

# **Blue Coat Malware Analysis Appliance 4.2.4 Administration Guide**

4/21/2015

© 2015 Blue Coat Systems, Inc. All rights reserved. BLUE COAT, PROXYSG, PACKETSHAPER, CACHEFLOW, INTELLIGENCECENTER, CACHEOS, CACHEPULSE, CROSSBEAM, K9, DRTR, MACH5, PACKETWISE, POLICYCENTER, PROXYAV, PROXYCLIENT, SGOS, WEBPULSE, SOLERA NETWORKS, DEEPSEE, DS APPLIANCE, CONTENT ANALYSIS SYSTEM, SEE EVERYTHING. KNOW EVERYTHING., SECURITY EMPOWERS BUSINESS, BLUETOUGH, the Blue Coat shield, K9, and Solera Networks logos and other Blue Coat logos are registered trademarks or trademarks of Blue Coat Systems, Inc. or its affiliates in the U.S. and certain other countries. This list may not be complete, and the absence of a trademark from this list does not mean it is not a trademark of Blue Coat or that Blue Coat has stopped using the trademark. All other trademarks mentioned in this document owned by third parties are the property of their respective owners. This document is for informational purposes only.

BLUE COAT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. BLUE COAT 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

Blue Coat Systems, Inc.  
420 N. Mary Ave.  
Sunnyvale, CA 94085

#### APAC

Blue Coat Systems, Inc.  
260 Orchard Road  
# 15-01, The Heeren  
Singapore 238855

#### Rest of the World

Blue Coat Systems International SARL  
3a Route des Arsenaux  
3eme Etage  
1700 Fribourg, Switzerland

## Table of Contents

|   |  |
|---|--|
| <b>1. Initial Setup.....5</b>               | <b>10. User Roles.....40</b>                         |
| 1.1. Assumptions.....5                      | 10.1. Create Users.....40                            |
| 1.2. Requirements.....5                     | 10.2. User–Role Privileges Matrix.....41             |
| <b>2. Network Setup .....6</b>              | 10.3. Generate API Keys.....42                       |
| 2.1. Network Configuration.....7            | <b>11. Licensing .....44</b>                         |
| <b>3. Base Images.....8</b>                 | <b>12. Storage Options.....44</b>                    |
| 3.1. Activating Base Images.....8           | 12.1. Internet Cloud Storage.....44                  |
| <b>4. iVM Profiles.....11</b>               | 12.2. Local Serialized Storage.....44                |
| 4.1. Build a New Profile.....11             | 12.3. Local Database Storage.....44                  |
| 4.2. Disable Automatic Update Checks.....15 | <b>13. Mag2.py Utility .....45</b>                   |
| 4.3. Application Installation.....17        | 13.1. Analyzing a ZIP Archive.....45                 |
| 4.4. Finalize and Build the Profile.....18  | <b>14. Health System .....46</b>                     |
| 4.5. Modifying Profiles.....19              | 14.1. Health State.....46                            |
| 4.6. Deleting Profiles.....19               | 14.2. Health Stats.....47                            |
| 4.7. EMET.....20                            | 14.3. Health Rules.....48                            |
| <b>5. Default Task Settings.....23</b>      | <b>15. Appendix: Base Image License Terms.....53</b> |
| 5.2. IntelliVM Options.....23               |  |
| 5.3. SandBox Options.....24                 |  |
| 5.4. MobileVM Options.....25                |  |
| <b>6. Task Firewalls.....26</b>             |  |
| 6.1. Modify Existing Firewalls.....26       |  |
| 6.2. Create a New Firewall.....28           |  |
| <b>7. Plugins.....30</b>                    |  |
| 7.1. Plugin Structure.....30                |  |
| 7.2. General Example.....31                 |  |
| 7.3. Proc Dump Example.....31               |  |
| <b>8. Services.....34</b>                   |  |
| 8.1. Reputation.....34                      |  |
| 8.2. VirusTotal.....34                      |  |
| 8.3. YARA.....35                            |  |
| <b>9. MAA Updates.....36</b>                |  |
| 9.1. Update Settings.....36                 |  |
| 9.2. Check for Updates.....37               |  |
| 9.3. Offline Updates.....38                 |  |

## 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.

| Analysis Settings ▼   | System Settings ▼  | System Info ▼      |
|-----------------------|--------------------|--------------------|
| IntelliVM Profiles    | Users              | System Information |
| Firewalls             | Network            | System Statistics  |
| Default Task Settings | Updates            |                    |
| Services              | License            |                    |
|                       | Date / Time        |                    |
|                       | Notifications      |                    |
|                       | Restart / Shutdown |                    |

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

## Related Documents

- *Blue Coat Malware Analysis Appliance Quick-Start Guide* (included with appliance)
- *Blue Coat Malware Analysis Appliance Analysis Center Guide*
- *Blue Coat Malware Analysis Appliance Remote API User Guide*
- *Blue Coat Malware Analysis Appliance System Configuration Guide*

## Help and Support

We strongly recommend that you read this guide thoroughly before attempting to configure the MAA and that you use it as a reference during installation, configuration, and ongoing usage.

If you encounter any difficulty with the setup or usage of the MAA appliance, please contact your Blue Coat sales representative or sales engineer, or visit our support website at [bluecoat.com/support/technical-support](http://bluecoat.com/support/technical-support).

## 1. Initial Setup

### 1.1. Assumptions

This document assumes that the user has already followed the steps in the *Quick-Start Guide* that was included with the Malware Analysis Appliance (MAA), which means that:

- The MAA has been unboxed
- The MAA has been rack-mounted or properly prepared for rack-mounting
- A network cable has been connected to the management port
- **Optional** — A null-modem cable connects the MAA to a serial terminal

### 1.2. Requirements

- Blue Coat MAA-S400 Series or MAA-S500 Series Malware Analysis Appliance
- System licenses for the Windows operating systems on the VMs
- System licenses for each application that is installed on a VM profile, as required by the vendor

## 2. Network Setup

Figure 1 displays the two possible Internet connections for an MAA: the **Backend** interface and the **Dirty Line** interface.

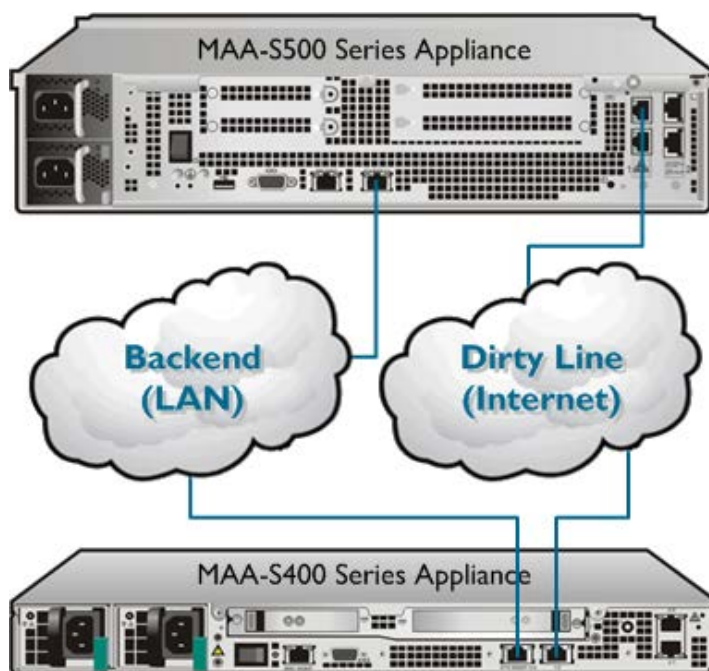


Figure 1 — Rear View: MAA-S500 Series and MAA-S400 Series Appliances

### Backend Interface

The **Backend** interface — the primary interface, called `eth0` by default — is connected to your organization's LAN. The MAA uses this interface for the UI connection, system and pattern updates, and base-image activation.

### Dirty Line Interface

The **Dirty Line** interface — the secondary interface, called `eth1` by default — is used by the VM profiles to access the Internet during analysis. (The SandBox uses an emulated network.) This connection should not pass through your organization's security measures. Any filtering is performed by the [Task Firewalls](#).

## 2.1. Network Configuration

During initial setup, the MAA obtains an IP address for the **Backend** interface via DHCP. To further configure network settings follow these steps:

2.1.1. Select **System Settings > Network**.

2.1.2. In the **Backend Settings** section, do one of the following:

- Select **DHCP**.
  - **Optional** — Specify a new interface name.
- Select **Static**.
  - **Optional** — Specify a new interface name.
  - Specify the IP address, netmask, gateway, and DNS server.

2.1.3. Click **Save Backend Settings**.

2.1.4. In the *Internet Settings (Dirty-line)* section, do one of the following:

- Select **Same as backend**. This option forces the VMs to use the **Backend** interface instead of the **Dirty Line** interface, which means that your organization's security measures are applied to the sample analyses in addition to the task firewalls.
- Select **DHCP**.
  - **Optional** — Specify a new interface name.
- Select **Static**.
  - **Optional** — Specify a new interface name.
  - Specify the IP address, netmask, and gateway.

2.1.5. Click **Save Internet Settings**.

2.1.6. **Optional** — In the *Proxy Settings* section specify a server for the MAA to use when accessing the Internet, for example, when contacting the update server. This proxy is not used by the VMs during activation or during sample analysis.

### 3. Base Images

Base images include complete Windows operating systems along with a number of preinstalled applications or components that are used to facilitate malware detection from various file types. Base images do not run directly within MAA. Instead, they are used to create profiles that actually run within the IntelliVM virtual machine framework.

Four (4) base images ship with MAA 4.2.x:

- Windows XP, Service Pack 3 (32-bit)
- Windows 7, Service Pack 1 (32-bit)
- Windows 7, Service Pack 1 (64-bit)
- Windows 8 (64-bit)

Also see [Appendix: Base Image License Terms](#)

---

**Note** Base images are installed at the factory; users cannot add new base images. However, users can create an unlimited number of custom profiles that are derived from the existing base images.

---

#### 3.1. Activating Base Images

Before you can build a profile on a base image, you must activate the base image with a license key.

3.1.1. Log in to the MAA web interface with Administrator credentials.

3.1.2. Select **Analysis Settings > IntelliVM Profiles**. The *IntelliVM Profiles* page is displayed.

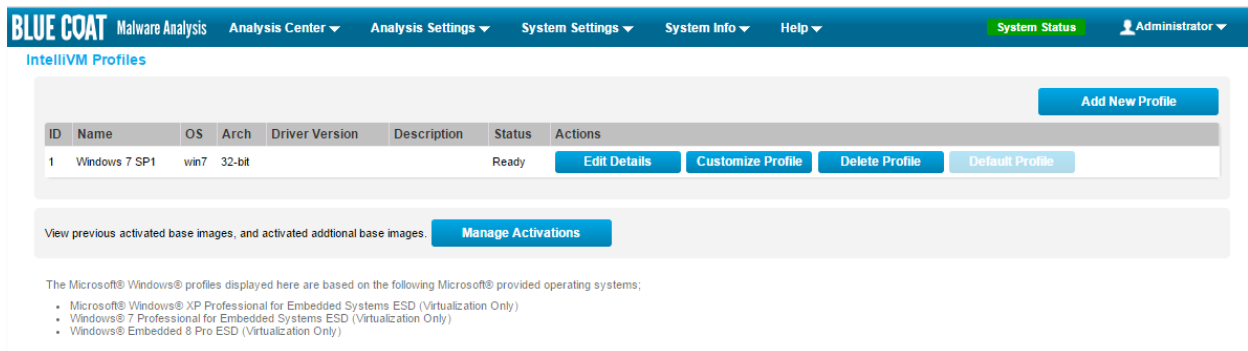
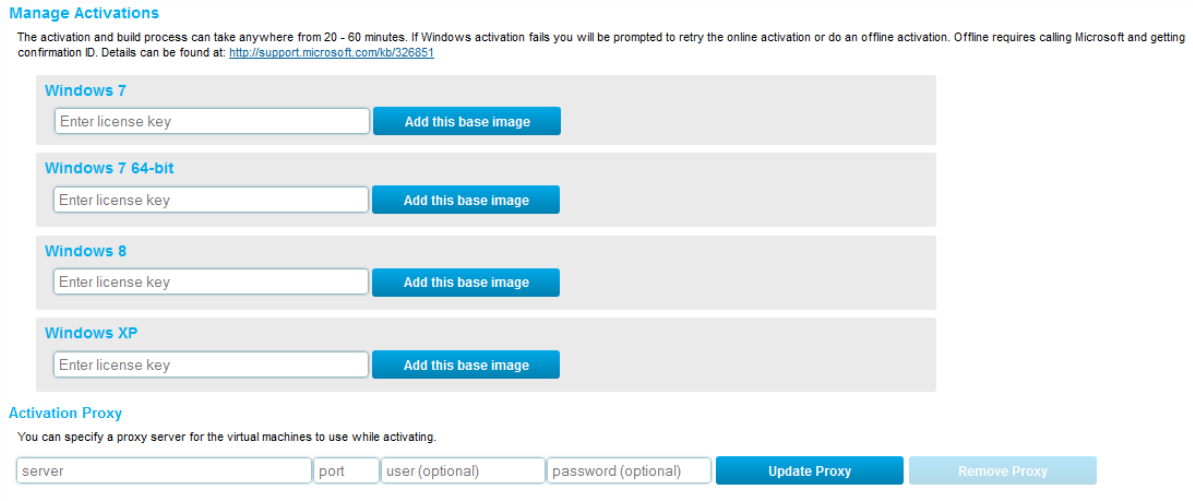


