Avecto

Defendpoint For Mac 4.1

Administration Guide v 2.3

April 2016

Table of Contents

1. Introduction 6

Technical benefits 6

2. Planning and Preparation 8

2.1. Defining User Roles 8

2.2. Supported platforms 8

3. Defendpoint Software Installation 9

3.1. Installing the Defendpoint Management Console 9

3.2. Installing the Defendpoint Client on a Mac computer 11

3.3. Creating a Standard User account 13

3.4. Launching the Defendpoint Management Console 14

4. Licensing 15

4.1.1. Inserting Licenses 15

5. Defendpoint Settings 16

6. Workstyles 17

6.1. Workstyle Wizard 17

6.2. Creating Workstyles 17

6.2.1. Disabling Workstyles 18

6.2.2. Workstyle Precedence 19

6.3. Filtering Workstyles 19

6.3.1. Account Filters 19

7. Managing Applications 21

7.1. Creating Target Application Groups 21

7.2. Inserting Binaries 21

7.3. Inserting Bundles 22

7.4. Inserting System Preference Panes 23

7.5. Inserting Packages 24

7.6. Inserting Application Templates 26

7.7. Application Rules 26

7.7.1. Inserting an Application Rule 27

7.7.2. Application Rule Precedence 27
8. End User Messaging 28
8.1. Creating Messages 28
8.2. Message Boxes 28
8.2.1. Message Design 29
8.2.2. Message Text 31
8.2.3. Managing Languages 31
8.2.4. Image Manager 32
8.2.5. Challenge / Response Authorization 33
9. Defendpoint Settings Management 37
9.1. Exporting and Importing Settings 37
9.2. Adding Defendpoint Settings to a Mac Client computer 37
9.3. Deleting Defendpoint Settings 38
9.4. Deleting Items and Conflict Resolution 38
10. Event Reporting 39
10.1. Events 39
10.1.1. Process Events 39
10.1.2. Configuration Events 40
10.1.3. User / Computer Events 40
11. Troubleshooting 41
11.1. General Troubleshooting Tips 41
11.1.1. Check Defendpoint is Installed and functioning 41
11.1.2. Check Settings are licensed 41
11.1.3. Check Workstyle Precedence 41
Appendices 42
Appendix 1. Built-in Groups 43
Appendix 2. Application Definitions 44
Appendix 3. Regular Expressions 46
Appendix 4. Application Templates 48
A 4.1. Creating Custom Application Templates 48
Appendix 5. Debug Logging 49

1. Introduction

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, so that only known good applications are able to run, while users have the freedom and flexibility to perform everyday tasks.

For the first time, you can achieve the same level of security and usabilityon a Mac as you can on a Windows PC.

Technical benefits

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 non admin 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. Simply 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 full control over text configuration.

Customizable messaging

Working seamlessly with OS X, Defendpoint for Mac suppresses 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 create flexible 'WorkStyles' based on the requirements of individuals and groups of users.

Supported platforms

- OS X 10.10 Yosemite
- OS X 10.11 El Capitan

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.

Role	Requirement for Admin Rights
Standard Corporate User	Problem applications and simple admin tasks.
Laptop User	Problem applications, intermediate admin tasks and authorized software installation.
Technical User	Complex applications, advanced admin tasks and as hoc software installation.

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. Supported platforms

- OS X 10.10 Yosemite
- OS X 10.11 El Capitan

Note: Ensure all OS X updates are applied.

3. 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.

3.1. Installing the Defendpoint Management Console

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

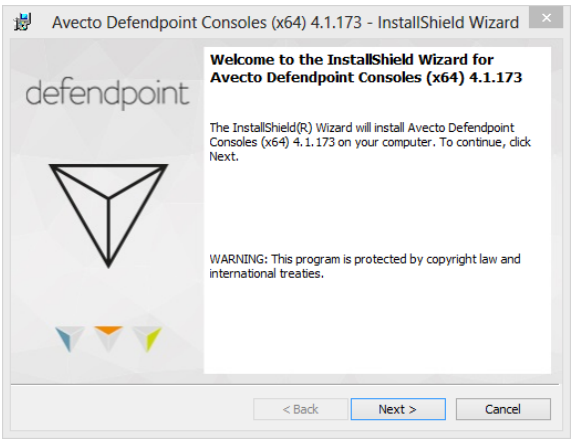
Log on to the Windows computer you would like to manage Defendpoint from, using an administrator account.

Install Defendpoint by running the appropriate installation package:

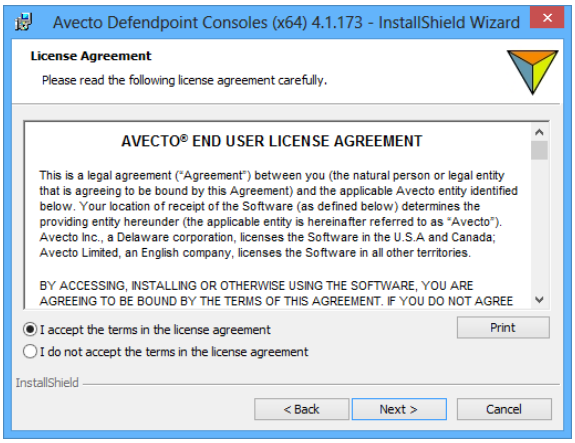
- For 32-bit (x86) systems run DefendpointManagementConsoles_x86.exe
- For 64-bit (x64) systems run DefendpointManagementConsoles_x64.exe

1. The installation will detect if any prerequisites are needed. Click **Install** to install any missing pre-requisites. This may take a few minutes.

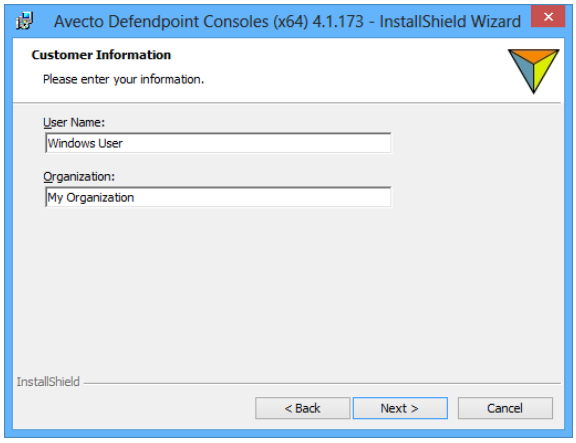
2. Once the prerequisites have been installed, the **Welcome** dialog will appear.



