Defendpoint for Mac 4.1 Release Notes

1.1. Supported Operating Systems

1.1.1. Defendpoint for Mac Client

- **Platforms**
  - Mac OS X 10.10 Yosemite
  - Mac OS X 10.11 El Capitan

1.1.2. Defendpoint Management Console

- **Platforms**
  - Windows XP SP3+
  - Windows Vista
  - Windows 7
  - Windows 8 / 8.1
  - Windows 10
  - Windows Server 2003
  - Windows Server 2008 / R2
  - Windows Server 2012 / R2

1.2. Prerequisites

1.2.1. For the Defendpoint Management Console:

- Microsoft Core XML Services 6.0 (XP SP2 only)
- Microsoft Visual C++ 2013 Redistributable
- Microsoft Group Policy Management Console (for Active Directory integration)

Note:

The executable version of the Management Console installation package includes all necessary prerequisites (excluding the Group Policy Management Console), and will automatically install them as necessary.

1.3. New 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 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 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.