Figure 2 — IntelliVM Profiles



3.1.3. Click **Manage Activations**. The **Manage Activations** page is displayed.



**Manage Activations**

The activation and build process can take anywhere from 20 - 60 minutes. If Windows activation fails you will be prompted to retry the online activation or do an offline activation. Offline requires calling Microsoft and getting confirmation ID. Details can be found at: <http://support.microsoft.com/kb/326851>

**Windows 7**

Enter license key

**Windows 7 64-bit**

Enter license key

**Windows 8**

Enter license key

**Windows XP**

Enter license key

**Activation Proxy**

You can specify a proxy server for the virtual machines to use while activating.

server  port  user (optional)  password (optional)

Figure 3 — Manage Activations Page

3.1.4. As needed, specify a proxy server that the iVMs can use to access the internet while activating the base images.

- **server** — IP number or hostname of the proxy server
- **port** — Port number of the server
- **user** — (optional) username to log on to the server
- **password** — (optional) password for the username

3.1.5. Click **Update Proxy** to save the settings.

- 3.1.6. Enter a license key for a base image and click **Add this base image**. The activation and build process will take 20–60 minutes.

**Manage Activations**

The activation and build process can take anywhere from 20 - 60 minutes. If Windows activation fails you will be prompted to retry the online activation or do an offline activation. Offline requires calling Microsoft and getting confirmation ID. Details can be found at: <http://support.microsoft.com/kb/326851>

|  |                            |
|--|----------------------------|
| <b>Windows 7</b>   | <b>Base Activated</b>      |
| This base image has profiles. If you want to remove this base image, first remove all profiles from the profile management page. |                            |
| <b>Windows 7 64-bit</b>  |                            |
| <input type="text" value="Enter license key"/>   | <b>Add this base image</b> |
| <b>Windows 8</b>   |                            |
| <input type="text" value="Enter license key"/>   | <b>Add this base image</b> |
| <b>Windows XP</b>  |                            |
| <input type="text" value="Enter license key"/>   | <b>Add this base image</b> |

**Activation Proxy**

You can specify a proxy server for the virtual machines to use while activating.

|                                     |                                   |  |  |                     |                     |
|-------------------------------------|-----------------------------------|--|--|---------------------|---------------------|
| <input type="text" value="server"/> | <input type="text" value="port"/> | <input type="text" value="user (optional)"/> | <input type="text" value="password (optional)"/> | <b>Update Proxy</b> | <b>Remove Proxy</b> |
|-------------------------------------|-----------------------------------|--|--|---------------------|---------------------|

Figure 4 — Base Image Activated

---

**Note** If the activation fails, you may need to perform an offline activation, which requires that you call Microsoft to get a confirmation ID. Consult [Microsoft Knowledge Base document 326851](#) for more information.

---

## 4. iVM Profiles

IntelliVM (iVM) kernel technology monitors system events for signs of malicious behavior in a virtualized environment. Profiles can be customized to add flexibility to analyze non-traditional malware and to precisely mirror custom environments to detect advanced and targeted threats.

Malware Analysis Appliance VMs are software-based emulations of physical computers. The VMs simulate the architecture, functionality, and connections of a standalone workstation or handheld device, but because the environment is not actually connected to a network, any malware that executes on a VM is unable to infect a real device or network.

By using various VM profiles to imitate real environments, analysts can quickly spot behavioral anomalies that are typical of anti-analysis and advanced malware evasion techniques. VMs can easily be set up to match various Windows and Android environments — such as patched and unpatched versions that run a variety of applications, browsers, and plugins — to quickly spot different malicious behaviors on multiple system types. VMs are then easily reverted to a known non-infected state for the next round of testing.

A profile consists of a base image plus customizations to replicate a particular Windows environment. Customizations can include commercial and custom applications, additional web browsers, and patches such as Windows Updates.

You can create, modify, or delete VM profiles as needed to replicate production environments or to test the behavior of malware across different configurations.

### 4.1. Build a New Profile

In this section, instructions are provided to build a new profile called "Sales Win 7."

4.1.1. Log in to the MAA web interface with [Administrator](#) credentials.

4.1.2. Select **Analysis Settings > IntelliVM Profiles**. The *IntelliVM Profiles* page is displayed.

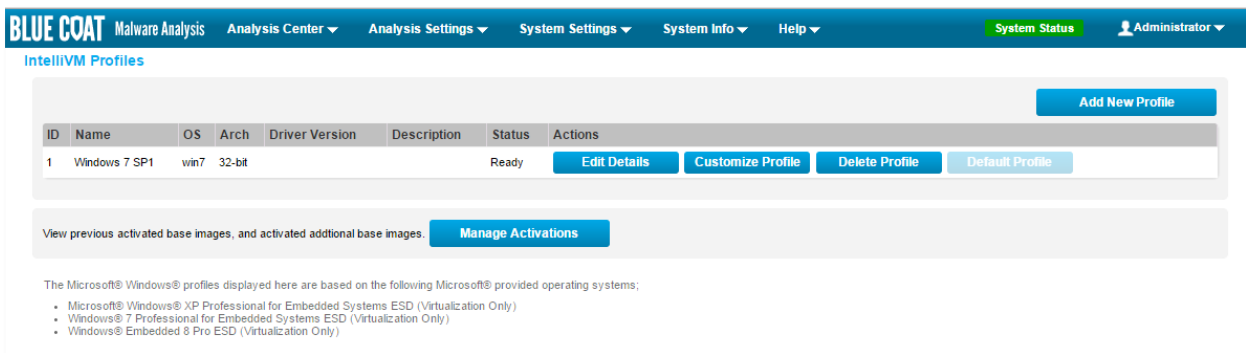
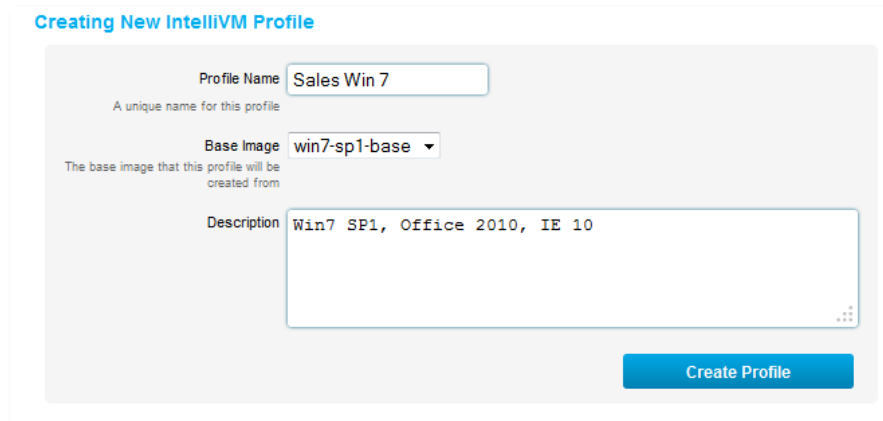


Figure 5 — IntelliVM Profiles Page

4.1.3. The first profile in the list, "Windows 7," was automatically built when the Windows 7 base image was activated. It is also automatically set as the default profile.

4.1.4. Click **Add New Profile**. The *Creating New IntelliVM Profile* page is displayed.



**Creating New IntelliVM Profile**

Profile Name:   
A unique name for this profile

Base Image:   
The base image that this profile will be created from

Description:

**Create Profile**

Figure 6 — Creating New IntelliVM Profile Dialog

4.1.5. For **Profile Name**, type a unique name for the profile.

4.1.6. For **Base Image**, select the desired image. Only the base images that you have licensed are displayed.

4.1.7. **Optional** — For **Description**, add any desired notations.

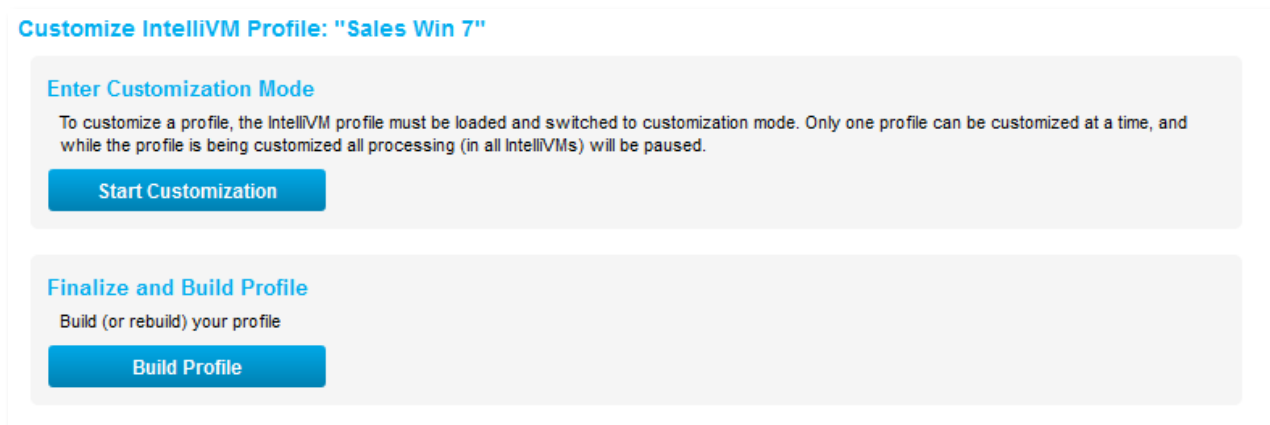
4.1.8. Click **Create Profile**. The *IntelliVM Profiles* page is displayed again, with the new profile in the list.

| ID | Name        | OS   | Arch   | Description                  | Status         | Actions                      |                                   |                                |                                 |
|----|-------------|------|--------|------------------------------|----------------|------------------------------|-----------------------------------|--------------------------------|---------------------------------|
| 1  | Windows 7   | win7 | 32-bit |                              | Ready          | <a href="#">Edit Details</a> | <a href="#">Customize Profile</a> | <a href="#">Delete Profile</a> | <a href="#">Default Profile</a> |
| 2  | Sales Win 7 | win7 | 32-bit | Win7 SP1, Office 2010, IE 10 | Requires Build | <a href="#">Edit Details</a> | <a href="#">Build Profile</a>     | <a href="#">Delete Profile</a> | <a href="#">Set as Default</a>  |

Figure 7 — IntelliVM Profiles List

**Note** Before a profile has been built, you may click **Edit Details** to change the base image. After the profile has been built, you cannot change the base image.

4.1.9. Click **Build Profile**. The *Customize IntelliVM Profile: [Profile Name]* page is displayed



**Customize IntelliVM Profile: "Sales Win 7"**

**Enter Customization Mode**

To customize a profile, the IntelliVM profile must be loaded and switched to customization mode. Only one profile can be customized at a time, and while the profile is being customized all processing (in all IntelliVMs) will be paused.

