an admin account (or account with sudo access)
2. Copy the exported XML settings to your desktop.
3. Open the Terminal, and run the following command:
   `sudo cp ~/Desktop/pguard.xml /etc/pguard/pguard.xml`
4. Once copied, the Defendpoint client will automatically load the new settings. No restart is required.

Do not delete or rename the `/etc/pguard/pguard.xml` file as this will interfere with the client machine's ability to enforce policy.

Chapter 6 - Testing Defendpoint

This chapter will revisit the tests done in Section 3 - Standard user experience without Defendpoint, highlighting the advantages of using Defendpoint Privilege Management to empower standard users on Macs, and the security benefits of Defendpoint Application Control.

Before doing these exercises, make sure that you have:

- Switched back to the standard user session you used earlier in this guide
- Closed any previously opened applications. Active applications are identified in the Dock by a dot beneath their icon. To ensure applications are closed properly, click on the application window and press ⌘ **+ Q**.

6.1 - Unlocking administrative preference panes

1. As a standard user open the **Date & Time** preference pane.
2. Click the padlock to unlock the preference pane.
3. The padlock will unlock and the **Date & Time** settings can now be altered by a standard user.

Defendpoint can be used to allow standard users to access preference panes that would normally require a privileged account. This not only empowers standard users to perform approved admin tasks, but also improves the experience of running those tasks by eliminating the need to repeatedly enter their credentials.

Try unlocking any other System Preference panes that are padlocked. The Defendpoint Settings are configured to intercept these and display a block/reason dialog. Rather than receiving an authorization dialog, with Defendpoint you can instead provide a more meaningful message, mitigating the need for an IT support call.

If you want to configure rules for other preference panes, refer to the Defendpoint for Mac Administration Guide.

6.2 - Installing a package

1. As a standard user double-click the package you downloaded and tried to install earlier.
2. Proceed through the installation wizard, and click **Install**.
3. The package will install successfully, without the standard user having to authorize a message.

Defendpoint can be used to allow standard users to install approved software packages that would normally require a privileged account. This not only empowers standard users to manage their own software installations and upgrades, but also improves the installation experience by eliminating the need to enter their credentials.

Try running any other installation package from the standard user's desktop, USB device, disk image (.dmg) or from any other untrusted location. The Defendpoint Settings are configured to intercept these and display a block/reason dialog. Rather than receiving an authorization dialog, with Defendpoint you can instead provide a more meaningful message, mitigating the need for an IT support call.

If you want to configure rules for other installation packages, refer to the Defendpoint for Mac Administration Guide.

6.3 - Opening a bundle

1. As a standard user, double-click the application bundle you downloaded and tried to run earlier.
2. The application will run successfully.
3. Now, run the application *iTunes*.
4. The application will be blocked from running, and the user will be presented with a Defendpoint message.

Defendpoint can be used to prevent the running of untrusted or unauthorized applications. By default, any application running from an untrusted location will automatically be blocked. Defendpoint can be configured to explicitly approve individual applications to run from these locations, so that users are still productive. This concept is called whitelisting, where only known applications can run.

Defendpoint can also be used to explicitly block applications even though they are running from trusted locations, for example system utilities and iTunes. This concept is called blacklisting, where individual applications can be blocked.

Defendpoint uses both whitelisting and blacklisting, in combination with Privilege Management, to give you a powerful yet lightweight way of controlling all application usage, preventing unknown, unapproved and potentially malicious apps from ever running.

Try running any other bundle application from the standard user's desktop, USB device, disk image (.dmg) or from any other untrusted location. The Defendpoint Settings are configured to intercept these and display a block/reason dialog. With Defendpoint you can provide a meaningful message, mitigating the need for an IT support call.

If you want to configure rules for other application bundles, refer to the Defendpoint for Mac Administration Guide.

6.4 - Running a binary using the command line

1. As a standard user, open the Terminal and type:
   `curl` <the server/website and file name of the file you want to download> `-o ~/Desktop/` <filename>

   For example, if you wanted to download the *Defendpoint for Mac* PDF from the Avecto website and call it *downloaded.pdf* you would type:
   ```
   curl https://avectoweb.blob.core.windows.net/cms/1465/datasheet-defendpoint-for-mac.pdf -o ~/Desktop/downloaded.pdf
   ```

2. The command will be blocked from running, and the user will be presented with a Defendpoint message.

Defendpoint can be used to prevent the running of specific binary applications on the command line, even though they are trusted. Defendpoint can also ensure that untrusted binaries introduced to the endpoint (either intentionally or maliciously) cannot be run.

If you want to configure rules for other binary applications, refer to the Defendpoint for Mac Administration Guide.

6.5 - Running sudo commands using the command line

1. As a standard user, open the Terminal and enter:
   `sudo cat /etc/sudoers`
2. The command runs automatically and the contents of the sudoers file appear in the Terminal.

Defendpoint enables you to configure rules that allow standard users to run sudo commands that they normally would not have permission to run. Defendpoint can also be used to block the ability to run specific sudo commands.

If you want to configure rules for other sudo commands, refer to the Defendpoint for Mac Administration Guide.

Chapter 7 - Conclusion

You have now completed the Getting Started Guide for Defendpoint for Mac. You have demonstrated the limitations that users experience when trying to run applications and tasks that require administrator privileges, and you have also demonstrated the risks to the organization through the misuse of unapproved applications.

You have installed Defendpoint, and have implemented settings that solve all of the challenges highlighted in this guide. You have demonstrated that standard users can be empowered, whilst simultaneously applying a well-managed and locked down environment that stops unknown and untrusted applications from executing.

If you want to know more about configuring Defendpoint for Mac, see the Defendpoint for Mac Administration Guide.