



CLAVISTER®

Clavister cOS Core Release Notes

Version 12.00.11

Clavister AB
Sjögatan 6J
SE-89160 Örnsköldsvik
SWEDEN

Head office/Sales: +46-(0)660-299200
Customer support: +46-(0)660-297755
www.clavister.com

Published 2018-09-19
Copyright © 2018 Clavister AB.

Clavister cOS Core

Release Notes

Version 12.00.11

Published 2018-09-19

Copyright © 2018 Clavister AB.

Copyright Notice

This publication, including all photographs, illustrations and software, is protected under international copyright laws, with all rights reserved. Neither this document nor any of the material contained herein, may be reproduced without written consent of the author.

Disclaimer

The information in this document is subject to change without notice. The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaim any implied warranties of merchantability or fitness for any particular purpose. The manufacturer reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of the manufacturer to notify any person of such revision or changes.

Limitations of Liability

UNDER NO CIRCUMSTANCES SHALL CLAVISTER OR ITS SUPPLIERS BE LIABLE FOR DAMAGES OF ANY CHARACTER (E.G. DAMAGES FOR LOSS OF PROFIT, SOFTWARE RESTORATION, WORK STOPPAGE, LOSS OF SAVED DATA OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES) RESULTING FROM THE APPLICATION OR IMPROPER USE OF THE CLAVISTER PRODUCT OR FAILURE OF THE PRODUCT, EVEN IF CLAVISTER IS INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHERMORE, CLAVISTER WILL NOT BE LIABLE FOR THIRD-PARTY CLAIMS AGAINST CUSTOMER FOR LOSSES OR DAMAGES. CLAVISTER WILL IN NO EVENT BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE AMOUNT CLAVISTER RECEIVED FROM THE END-USER FOR THE PRODUCT.

Table of Contents

1. Version Summary	4
2. New Features	4
2.1. New Features and Enhancements in cOS Core 12.00.11	4
2.2. New Features and Enhancements in cOS Core 12.00.10	4
2.3. New Features and Enhancements in cOS Core 12.00.09	5
2.4. New Features and Enhancements in cOS Core 12.00.08	6
2.5. New Features and Enhancements in cOS Core 12.00.07	8
2.6. New Features and Enhancements in cOS Core 12.00.06	8
2.7. New Features and Enhancements in cOS Core 12.00.05	8
2.8. New Features and Enhancements in cOS Core 12.00.04	8
2.9. New Features and Enhancements in cOS Core 12.00.03	9
2.10. New Features and Enhancements in cOS Core 12.00.02	9
2.11. New Features and Enhancements in cOS Core 12.00.01	10
2.12. New Features and Enhancements in cOS Core 12.00.00	10
3. Addressed Issues	13
3.1. Addressed Issues in cOS Core 12.00.11	13
3.2. Addressed Issues in cOS Core 12.00.10	13
3.3. Addressed Issues in cOS Core 12.00.09	15
3.4. Addressed Issues in cOS Core 12.00.08	15
3.5. Addressed Issues in cOS Core 12.00.07	17
3.6. Addressed Issues in cOS Core 12.00.06	18
3.7. Addressed Issues in cOS Core 12.00.05	18
3.8. Addressed Issues in cOS Core 12.00.04	19
3.9. Addressed Issues in cOS Core 12.00.03	20
3.10. Addressed Issues in cOS Core 12.00.02	21
3.11. Addressed Issues in cOS Core 12.00.01	21
3.12. Addressed Issues in cOS Core 12.00.00	21
4. New Features SSL VPN client	24
4.1. New Features and Enhancements in SSL VPN client 1.1.3	24
4.2. New Features and Enhancements in SSL VPN client 1.1.2	24
5. Addressed issues SSL VPN client	24
5.1. Addressed Issues in SSL VPN Client 1.1.3	24
6. Installation Instructions	24
6.1. Upgrade Considerations	24
6.2. Upgrading from a cOS Core 10.nn or 11.nn system	25
7. Known Limitations	25
8. Compatibility	26
9. Licensing	26
10. Getting Help	26

1. Version Summary

Clavister cOS Core 12.00.11 is the latest version of our award-winning network security operating system powering the Clavister Next Generation Firewall, our premium UTM security solution.