**Start Customization**

**Finalize and Build Profile**

Build (or rebuild) your profile

**Build Profile**

Figure 8 — Customization and Build Page

4.1.10. Click **Start Customization**.

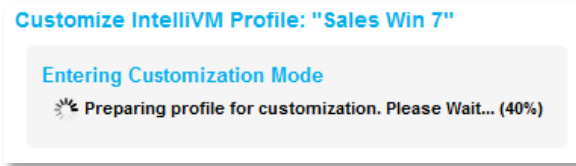


Figure 9 — Entering Customization Mode

4.1.11. Several minutes will elapse while the profile is prepared for customization.

---

**Caution** While you are in customization mode, all processing in all IntelliVMs is suspended.

---



Figure 10 — Manual Customization Message

4.1.12. When the profile is ready for customization, the following message is displayed: [To manually customize your profile you can connect via RDP to on port 3389/tcp. Default login credentials are "admin" with no password.](#)

---

**Note** It is recommended that you not close your browser while customizing a profile.

---

4.1.13. On a Windows workstation, launch Remote Desktop Connection. The *Remote Desktop Connection* dialog is displayed.

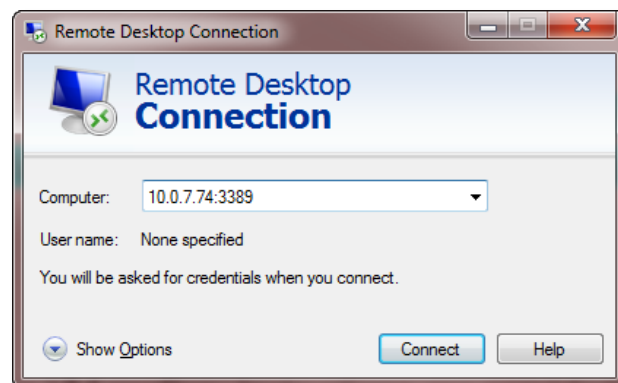


Figure 11 — Remote Desktop Connection Dialog

4.1.14. Click **Show Options**.

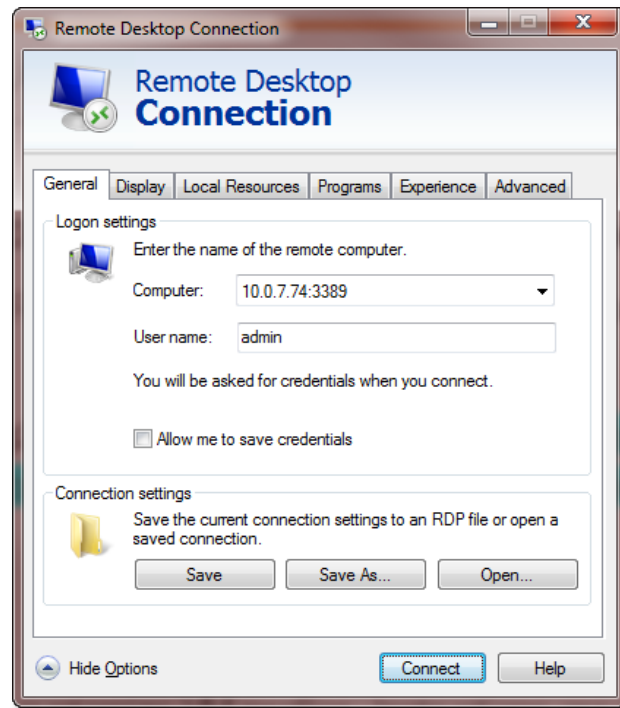


Figure 12 — Expanded Remote Desktop Connection Dialog

4.1.15. For **Computer**, type the IP address of the MAA and the port number in the following format:  
`<ip_address>:3389`.

4.1.16. For **User name**, type `admin`.

4.1.17. Click **Connect**, and then click **OK**. The desktop of the iVM is displayed.

## 4.2. Disable Automatic Update Checks

Before adding any customizations, verify that the applications that are already installed on the iVM are not checking for updates automatically:

- 4.2.1. From the Control Panel in the iVM, select **Windows Update** and verify that updates are not being installed automatically.

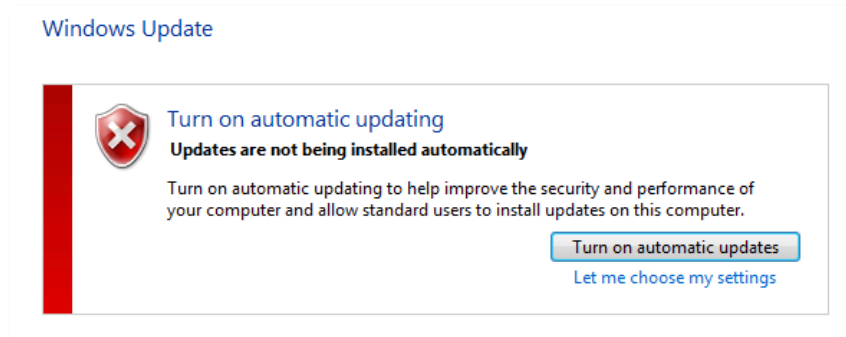


Figure 13 — Windows Update Control

- 4.2.2. Launch the Microsoft Silverlight Configuration dialog.

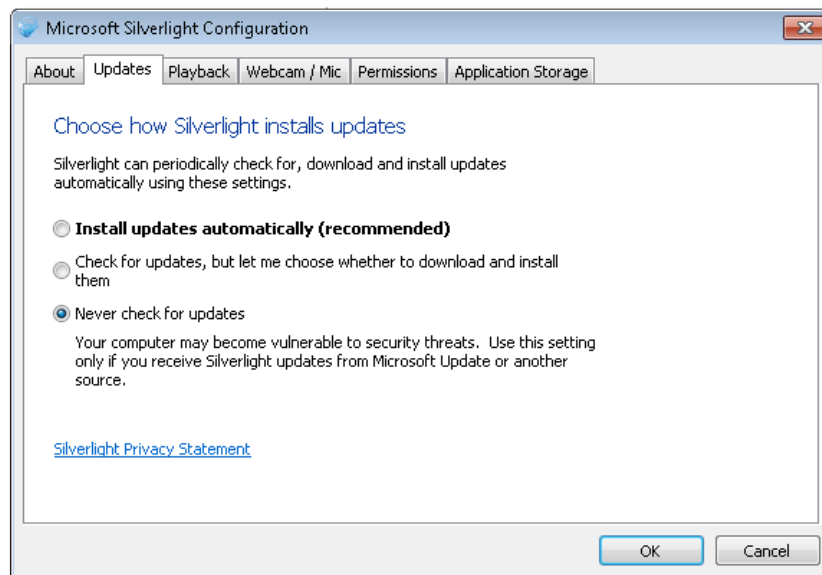


Figure 14 — Silverlight Updates Dialog

- 4.2.3. Click the **Updates** tab, and verify that **Never check for updates** is selected.

- 4.2.4. Launch the Adobe Reader, select **Edit > Preferences**, select **Updater** from the *Categories* list, and verify that **Do not download or install updates automatically** is selected.

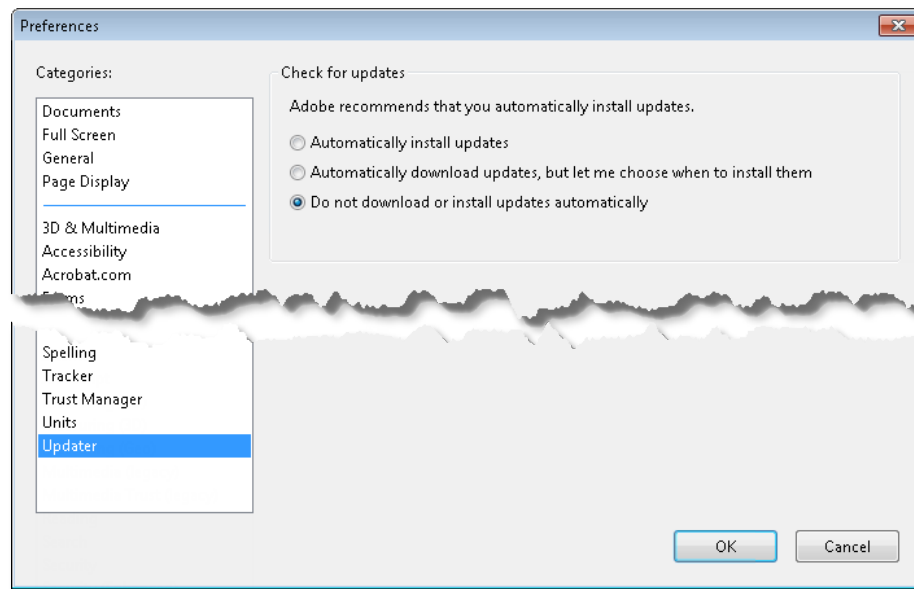


Figure 15 — Adobe Reader Preferences Dialog

- 4.2.5. For any other non-Microsoft applications that are on the iVM or that you later install, verify that the automatic update checks are disabled.
- 4.2.6. Do you want to further customize the iVM profile?

**Yes** — Continue the procedure.

**No** — Go to [Finalize and Build the Profile](#).



### 4.3. Application Installation

---

**Note** The customer is responsible for obtaining the appropriate licenses for software that is installed on the iVMs. Contact the vendors of the respective software to obtain the proper license type for the iVMs.

---

4.3.1. To transfer installation files to your iVM, use one of the following methods:

- From inside the iVM, map a shared network drive or folder.

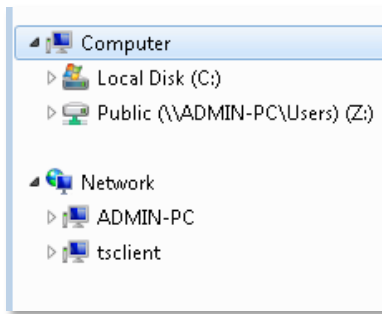


Figure 16 — Network Entities on the iVM

- Connect to the Internet to download software from an Internet resource or vendor site. (This connection is made through the **Backend** interface.)

---

**Note** To use a different proxy to access the Internet from inside the iVM, configure that proxy inside the iVM's Windows environment.

---

- The `tsclient` entity is the workstation that is accessing the iVM via Remote Desktop.

4.3.2. Install, license, and configure the applications to resemble a typical computing environment at your organization.

## 4.4. Finalize and Build the Profile

When you have finished customizing the profile, you must finalize and build it.

- 4.4.1. Log out of the Remote Desktop session.
- 4.4.2. Return to the *Customize IntelliVM Profile: [Profile Name]* page on the MAA's Web interface.
- 4.4.3. Click **Build Profile**.



Figure 17 — Profile Building

- 4.4.4. Several minutes will elapse while the profile is being built.
- 4.4.5. When the profile has finished building, select **System Settings > IntelliVM Profiles** to return to the *IntelliVM Profiles* page.

| ID | Name        | OS   | Arch   | Description                  | Status | Actions   |
|----|-------------|------|--------|------------------------------|--------|---|
| 1  | Windows 7   | win7 | 32-bit |                              | Ready  | <a href="#">Edit Details</a> <a href="#">Customize Profile</a> <a href="#">Delete Profile</a> <a href="#">Default Profile</a> |
| 2  | Sales Win 7 | win7 | 32-bit | Win7 SP1, Office 2010, IE 10 | Ready  | <a href="#">Edit Details</a> <a href="#">Customize Profile</a> <a href="#">Delete Profile</a> <a href="#">Set as Default</a>  |

Figure 18 — iVM List

- 4.4.6. The new profile is ready for use. You may begin to send samples to the new profile, or you may select one of the following:
  - **Edit Details** — Return to the *Creating New IntelliVM Profile* page and change the description or name. (You cannot change the base image of an already-built profile.)
  - **Customize Profile** — Click to add further customizations to the iVM profile.
  - **Delete Profile** — Click to delete the profile. This action cannot be undone.
  - **Set as Default** — Click to make this profile your default profile.

## 4.5. Modifying Profiles

You may modify two aspects of a profile: the iVM itself or the iVM's details.

