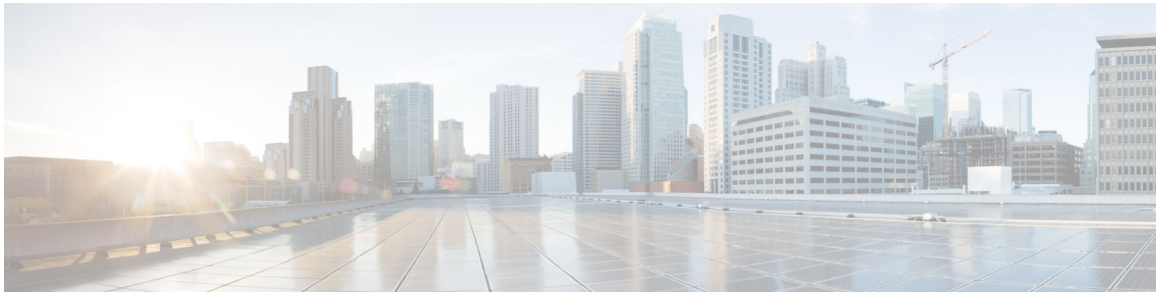

Release Notes for AsyncOS 10.6 for Cisco Web Security Appliances

Published: June 7, 2019

Contents

What's New In Cisco AsyncOS 10.6.0

The AsyncOS 10.6.0 release for Cisco Web Security appliances supports the following hardware models:

- S195
- S395
- S695
- S695F

For details, see

https://www.cisco.com/c/en/us/products/collateral/security/content-security-management-appliance/datasheet-c78-729630.html.

Note

- The L4 Traffic Monitor functionality is unavailable in this release due to the change in the way Free BSD 10.1 handles bridging.
- Web proxy bypassing, or blocking of domains or hostnames based on DNS IP snooping, dependent on L4 Traffic Monitor, is unavailable in this release.

Cisco Systems, Inc.
www.cisco.com

Feature	Description
Kerberos support for high availability clusters	While creating or editing an Active Directory realm, you can use the **Use keytab authentication** option in the Kerberos High Availability section, to enable Kerberos authentication for all appliances in high availability clusters. See the "Creating an Active Directory Realm for Kerberos Authentication Scheme", and "Creating a Service Account in Windows Active Directory for Kerberos Authentication in High Availability Deployments" topics in the user guide for more information.
Configure the number of Kerberos authentication helpers	You can use the CLI command `modifyauthhelpers` to configure the number of Kerberos authentication helpers.
List of Ciphers for AsyncOS for Cisco Web Security Appliances	A new document that lists the supported and unsupported ciphers (SSL and SSH) for AsyncOS for Cisco Web Security Appliances is available now. See https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html
SSH configuration	The following subcommands are added to the CLI command `sshconfig`: • `Incomplete SSH session timeout (in secs)` Default value is 60. • `Unsuccessful SSH login attempts allowed` Default value is 3.
FIPS mode update	The maximum number of password retry attempts permitted for access to the appliance through SSH is now 3.
Two-factor authentication	Cisco Web Security appliance now supports two-factor authentication that ensures secure access when you log into your appliance. You can configure two-factor authentication for your appliance through any standard RADIUS server that complies with a standard RFC. You can enable two-factor authentication through the web interface or the CLI: • System Administration > Users page in the web interface. See the Perform System Administration Tasks chapter in the user guide or online help. • `userconfig` > `twofactorauth` command in the CLI. See the Command Line Interface chapter in the user guide or online help. **Note** If your appliance is managed by a Security Management appliance, add the pre-shared keys in the Security Management and Web Security appliances using the `smaconfig` command in the CLI.

