Content Analysis 3.0.1.1 Release Notes

Product Version: 3.0

Release Date: March 24, 2020

Build Number: 249223

Document Date: March 24, 2020

Introduction

These release notes apply to Symantec Content Analysis 3.0.1.1. Refer to the *Content Analysis Quick Start Guide* poster (included with your appliance or available at Broadcom Tech Docs) for initial configuration and licensing details.

Release Notes Contents

Upgrade Path to Content Analysis 3.0.1.1

Caution: Direct upgrade from versions that have reached End of Life (EOL) is not supported.

Current Version	Upgrade Path	Notes
2.4.x	➔ 3.0.1	Direct upgrade is supported from all 2.4.x versions
2.3.5.1 or higher	➔ 3.0.1	Direct upgrade is supported from 2.3.5.1 or higher
2.3.1.x-2.3.4.x	➔2.3.5.1 or higher ➔3.0.1	Upgrade first to 2.3.5.1 or higher
2.2.x (EOL)	➔2.3.5.1-2.4.x ➔3.0.1	Upgrade to 2.3.5.1 or 2.4.x before upgrading to 3.0.1
2.1.x (EOL)	➔2.3.5.1 ➔3.0.1	Upgrade to 2.3.5.1 before upgrading to 3.0.1
1.3.7.8 (EOL)	➔2.3.5.1-2.4.x ➔3.0.1	Upgrade to 2.3.5.1 or 2.4.x before upgrading to 3.0.1
All versions prior to 1.3.7.8 (EOL)	➔1.3.7.8 ➔2.3.5.1-2.4.x ➔3.0.1	Upgrade to 1.3.7.8 before upgrading to 2.3.5.1 or 2.4.x, then upgrade to 3.0.1.

Note: Due to changes in the load-balancer protocol, if a standalone Malware Analysis appliance has the load-balancer protocol enabled (with the **`sandboxing > symantec-malware-analysis > load-balancer-support`** CLI command), you must upgrade both the Content Analysis and the Malware Analysis appliances to version 3.0. If you upgrade Content Analysis but not Malware Analysis (or vice versa), sandboxing submissions will fail.

Upgrade Procedure

Follow these steps to upgrade from Content Analysis 2.3.5.1 or 2.4.x to version 3.0.x.

Tip: If your Content Analysis appliances are being managed by Management Center, refer to the topic Upgrade System Images on Managed Devices for instructions on using MC to update your appliances.

1. Back up your Content Analysis configuration using the **Utilities > Configuration > Get Configuration** option in the Content Analysis web UI.

   > **Note:** Prior to upgrading to 3.0.x, verify that all of your Quick Analysis tasks have completed.

2. Log in to MySymantec. Follow the instructions in Knowledge Base article 151364 to download the Content Analysis 3.0.x image.

   > **Note:** During the upgrade process, Symantec recommends that you disable the Content Analysis appliance from receiving production traffic to prevent issues that could affect users while the system reboots. In addition, this will avoid potential loss of analysis data.

3. On the **System > Firmware** page in the management console, upload the system image. Reboot with the new image.
4. For this pre-release version of CA 3.0, it's necessary to perform a factory reset after upgrading.
   a. Connect to the serial port, enter enable mode, and issue the `restore-defaults factory-defaults` CLI command.
   b. Run the Initial Configuration Wizard to configure the Content Analysis network settings.

Downgrade Support

Because of infrastructure changes introduced in Content Analysis 3.x, downgrades to 2.x and 1.x are not supported; a factory reset would be required after downgrading.

Platform Support

> **Caution:** The CA 3.0 release is not supported on the CAS-S200 platform.

Platform	On-Box Sandboxing	iVMs Supported (Balanced Profile)	iVMs Supported (Sandboxing Profile)
Amazon Web Services instance		n/a	n/a
CASVA-100 and high-performance VA models (such as CAS-VA-C4S)		n/a	n/a
CAS-S200-A1		n/a	n/a
CAS-S400-A1	✓	2	2

Platform	On-Box Sandboxing	iVMs Supported (Balanced Profile)	iVMs Supported (Sandboxing Profile)
CAS-S400-A2	✓	2	3
CAS-S400-A3	✓	4	8
CAS-S400-A4	✓	4	12
CAS-S500-A1	✓	12	36

Product Compatibility

When integrating Content Analysis 3.0.x with other Symantec and third-party products, the following versions are required.