**Note** You cannot change the base image of an already-built profile.

4.5.1. Select **Analysis Settings > IntelliVM Profiles**.

| ID | Name        | OS   | Arch   | Description                  | Status | Actions                      |                                   |                                |                                 |
|----|-------------|------|--------|------------------------------|--------|------------------------------|-----------------------------------|--------------------------------|---------------------------------|
| 1  | Windows 7   | win7 | 32-bit |                              | Ready  | <a href="#">Edit Details</a> | <a href="#">Customize Profile</a> | <a href="#">Delete Profile</a> | <a href="#">Default Profile</a> |
| 2  | Sales Win 7 | win7 | 32-bit | Win7 SP1, Office 2010, IE 10 | Ready  | <a href="#">Edit Details</a> | <a href="#">Customize Profile</a> | <a href="#">Delete Profile</a> | <a href="#">Set as Default</a>  |

Figure 19 — iVM List

- To modify the details, click **Edit Details**. Edit either the profile name or its description, and then click **Save Changes**.

Editing "Sales Win 7" IntelliVM Profile

Profile Name   
A unique name for this profile

Base Image   
The base image that this profile will be created from

Description

[Save Changes](#)

Figure 20 — Editing Details

- To modify a profile, click **Customize Profile**, and then follow the instructions in steps 4.1.11 through 4.1.17 to access the iVM through Remote Desktop. When you have finished the modifications, you must build the profile again.

## 4.6. Deleting Profiles

4.6.1. To delete a profile select **Analysis Settings > IntelliVM Profiles**.

**Caution** Deleting a profile cannot be undone. If you do not intend to deactivate a particular base image, do not delete the last profile that is associated with that image. Deleting a profile that has tasks assigned to it will result in an **IVM\_Error** when that task reaches the top of the queue.

## 4.7. EMET

Microsoft® Enhanced Mitigation Experience Toolkit (EMET) is a utility that helps prevent vulnerabilities in software from being successfully exploited.

**Note** It is recommended that you first deploy EMET on a new profile to verify that it works as expected.

4.7.1. Download and install .NET Framework 4.0 on the iVM.

**Note** For EMET to work with Internet Explorer 10 on Windows 8, Microsoft KB 2790907 or a more recent version of the Compatibility Update for Windows 8 must be installed.

4.7.2. Download EMET 5.1 and the user-guide PDF from [technet.microsoft.com/security](http://technet.microsoft.com/security) and begin the installation.

4.7.3. On the *EMET Configuration Wizard* page, select **Keep Existing Settings** and click **Finish**.

4.7.4. From the **Start** menu open the EMET GUI.

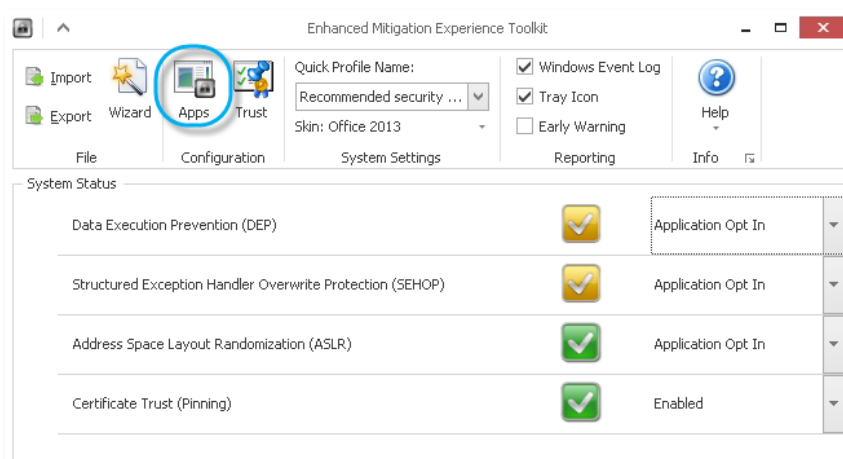


Figure 21 — Apps Button

4.7.5. Click the **Apps** button to open the *Application Configuration* window.

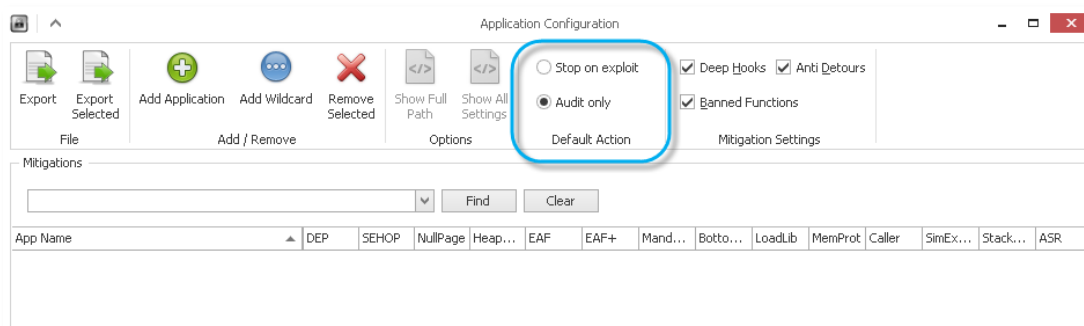


Figure 22 — Default Action

4.7.6. Change the default action to **Audit only**.

4.7.7. Click **Add Application** to add the executables that you want to monitor.

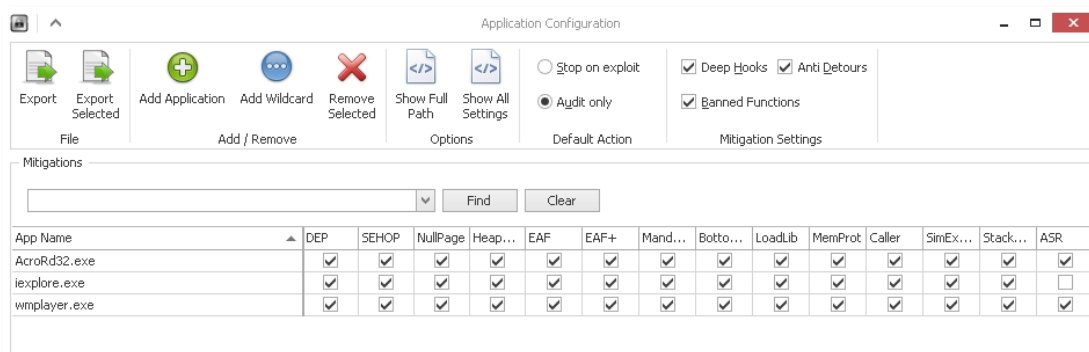


Figure 23 — Adding Applications

4.7.8. For each application, verify that the following features are enabled. (The other default features should be left as-is):

- EAF
- EAF+\*
- LoadLib
- MemProt
- Caller<sup>§</sup>
- StackPivot
- SimExecFlow<sup>§</sup>
- ASR\*

\* Further application settings are required; see the EMET user guide

<sup>§</sup> Applicable only with 32-bit processes

**Note** Some mitigations are not compatible with particular applications. Refer to Microsoft KB 2909257 to verify your settings and clear any incompatible mitigations.

4.7.9. Click **OK** to go back to the EMET default window.

4.7.10. On the iVM, start the applications that you added and click **Refresh**.

| Process ID | Process Name  | Running EMET |
|------------|---|--------------|
| 1380       | AcroRd32 - Adobe Reader 9.4                             | ✓            |
| 1704       | CI5VC - Content Index service                           |              |
| 340        | csrss - Client Server Runtime Process                   |              |
| 1460       | EMET_Service - EMET_Service                             |              |
| 1252       | explorer - Windows Explorer                             |              |
| 1052       | ieexplore - Internet Explorer                           | ✓            |
| 3460       | ieexplore - Internet Explorer                           | ✓            |
| 2888       | inetinfo - Internet Information Services                |              |
| 3428       | wmplayer - Windows Media Player                         | ✓            |
| 3772       | wmpnetwk - Windows Media Player Network Sharing Service |              |

⚠ The changes you have made may require restarting one or more applications


 Refresh

Figure 24 — Running EMET

- 4.7.11. Verify that the processes have a green check in the **Running EMET** column.
- 4.7.12. Close all applications, close the remote desktop session, and build the profile.
- 4.7.13. Verify that EMET works by running some samples that will trigger it. The following MD5 is of a known malware sample: C32AD4D6F6A00C85E6BD152852D5D09F (SimExecFlow and StackPivot).

---

**Note** Blue Coat is not able to provide actual samples because they are genuinely malicious. Visit the [VirusTotal](https://www.virustotal.com/) web site to obtain live malware samples.

---

## 5. Default Task Settings

New in version 4.2.1 is the ability to specify default task settings to be used for automatic sample submission — from the Security Analytics Platform or the Content Analysis System — and for samples that are submitted using the Web UI and RAPI.

---

**Note** Only a subset of available options can be set as defaults.

---

To configure default task settings, follow these instructions:

- 5.1.1. Select **Analysis Settings > Default Task Settings**.
- 5.1.2. For **Environment Type**, select one of the following. Click the item to see which options are available for that environment.
  - [IntelliVM](#) — Emulated Windows XP, 7, or 8 operating system
  - [SandBox](#) — Simulated Windows environment
  - [MobileVM](#) — Emulated Android operating system

### 5.2. IntelliVM Options

- 5.2.1. For **Event Collection**, select one or more checkboxes for the following:
  - **Drop all registry events** — Filter out registry events.
  - **Drop all file system events** — Filter out file system events.
- 5.2.2. Under **IntelliVM Options**, specify the **Execution time limit** in seconds.
- 5.2.3. For **Override file extension**, specify a file extension for the MAA to use if the file types and their extensions do not match.

---

**Note** MAA will detect the actual file type regardless of the extension (e.g., an **EXE** masquerading as a **PDF**) unless an entry is made here. If entered, MAA will treat the sample file(s) as the type entered.

---

- 5.2.4. Select **Get dropped files** to preserve any files that the sample creates. The files are saved as task resources and are automatically scanned by YARA rules.
- 5.2.5. Under *Analytics*, select one or both of the checkboxes for the following:
  - **Create an HTTP Archive resource from the packet capture (HAR)**
  - **Store body of HTTP requests in HAR**

---

**Note** Consult the *MAA Analysis Center Guide* for more information on HAR.

---

- 5.2.6. Click the **Advanced Options** tab.

5.2.7. Use *Execution Arguments* to control how the sample is launched. The default value is `{sample}`, which will be replaced with the fully qualified path of the sample. You can also use this space to pass parameters into IntelliVM plugins. For example:

- `paint.exe {sample}` — Opens the sample in `paint.exe`, regardless of file extension.
- `{sample} --param1 [parameter1]` — Passes values to the sample as it runs. (You would need to know which values the sample requests and in what order.)

5.2.8. For **Guest Path**, type a file path to override the default, which is `c:\Windows\temp`.

5.2.9. Under **Other Options**, select one or more of the checkboxes for the following:

- **Enable task logging** — Creates a task resource that contains debugging information about the task execution.
- **Save prefiltered event data** — Creates a task resource that contains the raw, unfiltered event data as a Google protocol buffer file (binary serialization).

5.2.10. Click the **Plugins** tab.

5.2.11. Select one of the iVM plugins, as desired. Click **View** to see the plugin's code. Following the `.py` extension is the owner of the plugin and the timestamp for the plugin's creation. See [Plugins](#) to see how to create and customize plugins.

- `ghost_user.py` — Emulates advanced user interaction, including navigating dialogs and multi-screen installers.
- `procdump.py` — Dumps the process memory and creates a task resource that is scanned by YARA.
- `example1.py` — Sample plugin that demonstrates the structure of a plugin
- `spyeye.py` — Sample plugin for deeper SpyEye sample analysis
- `run-iexplore.py` — Script for loading a URL into Internet Explorer

5.2.12. When you have selected all of the desired task parameters, click **Save as default**.

### 5.3. SandBox Options

5.3.1. Under *Event Collection*, select one or more checkboxes for the following:

- **Drop all registry events** — Filter out registry events.
- **Drop all file system events** — Filter out file system events.

5.3.2. Under *SandBox Options*, specify the **Maximum SandBox cycle count (in millions)**.

---

**Note** There is no default runtime for a SandBox task. SandBox execution is based upon clock cycles and CPU capabilities of the machine hosting the MAA. Approximately 20 million clock cycles equals one (1) second using modern hardware, where one instruction is processed within each cycle.

