Content Analysis Version 2.1.x Release Notes

Version: 2.1.1.1
Build: 201067
Release Date: 05/01/2017
Document Revision: 11/14/2017

Introduction

These release notes apply to the Symantec Content Analysis appliance. For release specific information, refer to the following sections:

- "Content Analysis 2.1.1.1 Release" on page 4

Note: Refer to the Content Analysis Quick Start poster included with your appliance for initial configuration and licensing details.

Upgrade to CA 2.1.x

WARNING! The upgrade process can take 15 minutes or more to complete, and during this time the appliance may appear to be hung. While Content Analysis is in the middle of a major upgrade, interrupting the process will damage the CA appliance. Do not power cycle the unit during the upgrade process! You will know that the upgrade is complete when you can successfully log in to the management console or the command-line interface.

Upgrade Path to CA 2.1.x

Current CA Version	Upgrade Directly to CA 2.1.x?
1.3.7.x	Yes
All versions released before 1.3.7.x	No (upgrade to CA 1.3.7.x first, and then upgrade to CA 2.1.x)

Upgrade Procedure

Follow the steps below to upgrade from CA 1.3.7.x to 2.1.x:

1. Back up your CA 1.3.7.x configuration using the **Utilities > Configuration > Get Configuration** option in the Content Analysis management console.
2. Log in to MySymantec (https://MySymantec.com) and download the CA 2.1.x image.

3. On the **System > Firmware** page in the management console, upload the system image.

Note: When upgrading from CA 1.3.7.5, do not use the **Upload System Image** option to upload a 2.1.x image file, as this method does not function properly in v1.3.7.5. (Note that this is *not* an issue in other 1.3.x versions or v2.x.) Instead, place the image on a web server and use the **System Image Retrieval** option.

Do not reboot yet!

4. Verify that **Utilities > Onboard Diagnostics** displays correctly. If not, you will need to reset the Baseboard Management Controller (BMC) when you get to step 6 below (but *do not* skip step 5).
5. Use a remote login utility to SSH to the appliance. Issue the **`shutdown`** CLI command to gracefully shut down the appliance.
6. If the Onboard Diagnostics page did not display in step 4 above, you need to reset the BMC by disconnecting the power cords for a couple minutes.
7. Power on the appliance. As noted above, the upgrade process can take 15 minutes or more to complete. Do not power cycle the appliance during the upgrade!

Generate New Certificate

In order to take advantage of the new SHA-256 certificate included in CA 2.1.1.1, you must regenerate the certificate after upgrading. If you do not regenerate, Content Analysis will still use the SHA-1 certificate.

To generate a SHA-256 certificate:

1. Upgrade to CA 2.1.1.1.
2. In the Content Analysis web management console, select **Settings > Web Management**.
3. Click **Certificate Management**.
4. Click **Create Certificate** and modify information as necessary.
5. Click **Save Changes**.

When the changes are saved, Content Analysis will use the new SHA-256 certificate.

Downgrade Support

Because of infrastructure changes introduced in CA 2.1, downgrades from CA 2.1.x to 1.x are not supported; a factory reset would be required after downgrading.

Platform Support

Platform	Support for CA 2.1.x	Support for On-Box Sandboxing	# of IVMs Supported
CASVA-100	Yes		NA
CAS-S200-A1	Yes		NA
CAS-S400-A1	Yes	✓	2
CAS-S400-A2	Yes	✓	2
CAS-S400-A3	Yes	✓	4
CAS-S400-A4	Yes	✓	4
CAS-S500-A1	Yes	✓	12

Web Browser Support

Symantec has tested the Content Analysis 2.1.x web management console with the following web browsers:

- Microsoft Internet Explorer version 11 (Note that IE 11 does not support upload of Windows base images to be used with the on-box sandboxing feature.)
- Mozilla Firefox version 2 and later, including latest stable release
- Google Chrome, latest stable release

Product Compatibility

When integrating Content Analysis 2.1.x with other Symantec and third-party products, the following versions are required.

- Symantec Reporter: v10.1.4.1 or later
- Symantec Management Center: v1.10.1 or later
- Symantec Endpoint Protection Manager: v14 or later
- FireEye AX: tested with v7.7.5, although other versions may work
- FireEye NX: any version
- Countertack: v1.x only
- Lastline: any version

Section A: Content Analysis 2.1.1.1 Release

Note: In order to take advantage of the new SHA-256 certificate included in CA 2.1.1.1, you will have to regenerate the certificate after upgrading. If you do not regenerate, Content Analysis will still use the SHA-1 certificate.

What's New in CA 2.1.1.1

This release of Content Analysis includes the following new features.