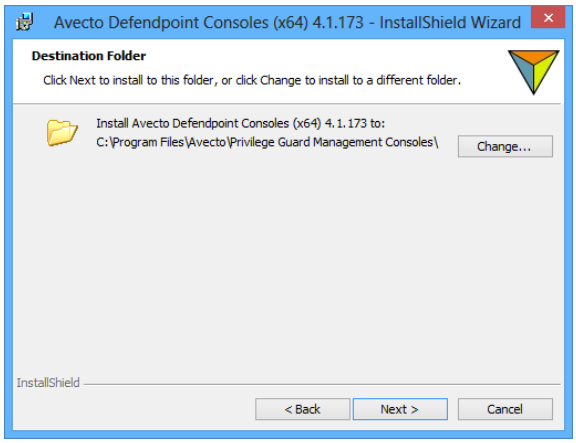
3. Click **Next** to continue. The **License Agreement** dialog will appear.



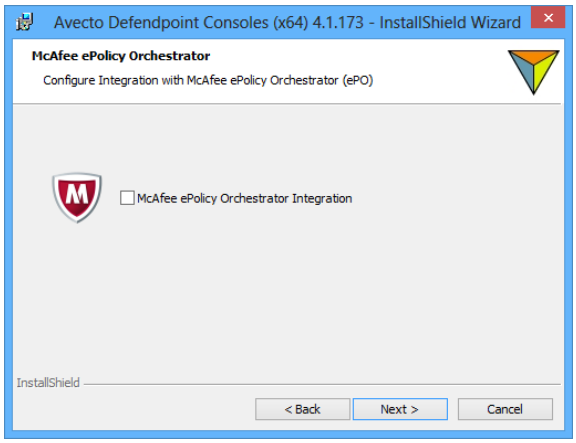
4. After reading the license agreement, select **I accept the terms in the license agreement** and click **Next** to continue. The **User Information** dialog will appear.



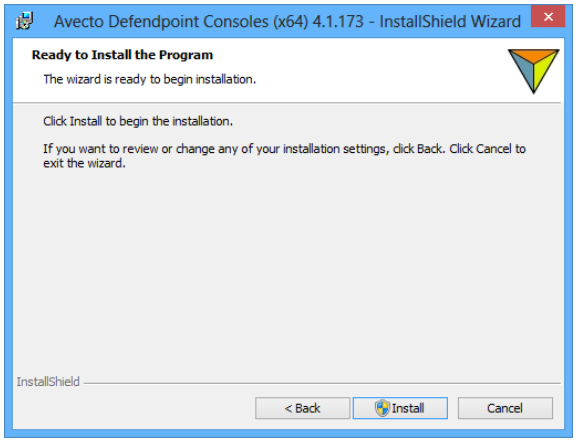
5. Enter your name and the name of your organization and click **Next** to continue. The **Destination Folder** dialog will appear.



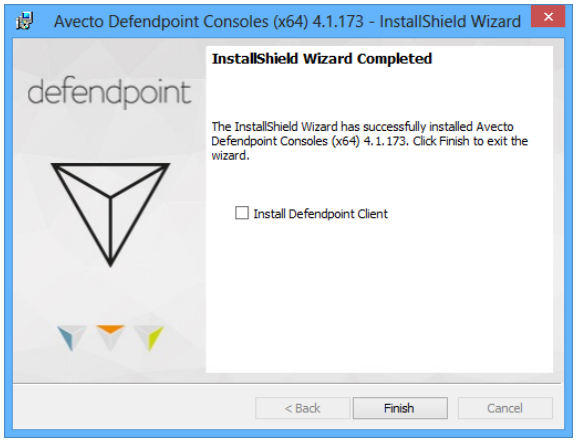
6. If you wish to change the default installation directory then click the **Change** button and select a different installation directory. Click **Next** to continue. The **McAfee ePolicy Orchestrator** dialog will appear.



7. Leave this option unchecked and click **Next** to continue. The **Ready to Install the Program** dialog will appear.



8. Click **Install**. The Management Console will begin installation. Once installed, you will be presented with the following screen giving you the option of installing the Defendpoint Client on the current Windows computer.



9. Uncheck this option and click **Finish**. The Defendpoint Console has now been successfully installed.

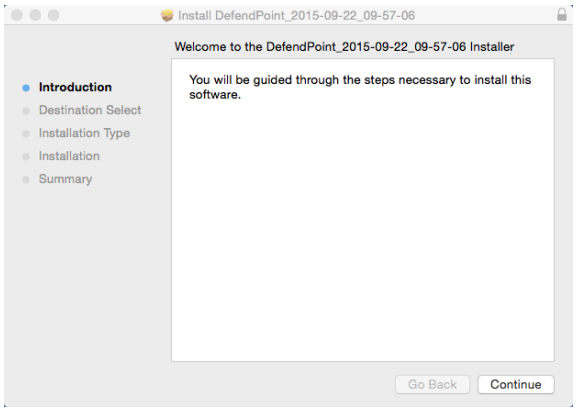
3.2. Installing the Defendpoint Client on a Mac computer

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

1. Log on to the Mac computer that the Defendpoint Client is to be installed on, using an administrator account.

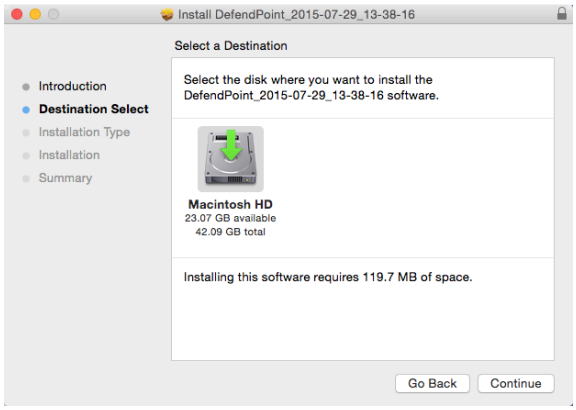
2. Install the Defendpoint Client by double-clicking the installation package *DefendpointClient.pkg.*

Note: The package is signed by Avecto and the padlock in the top-right corner can be selected, to view the certificate, to ensure its validity.