---



5.3.3. Select as many of the following checkboxes as desired:

- **Keep all SandBox summary events** — Filter no events (show all)
- **Keep the SandBox raw API events** — Preserve the API trace log in raw format
- **Keep the SandBox text API events** — Preserve the API trace log in text format
- **Generate SandBox PE Dump** — Perform portable executable memory dump
- **Get dropped files** — Preserve any files that the sample creates. The files are saved as task resources that are automatically scanned by YARA rules.

5.3.4. Click the **Advanced Options** tab.

5.3.5. Select one or both of the following checkboxes, as desired:

- **Enable Task Logging** — Creates a task resource that contains debugging information about the task execution.
- **Save Prefiltered Event Data** — Creates a task resource that contains the raw, unfiltered event data as a Google Protocol Buffer (GPB) file, a standard format for binary serialization.

5.3.6. When you have selected all of the desired task parameters, click **Save as default**.

## 5.4. MobileVM Options

5.4.1. Under *Mobile IntelliVM Options*, specify the **Execution time limit** in seconds.

5.4.2. Under *Analytics*, select one or both of the checkboxes for the following:

- **Create an HTTP Archive resource from the packet capture (HAR)**
- **Store body of HTTP requests in HAR**

---

**Note** Consult the *MAA Analysis Center Guide* for more information on HAR.

---

5.4.3. Click the **Advanced Options** tab.

5.4.4. Under **Other Options**, select one or more of the checkboxes for the following:

- **Enable task logging** — Creates a task resource that contains debugging information about the task execution.
- **Save prefiltered event data** — Creates a task resource that contains the raw, unfiltered event data as a Google protocol buffer file (binary serialization).

5.4.5. When you have selected all of the desired task parameters, click **Save as default**.

## 6. Task Firewalls

The MAA provides three (3) firewall options that can be selected on a per-task basis.

- **Isolated** — No network connectivity
- **Limited** — Prevents communications on ports 25 (mail), 139 (NetBIOS), and 445 (SMB)
- **Unlimited** — Full network access

Which firewall setting to use depends on the tradeoffs you are willing to make, as well as your organization's policies and risk tolerance. The more network access you allow, the better fidelity of test results because of the wider range of network activities that are recorded. On the other hand, executing live malware samples carries the risk that the sample will attempt to attack internal or external hosts.

For example, the URL [fixeghoh.koivaino.com](http://fixeghoh.koivaino.com) was subjected to two tasks, one with the **Isolated** firewall setting and the other with the **Unlimited** setting.

### Tasks for this sample

| ID                 | Start                   | State  | Environment           | Runtime         | Risk Score |  |
|--------------------|-------------------------|--|-----------------------|-----------------|------------|--|
| <a href="#">68</a> | 2014-11-25 20:58:33 UTC | Task Complete                                      | IntelliVM (Windows 7) | 60.057 seconds  | 7          |  |
| <a href="#">63</a> | 2014-11-25 20:03:32 UTC | Task Complete (No events generated from IntelliVM) | IntelliVM (Windows 7) | 120.138 seconds | 0          |  |

Figure 25 — Two Tasks for the Same URL; different Firewall Settings

Task 63 produced no results, whereas task 68 permitted the sample to contact more external resources, so it received a more accurate [risk score](#).

### 6.1. Modify Existing Firewalls

To modify the rules of a firewall, follow these steps:

6.1.1. Select **Analysis Settings > Firewalls**. The three task firewalls are displayed.

| List Firewalls |        | New Firewall |                           |                  |                            |  |
|----------------|--------|--------------|---------------------------|------------------|----------------------------|--|
| ID             | Delete | Inspect      | Name                      | Active           | Default for URL Submission |  |
| 1              |        |              | <a href="#">Isolated</a>  | Default Firewall |                            |  |
| 2              |        |              | <a href="#">Limited</a>   |                  | Default for URL Submission |  |
| 3              |        |              | <a href="#">Unlimited</a> |                  |                            |  |

Figure 26— Firewall List

6.1.2. Click **Set as Default** in the **Active** column to set the default firewall for file submissions.

6.1.3. Click **Set as Default** in the **Default for URL Submission** column to set the default firewall for URL submissions.

6.1.4. Click the **Inspect** icon for the firewall to modify. The **Details for Firewall #x** page is displayed.

**Details for Firewall #2**

Name: Limited

Delete: ☒ ☐

| ID | Priority | Source     | Destination    | Protocol | Action |                          |
|----|----------|------------|----------------|----------|--------|--------------------------|
| 3  | 1        | 0.0.0.0/0: | 0.0.0.0/0: 25  | tcp      | DROP   | <input type="checkbox"/> |
| 4  | 2        | 0.0.0.0/0: | 0.0.0.0/0: 139 | tcp      | DROP   | <input type="checkbox"/> |
| 5  | 3        | 0.0.0.0/0: | 0.0.0.0/0: 445 | tcp      | DROP   | <input type="checkbox"/> |
| 6  | 4        | 0.0.0.0/0: | 0.0.0.0/0:     | all      | ACCEPT | <input type="checkbox"/> |

[Delete selected rules](#)

[Back to list](#)

[Add new Rule to Firewall](#)

Leave the source or destination IP as blank to cover all of the IP range

Source:  :

Destination:  :

Protocol: ☐ tcp ☐ udp ☐ icmp ☐ all

Action: ☐ DROP ☐ REJECT ☐ ACCEPT

Description:

Priority:

[Add New Rule](#)

Figure 27 — Firewall Details Page

6.1.5. On this page you may perform one of the following actions:

- Select the check box(es) for a rule to delete and then click **Delete selected rules**.
- In the *Add New Rule to Firewall* box, specify the source and destination **IP:port** pairs, select the protocol and action, add a description and priority, and click **Add New Rule**.

## 6.2. Create a New Firewall

Follow these steps to create a new firewall.

6.2.1. From the firewall list, click the **New Firewall** tab. The **Add a new firewall to the system** page is displayed.

Figure 28 — New Firewall Dialog

6.2.2. Specify a name for the firewall and add a description, if desired.

6.2.3. Click **Create Firewall**. The details page for the new firewall is displayed.

Figure 29 — New Rule Dialog

6.2.4. Specify one or more rules for the firewall.

List Firewalls
New Firewall

Details for Firewall #4

Name
HTTPS

Delete
X

| ID | Priority | Source       | Destination  | Protocol | Action |  |
|----|----------|--------------|--------------|----------|--------|--|
| 7  | 1        | 0.0.0.0: 443 | 0.0.0.0: 443 | tcp      | ACCEPT |  |

Figure 30 — Firewall Rules List

6.2.5. When you have finished adding rules, return to the main list by clicking the **List Firewalls** tab.

## 7. Plugins

Plugins are a way to interact with an IntelliVM or sample during execution. Each sample can run exactly one plugin and are not available in the emulated SandBox environment. Plugins allows the IntelliVM to run, perform analysis upon the sample, and generate results based upon predefined criteria. Additional plugins can be found in the GitHub repository ([github.com/bluecoat-norway/Malware-Analyzer-G2](https://github.com/bluecoat-norway/Malware-Analyzer-G2)). Talk to your sales engineer about getting access.

With the MAA plugin capability, you can also achieve some of the benefits of forensic investigation and/or static analysis while taking advantage of the automated dynamic analysis simultaneously. MAA's plugins are Python scripts that can interact with the IntelliVMs. They can interact before, during, and after sample execution, and are limited only to what a particular analyst can program. Such features as memory dumping, hook detection, and DLL injection are already present as plugins; when run as part of a dynamic analysis, they provide the relevant information as resources available for download when the automated analysis finishes, typically after about sixty seconds.

### 7.1. Plugin Structure

Plugins are written in Python. Out of the box, any standard Python library can be used for processing. Additional libraries can be installed during the customization process using the standard Python method.

There are three callbacks in a plugin:

```
def guest_pre_exec():  
    pass  
def guest_exec():  
    pass  
def guest_post_exec():  
    pass
```

#### guest\_pre\_exec()

This is called before the main `guest_exec` function. This callback could be used to initialize or set up the guest environment (e.g. proxy settings, debugger hooks, software configuration).

---

**Note** The execution context is a service account rather than the **Admin** user; keep this in mind when setting **HKCU/\*** keys and changing other settings.

---

#### guest\_exec()

This is called after `guest_pre_exec`. This callback should first invoke the event listener `START_MONITOR` and then execute the target sample. The default technique is to use the built-in function `SHELLEXECUTE`. `guest_exec` must return quickly; therefore, the method used to execute the target sample must return immediately.

```
subprocess.call("calc.exe") # BAD, blocks until process exits  
subprocess.Popen("calc.exe") # GOOD, process forks  
SHELLEXECUTE("calc.exe") # GOOD, command is injected into explorer.exe
```

#### guest\_post\_exec()

This is called after either the timeout value has been reached, or all tainted processes have exited. If the timeout value has been reached, the target process may still be running. This callback could be used to inspect memory, collect dropped files or perform any additional post-processing.

## 7.2. General Example

This is a basic "hello world" script that shows part of what can be done. In the `guest_pre_exec()` callback, data is written to a text file and then Notepad is started. The call to `ANTIVMTRICKS()` modifies the VM to avoid some of the more common ways of doing virtual environment detection.

```
import os, sys
import subprocess

def guest_pre_exec():
    ANTIVMTRICKS()
    with open('c:\\hello.txt', 'w') as f:
        f.write('Hello from guest_pre_exec')

    SHELLEXECUTE('notepad c:\\hello.txt')

def guest_exec():
    START_MONITOR(EXEC_ARGS)
    SHELLEXECUTE(EXEC_ARGS)

def guest_post_exec():
    ADD_RESOURCE('c:\\hello.txt')
```

## 7.3. Proc Dump Example

This plugin will dump memory for the analyzed process, and, optionally, any processes whose memory was written to by the analyzed process. It can also scan memory for user-mode hooks.

---

**Note** The process-dump plugin is included with MAA and is used for doing memory captures of a process. The full script is too long to be posted here but can be seen in the MAA or on [GitHub](#).

---

### Memory Dump Options

- **Flat memory dump file (`memdump`)** — For each dumped process, a file is created that contains all the memory contents for that process. The memory is dumped contiguously, with no metadata about memory type, addresses, etc. It is primarily useful for string or binary signature searching.
- **Crash dump file (`crashdump`)** — For each dumped process, a crash dump file is created. The file can be loaded into WinDbg and queried as if the process were suspended in the debugger.
- **Rebuild PE file (`rebuild-pe`)** — This option is useful only for packed samples. It instructs the plugin to attempt to restore the original PE file for the analyzed sample by rebuilding its import table, writing out the unpacked code, and updating the entry point address. The restored PE is written to a file called `rebuilt.ex_`. This implementation is currently rather limited, and is most effective on UPX-packed binaries.

### Analysis Options

- Hook detection ([find-hooks](#)): Searches tainted processes for both inline and import address table hooks and outputs hooked API name and destination address and module name to log file.

### Usage

The `mag2.py` script can be used to execute this plugin on a MAA system. The following command will run the plugin with default options against the file `write_proc_mem.exe` on the (non-existent) [maa.bluecoat.com](http://maa.bluecoat.com) server:

```
>> python mag2.py --ssl -r maa.bluecoat.com create-task -e ivm --sample-file
write_proc_mem.exe --saveresources --primary-resource __SYSTEM__:procdump.py --show-log
```

To run the plugin with different options, use the `--exec-args` option as shown below:

```
>> python mag2.py --ssl -r maa.bluecoat.com create-task -e ivm --sample-file
write_proc_mem.exe --saveresources --primary-resource __SYSTEM__:procdump.py --show-log
-- exec-args " -m -i explorer -f|{sample}"
```

`{sample}` should be typed exactly as shown, including curly braces.

### Options

The following options can be passed to the script:

|    |                 |  |
|----|-----------------|--|
| -m | --memdump       | Create flat memory dump file(s)  |
| -c | --crashdump     | Create crash dump file(s)  |
| -t | --tainted-procs | Dump all processes whose memory was tainted (i.e. written to) by the analyzed process. |
| -r | --rebuild-pe    | Attempt to rebuild original PE file (useful only for packed samples).                  |
| -I | --inject PROC   | Inject sample as DLL into either Windows Explorer ("explorer") or IE ("iexplore").     |
| -f | --find-hooks    | Search tainted processes for user-mode API hooks.                                      |

By default, only the analyzed process' memory will be dumped, and no analysis will be performed.



