Mike Weinstein Logout   🌐 Change Language

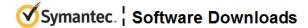**✓Symantec.** ┆ **Software Downloads**   ☰

Technical Support

Product Download

Content Analysis 2.3.1.1

| **Files** | View End User License Agreement ⧉ |

                                    ❓ Download Help

From this page you can download and obtain information about the specific product(s) below.

Upgrade Path to CA 2.3.x

Current CA Version	Upgrade Path
2.2.x	⇒ 2.3.x (direct upgrade)
2.1.x	⇒ 2.3.x (direct upgrade)
1.3.7.x	⇒ 2.1.x ⇒ 2.3.x
All versions released before 1.3.7.x	⇒ 1.3.7.x ⇒ 2.1.x ⇒ 2.3.x

Downgrade Support

❒ Because of infrastructure changes introduced in CA 2.x, downgrades to 1.x are
not supported; a factory reset would be required after downgrading.
❒ Downgrades from CA 2.3 to CA 2.2 and 2.1 are supported (with several
caveats; see below).

On-Box Sandboxing Downgrade Considerations

❒ Any IVM profile that existed in CA 2.1 will migrate properly to CA 2.2+. If
you customize an IVM profile in CA 2.2+ and then downgrade to 2.1, the
profile will not work unless you set the profile password to <blank>. To do
this, customize the IVM profile, open a command window, and type: net user
Admin "". This can be done before or after the downgrade.
❒ Any IVM profiles added or imported in 2.2+ will be removed after a
downgrade to 2.1. For example, if you downgrade to CA 2.1.1, you will lose
any profiles that were imported from a different Content Analysis appliance.

❒ If you add aWindows 10 base image in 2.2+ and downgrade to 2.1, the base

image and profile will be removed (sinceWindows 10 base images were not

supported in 2.1).

❒ If you downgrade from CA 2.3 to 2.2, re-running tasks that used ghost_user_with_unpacker.py (a plugin added in CA 2.3) will result in undefined behavior. Symantec recommends that you remove these invalid

tasks after downgrading; this applies to any tasks that use profiles and/or

plugins not available in the earlier release.

Other Downgrade Considerations

❒ After a downgrade from CA 2.3.1 to 2.1.1, Kaspersky and Sophos AV patterns

are no longer available, even after a Force Update. This problem occurs only

on the CAS-S200; CAS-S500 and CAS-S400 are not impacted by this issue. This

is not an issue when downgrading from CA 2.3.1 to 2.2.1. Workaround: Perform a factory reset using the restore-defaults factory-defaults CLI command. [CAS-5218]

❒ Some settings modified in an upgraded release may not be preserved if you

later downgrade, allowing the appliance to return to its state before the upgrade. For example, if you upgrade from CA 2.2 to 2.3, add LDAP, RADIUS, or local users, and then downgrade back to CA 2.2, the users you

added in CA 2.3 are not listed in the 2.2 configuration. This is expected behavior when downgrading.

| DOWNLOAD SELECTED FILES | Show All Files ☰ | 2 Files |

☐➕ File Description	⬍	File Size ⬍
☐➕ ca_2_3-213733.bcsi		1.2 GB
☐➕ Content_Analysis_2.3_Release_Notes.pdf		124.6 KB

DOWNLOAD SELECTED FILES