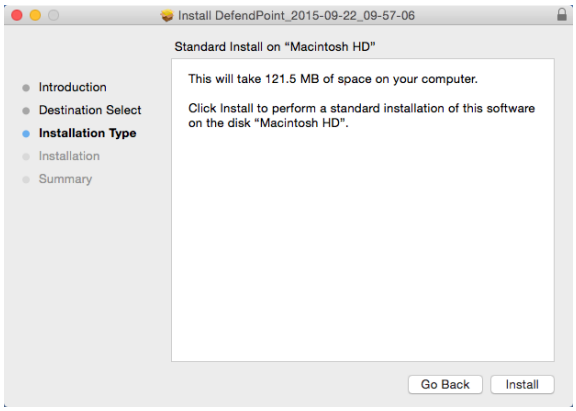


3. Click **Continue** to install the Defendpoint Client.

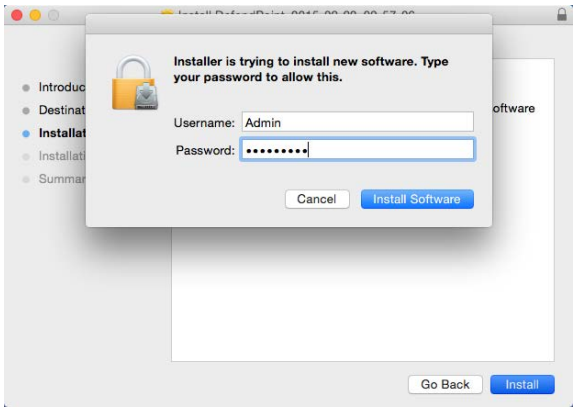
4. The **Destination Select** dialog will be displayed. The default setting is the Macintosh HD.



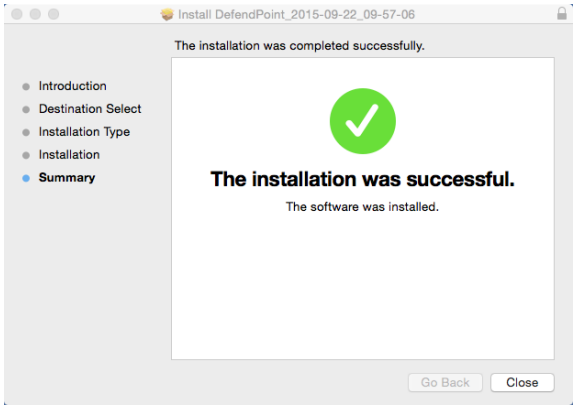
5. Click **Continue** and the **Installation Type** dialog will be displayed confirming the size and destination of the software install.



6. Click **Install**. An Apple authorization dialog will display. Enter the administrator credentials and click **Install Software**.



7. The software installation will commence and on completion the **Summary** dialog will be displayed.



8. Click **Close** to complete the installation of the Defendpoint for Mac Client.

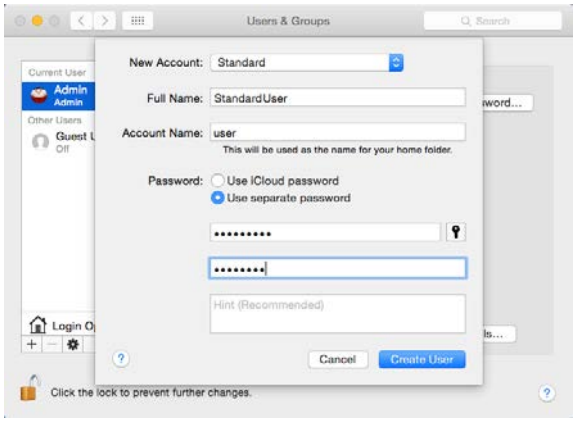
3.3. Creating a Standard User account

This section is only required if the Mac computer on which you are evaluating Defendpoint does not have a standard user account.

1. Using the local admin account open the **Users & Groups** preference pane from the **System Preferences** folder.

2. Unlock the preference pane by clicking the padlock and entering your admin credentials.

3. Click on the **+** button to create a new Standard user and complete the dialog as shown below.



4. Close the **Users & Groups** preference pane.

3.4. Launching the Defendpoint Management Console

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

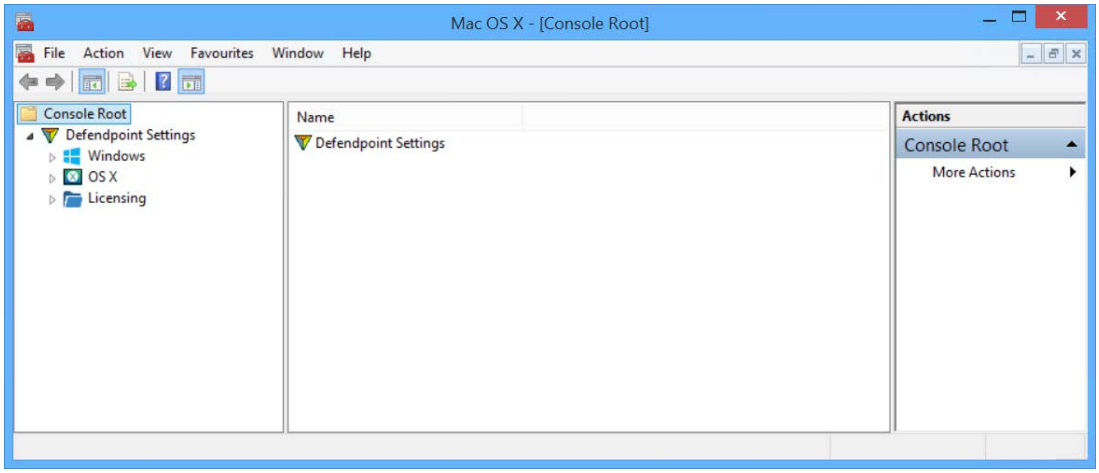
From your administrator account launch the Microsoft Management Console (MMC.exe). Simply type '**MMC**' into the **Search Box** from the **Start Menu** and press the **Enter** key.