### example

The [write\\_proc\\_mem.exe](#) binary demonstrates the use of this plugin. It spawns `notepad.exe`, allocates memory to it, and then writes the string `my_evil_string` in that memory. If you run the plugin with the `--tainted-procs` option, it will create a memory dump for `notepad.exe`, and you can [grep](#) the dump file(s) for the injected string.

### Adding a Plugin

Plugins can be added via the remote API, or via [the mag2.py utility](#). Plugins are considered sample resources and must be added as such.

### Syntax

```
mag2.py import-ivm-plugin [--owner OWNER] the_ivm_plugin_path
```

The owner parameter is optional and can be used to make the plugin available only to a single user. The same process is used to update a plugin after changes have been made.

---

**Note** The plug-in integer ID will be updated with each import. If you call this plugin from scripts you will need to update them after changing the plugin. No changes are needed in the UI.

---

If you wish to do this manually, review the [mag2.py](#) script and the RAPI documentation for the [POST /rapi/samples/resources](#) REST call.

## 8. Services

Select **System Settings > Services** to access the controls for MAA services.

### 8.1. Reputation

New in 4.2.1 is a preview of two integration features with the Blue Coat Global Intelligence Network (GIN): Web Reputation and File Reputation Services.

Both services are disabled by default; both require that the MAA have Internet access on port 443.

Select **Analysis Settings > Services** and click the **Reputation** tab to enable or disable these features. To further configure these services, consult the MAA System Configuration Guide under [\[analytics\]](#).

#### Web Reputation

The Web Reputation Service leverages the [WebPulse Site Review](#) database, which contains ratings for millions of web sites. The rating system includes informational [categories](#) such as Education, Art/Culture, and Humor/Jokes as well as warnings such as Malicious Outbound Data/Botnets, Phishing, and Spam.

#### File Reputation

The File Reputation Service delivers real-time file reputation intelligence by leveraging the Blue Coat File Reputation Service. Enable this feature to identify known-bad files, which can be embedded within nearly every file type that is delivered over common file protocols.

### 8.2. VirusTotal

If you have a subscription to the VirusTotal lookup service, follow these steps:

- 8.2.1. Select **Analysis Settings > Services** and click the **VirusTotal** tab.
- 8.2.2. Enter the key in the space provided and click **Update VirusTotal Key**.

---

**Note**    **Obtaining a VirusTotal key is the responsibility of the user.**

---

**Disclaimer:** This feature is provided on an [AS-IS](#) basis. Blue Coat has no control of, and is not responsible for, information and content provided (or not) by VirusTotal. Customer is obligated to comply with all terms of use regarding the foregoing, including quotas that may be imposed by VirusTotal. Blue Coat shall not be liable for any discontinuance, availability or functionality of the features described herein.

## 8.3. YARA

YARA is a tool that helps malware researchers to identify and classify malware families. With YARA, researchers can create descriptions of malware families based on textual or binary information contained within representative samples. These descriptions are encapsulated as rules consisting of patterns and logic based on Boolean expressions. Rules can be applied to static files or to running processes to determine if a sample belongs to a particular malware family.

Official YARA documentation and updates are located at [plusvic.github.io/yara/](https://plusvic.github.io/yara/)

YARA is disabled by default. To enable YARA, follow these steps:

### In the Web Interface

- 8.3.1. Select **Analysis Settings > Services** and click the **YARA** tab.
- 8.3.2. Click **Enable YARA**.

### From the Console

- 8.3.3. Initiate an SSH session with the MAA using the [g2](#) username and corresponding password.
- 8.3.4. Type the following and press **Enter**:

```
df-config-mgr -w main.yara_enabled True
```

### YARA File Updates

The Malware Analysis Appliance is preloaded with a set of YARA rules. To update these rules, you have the following options:

- **Overwrite current file** — Click **Upload New YARA file** and select a new file.
- **Add to the current file** — Click **Append to YARA file** and select a file to add its rules to the current file.
- **Edit the current file** — Click **Download YARA file** to download [yara\\_rules.yar](#) to your workstation. Edit the file [according to YARA syntax](#), click **Upload New YARA file**, and upload the edited file.
- **Delete the current file** — Click **Delete YARA file** to delete all YARA rules. No YARA hits will occur until a new YARA file is uploaded.

## 9. MAA Updates

Two types of updates are available for the MAA: system software and patterns. Patterns are updated more frequently than system software and can be installed independently of system updates.

To access the update pages, select **System Settings > Updates**.

### 9.1. Update Settings

The update settings specify what happens when a pattern or system update becomes available online.

9.1.1. Click the **Update Settings** tab.

9.1.2. Select the **Automatically download updates** check box to automatically download any file that is detected when you check for updates. If you do not select this check box, new files will be listed on the *Available Updates* page and you will have to [initiate the download manually](#).

9.1.3. When the **Automatically download updates** check box is selected, you have two more options to select:

- **Non-disruptive updates** — A non-disruptive update causes minimal downtime. Select **Manual** or **Automatic** to specify how the update is to be installed.
- **Disruptive updates** — A disruptive update causes more downtime than a non-disruptive update. Select **Manual** or **Automatic** to specify how the update is to be installed.

---

**Note** By default, an update is "disruptive" if it takes longer than 5 minutes to install. That threshold is controlled by the `update.passive_threshold` parameter. See the [MAA System Configuration Guide](#) for more information.

---

9.1.4. **Optional** — Specify a Web proxy that the MAA will use to contact the update server ([ma-updates-us-west-1.s3.amazonaws.com](#)).

## 9.2. Check for Updates

To check for available updates, follow these steps:

- 9.2.1. Click the **Available Updates** tab.
- 9.2.2. Click **Check for updates**. The MAA accesses the Blue Coat update server.
- 9.2.3. Any new system or pattern files are displayed.

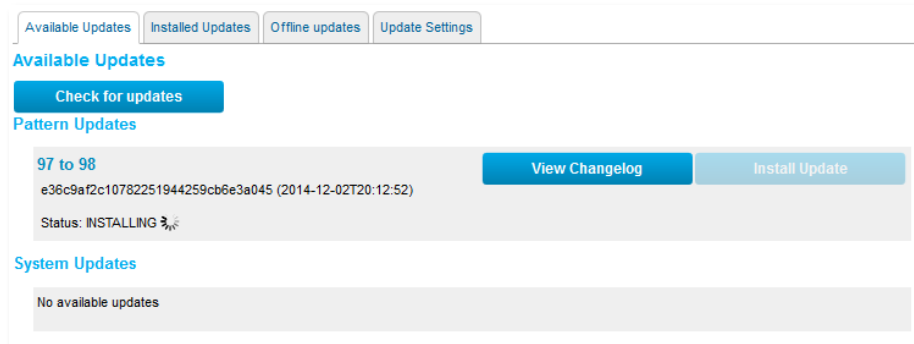


Figure 31 — Automatic Pattern File Installation

- 9.2.4. According to your update settings, one of two things happens:
  - The new file is automatically installed.
  - The new file entry remains on this page until you click **Install Update**.
- 9.2.5. After a file has been updated, you can view it by clicking the **Installed Updates** tab, where you can view the change log.

### 9.3. Offline Updates

If you prefer not to automatically check for, download, or install updates, you can use the manual process.

- 9.3.1. On the *Update Settings* tab, clear the **Automatically download updates** check box.
- 9.3.2. Click the **Offline Updates** tab.
- 9.3.3. Click **Download telemetry file** to save [telemetry.json](#) to your workstation.
- 9.3.4. Go to [maa-updates.es.bluecoat.com](http://maa-updates.es.bluecoat.com). Click **Browse** to select and upload [telemetry.json](#).

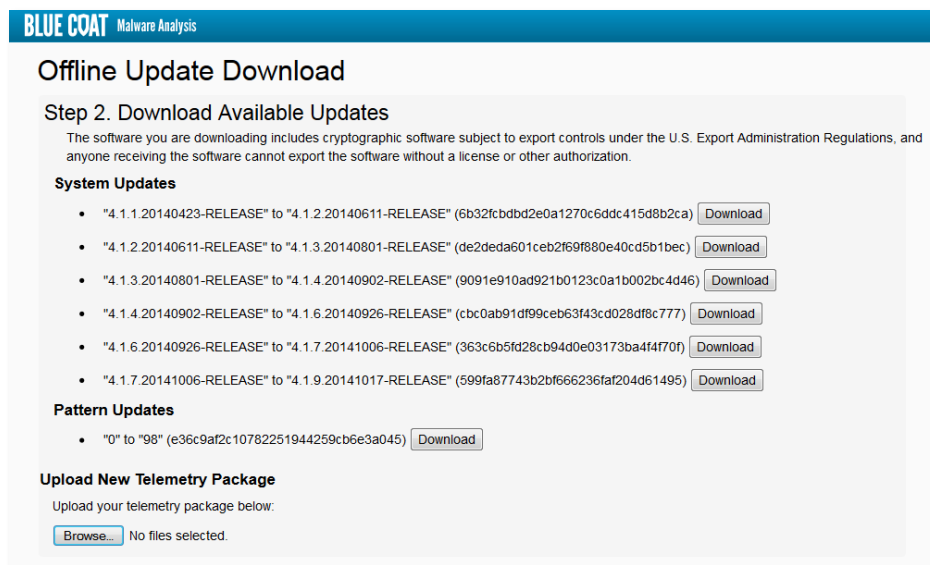


Figure 32 — List of Available Updates

- 9.3.5. If there are any updates available for your MAA, they are listed on this page. Click **Download** for each update file.

---

**Note** If there are multiple entries for the system updates, you should download all of them, unless you have a specific reason not to. Pattern updates are optional but recommended.

---

- 9.3.6. Return to the *Offline Updates* page on the MAA UI and click **Upload update package** to select and upload the files that you have downloaded.

9.3.7. Click the **Available Updates** tab to see the new updates.

|  |                               |
|--|-------------------------------|
| <b>System Updates</b>  |                               |
| <b>4.1.2.20140611-RELEASE to 4.1.3.20140801-RELEASE</b><br>de2deda601ceb2f69f880e40cd5b1bec (2014-12-02T18:58:21)<br>Requires version 4.1.2.20140611-RELEASE<br>Status: DOWNLOADED | View Changelog Install Update |
| <b>4.1.4.20140902-RELEASE to 4.1.6.20140926-RELEASE</b><br>cbc0ab91df99ceb63f43cd028df8c777 (2014-12-02T18:56:58)<br>Requires version 4.1.4.20140902-RELEASE<br>Status: DOWNLOADED | View Changelog Install Update |
| <b>4.1.3.20140801-RELEASE to 4.1.4.20140902-RELEASE</b><br>9091e910ad921b0123c0a1b002bc4d46 (2014-12-02T18:56:35)<br>Requires version 4.1.3.20140801-RELEASE<br>Status: DOWNLOADED | View Changelog Install Update |
| <b>4.1.1.20140423-RELEASE to 4.1.2.20140611-RELEASE</b><br>6b32fcbdbd2e0a1270c6ddc415d8b2ca (2014-12-02T18:58:32)<br>Status: DOWNLOADED  | View Changelog Install Update |

Figure 33 — List of System Updates

---

**Note** If there are multiple system updates, only the next file in the upgrade path can be installed.

---

9.3.8. Click **Install Update** to install the new files.

9.3.9. After a file has been installed, you can click the **Installed Updates** tab to view the change log.

## 10. User Roles

Any number of users can be created to access the Malware Analysis Appliance. To each user, a role is assigned with its respective permissions. Multiple API keys can be generated for each user to use with remote APIs, pub-sub APIs, and for integration with the Security Analytics Platform or Content Analysis System.

