Product Download

CAS 1.3.7.5

Files View End User License Agreement Download Help

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

Description:
Patch Support Policy

The Patch Release version which you are about to download is intended to deliver a specific code fix(es) for issues experienced in certain situations based on given topologies or device configuration. Download and use of any Patch Release version should only be done if so instructed by Blue Coat Support personnel. Note that any patch release will be removed from the download site after the code changes are integrated into a subsequent Maintenance Release.

Resolved Bugs

- B#239977 - PDFs causing ICAP server error
- B#244436 - CAS deflates contents but responds with Content-Encoding:deflate
- B#237899 - CAS blocking download due to max total file size exceeded
- B#243986 - Immediately logged out of UI after signing in
- B#243118 - AV service restarts and config file gets corrupted
- B#243780 - Files dropped in CAS log with no explanation
- B#243260 - SNMPv3 alerts setting username string authentication failure
- B#240642 - Upgrade of device corrupts service.ini
- B#213527 - MTUs not working with Sophos

Security Fixes

- SA118 - Apache Tomcat Vulnerabilities
- SA126 - OpenSSH Vulnerabilities (full fix)
- SA132 - OpenSSL Vulnerabilities
- SA134 -"Dirty COW" Linux Kernel Vulnerabilities
- SA137 - NSS Vulnerabilities

Upgrade Notes

When upgrading from CA 1.3.7.5, do not use the Upload System Image option to upload an 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.

Downgrade Notes

The changes to security features in 1.3.7.X introduce new mechanisms for securing the appliance configuration. As such, if you downgrade from this release to 1.3.6.X, you will need to perform several additional steps before you can access the web management console following a downgrade:

1. Downgrade to the Content Analysis release of your choice.
2. Connect to the appliance through the serial console and choose option 2, Setup.
3. When prompted to regenerate ICAP and Web certificates, enter Yes.
4. Enter a new admin password.
5. Once the wizard is complete, enter restore-defaults reset-web to reset the Content Analysis Web server process.
6. Choose option 1, Command Line Setup
7. Enter enable mode by typing "en" and entering password
8. use the restore-defaults reset-web command
9. The web management console should now be running on port 8082 using https (example: https://my-machine-ip:8082)

After the above steps are complete, you can log in to the web management console normally.

DOWNLOAD SELECTED FILES

□	File Description	File Size
□	CAS_1_3-201666.bcsi	654.3 MB
	CAS 1.3.7.5 Compressed File Contents	

HTTPS Download	cas_1_3-201666.bcsi
File Type	
Operating System	
Product Description	
MD5 Signature	c706c73c3d0009a24893695ab82540bc

DOWNLOAD SELECTED FILES