For a list of appliances that are supported by this version of Clavister cOS Core, please refer to the Compatibility section.



Important

If you are using InControl for centralized management please note that cOS Core 12.00.11 requires InControl version 1.83.00 or later. We recommend always using the latest version.



Important

*Clavister cOS Core 12.00.11 requires a Clavister subscription covering **Sept 1, 2018**. Make sure that this is covered before trying to upgrade the system, otherwise the system will enter a "License Lockdown" mode.*

2. New Features

The following sections detail new features and enhancements in Clavister cOS Core 12.00.11. For a complete list and description of all the features in Clavister cOS Core 12.00.11, refer to Clavister cOS Core Administration Guide 12.00.11.

2.1. New Features and Enhancements in cOS Core 12.00.11

- **NTP sync compatibility update**
Some NTP servers would return a 'RATE' error when the firewall was requesting time too quickly (on the same connection) so a delay has been added for compatibility. In addition, the source port for this connection has been changed from a fixed to a random port number.
- **Status page improvement**
The connections status page has been improved. The amount of data transferred on the connection is now shown in the table. Bytes from the originator, bytes from the terminator and total amount of bytes are shown.

2.2. New Features and Enhancements in cOS Core 12.00.10

- **General FQDN Policy Support**
It is now possible to configure and use FQDN address objects in Intrusion Detection, Threshold rules, IP policies, Traffic shaping and Policy Based Routing rules.
- **DNS Monitoring and Control**
The system has been enhanced with DNS monitoring support. By configuring an IP policy with a DNS profile (DNS-ALG), it is now possible to both monitor and control what type of DNS traffic that is allowed in the network. The DNS profile also plays a central role for FQDN Address objects configured with wildcard FQDN names. The DNS inspector uses the clients' DNS queries to populate the system's DNS cache which in turn is used by various FQDN supporting rule types.
- **Wildcard Support for FQDN Policies**
The FQDN address support for several system features has been improved with wildcard

support. It is now possible to configure Intrusion Detection, Threshold rules, IP policies, Traffic shaping and Policy Based Routing using FQDN address objects configured as domain filters. This will only work when combined with the new DNS-ALG to make the system learn the IP addresses for configured FQDN filters by monitoring clients' DNS traffic.

- **Removed Timezone and manual DST configuration**
The Timezone configuration has been converted to Location configuration and the manual DST configuration has been removed.
- **The IPsec interface "VPN Clients" renamed to "Roaming VPN"**
The simplified IPsec interface that was previously called "VPN Clients" had a name which could be confusing by referring to clients when the tunnel type actually is used when acting as a server. As of this release it is called "Roaming VPN".
- **New setting for "Non-Managed" categories for Email Control**
The Email Control Profile has been enhanced so the user can specify whether non-managed categories should be denied or allowed.
- **Enhanced WebUI ping tool**
It is now possible to specify FQDN/DNS names when using the WebUI Ping tool.
- **IP Reputation Database Improvements**
Improvements have been made to minimize any negative effects on performance when downloading and installing new IP reputation database updates.
- **ARP cache entry flushed on DHCP assignment**
The system's ARP cache could contain a MAC address of the previous DHCP lease holder. Any ARP cache entry matching an old lease is now removed when a client is offered an IP.
- **Usage filter capabilities for rules CLI command**
The rules CLI command has been extended with rule usage filter capabilities. For instance it will be possible to filter out rules that have never been used since the last system restart.
- **Enhanced WebUI view for IDP**
The overview page when viewing configured IDP rules has been enhanced with another column showing the configured/chosen service.
- **Better warnings for Real-Time Monitor Alerts**
A configuration warning for Device Monitor has been improved so that it now clearly states which Device Monitor object the warning is related to.
- **Updated GeoIP Database**
The GeoIP database has been updated to the 2018-05-01 release.
- **New Application Control Library**
The Application Library has been updated to version 1.380.
- **Desktop models E5 and E7 going End Of Life**
The firewall model E7 will be declared End Of Life on June 1st 2018 and E5 on December 11th 2018. This means that no more maintenance releases will be released for the E7. If you wish to receive further support and updates, get in touch with a Clavister partner to replace the firewall with a supported model.