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

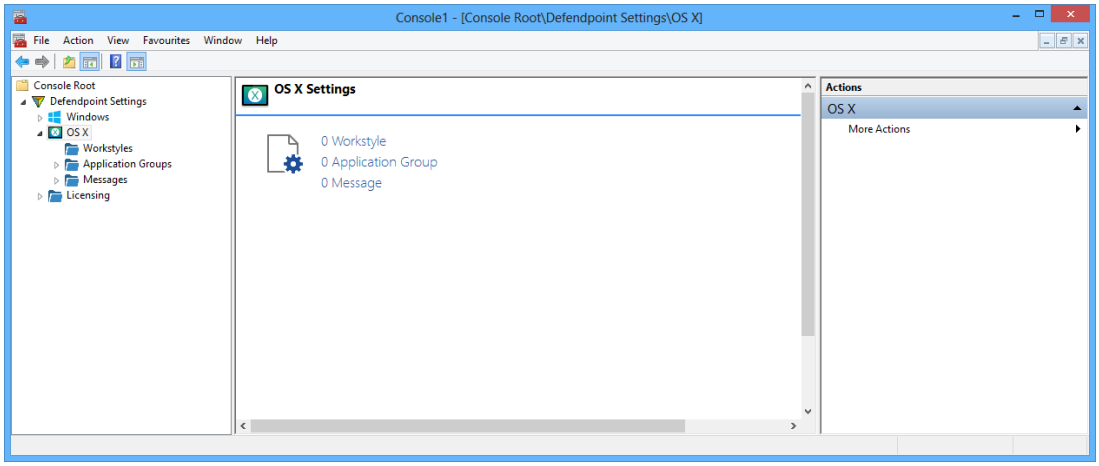
1. Select **File** from the menu bar and select **Add/Remove Snap-in**.

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.



4. Licensing

The Defendpoint Client will not function unless it receives a valid license code.

4.1.1. Inserting Licenses

To insert a license:

1. Expand the **Defendpoint Settings** node.
2. Select the **Licensing** node.
3. Type the license code that you have received 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 into the list of current licenses.

5. Defendpoint Settings

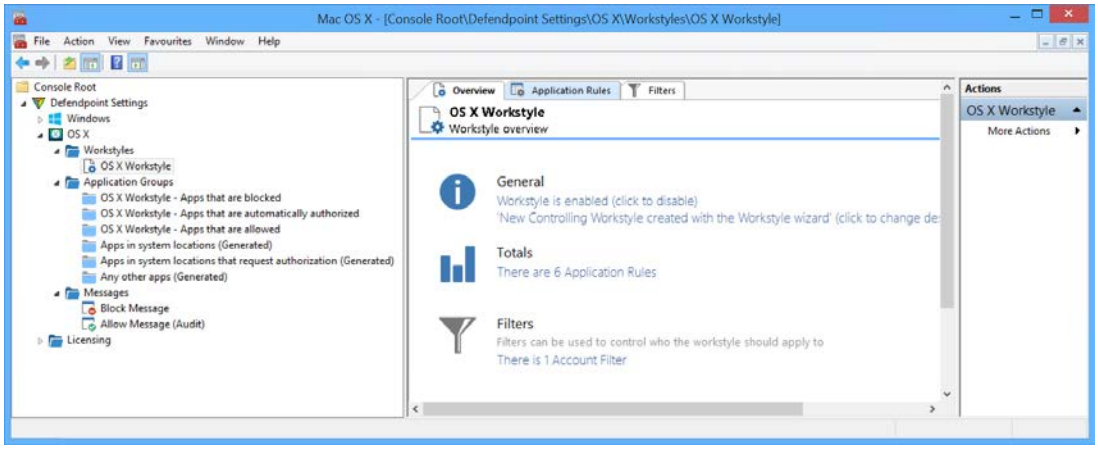
The Defendpoint Settings editor will automatically save any changes back to the local XML file.

Automatic saving may be disabled, by deselecting the **Auto Commit Settings** menu option on the **Defendpoint Settings** node, but this is not recommended unless you are having performance issues. If you deselect the **Auto Commit Settings** option then you must select the **Commit Settings** menu option to manually save any changes back to the local XML file. The **Auto Commit Settings** option is persisted to your user profile, so it will be set for all future editing of Defendpoint Settings.

If you expand the **OS X** node you will see three nodes:

1. **Workstyles** - assign privileges to applications.
2. **Application Groups** - define logical groupings of applications.
3. **Messages** - define end user messages.

Once a workstyle has been created and selected in the tree pane, the workstyle tabs will be displayed in the details pane.



There are three tabs. You can toggle individual tab displays on and off from the tab drop-down menu at the top right of the details pane.

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

Note: Tabs that contain active settings cannot be toggled off.

6. Workstyles

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

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

6.1. 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 two types of workstyle that can be created in Defendpoint:

- **Controlling workstyle** - allows you to apply rules for access to binaries, bundles packages and system preference panes.
- **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 **Account 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

Defendpoint for Mac includes two core modules. Only controlling workstyles incorporate these modules. A controlling workstyle may incorporate both of the modules. The two core modules are:

- Privilege Management
- Application Control

For more information on the Defendpoint Modules please refer to the Introduction section of this guide.

6.2. Creating Workstyles

To create a workstyle:

1. Expand the **Defendpoint Settings** 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*:

5. **Controlling** - allows you to apply controls for access to applications and privileges and to define sandboxing

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

6. Click **Next**.

7. Select a filter for the new workstyle. The default choice is **Standard users only**. If you wish to apply the new workstyle to all users (including administrators), select **Everyone, including Administrators**.

8. If you are creating a Controlling workstyle, select one or both Defendpoint Modules and click **Next**.

9. The workstyle wizard will display pages appropriate to the Defendpoint module(s) you selected in Step **8**. Complete the pages relevant to the workstyle type and any modules you have selected.

10. 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.