### 10.1. Create Users

To create a new user account, follow these steps:

10.1.1. Select **System Settings > Users** and click the **New User** tab.

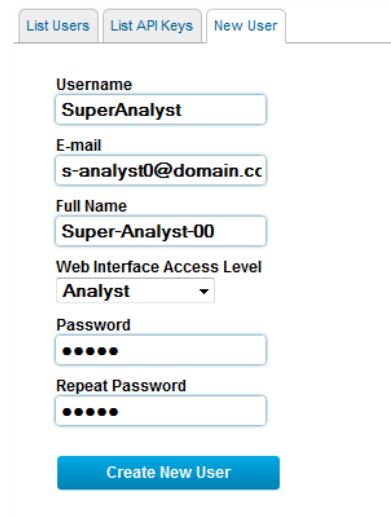


Figure 34 — New User Page

10.1.2. Fill in the fields as follows (All fields are required):

- **Username** — Type a unique name for the account. Only the characters [A–Z](#), [a–z](#), [0–9](#), dot ([.](#)), underscore ([\\_](#)), and "at" ([@](#)) are permitted.
- **E-mail** — Type an email to associate with the username.
- **Full Name** — Type the name to be displayed on the UI.
- **Web Interface Access Level** — Consult the [User–Role Privileges Matrix](#) for specific permissions.
- **Password/Repeat Password** — Type and retype the account password.

10.1.3. Click **Create New User**.



## 10.2. User–Role Privileges Matrix

Consult the table below to see which privileges are assigned to each user role.

| Privilege                                | Guest | Observer | Analyst | Super-Analyst | Sysconfig | Administrator |
|--|-------|----------|---------|---------------|-----------|---------------|
| View Basic System Information            | X     | X        | X       | X             | X         | X             |
| View System Patterns                     | X     | X        | X       | X             | X         | X             |
| Create Samples                           |       |          | X       | X             |           | X             |
| Create Tasks from Own Samples            |       |          | X       | X             |           | X             |
| Create Resources                         |       |          | X       | X             |           | X             |
| Create Patterns                          |       |          | X       | X             |           | X             |
| View System Resources                    |       |          | X       | X             |           | X             |
| View All Samples                         |       | X        |         | X             |           | X             |
| View All Tasks                           |       | X        |         | X             |           | X             |
| View All Resources                       |       | X        |         | X             |           | X             |
| View All Patterns                        |       |          |         | X             |           | X             |
| Create Tasks from All Samples            |       |          |         | X             | X         | X             |
| View and Purge Task Queries              |       |          |         | X             | X         | X             |
| View Vtop Data                           |       |          |         | X             | X         | X             |
| View System Health                       |       |          | X       | X             | X         | X             |
| Create, Modify, and Delete iVM Profiles  |       |          |         |               | X         | X             |
| Update System License                    |       |          |         |               | X         | X             |
| Update System Software                   |       |          |         |               | X         | X             |
| Create Modify, and Delete Task Firewalls |       |          |         |               | X         | X             |
| View and Set Network Configuration       |       |          |         |               | X         | X             |
| Enable YARA                              |       |          |         |               | X         | X             |
| Upload/Download YARA Files               |       |          |         |               | X         | X             |
| Enable/Disable Web and File Reputation   |       |          |         |               | X         | X             |
| Configure Default Task Settings          |       |          |         |               | X         | X             |
| View System Statistics                   |       |          |         |               | X         | X             |
| View syslog                              |       |          |         |               | X         | X             |
| View Advanced System Information         |       |          |         |               | X         | X             |
| Create, Modify, and Delete Users         |       |          |         |               | X         | X             |

| Privilege                                  | Guest | Observer | Analyst | Super-Analyst | Sysconfig | Administrator |
|--|-------|----------|---------|---------------|-----------|---------------|
| Create, Modify, and Delete VM Firewalls    |       |          |         |               | X         | X             |
| Modify System Health Rules                 |       |          |         |               | X         | X             |
| Create, Modify, and Delete iVM Base Images |       |          |         |               |           | X             |
| Shut Down or Restart                       |       |          |         |               | X         | X             |

### 10.3. Generate API Keys

To generate an API key for a user account, follow these steps:

10.3.1. Select **System Settings > Users** and click the **List Users** tab.

10.3.2. For the user account, click its UID.

10.3.3. Scroll down to the *API Keys* section.

Figure 35 — API Keys Section

10.3.4. For **API Key Label**, type a name for the key. For example, if this key is to be used to integrate with Security Analytics, you could call it [SA-key](#).

10.3.5. For **API Key Access Level**, select an access level. This level can be different from — including higher than — the level that the user has to access the MAA UI.

10.3.6. Click **Add New Key**.

Figure 36 — API Key Created Dialog

10.3.7. The *API Key Created* dialog is displayed. **DO NOT CLOSE THIS DIALOG YET.**

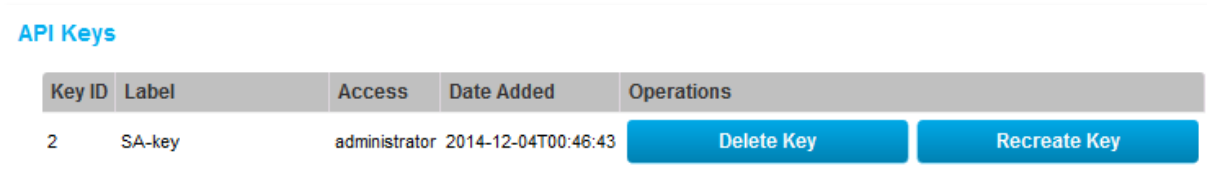
10.3.8. Copy the key and distribute it as needed.

---

**CAUTION** You cannot retrieve this key after you close the dialog.

---

10.3.9. Click **close window**. The key is displayed in the list.



| Key ID | Label  | Access        | Date Added          | Operations  |
|--------|--------|---------------|---------------------|---|
| 2      | SA-key | administrator | 2014-12-04T00:46:43 | <a href="#">Delete Key</a> <a href="#">Recreate Key</a> |

Figure 37 — API Keys List

10.3.10. If you lose the key, you can click **Recreate Key** to generate a new key; however, recreating the key makes the previous key immediately obsolete. You will need to replace the old key in all applications that use it to maintain connectivity.

## 11. Licensing

To view the *Blue Coat Systems, Inc. License Agreement*, select **Help > Licensing**. Also see [Appendix: Base Image License Terms](#).

To update your MAA license, select **System Settings > License**, and click **Upload new license file** to upload a new file that you have obtained from Blue Coat.

Contact your Blue Coat Sales Representative for more information.

## 12. Storage Options

The MAA provides multiple data storage options designed to support individual users, groups of local users, and teams of geographically distributed users.

### 12.1. Internet Cloud Storage

The MAA supports Internet cloud storage in Amazon S3 format. Amazon S3 provides a simple web services interface that can be used to store and retrieve any amount of data, at any time, from anywhere on the web. It gives developer access to the same highly scalable, reliable, secure, fast, inexpensive infrastructure that Amazon uses to run its own global network of web sites.

---

**Note** It is the responsibility of the user to obtain an Amazon S3 cloud storage account.

---

### 12.2. Local Serialized Storage

The MAA supports local serialized storage in the Google Protocol Buffer format. Protocol buffers are Google's language-neutral, platform-neutral, extensible mechanism for serializing structured data — similar to XML but smaller, faster, and simpler. You can define how you want your data to be structured once, then you can use specially generated source code to write and read your structured data to and from a variety of data streams and using a variety of languages — Java, C++, or Python.

### 12.3. Local Database Storage

The MAA includes an embedded relational database, designed with an efficient schema and optimized for performance. The database is also open for integration and query by customers using third-party tools.

## 13. Mag2.py Utility

`mag2.py` is a Python program that can be found in the [opt/mag2/github/Malware-Analyzer-G2/utilities/](#) directory on the MAA appliance. It is both a command-line tool for performing various operations and a place to see examples on how to interact with the appliance.

```
$ python mag2.py
```

### Usage

```
mag2.py [-h] -r MAG2_RAPI [-s] [--trace]
```

```
{maintenance-mode,show-license,update-license,get-config,set-config,export-patterns,import-
patterns,list-vm-profiles,list-ivm-plugins,import-ivm-plugin,upload-sample,create-task}
```

Individual commands will show more options when you issue them without additional arguments.

```
$ python mag2.py create-task
```

```
$ usage: mag2.py create-task  [-h] [-e {sbx,ivm}] [--owner OWNER] [--no-wait]
                             [--zip-password ZIP_PASSWORD] [--profile PROFILE]
                             [--primary-resource-id PRIMARY_RESOURCE_ID | --primary-resource
PRIMARY_RESOURCE | --primary-resource-file PRIMARY_RESOURCE_FILE]
                             [--ivm-time IVM_TIME] [--ivm-firewall IVM_FIREWALL]
                             [--ivm-get-dropped] [--ivm-capture-all]
                             [--exec-args EXEC_ARGS] [--save-all] [--save-pdf]
                             [--save-gpb] [--save-json] [--save-dropped]
                             [--save-resources] [--show-log] [--open-pdf]
                             (--sample-id SAMPLE_ID | --sample-file SAMPLE_FILE |
                             --sample-zip SAMPLE_ZIP | --url URL)
```

### 13.1. Analyzing a ZIP Archive

You cannot analyze the contents of a [ZIP](#) archive of multiple samples or a password-protected [ZIP](#) of a single file if you submit it through the UI.

To extract or decrypt a [ZIP](#) file, you can use the API or the `mag2.py` command-line utility.

```
mag2.py upload-sample [-h] [--owner OWNER]
                     [--zip-password ZIP_PASSWORD]
                     (--sample-file SAMPLE_FILE | --sample-zip SAMPLE_ZIP)
```

To do this through the API, review the [mag2.py](#) code or consult the RAPI documentation in the Web UI (**Help > Remote API**).

## 14. Health System

The MAA Health System is comprised of the following elements working together: (1) a health daemon that collects system metrics; (2) a set of configurable health rules and; (3) an evaluation system that assesses the collected metrics. The result of the evaluation represents the overall health state of the system. The Health System is accessible via the remote API, with results and events available for publication to Redis and WebSockets.

### 14.1. Health State

The health state of a MAA system is one of three (3) possible values:

- **0 — Green** means that all systems components are running fine
- **1 — Yellow** indicates one or more issues that could lead to serious problems if not addressed soon
- **2 — Red** warns of critical issues that are negatively affecting current MAA operational capabilities

The health state is visible in the upper-right corner of the Web UI. The background of the **System Status** text is green, yellow, or red according to the health state.

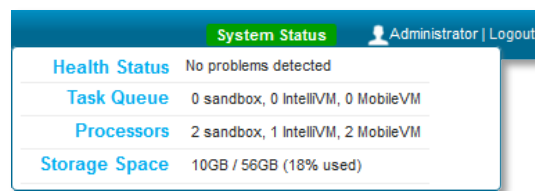


Figure 22 — System Status Indicator on the UI

The command below returns the current state of the MAA as a numeric and color value. In a non-green state, the command also returns a list of issues that caused the state change.

```
$ curl -X GET https://<MAA>/rapi/system/health
```

#### example 1

Remote API results that indicate a healthy system.

```
"results": {
  "health_color": "green",
  "health_state": 0,
  "health_state_reasons": []
}
```

#### example 2

Remote API indicates a current situation that could lead to a serious problem later

```
"results": {
  "health_color": "yellow",
  "health_state": 1,
  "health_state_reasons": [
    "mounts_percent"
  ]
}
```

## 14.2. Health Stats

The health stats API returns all of the metric data used to calculate the health state of the MAA instance.

This returned data—the exact same data that is used for the internal metric evaluation—could also be used to perform the metric evaluation externally, ideal for centrally monitoring the health of one or more MAA instances.

The command below retrieves the `health_stats` data.

```
$ curl -X GET https://<MAA>/rapi/system/health_stats/(?P[\w\.-]+)
```

---

**Note** Keep in mind that this call returns all of the counters precisely formatted in JSON—which is an "expensive" Redis call in terms of performance. Depending on your system, such a call could diminish the performance of your browser.

---

Commands can also specify sections of interest; `mounts`, for example, returns the following information:

```
"mounts": {
  "/dev/sda1": {
    "free": 1459855724544,
    "percent": 13.8,
    "total": 1798153564160,
    "used": 248297857024
  },
  "/dev/sdb1": {
    "free": 230507638784,
    "percent": 16.4,
    "total": 293207924736,
    "used": 48022110208
  }
}
```

### 14.3. Health Rules

Every decision made within the metric evaluation system is based on health rules stemming from either: (1) default rules or (2) rules defined by the administrator of the MAA instance.