2.3. New Features and Enhancements in cOS Core 12.00.09

- **Server Offline Notification for Server Load Balancing**
The Server Load Balancing feature has been extended with capabilities to send TCP Reset packets on established connections to a server that goes offline. Two modes of operation are available. The system can either passively send a TCP Reset packet when the system receives a packet from a client on a connection where the server has been flagged as offline. The

second alternative is to actively send a TCP Reset as soon as a server is detected to be offline, without waiting for the client to first send a packet. The second alternative requires additional state tracking within the system and thus more RAM resources.

- **Increased Browser Cache Time for WebUI Objects**
The HTTP header that tells the web browser how long a static object (like javascript files and images) can be cached has been updated. The web user interface now allows static object to be cached for 30 days, instead of 4 hours. The implemented fix will improve loading times.
- **Packet capture support for multiple ports**
The Packet Capture (pcapdump) function in the WebUI and CLI now supports using filters with multiple ports and ranges such as "67,68, 8080-8088".
- **IPv6 and FQDN netobject support for time server**
The time servers can now be configured with FQDN objects and/or IPv6 addresses. Existing time server configurations are automatically upgraded to use FQDN objects.
- **Updates to "ike-snoop" command**
The "ike-snoop-brief" command has been reworked to give fewer lines of output but with more information than before. It now prints some parts of the header like exchange type, SPIs and message ID together with the payload types of the packet. All this and the IPs/ports of the peers are written on two lines for each packet.
- **New filter option when deleting IKE and IPsec SAs by CLI command**
The "ike-delete" command has been extended with a "-tunnel" option that filters SAs on the IPsec interface they were negotiated on.

2.4. New Features and Enhancements in cOS Core 12.00.08

- **Improved HTTPS Performance**
HTTPS support has been added to the LW-HTTP engine. The LW-HTTP engine provides an HTTPS throughput performance boost of roughly 400%. The LW-HTTP engine supports Web Content Filtering and URL Blacklisting for HTTPS connections and is automatically enabled when used in an IP Policy with connected Web Profile. Existing IP Policy HTTPS configurations are automatically upgraded and will be using the new LW-HTTP engine when used with a Web Profile.
- **More secure self-signed certificates**
The default SSL certificate on the firewall is now generated using SHA-256 as the signature hash algorithm. This is also the hash algorithm used when generating new self-signed certificates through the web user interface. The system can no longer generate certificates with weak keys (512 and 1024 bits).

The HTTPS admin certificate is not automatically replaced during an upgrade. It is highly recommended to generate a new certificate if the configuration uses a weak HTTPS certificate (signed with SHA-1 and/or fewer than 2048 bits).
- **Added MAC Vendor information to Neighbor Devices list**
The Neighbor Devices information has been extended to show MAC Ethernet Vendor information in both the WebUI and the CLI.
- **Server Load Balancing functionality enhanced for unreachable servers**
The Server Load Balancing service will now respond with a reset (TCP RST / ICMP Port Unreachable) if it receives data from a client and monitor instance has detected the destination server down.
- **Default setting for minimum TLS version updated to TLS v1.2**
The new default setting for the minimum TLS version for SSL connections is now TLS v1.2, upgraded configurations will not be affected.

It is highly recommended to change minimum TLS version to v1.2 for existing configurations.

- **Updated default setting for allowing autocomplete on login page**
The default setting for WebUIAllowLoginAutoComplete has been updated to false, upgraded configurations will not be affected.
- **Shorter wait times when saving a new configuration in the web user interface**
The save and activate page, the upgrade page and the reset page have been improved. The browser now checks if cOS Core is up and running again, and if so refreshes the page instead of waiting until the timer has counted down to zero.
- **Improved Interface Status page**
The Interface Status page has been updated to show an overview of Ethernet and VLAN interfaces. The detailed interface information is still available as before.

On the detailed page more IPv6 information has been added and more details are shown for VLAN interfaces.
- **Web User Interface grid view enhancements**
Forward Routing Table and Return Routing Table have been added to the Policy-based Routing Rules grid.

More IPv6 information has been added in the Ethernet Interface grid, the VLAN Interface grid and the Link Aggregation Interface grid.