11. Select whether you would like to activate the workstyle now.

12. 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 and filters.

These auto-generated elements are appropriate to the options that are selected in the workstyle wizard.

6.2.1. Disabling Workstyles

When a workstyle is disabled it's settings will still be saved to the local XML file but they will not be active.

To disable a workstyle:

1. Select the workstyle (in the tree pain or details pane).

2. Right-click the workstyle and then click **Disable Workstyle**.

To enable a workstyle (that is currently disabled):

1. Select the workstyle (in the tree pain or details pane).

2. Right-click the workstyle and then click **Enable Workstyle.**

6.2.2. 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 give a workstyle a higher precedence:

1. Right-click the workstyle and then select **Move Up**.
2. Repeat step **2** until you have the workstyle positioned appropriately.

To give a workstyle 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.

6.3. Filtering Workstyles

The **Filters** tab of a workstyle can be used to further refine when a workstyle will actually be applied.

- By default a workstyle will apply to all users/computers who receive it. However, you can add one or more filters that will restrict the application of the workstyle:
- **Account Filter** – this filter restricts the workstyle to specific users or groups of users.

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

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, right-click the filter and check the option **Apply this filter if it does NOT match**.

6.3.1. Account Filters

Account filters specify 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. On the **Filter** tab click **Add a filter....**
2. Click **Add an Account Filter**.
3. Select either **Add a new local OS X account** or **Add a new domain account**.
4. The **Add Account** dialog will appear.
5. Enter the relevant user or group details and click **OK**.

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 within one Account filter, and want to apply the workstyle only if ALL entries in the Account filter match, then check 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.

7. Managing Applications

Application groups are used to define logical groupings of applications.

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

7.1. Creating Target Application Groups

To create a target application group:

1. Expand the **OS X** node.
2. Select the **Application Groups** node.
3. Right-click the **Application Groups** node and then click **New Application Group**.
4. A new application group will be created (**Application Group 1**). You can rename the group by double-clicking on the group name. You can now add applications to the application group.

Application Group Description

You may set a description for an application group by accessing the application group properties:

1. Right-click the **Application Group** and then click **Properties**.
2. Set the **Description** in the **Properties** dialog.
3. Click **OK**.

7.2. Inserting Binaries

To insert a binary:

1. Select the relevant application group.
2. Right-click in the details pane to access the context menu.
3. Select **Insert Application** and then select **Binary…** from the sub-menu.
4. After selecting an application type to insert, the **Insert Application** wizard is launched.
5. Enter a **File or Folder Name** for the application or click the **Template…** button. For more information about Application Templates please refer to

6. Inserting Application Templates.
7. Click **Next**.
8. Enter a description for the application (the description will automatically be extracted from the file you entered, if it has a description).
9. Click **Next**.
10. Configure the **Application Definitions** for the application. For information about application definitions see below.
11. Click **Next**.
12. Click **Finish**.

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.

The **Insert Application** wizard provides various 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 or Folder Name
- File Hash (SHA-1 Fingerprint)

7.3. Inserting Bundles

To insert a bundle:

1. Select the relevant application group.
2. Right-click in the details pane to access the context menu.
3. Select **Insert Application** and then select **Bundle…** from the sub-menu.
4. After selecting an application type to insert, the **Insert Application** wizard is launched.
5. Enter a **File or Folder Name** for the application or click the **Template…** button. For more information about Application Templates please refer to

6. Inserting Application Templates.
7. Click **Next**.
8. Enter a description for the application (the description will automatically be extracted from the file you entered, if it has a description).
9. Click **Next**.
10. Configure the **Application Definitions** for the application. For information about application definitions see below.
11. Click **Next**.
12. Click **Finish**.

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.

The **Insert Application** wizard provides various 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 or Folder Name
- File Hash (SHA-1 Fingerprint)
- Source
- File Version matches
- URI
- Application requests authorization

7.4. Inserting System Preference Panes

To insert a system preference pane:

1. Select the relevant application group.
2. Right-click in the details pane to access the context menu.
3. Select **Insert Application** and then select **System Preference Pane…** from the sub-menu.
4. After selecting an application type to insert, the **Insert Application** wizard is launched.
5. Enter a **URI** for the application or click the **Template…** button. For more information about Application Templates please refer to Inserting Application Templates.
6. Click **Next**.
7. Enter a description for the application (the description will automatically be extracted from the file you entered, if it has a description).
8. Click **Next**.

9. Configure the **Application Definitions** for the application. For information about application definitions see below.

10. Click **Next**.

11. Click **Finish**.

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.

The **Insert Application** wizard provides various 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 or Folder Name
- File Hash (SHA-1Fingerprint)
- Source
- File Version matches
- Application requests authorization

Note: Some 3rd party preference panes may behave as a Bundle application type when their padlocks are clicked by a user. If you are unable to match the preference pane as a Preference Pane type, check the audit log and use a Bundle type to match the preference pane, using the 'Path' property that has been audited by Defendpoint. For more information please see Appendix 5 Debug Logging.

7.5. Inserting Packages

To insert a package:

1. Select the relevant application group.

2. Right-click in the details pane to access the context menu.

3. Select **Insert Application** and then select **Package…** from the sub-menu.

4. After selecting an application type to insert, the **Insert Application** wizard is launched.

5. Enter a **File or Folder Name** for the application.

6. Click **Next**.

7. Enter a description for the application (the description will automatically be extracted from the file you entered, if it has a description).

8. Click **Next**.

9. Configure the **Application Definitions** for the application. For information about application definitions see below.

10. Click **Next**.

11. Click **Finish**.

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.

The **Insert Application** wizard provides various 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 or Folder Name
- File Hash (SHA-1Fingerprint)
- Application requests authorization

Note: Only one package may be opened by the Installer at any one time. Any attempt to open and install a second package whilst the first package is open will result in the termination of the Installer and neither package will be installed; any package that was in the process of installing will be interrupted and the installation may be incomplete.

7.6. Inserting Application Templates

Application Templates provide a simple way to pick from a list of known applications. A standard set of templates are provided, which cover binaries, bundles and system preference panes.

Each category then has a list of applications. Picking an application will cause the Application dialogs to be pre-populated with the appropriate information.