- Symantec Reporter 10.1.4.1 or later
- Symantec Management Center 1.10.1.3 or later
- Symantec Endpoint Protection Manager 14 or later
- Symantec Messaging Gateway 10.6.3 or later
- Symantec Malware Analysis 4.2.11 or later (ciphers in earlier versions are incompatible with CA 2.3)
- Symantec Security Analytics: 7.3.1 or later (Version 7.3.1 requires that the user name for CA integration be **admin** or **apiuser**. For versions 7.3.2 and later you can specify any account name.)
- FireEye AX 8.0.0 has been tested, although other versions may work
- FireEye NX—any version
- Countertack 1.x only
- Lastline—any version

Web Browser Support

Symantec has tested the Content Analysis 3.0.x web management console with the following web browsers:

- Microsoft Internet Explorer version 11 (Note that IE 11 does not support file uploads larger than 4GB; this may affect ISO and base image imports for on-box sandboxing.)
- Mozilla Firefox, latest stable release
- Google Chrome, latest stable release

New Features in Content Analysis 3.0.1.1

New features in Content Analysis 3.0 include the following.

IPv6 Support

For version 3.0, Content Analysis supports IPv6 in the following areas:

- Dual IPv4/IPv6 networks, including an IPv6 and IPv4 router for accessing IPv4 networks
- Network settings can be IPv4 and/or IPv6:
  - Interfaces
  - Default gateway
  - DNS servers
  - Static routes
- Management interface – Web UI and REST APIs
- Servers for alert notifications (email, syslog, and SNMP traps)
- Reporter server
- Proxy server
- SSH CLI access
- SNMPv2 and v3
- NTP for the Content Analysis side
- iVM profile customization (see also IPv6 Limitations below)
- Symantec Malware Analysis appliance

> **Note:** Malware Analysis functions require that you enable IPv6 with the following command: **`ma-settings network ipv6 enabled`**

- ICAP connections with IPv6 clients
- IPv6 support for these features requires a NAT64 translator:
  - External lookups
  - Malware Analysis pattern downloads

  - iVM ISO import, if importing from an external IPv4 network
  - Profile import/export, if importing from an external IPv4 network
  - Symantec web services communications

- IPv6 limitations:
  - If the management IP address is IPv6, you cannot use KMS to activate Windows in an iVM, nor can you use product key online activation. After a product key online activation fails, you will be given an option to do offline activation. With offline activation, Windows will generate an installation ID that you provide to Microsoft via phone; Microsoft will then give you a confirmation ID to complete the Windows activation.
  - The dirty line supports IPv4 only, so a Content Analysis appliance on an IPv6-only network needs a separate IPv4 connection; otherwise, samples will not have connectivity to the internet during iVM detonation.
  - During customization of IntelliVM profiles, IPv4 access from within the iVM is not available in an IPv6-only network.
  - Alerts for Malware Analysis task completions are not sent to syslog servers that have an IPv6 address. Note that this only applies to alerts that are configured with the **`ma-settings remote_syslog`** CLI command.

> **Note:** Further IPv6 support will be available in future versions of Content Analysis.

Support for Mutual SSL and SSH Authentication

Users can now authenticate to the Content Analysis Web UI or an SSH utility with a Common Access Card (CAC) or client certificate.

Idle Detection for File Detonation

In earlier versions of Content Analysis a file would be opened in an IVM and then kept open for 60 seconds, even though in most cases there are few or no events after opening the file. In Content Analysis 3.0 most PDFs and Office files that are opened in Adobe Reader 9 and earlier will remain open for only 10-15 seconds. (This feature is not yet compatible with Adobe Reader DC and Office 2013 running on Windows 10.)

SHA256 Hash Support for Black and White Lists

You can now add SHA256 hashes to the black and white lists along with SHA1 hashes.

PE/EXE Information in Activity Report

At the top of the Activity Report on the task summary is a new **PE_info** field that displays the file description, file version, company name, and copyright information.

Dynamic Information in Static Event List

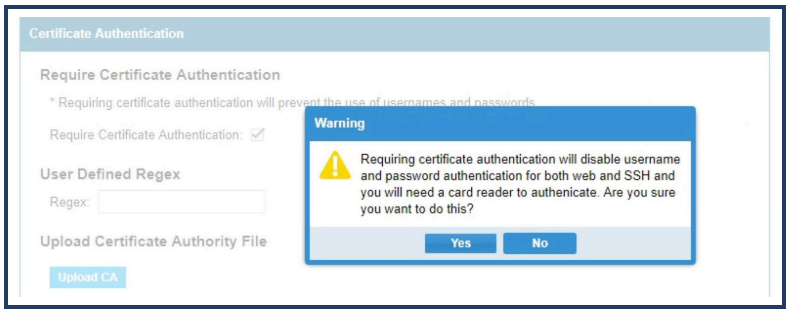
Because the line between static and dynamic events is increasingly blurred, dynamic information is now included in the Static Event List.