A column for authentication source has been added to the page of the Remote Management objects.
- **HTTP Protocol Upgrade Control**
A new setting has been added to the Web Profile to control whether HTTP Protocol Upgrade shall be allowed or not. The default behavior is to allow Protocol Upgrade which is commonly used for e.g. Web Sockets.
- **CLI command output updates**
The CLI command "dns" now also shows IP version for each configured server.

The CLI command "routemon" has been updated and now contains metric information for the routes.
- **Data Usage Filter added to "connection" CLI Command**
The "connection" CLI command has been extended with the possibility to filter connections based on the amount of data that has been processed on the connection.
- **Running statistics via the REST API**
The REST API has been enhanced and can now provide some statistical values. The information is similar to the information that can be retrieved using the "stats" CLI command. The path for the new method is /api/oper/stats and the only supported method is GET.
- **Device comment on the Web User Interface Dashboard**
The device comment has been added to the dashboard page. The comment and the device name can be changed on the System->Device->Name configuration page.
- **Updated GeoIP Database**
The GeoIP database has been updated to the 2018-01-02 release.
- **Application Control updates**
A new ixEngine version 5.2 has been included for the Application Control feature. The Application Library has been updated to version 1.370.1.

2.5. New Features and Enhancements in cOS Core 12.00.07

- **IPv6 support for SSH Remote Management**
It is now possible to configure an HTTP/HTTPS Management access filter with IPv6 networks or addresses, allowing IPv6 management access to the SSH interface.
- **Pre-allocation of HTTP sessions**
To improve performance directly after booting up, up to 50,000 HTTP sessions can be pre-allocated by the system. The number of allocated sessions is dependent on the number of sessions configured on service objects with the protocol set to HTTP. Pre-allocation will not occur on systems with 256MB of RAM or less.
- **License expiration notification**
A notification is now shown when a user logs in to the web user interface if the license on the unit has expired.
- **Enhanced support for character encoding in email attachments**
The mail header parsing has been enhanced with support for the mime parameter "filename" encoded in UTF-8 according to RFC2184.
- **New Application Control Library**
The Application Library has been updated to version 1.360.2.

2.6. New Features and Enhancements in cOS Core 12.00.06

No new features were introduced in the 12.00.06 release.

2.7. New Features and Enhancements in cOS Core 12.00.05

- **New Neighbor Devices status page**
A status page of neighbor devices has been added to the web user interface. The status page indicates the presence and status of neighboring devices that are communicating through the device.
- **DHCP status enhancement**
The DHCP status page for leases/mappings now shows the hostname and/or configured name for the leased addresses when applicable.
- **Dashboard graph time span change**
The dashboard graph showing 2 minutes now shows 6 minutes instead.
- **Update to stat CLI command**
The 'Last Shutdown' row of the stats CLI command was renamed to 'Last Event' to make it more clear since the log can contain entries not related to an actual system shutdown/restart (such as a reconfigure).
- **Updated GeoIP Database**
The GeoIP database has been updated to the 2017-11-06 version.

2.8. New Features and Enhancements in cOS Core 12.00.04

- **CLI enhancement for appending values**
Changing the value of a property that holds a list could only be done by replacing the entire list. Now an append and a remove operator have been added to the "set" command.
- **Device name in menu path**
To make it easier to identify the device for administrators configuring multiple devices, the device name has been added to the menu path at the top of configuration pages.

-
- **The option to disable AV/IDP signature update after reconfigure or HA activation**
Previously a check for updated AV/IDP signature files (and possibly a download if they were outdated) were always performed after a reconfigure or an HA failover. This can now be configured not to take place and the check for updated signature files will only take place according to the configured schema.
 - **Antivirus Advisory Link for Virus Found HTTP Page**
A clickable advisory link has been added to the 'virus found' web page displayed when a virus has been detected in an HTTP stream.
 - **Updated GeolP Database**
The GeolP database has been updated to the 2017-09-06 version.