To insert an Application Template:

1. Select the relevant Application group.
2. Right-click the applications list in the details pane to access the context menu.
3. Select **Insert Application** and then select **Application Template** from the sub-menu.
4. The **Application Template** dialog will appear.
5. Use the search box to locate a specific application template or scroll through the available templates.
6. Select one or more application templates (using the **Ctrl** key).
7. Click **OK** to add the selected application templates to the application group.

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.

7.7. Application Rules

Application Rules are applied to applications that are launched either directly by the user or by a running process. They can be created and edited from the workstyle **Application Rules** tab. If you have a blank workstyle you can create rules from the workstyle **Overview** tab.

The **Application Rules** tab can be used to enforce rules for whitelisting, monitoring and application discovery, and handling OS X Authorization Requests.

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.
- OS X Authorization Requests – Any process that requests authorization from the operating system.

Auditing

- Raise an Event – An event will be logged to the client machine's syslog file.

7.7.1. Inserting an Application Rule

To insert an application rule:

1. Select the relevant workstyle in the tree pane.
2. Select the **Application Rules** tab in the details pane.
3. Right-click in the **Application Rules** tab and click **Insert Application Rule…**. The **Create Application Rule** dialog will appear.
4. Select the relevant application group from **Target Application Group > Click to select…** 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. For more information see End User Messaging.
7. If the Application Definition - **Application requests authorization** - is a matching criteria for an application, you have the choice of letting Defendpoint handle the authentication (**Authorize**) or letting OS X handle the authentication **(Passive (No Change)**.
8. If **OS X Authorization Request**s is enabled you have the choice of Defendpoint handling the authentication (**Authorize**) or OS X handling the authentication (**Passive (No Change)**).
9. If you wish to audit the Application rule being matched then select **On** for **Raise an Event**. This will log events to the syslog.

7.7.2. Application Rule Precedence

If you add more than one Application rule to a workstyle then entries that are higher in the list will have a higher precedence. Once an application matches an Application rule, no further rules or workstyles will be processed. If an Application 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. Right-click the rule and then select **Move Up**.
2. Repeat step **1** until you have the **Rule** positioned appropriately.

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.

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

8. End User Messaging

You can define any number of end user messages. Messages 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*.

Once defined, a message may be assigned to an individual rule in the **Application Rules** tab by editing the rule.

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

8.1. Creating Messages

To create a message:

1. Select the **Messages** node.
2. Right-click the **Messages** node and select **New Message…**.
3. The **New Message** wizard will appear.
4. Select a message template from the **Message Box** template drop-down list.
5. Click **Next**.
6. Customize the message (more advanced message configuration can be performed after the message has been created).
7. Click **Finish**.

A new message will be created under the **Messages** node. You can rename the message by double-clicking on the message name.

You may now further refine the message by selecting it and editing the properties which are displayed in the right hand pane under the **Message Design** and the **Message Text** tabs.

8.2. Message Boxes

Message boxes provide an effective way of alerting the user before an *action* is performed. For example, advising that an application launch has been blocked or allowed or that anauthorization request has been granted.

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

Message boxes are assigned to application rules.

Message Description

You may set a description for a message by accessing the properties for a message:

1. Right-click the **Message** in the tree pane and select **Properties**.
2. Set the **Description** in the **Properties** dialog.
3. Click **OK**.

8.2.1. 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 be updated. To test the message box use the preview facility (program and content information will contain appropriate placeholders).

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

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.

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).

- **User Reason Type** – 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.

Authorization Settings

- **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 **"…"** 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.

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.

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.

8.2.2. Message Text

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

As you change the message text the preview message will automatically be updated, based on the selected language. To test the message box simply click the preview message (any program or content information will contain placeholders).

8.2.3. 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. Click in the languages drop-down list and click **Add a Language…**.
2. The **Insert Language** dialog will appear.
3. Select the relevant language (and region) from the drop-down box.
4. Click **OK**.

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 **Make this the default language**.

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 to the default language. You must always have at least one language defined.

Setting the Message Text

It is highly recommended that you change the default text strings, as many are simply placeholders, and all are 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.

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

Changing the pre-defined Drop-down User Reasons

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. Click the '**…**' button to the right. The **Approved Reasons** dialog will be displayed.
3. Use the **Add** and **Remove** buttons to edit the **Approved 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. It is highly recommended 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.

8.2.4. Image Manager

The Image Manager associated with message creation allows you to **Add**, **Modify**, **Export** 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 only accessible when the **Background Type** field on the **Message Design** tab is set to **Custom Image**. The **Custom Image** field is then enabled. Click the '**...**' button to the right. The **Manage Images** dialog will be displayed.

To add an image to a message:

1. Click **Add**.
2. The **Image Properties** dialog will appear.
3. Click **Import**.
4. Browse for an image and click **Open**.
5. Set a description for the image.
6. Click **OK**.

To modify an image:

1. Select the image in the list and click **Modify**.
2. The **Image Properties** dialog will appear.
3. Click **Import**.
4. Alter the description and click **OK**.

To export an image:

1. Select the image in the list and click **Export**.
2. Browse to a folder and click **Save**.

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.

8.2.5. 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. Right-click the **Defendpoint Settings** node and choose **Set Challenge / Response Authorization Key...**.

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:

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

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 Defendpoint Management Console.

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:

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

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 Privilege Guard 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**.

Note: PGChallengeResponseUI.exe is a standalone utility and can be distributed separately to the Defendpoint Management Console.

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:

```
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
```

9. Defendpoint Settings Management

Defendpoint for Mac allows you to deploy the Defendpoint Settings to a Mac client computer using an XML file. You will need to employ a suitable deployment mechanism to distribute the XML file to your client computers.

You must name the settings file **`pguard.xml`** once it is deployed, otherwise the Defendpoint Client will not load the settings. If you make changes to the Defendpoint Settings, simply redeploy the modified XML file and the Defendpoint Client will automatically reload the settings.

For information see the Adding Defendpoint Settings to a Mac Client computer section.

9.1. Exporting and Importing Settings

The Defendpoint Settings will need to be exported to an XML file for distribution to the Mac client computers.