Support for Windows 10 Version 1809

See Supported Windows ISOs for Content Analysis (DOC11424) for the complete list of supported ISOs.

Behavior Changes

- Memory usage is calculated differently from previous versions. This more-accurate method results in a higher amount than previously. For example, a 55% memory usage in earlier versions would now be calculated as 75%.
- Selecting the **Require Certificate Authentication** option (**Settings > Web Management**) now prompts you to confirm your decision:



The Require Certificate Authentication checkbox is selected or cleared automatically depending on your selection.

Resolved Issues in Content Analysis 3.0.1.1

The following issues have been resolved in Content Analysis 3.01.1:

- LDAP certificates were not included when settings were exported. [NPPCAS-65861]
- After a network route was added, a modification to that route caused it to be deleted. [NPPCAS-5471]
- Content Analysis displayed an error message if you tried to download a base image while the system was in the process of downloading another base image. [NPPCAS-5113]
- The on-box sandboxing feature required that the Sandbox Broker license also be enabled. [NPPCAS-1430]
- An invalid iVM profile error was returned by the new scan API. [NPPCAS-65765]
- When rebuilding a profile the "driver out of date" message was displayed. [NPPCAS-65886]
- In the MIB, the published version was shown as 2.1.1.1 instead of the current version. [NPPCAS-65690]
- API keys could not be created for usernames with non-ASCII characters. [NPPCAS-65742]
- Tasks from versions previous to 2.4.1 were not searchable. [NPPCAS-65754]
- LDAP certificates could not be edited in the UI. [NPPCAS-65860]
- Detonation of **basic-events-x86.exe** sometimes failed on Windows XP. [NCPPCAS-65997]
- The AML threat score was not displayed. [NPPCAS-65940]
- After cancelling a large sample that was submitted manually, the previously submitted files were not processed. [NPPCAS-65946]
- Windows dumped full system memory when a bug was detected, rendering the iVM inoperable for a long time. [NPPCAS-65884]
- The closed-network Symantec AV uploads did not support HTTPS. [NPPCAS-6796]
- Attempting to open the help file on the *Task Details* page returned a 404 error. [NPPCAS-6571]
- A sample did not generate a memdump. [NPPCAS-5902]
- The "Sending Request" message continued to be displayed even after downloading a base image from a URL was successful. [NPPCAS-5455]
- Secure ICAP failed to negotiate handshakes with DHE and ECDHE ciphers. [NPPCAS-6657]
- With enhanced scanning enabled for Kaspersky AV, an error was returned when UTF-8 was used in the **`Content-Disposition`** header. ICAP errors were also produced. [NPPCAS-65795, 6204]
- The AV service was restarted by the watchdog when non-secure ICAP was disabled. [NPPCAS-65730]
- Malware reports showed UTC time instead of local time. [NPPCAS-65729]

- A certificate chain that was imported via the web UI was not presented as imported, and if it had a strong password it resulted in failure. [NPPCAS-65673, 65707]
- Polling OID 1.3.6.1.4.1.3417.2.1.1.1.4.0 resulted in a **`No such instance currently exists`** error message. [NPPCAS-6649]
- SSL ciphers for the management console did not update after being configured. [NPPCAS-6265]
- McAfee updates were out of date. [NPPCAS-5454]
- RADIUS authentication requests were being rejected. [NPPCAS-5453]
- AV file directories were not cleared during a force update. [NPPCAS-5213]
- Blocking TMP files resulted in all files larger than 10MB to be blocked. [NPPCAS-5201]
- In some cases, upgrading to 2.3.x from 2.2.x produced this error: **`unregister_netdevice: waiting for lo to become free. Usage count =1`**. [NPPCAS-1288]

Security Advisories Addressed in 3.0.1.1

Content Analysis 3.0.1.1 addresses vulnerabilities in the following Symantec Security Advisories:

- SA110–Java Deserialization Vulnerabilities
- SA133–Birthday attack against DES, 3DES, and Blowfish
- SA144–OpenSSH Vulnerabilities

Consult the Symantec Enterprise Security Advisories for the latest information on Content Analysis security vulnerabilities and fixes:

https://support.broadcom.com/security-advisory/security-advisories-list.html

Known Issues

This table tracks some of the latest known issues.