2.9. New Features and Enhancements in cOS Core 12.00.03

- **Redirect Support for Web Profiles**
The existing whitelist and blacklist feature in web profiles has been extended with redirect support. It is now possible to configure a URL filter and redirect all matching traffic to another web page.
- **Shared address sender for High Availability timesync**
Timesync messages (NTP requests) were always sent using the local address as sender. The active HA node will now use the shared address for NTP requests.
- **Changed default file names of logs**
The file name of log files downloaded from the WebU has been improved with an indication of which type of log the file contains.
- **User defined Brute Force Protection settings**
Users can now define how many failed login attempts will be allowed on an admin/auditors account, as well as the number of seconds that account will be locked out.
- **Web Content Filter Reclassify Support**
The reclassify-setting used for Web Content Filtering has changed from providing a local submit form to provide a link to an external reclassification page. This change allows web profile configurations to use the faster LW-HTTP ALG even in scenarios where reclassification is allowed. The default 'ReclassifyURL' and 'RestrictedSiteNotice' banner files have been updated and any custom banner files are compatible so that they now show the new reclassify link.
- **High Availability (HA) status added to the dashboard**
HA status is now available again on the Web User Interface Dashboard. The status section is only shown on firewalls where HA is enabled.
- **New Application Control Library**
The Application Library has been updated to version 1.340.
- **Updated GeolP Database**
The GeolP database has been updated to the 2017-08-02 release.

2.10. New Features and Enhancements in cOS Core 12.00.02

- **SNMPv3 Traps**
The system now supports SNMPv3 Traps allowing authentication and encrypted communication for traps. Note that the SNMPv3 engine ID might change when upgrading to this version.

2.11. New Features and Enhancements in cOS Core 12.00.01

- **Support for new hardware models**

2.12. New Features and Enhancements in cOS Core 12.00.00

- **IP Reputation Powered by Webroot**

The system has been enhanced with IP reputation technology provided by Webroot. The firewall monitors all connections made through the system and provides a reputation score for the source and destination addresses. For IP addresses with a low reputation a threat category is logged together with the score. The web user interface has also been extended with an IP Reputation status page allowing additional filtering of IP reputation scores. The IP reputation database updates frequently with inclusions and exclusions of malicious IP addresses. Therefore the feature requires constant access to the Clavister Service Provisioning Network (CSPN) for cloud lookups and updates of the local database and cache mechanisms. IP Reputation requires a license.

IP Reputation is not available on E5, E7 or SG60 due to hardware limitations.

- **Threat Prevention Concept**

A new Threat Prevention section has been developed to group together threat prevention mechanisms within the web user interface and the centralized management software InControl. The Threat Prevention section includes both existing features as well as new features like Botnet, Scanner and DOS Protection. Existing features that have been moved into the Threat Prevention concept are Access Rules, IDP Rules, Threshold Rules and ZoneDefense configuration. In addition, the global IP Whitelist has also been positioned within Threat Prevention to exclude traffic from the mentioned threat prevention mechanisms.

- **GeoIP DOS Protection**

It is now possible to configure and block traffic from unwanted regions using GeoIP DOS Protection. The GeoIP DOS protection feature blocks traffic in the firewall at an early stage of the packet flow utilizing less processing power than normal IP rules/policies. It is suitable in scenarios where traffic from certain regions is not expected and can be used to minimize the DOS and malware attack surface from foreign regions.

- **Denial of Service Protection**

The system now supports Denial of Service Protection utilizing IP Reputation technology provided by Webroot. DOS Protection will when enabled, analyze the source IP address of a packet before allowing new connections to be opened. If the IP address is found to be a known DOS source, the IP address is automatically blacklisted for one minute. DOS Protection is a part of the new Threat Prevention concept.

- **Scanner Protection**

The system now supports Scanner Protection utilizing IP Reputation technology provided by Webroot. Scanner Protection will when enabled, analyze the source IP address of a packet before allowing new connections to be opened. If the IP address is found to be a known source performing reconnaissance such as probes, host scan or password brute force, the IP address is automatically blacklisted for one minute. Scanner Protection is a part of the new Threat Prevention concept.

- **Botnet Protection**

The system now supports Botnet Protection utilizing IP Reputation technology provided by Webroot. Botnet Protection will when enabled, analyze the source and destination IP addresses of a packet before allowing new connections to be opened. If any IP address is found to be part of a botnet, the botnet IP address will be blacklisted for one minute, preventing any traffic to and from the blacklisted address. Botnet Protection is a part of the new Threat Prevention concept.