To export the Defendpoint Settings to an XML file:

1. Select the **Defendpoint Settings** node.
2. Right-click and select **Export…**.
3. Select an appropriate destination for the exported XML file.

To import the Defendpoint Settings from an XML file:

1. Select the **Defendpoint Settings** node.
2. Right-click and select **Import…**.
3. Select the appropriate XML file.
4. When prompted, either click **Yes** to merge the imported settings into the current settings or **No** to overwrite the current settings.

9.2. Adding Defendpoint Settings to a Mac Client computer

To add the Defendpoint settings to a Mac computer:

1. Logon to the Mac computer using your admin account.
2. Browse to the location of the Defendpoint Settings file (*pguard.xml*) and copy the file to the Mac desktop.
3. From the Terminal application type the following command:

```
sudo cp ~/Desktop/pguard.xml /etc/pguard/pguard.xml
```

4. Press **Enter** and submit your admin credentials. The file will be copied into the folder **`/etc/pguard/`** on the Mac computer, overwriting any existing file of the same name.

As soon as the **`pguard.xml`** file is placed in this folder Defendpoint is active on the Mac computer.

Note: Overwriting the /etc/pguard/pguard.xml config file is an allowed and accepted method of updating the Defendpoint Settings. Do note delete the pguard.xml file as this will interfere with the client machine's ability to enforce policy. If the guard.xml file is deleted from a client machine, replace the file and restart the machine.

9.3. Deleting Defendpoint Settings

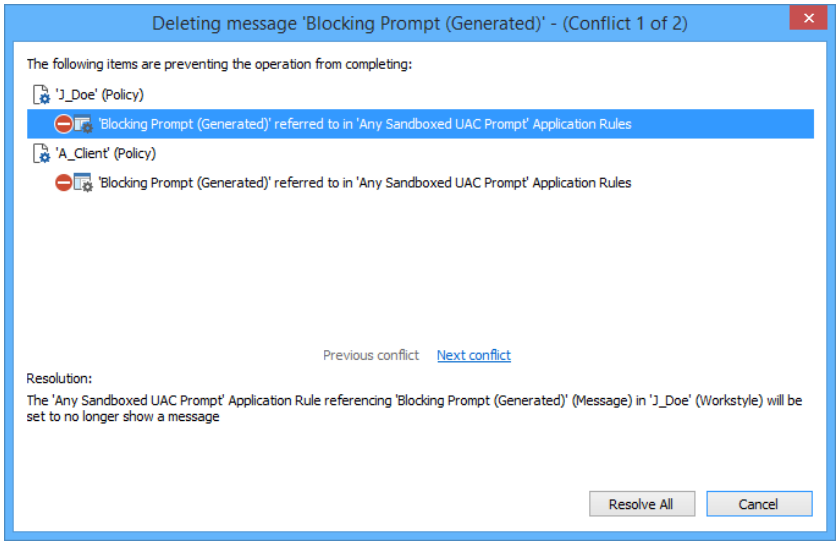
To delete Defendpoint Settings:

1. Select the **Defendpoint Settings** node and from the details pane click **Delete…**.
2. When prompted for confirmation, click **Yes** to delete the Defendpoint Settings.

9.4. Deleting Items and Conflict Resolution

Some items within the Defendpoint Settings are referenced in other areas, such as **Application Groups** and **Messages**. These items can be deleted at any time, and if they are not being referenced elsewhere, they delete without any further action required.

When an item is deleted, the Defendpoint Console will check for any conflicts which may need to be resolved. If the item being deleted is already in use elsewhere in your settings, then a conflict will be reported which will need to be resolved.



You can review each detected conflict and observe the automatic resolution which will take place if you proceed. If more than 1 conflict is reported, use the **Next conflict** and **Previous conflict** links to move between conflicts.

If you wish to proceed, click **Resolve All** to remove the item from the areas of your Defendpoint Settings where it is currently in use.

10. Event Reporting

10.1. Events

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

The following events are logged by the Defendpoint Client:

10.1.1. Process Events

Event ID	Description
100	Process has started with admin rights added.
106	Process has started with no change.
116	Process execution was blocked.
117	Process was stopped terminated.
120	Process execution was cancelled by the user
199	Process execution was blocked, the maximum number of challenge/response failures was exceeded.

Each process event contains the following information:

- FileName
- ProcessId
- ParentProcessId
- Workstyle
- ApplicationGroup
- Reason
- FileHash

10.1.2. Configuration Events

Event ID	Description
10	Defendpoint not licensed for configured action
200	Successfully loaded Defendpoint configuration (information)
201	Loaded Defendpoint configuration but encountered non-critical problem (warning)
202	Failed to load Defendpoint configuration (error)
210	Successfully downloaded Defendpoint configuration

10.1.3. User / Computer Events

Event ID	Description
400	Defendpoint Service started (information)
401	Defendpoint Service stopping (Information)

11. Troubleshooting

11.1. General Troubleshooting Tips

11.1.1. 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 that the Defendpoint logo is present in the OS X Status menus on the menu bar as shown below.

11.1.2. Check Settings are licensed

One of the most common reasons for Defendpoint not functioning is the omission of a valid license from the Defendpoint Settings. To avoid problems it is simpler to add a valid license to every set of Defendpoint Settings that you create. If Defendpoint is not licensed an event will be raised in the syslog.

11.1.3. Check Workstyle Precedence

Assuming that Defendpoint is functioning and licensed, most other problems are caused by configuration problems or workstyle precedence problems.

Once an application matches an application group entry in the **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 Application rules in a workstyle then entries higher in the list have a higher precedence.

Appendices

- **Appendix 1** – Built-in Groups
- **Appendix 2** – Target Definitions
- **Appendix 3** – Regular Expressions
- **Appendix 4** – Application Templates
- **Appendix 5** – Debug Logging

Appendix 1. Built-in Groups

Defendpoint includes a number of built-in groups that may be used in any Application rule. These groups provide a simple and convenient way of applying broad rules to applications, in particular when defining 'catch-all' rules. Built-in groups also help to simplify your configurations by reducing the amount of groups.