On-box Sandboxing

In Content Analysis 2.1.1.1, Malware Analysis is now an integrated, on-box technology for detecting and analyzing unknown, advanced, and targeted malware. This adaptive and customizable sandbox solution delivers comprehensive malware detonation and analysis using a unique, dual-detection approach to quickly analyze suspicious files and URLs, interact with running malware to reveal its complete behavior, and expose zero-day threats and unknown malware.

Note that enabling the on-box sandboxing will decrease the throughput for the appliance, but will also increase your detection capabilities.

The on-box Malware Analysis dual-detection approach combines virtualization and emulation to capture more malicious behavior across a wider range of custom environments.

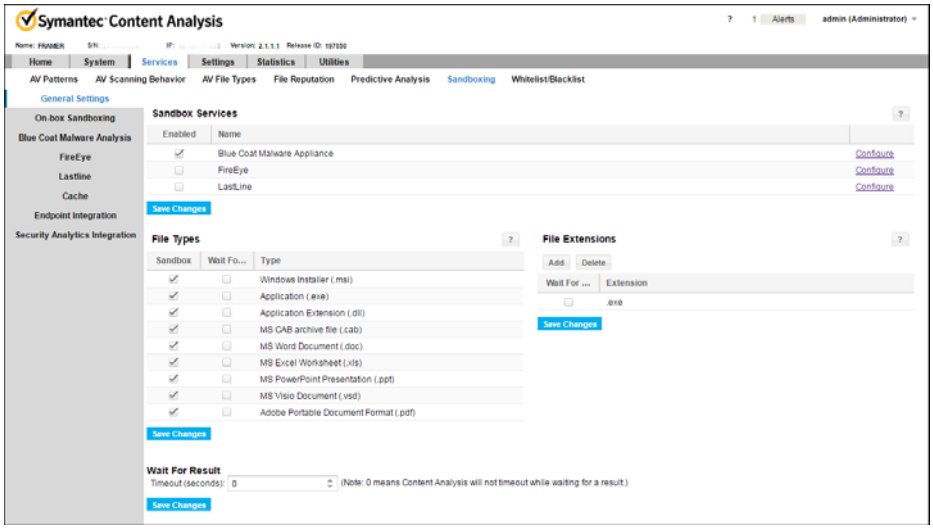
- **Emulation Sandbox:** An instrumented, fully controlled, replicated PC computing environment emulates Windows systems to detect malware that otherwise will not detonate within a virtualized environment
- **Virtualization Sandbox:** Custom analysis profiles replicate a Windows 7 64-bit production environment, including applications and browsers used. The sandbox can quickly spot anomalies and behavioral differences that unveil anti-analysis, sleep, and other advanced evasion techniques. A virtualized Android sandbox detects and analyzes mobile threats traversing enterprise networks.

See Use On-box Sandboxing in the Content Analysis 2.1 WebGuide.

Note: The Content Analysis VA and CAS S200 appliances do not support on-box sandboxing.

Improved Sandboxing UI

To better accommodate the expansion of sandboxing options in CA 2.1.1.1, the sandboxing UI screens and menus have been reorganized.



Integration with Symantec Endpoint Protection Manager

When Content Analysis is integrated with Symantec Endpoint Protection Manager (SEPM), the endpoint computers are managed by SEPM and proxied through a ProxySG that is connected to Content Analysis. After configuring SEPM to work with Content Analysis, the administrator will be sent a threat alert when sandbox analysis reveals a file to be malicious. The admin then has the option of adding the file hash to a file fingerprint hast list (blacklist) on the SEPM. Once the SEPM knows about this threat, no other end users will be able to run the file since it is on the endpoint blacklist; this stops the lateral spread of a malicious file on the network. In addition, administrators have the option of running SEPM remediation policy to clean up the initial infection.

See Integrate with Symantec Endpoint Protection Manager in the Content Analysis 2.1 WebGuide.

Expanded Command-Line Interface

CA 2.1.1.1 includes a robust set of CLI commands for configuring and monitoring the appliance. Documentation for all CLI commands have been compiled into a single PDF. Alternatively, you can view the documentation for a single command by selecting the command from a drop-down list in the WebGuide.

See *Content Analysis 2.1 Command Line Interface Guide* (PDF) or CLI Commands in the Content Analysis 2.1 WebGuide.

Recent Threats Report

The Recent Threats report lists the 1000 most-recent threats, 20 threats per screen page. For each threat, the report lists the date and time of detection, the name of the malicious file, the URL link to the file, the user who attempted to download the file, Content Analysis suggested action (block or serve), and a link to a full report on the threat.