Feature	Description
Network Time Protocol (NTP) updates	• You can now configure the query interval and sync up delay time for NTP queries. You can enable authentication for NTP responses and requests sent and received between the appliance and NTP servers. MD5 and SHA1 are supported. You configure these settings through the web interface or the CLI: – System Administration > Time Settings page in the web interface. See the Perform System Administration Tasks chapter in the user guide or online help. – `ntpconfig` command in the CLI. See the Command Line Interface chapter in the user guide or online help.
FIPS mode updates	You can enable automatic shutdown of the appliance when logging of critical information fails. See the Perform System Administration Tasks chapter in the user guide or online help.
Logo support for the administrator login banner	You can use the `adminaccessconfig > logo` CLI to select a logo for the administrator login banner. See the Command Line Interface chapter in the user guide or online help.
User login status display for administrative user login	You can now see a list of successful and unsuccessful logins made through various protocols, independent of source IP addresses. This is displayed in the web interface and CLI, only for administrative users after logging in.
Forced re-authentication for non-administrative users after user type change	Users will be asked to re-authenticate after any user type changes made by an administrator. This change in user type will be displayed in the web interface, after the user re-authenticates. See the Perform System Administration Tasks chapter in the user guide or online help.
Samba upgrade	Samba version has been upgraded to version 4.5.8
SMB v2 and v3 support	SMB v2 and v3 protocols are now supported.
Enable or Disable Incremental Updates	You can use the CLI command `updateconfig > setup` to enable or disable incremental updates from the Web Reputation service. If you disable incremental updates, the appliance will continue to download the full updates from the Cisco server. **Note** Disabling incremental updates will result in delays in receiving updated web reputation information on the appliance. For more information, see the "Web Security Appliance CLI Commands" topic in the user guide.

Feature	Description
Support for Outbound ACL on the management port	A new subcommand OUTBOUNDACL is added to the CLI command `fipsconfig` to restrict IP addresses on the management port. Using this subcommand, you can configure IP addresses to which you want to restrict the appliance from making any outbound connections. This subcommand is available only in FIPS mode. You can perform the following actions using the subcommand OUTBOUNDACL: • Add New • Edit • Delete Clear
Support to configure login history	A new subcommand LOGINHISTORY is added to the CLI command `adminaccessconfig` to configure the number of days for which the login history is retained. Default value is 1 day. This is available in both FIPS and non-FIPS mode.
Support to configure maximum concurrent login sessions	A new subcommand MAXSESSIONS is added to the CLI command `adminaccessconfig` to configure the maximum number of concurrent sessions of the appliance through the Command Line Interface and web interface. Default value in FIPS mode is 3 and non-FIPS mode is 10. This is available in both FIPS and non-FIPS mode
WBRS enhancement	Currently when the WBRS update fails, it will revert to factory default settings. The new WBRS enhancement ensures that if the WBRS update fails or downloading the files fail during the update process, the WBRS reverts to the previous version. It will not revert to factory default settings.
Office 365 Web Service External URL Categories	You can configure your appliance with Microsoft Office 365 web service's external live feed which serves URLs and IPs. The web service URL must not contain a *ClientRequestId*, and must have JSON as the format.

Upgrading to AsyncOS 10.6.0

Upgrade paths are not available as this is a manufacturing release for x95 platforms.

Related Documentation

Documentation for this product is available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html.

Documentation for Cisco Content Security Management Appliances is available from http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html.

Support

Cisco Support Community

Cisco Support Community is an online forum for Cisco customers, partners, and employees. It provides a place to discuss general web security issues as well as technical information about specific Cisco products. You can post topics to the forum to ask questions and share information with other Cisco users.

Access the Cisco Support Community for web security and associated management:

https://community.cisco.com/t5/web-security/bd-p/5786-discussions-web-security

Customer Support

Note To get support for virtual appliances, call Cisco TAC and have your Virtual License Number (VLN) number ready.

Cisco TAC: Visit http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Support Site for legacy IronPort: Visit http://www.cisco.com/web/services/acquisitions/ironport.html.

For non-critical issues, you can also access customer support from the appliance. For instructions, see the User Guide or online help.