



Blue Coat Malware Analysis Appliance 4.2.11 Administration Guide

2/2/2017



Copyright © 2017 Symantec Corp. All rights reserved. Symantec, the Symantec Logo, the Checkmark Logo, Blue Coat, and the Blue Coat logo are trademarks or registered trademarks of Symantec Corp. or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE. SYMANTEC CORPORATION PRODUCTS, TECHNICAL SERVICES, AND ANY OTHER TECHNICAL DATA REFERENCED IN THIS DOCUMENT ARE SUBJECT TO U.S. EXPORT CONTROL AND SANCTIONS LAWS, REGULATIONS AND REQUIREMENTS, AND MAY BE SUBJECT TO EXPORT OR IMPORT REGULATIONS IN OTHER COUNTRIES. YOU AGREE TO COMPLY STRICTLY WITH THESE LAWS, REGULATIONS AND REQUIREMENTS, AND ACKNOWLEDGE THAT YOU HAVE THE RESPONSIBILITY TO OBTAIN ANY LICENSES, PERMITS OR OTHER APPROVALS THAT MAY BE REQUIRED IN ORDER TO EXPORT, RE-EXPORT, TRANSFER IN COUNTRY OR IMPORT AFTER DELIVERY TO YOU.

Americas:

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

Rest of the World:

Symantec Limited
Ballycoolin Business Park
Blanchardstown, Dublin 15, Ireland

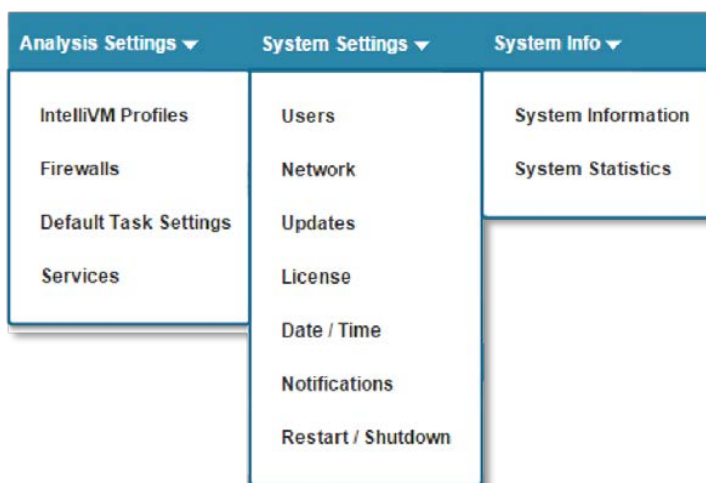
Table of Contents

1. Initial Setup	7	<i>7.2. Create a New Firewall.....</i>	<i>32</i>
1.1. Assumptions	7	8. Plugins	34
1.2. Requirements	7	8.1. Plugin Structure.....	34
2. Network Setup	8	8.2. General Example.....	35
2.1. Network Configuration.....	9	8.3. Proc Dump Example.....	35
3. Basic Actions	11	9. Enhance Analysis with Services.....	38
3.1. Change Password.....	11	9.1. Reputation.....	38
3.2. Log Out.....	11	9.2. VirusTotal.....	38
3.3. Restart or Shutdown.....	11	9.3. YARA.....	39
4. Base Images.....	12	9.4. Advanced Features.....	40
4.1. Activating Base Images	12	10. MAA Updates.....	43
5. iVM Profiles.....	15	10.1. Update Settings.....	43
5.1. Build a New Profile.....	15	10.2. Check for Updates.....	44
5.2. Disable Automatic Update Checks	19	10.3. Offline Updates.....	45
5.3. Application Installation.....	21	11. Define Access with User Roles.....	47
5.4. Finalize and Build the Profile.....	22	11.1. Create Users.....	47
5.5. Modifying Profiles.....	23	11.2. User Role Privileges Matrices.....	49
5.6. Deleting Profiles.....	23	11.3. Generate API Keys.....	52
5.7. EMET.....	24	12. Licensing	54
6. Default Task Settings	27	13. Storage Options.....	54
6.2. IntelliVM Options.....	27	13.1. Internet Cloud Storage.....	54
6.3. SandBox Options.....	28	13.2. Local Serialized Storage.....	54
6.4. MobileVM Options.....	29	13.3. Local Database Storage.....	54
7. Task Firewalls	30	14. Mag2.py Utility	55
7.1. Modify Existing Firewalls.....	30	14.1. Analyzing a ZIP Archive.....	55

15. Health System	56
15.1. Health State	56
15.2. Health Stats.....	57
15.3. Health Rules.....	58
16. System Time	59
16.1. Configure the Local Time Settings.....	59
16.2. Enable / Add NTP Servers.....	59
17. Monitoring and Event Logging.....	61
17.1. Enable Syslog.....	61
17.2. Enable SNMP Polling.....	61
18. Appendix.....	64
18.1. System Processes	64
18.2. Syslog Raw Output.....	64
18.3. Create a Customer SSL Certificate and Key with CLI.....	66
19. Terms of Agreement	67
19.1. Base Image License Terms.....	67

About this Guide

This manual is intended for users with [Administrator](#) or [Sysconfig](#) permissions on the Blue Coat Malware Analysis Appliance (MAA). The functions that are found under the **Analysis Settings**, **System Settings**, and **System Info** menus are addressed.



This manual assumes that the reader is well versed in network terminology and operations, and is familiar with malware in general and malware analysis in particular. An understanding of Windows system events and network intrusion techniques is helpful as well.

System Requirements

The Malware Analysis appliance contains all of the necessary hardware, software, and connectivity needed to analyze malware in isolated or networked environments.

Suggested Browsers

The following browsers support the Malware Analysis appliance user interface:

Browser	Version
Google Chrome	44.0.2403.130 m (Windows)
Firefox	40.0.3 (Windows)
Safari	9.0 (10601.1.56.2) (Mac OS)
Opera	32.0.1948.69 (Windows)
Internet Explorer	11.0.9600

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.