Time Stamp	File Name	URL	Authenticated User	Suggested Action	
2016-10-01 08:27:37 (PDT)	eicar%20%28another%20cop...	http://localhost/eicar%20%28anot...		BLOCK	View Report
2016-10-01 08:27:37 (PDT)	eicar_com%20%28copy%29.zip	http://localhost/eicar_com%20%2...		BLOCK	View Report
2016-10-01 08:27:36 (PDT)	eicar%20%283rd%20copy%2...	http://localhost/eicar%20%283rd...		BLOCK	View Report
2016-10-01 08:27:35 (PDT)	eicar.com.txt	http://localhost/eicar.com.txt		BLOCK	View Report
2016-10-01 08:27:35 (PDT)	eicar_com.zip	http://localhost/eicar_com.zip		BLOCK	View Report
2016-10-01 08:27:35 (PDT)	eicar%20%28copy%29.com.txt	http://localhost/eicar%20%28copy...		BLOCK	View Report
2016-10-01 08:27:34 (PDT)	eicar%20%286th%20copy%2...	http://localhost/eicar%20%286th...		BLOCK	View Report
2016-10-01 08:27:33 (PDT)	eicar%20%284th%20copy%2...	http://localhost/eicar%20%284th...		BLOCK	View Report

See View Recent Threats Reports in the Content Analysis 2.1 WebGuide.

File Submission REST API

Symantec provides a REST API for submitting individual files to Content Analysis for evaluation using the current configuration. The API is available to people or programs that want to know how Content Analysis would evaluate a file but don't want to translate it into ICAP, the web-centric protocol that Content Analysis uses. Examples of how the API can be used:

- Use the API with an email gateway to evaluate file attachments.
- Create a script running on a file server to periodically check for malicious files.
- Create a program that submits individual files so that an analyst can see if they are malicious or contain viruses.

Note: This version of the REST API is considered to be phase 1 and is a limited submission API.

The API is asynchronous and uses WebSocket protocol, which provides full-duplex communication channels over a single TCP connection, to deliver the scanning verdicts to the client. This document describes how to subscribe to the WebSocket, process the results, and submit files for evaluation.

See the *Developer's Guide for Content Analysis File Submission REST API* (PDF).

Upgrade Notes and Behavior Changes

WARNING! The upgrade process can take 15 minutes or more to complete, and during this time the appliance may appear to be hung. While Content Analysis is in the middle of a major upgrade, interrupting the process will damage the CA appliance. Do not power cycle the unit during the upgrade process! You will know that the upgrade is complete when you can successfully log in to the management console or the command-line interface.

- The CA 2.1 Virtual Appliance requires more memory than previous versions (16 GB RAM vs. 8 GB RAM). You may need to add memory when upgrading from CA 1.3 to CA 2.1.

- Static Analysis in CA 1.3 is now called Predictive Analysis in CA 2.1.
- The File Reputation scoring system has changed in CA 2.1. In previous versions, the service used a 0-10 trust score system, with low scores being untrusted and high scores being considered safe. In CA 2.1, the service uses reputation scores, numbers (1-10) that indicate whether files are known to be trusted or malicious; low scores are less likely to be threats whereas high scores are more likely. Depending on the reputation score, files are then either blocked if the score is high, passed to the user as safe if the score is low, or processing continues with antivirus scanning and sandboxing if the service doesn't know whether the file is malicious.
- TTF is no longer a supported file type that can selected for sandboxing submission. If you had selected the TTF file type in CA 1.3.x, upon upgrade to CA 2.1.x, that file type will be removed from the list and will not be sent to sandboxing. [B# CAS-2838]
- CA 2.1.x requires the system to have a user named *admin* with an administrator role and does not allow you to delete it. Because CA 1.3 did not have this requirement, the following situations may occur after upgrading to CA 2.1.x:
    - If an admin user did not exist in CA 1.3, CA 2.1.x will create an admin user with no password. You should immediately go to the **Settings > User > Local Users** page and assign a password to the admin user.
    - If the admin user had a *read-only* role in CA 1.3, CA 2.1.x will change the role of the admin user to *administrator*. [B# CAS-2837]
- The password (if set in CA 1.3) for entering enable mode in the CLI will not be migrated to CA 2.1.x. Use the **`enable-password`** CLI command to specify a password for entering enable mode. [B# CAS-3200]

  ```
  (config-authentication)# enable-password
  ```
- Troubleshooting logs and core files are not migrated during an upgrade to CA 2.1.x. [B# CAS-3215]
- If you had configured static routes in CA 1.3, all routes associated with a NIC might fail to migrate after upgrading to CA 2.1.x. This situation could happen if the next hop for any route is not accessible when the appliance is upgraded; if this occurs, all of the route settings associated with the same NIC will be removed from the configuration. [B# CAS-2893]
- In CA 1.3, any unconfigured NICs (those with no address assigned) are automatically enabled, whereas in CA 2.1.x, NICs that are unconfigured are disabled. On upgrade to CA 2.1.x, any NICs that were not configured in CA 1.3 will not automatically be available in CA 2.1.x. Therefore, you will need to enable the NIC in the CLI before you can use or configure it in the UI. [B# CAS-2330]

  For example: `(config)# interface 2:0 enable`

Content Analysis 2.1.1.1 Known Issues

CA 2.1.1.1 has the following known issues.