---

**Note** Consult the [\[cleanup\]](#) section of the [MAA System Configuration Guide](#) to see configurable parameters that are related to the health system.

---

The command below queries the MAA for the system's current metrics rule settings.

```
$ curl -X GET https://<MAA>/rapi/system/health_rules
```

```
"system": {
  "enabled": "True",
  "query_interval": "30",
  "system_memory_percent_red": "100",
  "system_memory_percent_yellow": "95",
  "system_swap_memory_used": "0"
}
```

The switch [enabled](#) allows the administrator to enable or disable specific rule sections. The [query\\_interval](#) defines the time interval (in seconds) in which the health daemon refreshes that particular section of the rules.

```
$ curl -X POST -d "key=enabled&value=False" https://<MAA>/rapi/system/health_rules/system
```

This example would disable the [system](#) section of the MAA.



## 15. System Time

The Malware Analysis Appliance uses the current Central European Time (CET) to mark various system events. The appliance accesses the Network Time Protocol (NTP) servers to obtain accurate CET time and synchronizes its time clock to ensure the time remains in sync between your systems. By default, MAA connects to an NTP server in the order they are listed (up to a maximum of 3) and acquires the CET time. If no NTP servers are listed, or the appliance cannot access any of the listed servers, NTP is automatically disabled.

Alternatively, the MAA can be configured to record time stamps in local time. To set the local time, you must configure the time based on your time zone.

---

**Note** By default system events are initially set to CET time while MAA events are stored in UTC, but are displayed using local time zone.

---

### 15.1. Configure the Local Time Settings

To manually update the current date and system time, follow these steps:

15.1.1. Select **System Settings > Date / Time**. The **Set System Date/Time** settings display.

15.1.2. Enter the system date, time, and then select your timezone.

15.1.3. Click **Update Date and Time**.

### 15.2. Enable / Add NTP Servers

To enable NTP or add additional NTP servers, follow these steps:

15.2.1. Select **System Settings > Date / Time**. The **Network Time Protocol (NTP) Settings** display.

15.2.2. Select the **Enable NTP** checkbox.

15.2.3. Enter up to 3 NTP servers. By default, the MAA comes preconfigured with the following NTP servers:

1. 0.pool.ntp.org
2. 1.pool.ntp.org
3. 2.pool.ntp.org

15.2.4. Click **Update NTP Settings**.

---

**Note**    Updating the system time settings triggers an automatic reboot. After the system restarts, you must re-login.

---

## 16. Monitoring and Event Logging

The Malware Analysis Appliance supports syslog event-monitoring and SNMP (version 1 and 2) for network management. This allows the appliance to send task summary data (refer to the *Analysis Center Guide* for more information about **Task Summary** content) to an external syslog server as well as allow a system administrator to monitor and collect information.

The task report data sent to SNMP allows unidirectional access to the appliance. SNMP collects key information samples, including:

- List of running processes / services
- Status of network interfaces
- System uptime

### 16.1. Enable Syslog

To enable Syslog, follow these steps:

---

**Note** Consult the [Appendix: Syslog Raw Output](#) to see details about the contents of the syslog message.

---

16.1.1. Select **System Settings > Notifications**. The **Syslog Settings** display.

16.1.2. Select the **Enable Remote Syslog** checkbox.

16.1.3. Enter the syslog **Server** and **Port** information.

16.1.4. Select the syslog **Protocol** type from the dropdown menu. UDP is set as the default syslog protocol.

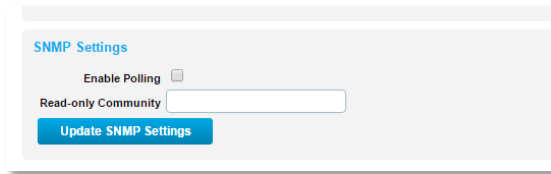
16.1.5. Click **Update Syslog Settings**.

16.1.6. (Optional) Verify that syslog is working by clicking **Generate Message**. This sends a test message to the specified syslog server.

### 16.2. Enable SNMP Polling

To enable SNMP polling, follow these steps:

16.2.1. Select **System Settings > Notifications**. The **SNMP Settings** display.

A screenshot of a web-based configuration window titled "SNMP Settings". The window has a light gray background and a thin border. Inside, there is a section labeled "SNMP Settings" in blue text. Below this, there is a checkbox labeled "Enable Polling" which is currently unchecked. Underneath the checkbox is a text input field labeled "Read-only Community" which is empty. At the bottom of the window is a blue button with white text that says "Update SNMP Settings".

SNMP Settings

Enable Polling ☐

Read-only Community

Update SNMP Settings

16.2.2. Select the **Enable Polling** checkbox.

16.2.3. Enter a valid read-only SNMP community string.

16.2.4. Click **Update SNMP Settings**.

## 17. Appendix

The following sections describe supplementary details about the MAA.

### 17.1. System Processes

The MAA must run the following processes for normal operation.

| Process   | Arguments                           |
|---|-------------------------------------|
| /usr/bin/supervisord  | N/A                                 |
| /usr/sbin/mysqld  | N/A                                 |
| /usr/lib/erlang/erts-5.8.5/bin/epmd                             | N/A                                 |
| /usr/bin/redis-server /etc/mag2/redis-6379.conf                 | N/A                                 |
| /usr/bin/redis-server /etc/mag2/redis-6380.conf                 | N/A                                 |
| /usr/sbin/apache2   | N/A                                 |
| python /opt/mag2/usr/share/mag2/pyscripts/update-daemon.pyc     | N/A                                 |
| python /opt/mag2/usr/share/mag2/pyscripts/df-config-mgr.pyc     | N/A                                 |
| python /opt/mag2/usr/share/mag2/pyscripts/rapi2.pyc             | N/A                                 |
| python /opt/mag2/usr/share/mag2/pyscripts/df-health-monitor.pyc | N/A                                 |
| python /opt/mag2/usr/share/mag2/pyscripts/ivmcontrold.pyc       | N/A                                 |
| python /opt/mag2/usr/share/mag2/pyscripts/mq-consume-events.pyc | N/A                                 |
| python /opt/mag2/usr/share/mag2/pyscripts/start-sbx.pyc         | N/A                                 |
| python /opt/mag2/usr/share/mag2/pyscripts/start-vbox.pyc        | N/A                                 |
| python /opt/mag2/usr/share/mag2/pyscripts/start_drd.pyc         | N/A                                 |
| python /opt/mag2/usr/share/mag2/pyscripts/ivmdhcp.pyc           | N/A                                 |
| python /opt/mag2/usr/share/mag2/pyscripts/cleanup-daemon.pyc    | N/A                                 |
| node /opt/mag2/usr/share/mag2/node.js/web-router.js             | --port=80 --ssl=0 --serve-static=1  |
| node /opt/mag2/usr/share/mag2/node.js/web-router.js             | --port=443 --ssl=1 --serve-static=1 |
| python /opt/mag2/usr/share/mag2/pyscripts/reconfig.pyc          | N/A                                 |

## 17.2. Syslog Raw Output

The raw syslog output generated by the MAA includes various output values within a comma separated, key value pair message structure, as shown in the following example:

```
Mar 13 15:29:05 192.168.1.221 Mar 13 15:28:59 mag2 MA_tasks: {"profile":
"win7base", "description": "Windows7 SP1, IE10", "filetype":
"document:pdf:v1.5", "sample_id": 1, "date": "2015-03-13T14:45:23", "md5":
"3001a822333467f1645fc6a48bd790aa", "global_risk_score": 9, "task_id": 3,
"top_hits": [{"pattern_score": 9, "pattern_match": "File reputation:
Malware"}, {"pattern_score": 6, "pattern_match": "PDF file contains
Javascript"}, {"pattern_score": 1, "pattern_match": "YARA score 1"}],
"label": "3001a822333467f1645fc6a48bd790aa", "environment": "ivm",
"sample_source": "www" }
```

The raw output shown above includes the following output values:

| Output Value      | Description   | Example   |
|-------------------|---|---|
| profile           | Name of the IntelliVM profile used to replicate the environment.  | win7base  |
| description       | The description of the IntelliVM profile as added by the user.  | Windows7 SP1, IE10  |
| filetype          | The actual type of file as identified by MAA, regardless of the file extension shown in the filename  | document:pdf:v1.5   |
| sample_id         | The unique identifier assigned to the sample by the MAA. Can be used to search for and open the related <b>Sample Details</b> page.   | 1   |
| date              | Date and time a sample was uploaded to the MAA.   | 2015-03-13T14:45:23   |
| md5               | 128-bit cryptographic hash using the Message-Digest 5 algorithm   | 3001a822333467f1645fc6a48bd790aa  |
| global_risk_score | Numeric value from 0 to 10, automatically assigned by MAA, determined by the patterns that triggered during the sample execution.   | 9   |
| task_id           | The unique task identifier tag that is generated automatically by the MAA system. Can be used to search for and open the related <b>Task Report</b> page.   | 3   |
| top_hits          | <p>The individual scores produced by the MAA file reputation / classification systems for a given item.</p> <p><b>Note:</b> Top hits are limited by the number of <u>complete</u> messages available to fill remaining message space.</p> | <ul style="list-style-type: none"> <li>pattern_score: 9, pattern_match: File reputation: Malware</li> <li>pattern_score: 6, pattern_match: PDF file contains Javascript</li> <li>pattern_score: 1, pattern_match: YARA score 1</li> </ul> |
| label             | By default the filename of the object; may be changed via the UI or the API   | 3001a822333467f1645fc6a48bd790aa  |
| environment       | The emulated/simulated operating system environment.  | ivm   |
| sample_source     | The origin of the sample.   | www   |

---

**Note** The maximum length of a syslog message is constrained to 2048 bytes as dictated in RFC-5424. For more information about syslog , see [RFC 5424](#) at the *Internet Engineering Task Force*.

---

## 18. Terms of Agreement

### 18.1. Base Image License Terms

The MAA Product is provided with a Microsoft® Product Identifier Card that includes Microsoft Certificates of Authenticity (COAs), with the COAs provided based on the customer's representation to Blue Coat as to whether or not it has in place a valid Microsoft Volume Licensing Agreement that includes Software Assurance.

For customers purchasing the Blue Coat Malware Analysis Appliance with a valid Microsoft Volume Licensing Agreement that includes Software Assurance

User must have a valid Microsoft Volume Licensing agreement and must purchase Software Assurance for each COA provided.

The user is licensed to use any combination of the following Microsoft Windows Operating System products running in simultaneous Instances, provided that in no event may the number of simultaneously running Instances exceed the number of COAs provided on the Microsoft Product Identifier Card.

- Microsoft Windows XP Professional for Embedded Systems ESD (Virtualization Only)
- Windows 7 Professional for Embedded Systems ESD (Virtualization Only)
- Windows Embedded 8 Pro ESD (Virtualization Only)

For customers purchasing the Blue Coat Malware Analysis Appliance without a valid Microsoft Volume Licensing Agreement that includes Software Assurance

If the user is not party to a valid Microsoft Volume Licensing agreement that includes Software Assurance, the COAs provided on the Microsoft Product Identifier card will be product-specific, with the same number of COAs provided for each available product. In this case, the user is licensed to use any combination of Microsoft Windows Operating System products running in simultaneous Instances, provided that in no event may the number of simultaneously running Instances exceed a number equal to the number of COAs provided for each relevant product. (That is, if, for example, the Microsoft Product Identifier card shipped with the product includes 12 COAs for Windows XP Professional and 12 COAs for Windows 7 Professional, the product may run up to 12 total Instances of any combination of products).

For these purposes, the following definitions apply:

- "Operating System Environment" or "OSE" means all or part of an operating system Instance, or all or part of a virtual (or otherwise emulated) operating system Instance which enables separate machine identity (primary computer name or similar unique identifier) or separate administrative rights, and instances of applications, if any, configured to run on the operating system Instance or parts identified above. There are two types of OSEs, physical and virtual. A physical hardware system can have one Physical OSE and/or one or more Virtual OSEs.
- "Physical OSE" means an OSE that is configured to run directly on a physical hardware system. The operating system Instance used to run hardware virtualization software (e.g. Microsoft Hyper-V or similar third-party technologies) or to provide hardware virtualization services (e.g. Microsoft virtualization technology or similar third-party technologies) is considered part of the Physical.