Found In	Issue	Fixed In
3.0.1.1	Alerts for Malware Analysis task completions are not sent to syslog servers that have an IPv6 address. Note that this only applies to alerts that are configured with the **`ma-settings remote_syslog`** CLI command. [NPPCAS-66770]	
3.0.1.1	When you shut down the system in the Web UI, a message box appears that is titled "Could not connect to server." This message is to be expected. After you close the message box, the system will shut down, and you should refresh the browser page as instructed. [NPPCAS-66714]	
2.4.1.1	In some cases enabling **`winrm`** fails on CAS-S400-A1 and CAS-S400-A2. [NPPCAS-5821]	
2.4.1.1	The closed-network Symantec AV uploads do not support HTTPS. [NPPCAS-6796]	3.0.1.1
2.4.1.1	Windows dumps full system memory when a bug is detected, rendering the iVM inoperable for a long time. [NPPCAS-65884]	3.0.1.1
2.4.1.1	After cancelling a large sample that was submitted manually, the previously submitted files are not processed. [NPPCAS-65946]	3.0.1.1
2.4.1.1	The AML threat score is not displayed. [NPPCAS-65940]	3.0.1.1
2.4.1.1	Detonation of **basic-events-x86.exe** sometimes fails on Windows XP. [NCPPCAS-65997]	3.0.1.1
2.4.1.1	An invalid iVM profile error is returned by the new scan API. [NPPCAS-65765]	3.0.1.1
2.4.1.1	When rebuilding a profile the "driver out of date" message is displayed. [NPPCAS-65886]	3.0.1.1
2.4.1.1	In the MIB, the published version is shown as 2.1.1.1 instead of the current version. [NPPCAS-65690]	3.0.1.1
2.4.1.1	API keys cannot be created for usernames with non-ASCII characters. [NPPCAS-65742]	3.0.1.1
2.4.1.1	Tasks from versions previous to 2.4.1 are not searchable. [NPPCAS-65754]	3.0.1.1
2.4.1.1	LDAP certificates cannot be edited in the UI. [NPPCAS-65860]	3.0.1.1
2.4.1.1	LDAP certificates are not included when settings are exported. [NPPCAS-65861]	3.0.1.1
2.3.5.1	When updating the performance profile a "configuration locked" error is returned on the back end, and in the web UI clicking **Save** returns a *Failed* message. Attempting the update again resolves the problem. [NPPCAS-6459, 65880]	2.4.1.1
2.3.5 and earlier	During Symantec AV upgrades the process could potentially dump the core. [CARRERA-12515]	2.4.1.1
2.3.5.1	Sometimes pattern updates must be forced after an upgrade or downgrade. [NPPCAS-6592]	
2.3.5.1	When SNMP settings are configured in the CLI, they cannot be modified in the web UI. [NPPCAS-2723]	2.4.1.1
2.3.5.1	After a network route is added, a modification to that route causes it to be deleted. [NPPCAS-5471]	3.0.1.1

Found In	Issue	Fixed In
2.3.5.1	When integrating with ASG 6.6.x, the port number cannot be changed in the web UI. [NPPCAS-5640]	2.4.1.1
2.3.5.1	Symantec AV pattern updates are not logged. [NPPCAS-6231]	2.4.1.1
2.3.1.1	Content Analysis displays an error message if you try to download a base image while the system is in the process of downloading another base image. [NPPCAS-5113]	3.0.1.1
2.3.1.1	When subsequent instances of an existing Windows OS version are added to on-box sandboxing, Content Analysis creates the base image but does not automatically create the iVM profile. [NPPCAS-4664]	
2.2.1.1	In rare situations, when a request modification (REQMOD) service is in use, Symantec AML may not catch MIME-encoded requests. [NPPCAS-4463]	
2.1.1.1	The on-box sandboxing feature requires that the Sandbox Broker license also be enabled. [NPPCAS-1430]	3.0.1.1
2.1.1.1	When Content Analysis uses multiple sandboxing vendors, the FireEye alert and email contains the threat score from other vendors. [NPPCAS-3440]	

Symantec Support and Documentation

- Direct your support questions regarding this release to Symantec Support. For more information, visit https://support.broadcom.com/security
- For feedback on the Content Analysis documentation, send emails to documentation.inbox@broadcom.com.
- With Symantec's knowledge base subscription service, you can receive proactive email notifications when new articles are published, or when existing topics are updated with new information. For details, see Knowledge Base article 179888.

Legal Notice

Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Copyright © 2020 Broadcom. All Rights Reserved.

The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, please visit www.broadcom.com.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

Tuesday, March 24, 2020