



ASU McAfee Usage and Administration Standard

Version 0.1
May 2009

Table of Contents

1 PURPOSE	3
2 SCOPE	3
3 ENVIRONMENTS	3
4 AVAILABLE SOFTWARE	3
5 STANDARD	3
5.1 Deskside Support	3
5.1.1 <i>EPO Agent</i>	3
5.1.2 <i>McAfee Software Distribution on Desktops</i>	4
5.1.3 <i>McAfee Software Support</i>	4
5.1.4 <i>OU Tree</i>	4
5.1.5 <i>OU Policies</i>	4
5.2 University Technology Office: Operations	4
5.3 University Technology Office: Information Security Office	4
6 APPENDIX A	6

1 PURPOSE

The purpose of this document is to define administrative duties and responsibilities regarding the University endorsed McAfee software.

2 SCOPE

The standard set in this document will apply to the following Organizational Unit (OU) responsible for administrative tasks regarding McAfee ePolicy Orchestrator:

- Deskside support groups defined throughout the University
- The University Technology Office (UTO) Operations and Security Group (Ops)
- The Information Security Office

3 ENVIRONMENTS

Environments impacted by the McAfee product are ASU owned servers, desktops and laptops. The servers running the product are as follows:

- Development – <https://mcafeedev1.asu.edu:8443>
- Production – <https://mcafeeprod1.asu.edu:8443>

4 AVAILABLE SOFTWARE

The following items are McAfee licensed products available to the University:

- McAfee Total Protection Endpoint - Adv.
 - AntiSpyware Enterprise Module v8.7
 - Host Intrusion Prevention v7.0
 - NetShield for Netware v4.63
 - SiteAdvisor Enterprise 1.6
 - SiteAdvisor Enterprise Plus v2.0
 - VirusScan Command Line Scanners
 - VirusScan Enterprise v8.7i
 - Anti-Spam Activation for GSD v7.0
 - Anti-Spam Activation for GSE v7.0
 - Anti-Spam Activation for GSE v7.0.1
 - Anti-Spam Activation for MSDL, v7.5 on Linux
 - ePO roll out package for the SpamKiller 2.1
 - GroupShield 6.0.2 for Microsoft Exchange 2000/2003
 - GroupShield 6.0.3 for Microsoft Exchange 2007
 - GroupShield 7.0.1 for Microsoft Exchange 2003/2007
 - SpamKiller Version 2.1.2 for Microsoft Exchange 2000 / 2003
 - SpamKiller Version 2.1.3 for Microsoft Exchange 2007
 - WebShield SMTP 4.5 MR3 (ePO 3.6.x Only)
- McAfee VirusScan for Mac
- McAfee VirusScan for NetApp

5 STANDARD

The following sections define the standard the University will abide by in regards to support and usage of the McAfee ePolicy Orchestrator product.

5.1 Deskside Support

5.1.1 EPO Agent

Deskside support is responsible for making sure the ePO agent is installed on all systems that will be utilizing any McAfee product provided by the University. The agent acts as communication for

enforcing general base policies set by the Information Security Office and receiving the latest DAT updates from the McAfee site. Deskside support will be given access in the EPO interface to wake up agents, create agent tasks, delete clients, and create and view reports.

5.1.2 McAfee Software Distribution on Desktops

Deskside support is to determine which McAfee software should be placed onto desktops in supported areas. The appropriate governance area (e.g. Deskside Summit, TAG MAC group, WNUG, etc.) should determine decisions regarding software versioning. When an agreement regarding software has been made, the proper deskside manager should submit a formal request to Ops and the Change Management Board to obtain and install the software onto the EPO Server.

Deskside groups are permitted to configure the software deployment client tasks and choose where to apply them, thus allowing them to choose the targets for deployment. Note that Ops will not be actively participating in software deployment

5.1.3 McAfee Software Support

Deskside support is responsible for the troubleshooting of the McAfee Agent and all McAfee software deployed via the Agent on the workstation. Deskside will be given access to view logs and initiate server-agent communication from the EPO Server to aid in this support role. Operations will provide a second tier support model for the deskside companies as defined in section 5.2.

5.1.4 OU Tree

The EPO system tree will be populated and defined based on the OU LDAP/AD structure. Systems are automatically moved to the appropriate EPO branch based on their location in AD. If the machines are moved to another branch, they will be moved back by the hourly synchronization task. Systems not belonging to an OU will be automatically placed in the Lost and Found branch for their responsible deskside support groups to manage. Deskside managers will be granted permissions to manipulate computer objects, create group folders not synchronized with AD, and client tasks on all branches in EPO via inherited permissions granted at the EPO root. As such, more granular administration privileges to sub-branches will not be granted.

5.1.5 OU Policies

McAfee software is managed via policies. The policy settings are defined by the Information Security Office with consultation from the deskside companies. If changes to the policies are required, the deskside groups will bring the requested changes to the attention of the Information Security Office. All changes performed must first be approved by the Change Management Board. The Information Security Office will define which EPO policy changes need to be made and will work with Ops and Change Management to get the changes put into place. The Information Security Office will provide final sign-off on all changes after a review of the implementation. The configuration of base policies can be found in Appendix A.

5.2 University Technology Office: Operations

Operations is tasked with maintaining availability of the McAfee EPO server. These tasks include maintaining user logins and delegating roles, the AD synch, scheduling server tasks, and any other tasks specifically relating to the EPO server. In addition, Ops will work with the deskside companies as Tier 2 support for issues regarding agent to server communications, failed software updates, or other EPO server related tasks. Changes to the EPO server should go through the proper Change Management Process.

5.3 University Technology Office: Information Security Office

Policy changes will be defined, documented, and configured by an Information Security Office representative. Prior to policy changes, the Information Security Office should make a request to

the Change Management Board. Upon approval of the change, the Information Security Office should submit a request for implementation of the changes to the Operations MSS group.

6 APPENDIX A