- When upgrading from CA 1.3.7.5, do not use the **Upload System Image** option to upload a 2.1.x image file, as this method does not function properly in v1.3.7.5. (Note that this is *not* an issue in other 1.3.x versions or v2.x.)

  Workarounds: Place the image on a web server and use the **System Image Retrieval** option. Alternatively, reboot into another existing 1.3.7.x release before using the **Upload System Image** option.

- Content Analysis appliances running CA 2.1 can be managed by Management Center 1.10 or later versions. Note that previous versions of Management Center, such as MC 1.9, cannot authenticate to CA 2.1 appliances.

- The on-box sandboxing feature requires that the Sandbox Broker license also be enabled. If it's not enabled, samples won't be submitted to on-box sandboxing for processing. [B# CAS-1430]

- Content Analysis is able to decompress/extract files from archives that have been compressed with gzip, bzip2, xz, lzip, and several other popular compression algorithms. If the archive uses a supported compression algorithm, CA will be able to decompress the archive and send files within the archive to configured sandboxes for analysis. For zip and tar files with alternate compression algorithms (Lzma, ppmd, deflate), CA will not be able to decompress the file but will send the archive to the sandbox if CA is configured to send this file type. Whether the sandbox application or service can decompress the archive and analyze its contents depends on the capabilities of the program. In the case of Symantec Malware Analysis, archives will bypass sandbox analysis. [B# CAS-2813]

- After running the initial configuration wizard, Content Analysis creates a default ICAP certificate using the common name from NIC 0:0, even if this NIC was not configured. Because the ProxySG uses the certificate's common name to verify Content Analysis' identity, the ProxySG will not be able to verify the identity if this field is blank and will fail to connect to the CA. To avoid this problem, configure 0:0 before other NICs. If you cannot configure 0:0 first and plan to use secure ICAP, you can generate a new ICAP certificate using the appropriate common name. [B# CAS-2724]

- Historical connections are not persisted and will clear on shutdown. [B# CAS-3190]

- When Content Analysis is integrated with Security Analytics and SNMP trap alerts are enabled for the Sandboxing Threat Admin Alert (Asynchronous), the Security Analytics report URL does not show in the trap message. [B# CAS-3156]

- SEPM/CA integration does not work properly through an explicit proxy (that is, when the **Use HTTP Proxy** is selected). [B# CAS-3379]

- In the MIB, bchrSerial.0 shows *SNMP No Such Object* instead of the serial number. [B# CAS-2402]

- Load balancing between external appliances and the on-box sandboxing service may result in a slight detection difference within your load balanced cluster, and if CA is not properly configured, a sample may not get processed. [B# CAS-2808]
- The on-box sandboxing settings for firewall and dirty line network are not stored in the exported configuration file. [B# CAS-1564]

CLI Issues

- When you configure a password parameter on the command line, the password displays in plain text. WORKAROUND: To obfuscate the password, do not enter the password on the same line as the command; instead, press Enter and type the password when prompted. [B# CAS-2092]

  Example:

  ```
  # sandboxing symantec-endpoint-protection password
  (<Encrypted string>): ****
  ```

- The CLI includes an option to configure heuristics for McAfee (**`services mcafee heuristic`**); however, this option is not supported on McAfee. [B# CAS-3286]
- If you use the CLI to configure NIC 0:0 as the dirty line interface for on-box sandboxing, the CA management console will become inaccessible. If this happens, use the CLI to configure a different NIC as the dirty line interface. [B# CAS-3377]
- Password restrictions configured with the **`password-policy`** CLI command are not enforced. [B# CAS-2616]
- The TLS settings configured with the **`web-management https handshakes`** CLI command are non-functional. [B# CAS-3081]

Symantec Support

Direct support questions regarding this release to Symantec Support for Blue Coat products. For more information, visit:
https://support.symantec.com

For feedback on the Content Analysis documentation, send emails to documentation_inbox@symantec.com.

Americas:

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

Rest of the World:

Symantec Limited
Ballycoolin Business Park
Blanchardstown, Dublin 15, Ireland