Group	Criteria	Valid Types
Apps in system locations (Generated)	All applications located in trusted system locations	Binaries and Bundles
Apps in system locations that request authorization (Generated)	All applications in located trusted system locations that will trigger an authorization request	Bundles and System Preference Panes
Apps that are allowed	Applications that you choose to allow to execute	Binaries, Bundles, Packages and System Preference Panes
Apps that are automatically authorized	Any applications that request authorization from OS X and you choose to automatically authorize	Binaries, Bundles, Packages and System Preference Panes
Apps that are blocked	Applications that you choose to block execution	Binaries, Bundles, Packages and System Preference Panes
Any other apps (Generated)	Any other applications not specified in the other generated groups	Binaries, Bundles, Packages and System Preference Panes

Appendix 2. Application Definitions

Application definitions allow you to target applications based on specific properties. When an application is executed, Defendpoint will query the properties of the application and attempt to match them against the definitions in the application group entry. If a match is made, then the rule is applied. If any of the definition do not match, then the rule will not apply and Defendpoint will attempt to match against subsequent rules and workstyles.

The following list describes all of the available Application definitions:

Application requests authorization

Any process that requests authorization from the operating system. Applications are validated by matching **Auth Request URI**. 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

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. Environment Variables are also supported.

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.

File Hash (SHA-1 fingerprint)

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.

File Version matches

If the file 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.

URI

The Uniform Resource Identifier attached to a Bundle. Applications are validated by matching the URI. You may choose to match based on the following options:

- Match Case
  - No / Yes
- Perform Match Using
  - Exact Match
  - Starts With
  - Ends With
  - Contains
  - Regular Expressions

Appendix 3. Regular Expressions

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.

Metacharacter	Meaning
Any character except [\^$.|?*+()	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)
\ (backslash)	Escape character: interpret the next character literally.
. (dot)	Matches any single character.
[ ]	Indicates a character class. Matches any character inside the brackets (for example, [abc] matches "a", "b", and "c").
^ (caret)	If this metacharacter occurs at the start of a character class, it negates the character class. A negated character class matches any character except those inside the brackets (for example, [^abc] matches all characters except "a", "b", and "c"). If ^ is at the beginning of the regular expression, it matches the beginning of the input (for example, ^[abc] will only match input that begins with "a", "b", or "c").
- (minus character)	In a character class, indicates a range of characters (for example, [0-9] matches any of the digits "0" through "9").
?	Indicates that the preceding expression is optional: it matches once or not at all (for example, [0-9][0-9]? matches "2" and "12").
+	Indicates that the preceding expression matches one or more times (for example, [0-9]+ matches "1", "13", "666", and so on).
*** (asterisk)**	Indicates that the preceding expression matches zero or more times
| (vertical pipe)	Alternation operator: separates two expressions, exactly one of which matches.
??, +?, *?	Non-greedy versions of ?, +, and *. These match as little as possible, unlike the greedy versions which match as much as possible. Example: given the input "<abc><def>", <.*?> matches "<abc>" while <.*> matches "<abc><def>".

( )	Grouping operator. Example: (\d+,)*\d+ matches a list of numbers separated by commas (such as "1" or "1,23,456").
{ }	Indicates a match group. The actual text in the input that matches the expression inside the braces can be retrieved through the CAtlREMatchContext object.
****	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). Example: <{.*?}>.*?</\0> matches "<head>Contents</head>". Note that in C++ string literals, two backslashes must be used: "\\+", "\\a", "<{.*?}>.*?</\\0>".
$	At the end of a regular expression, this character matches the end of the input. Example: [0-9]$ matches a digit at the end of the input.
|	Alternation operator: separates two expressions, exactly one of which matches (for example, T|the matches "The" or "the").
!	Negation operator: the expression following ! does not match the input. Example: a!b matches "a" not followed by "b".

For more information, see
http://msdn.microsoft.com/en-us/library/k3zs4axe(v=vs.71).aspx

Appendix 4. Application Templates

Defendpoint ships with some standard application templates to simplify the definition of applications. The standard application templates are split into three categories:

- Binaries
- Bundles
- System Preference Panes

A 4.1. Creating Custom Application Templates

Application templates are stored as XML files in:

```
%ALLUSERSPROFILE%\Application Data\Avecto\Privilege Guard Templates\
```

The Standard Application Templates are stored in a single file named **`OSXTemplates.xml`**, and it is highly recommended that you do not change these templates.

Instead, you should create your own XML template files. Application templates are simply a set of Application groups that have been exported from the Defendpoint Management console as an XML file.

To create a set of application templates, simply create some Application groups and populate the Application groups with applications. The Application groups will become the Categories, and the applications in each application group will be the list of Applications for that Category. Once you have defined your application templates, simply export the settings to an XML file:

1. Select the **Defendpoint Settings** node.
2. Right-click and select **Export…**.

Note: The XML file that you export must be saved with a prefix of OSX e.g. OSX_My_Templates.xml

To import an application template file back into the management console for editing:

1. Select the **Defendpoint Settings** node.
2. Right-click and click **Import…**.
3. When prompted click **No** to overwrite the current workstyles.

Remember to re-export your application templates once you've modified them.

The final step is to copy your application templates to the application templates directory on any machines where the management console is being used to create Defendpoint settings. The management console automatically loads all of the application templates in the application templates directory and merges them to create a single list of categories.

Appendix 5. Debug Logging

All logging, apart from Auditing, is disabled by default. To enable debug logging open a terminal and execute the command:

```
sudo /usr/local/libexec/Avecto/Defendpoint/1.0/configure/installdbglogs.sh
```

No restart is required. Once debug logging has been enabled Defendpoint will log debug data to the following log files:

- **/private/var/log/pguard/pgdaemon.log**
- **/private/var/log/pguard/pggui.log**
- **/private/var/log/pguard/pgpolicyserver.log**

To disable debug logging open a terminal and execute the command:

```
sudo /usr/local/libexec/Avecto/Defendpoint/1.0/configure/uninstalldbglogs.sh
```

No restart is required. Existing debug log files will not be removed however it is safe to manually remove them if required.

Note: When a 3rd party preference is passively audited, it will also be audited as a bundle application type. Use the audit log to identify the **type** that an application should be targeted as in an application rule.