-
- **HTTP/HTTPS Remote Management over IPv6**
It is now possible to configure an HTTP/HTTPS Management access filter with IPv6 networks or addresses, allowing IPv6 management access to the web user interface.
 - **New graphical profile**
The web user interface graphical profile has been updated to match the new company color and design guidelines.
 - **New WebUI System Overview**
The system overview page in the web user interface has been re-made to give more informative statistics of the traffic processed and analyzed by the firewall. New real-time graphs of blocked threats and malware have been added in addition to information of authenticated users and neighbor devices.
 - **Re-designed and Improved IPsec Status Page**
The IPsec status page has been redesigned to give a better overview of configured and established tunnels.
 - **Updated Styling for default user-auth Login Pages**
The styling for the default user-auth login pages has been updated to reflect the new styling and to work better on mobile platforms.
 - **Support for Elliptic Curve Ciphers**
Elliptic curve cryptography ciphers have been added for the TLS-ALG, WebUI Management and SSL-VPN. The new ciphers are TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA and TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256.
 - **UDP and TCP Traceroute Support**
The 'traceroute' CLI command has been extended with UDP and TCP protocol support for both IPv4 and IPv6.
 - **Persistent WebUI HTTP Connections**
The internal web server now supports persistent HTTP connections which reduces the number of connections required for HTTP/HTTPS management.
 - **Download anonymized configuration file**
A possibility to download an anonymized configuration file where sensitive data (such as PSK, user passwords, certificates) is replaced with standard template values has been added.
 - **Improved DHCP Server Logging**
Log messages produced by the firewall when a DHCP lease is given out now includes the host name of the receiving client, if available.
 - **Clear screen CLI Command**
A new 'clear' CLI command that clears the screen has been added.
 - **Updated 'techsupport' output**
When executing the 'techsupport' CLI command or downloading the Technical Support File from the WebUI, the commands: 'hwm' and 'pciscan' are executed in addition to all the previous commands.
 - **Updated Configuration and System Backup default Filenames**
When creating a configuration or system backup, the configured device name will be part of the file name of the downloaded file.
 - **Changed default file names of logs**
The file name of log files downloaded from the Web User Interface has been improved with an indication of which type of log the file contains.

-
- **Hardware Acceleration of TLS Handshake**
The TLS handshake will, on supported models, be handled by the built-in hardware accelerator. This will greatly improve the number of HTTPS session establishments that can be handled by the firewall. Supported models: E80, W20, W30, W40 and W50.
 - **IPsec tunnel configuration defaults to IKE version 2**
IKEv2 is now the default IKE version when creating new IPsec tunnels.
 - **Forced Safe Search Removed**
Forced use of Safe Search for search engines is no longer supported by the HTTP ALG and the Web Profile. The feature has been removed.
 - **Prevent disabling an interface with a MAC bound to the license**
If the interface with the licensing MAC address is disabled or deleted, the configuration activation will fail with an error message in order to prevent the device from entering lockdown mode.
 - **New Application Control Library**
The Application Library has been updated to version 1.320.
 - **Updated GeoIP database**
The GeoIP database has been updated to use the 2017-05-02 version.

3. Addressed Issues

The following sections detail the addressed issues in Clavister cOS Core 12.00.11 release.

3.1. Addressed Issues in cOS Core 12.00.11

- **COP-17144:** SNMP statistics was not available for some IP Policies.
- **COP-19493:** Upgrading a firewall could cause reboot loops if OSPF interfaces referred to an IPsecTunnel as interface and the network wasn't set.
- **COP-20487:** The firewall did not always use the fastest DCC server.
- **COP-20786:** Unknown algorithms in received IPsec proposal lists for IKEv1 could fail the whole negotiation.
- **COP-20843:** The system did not handle SNMPv3 Discovery requests correctly.
- **COP-20870:** On rare occasions, firewalls using DPDK as interface driver could make an unexpected restart.
- **COP-20973:** After a reconfiguration when changing the IPsec ConfigModePool object, the system could restart unexpectedly.
- **COP-21025:** An SNMPv3 event receiver did not use the specified routing tables when attempting connections to their specified IP addresses if the configured routing table was different from the main routing table.
- **COP-21090:** The CLI memory command formatting was incorrect and some values could exceed the set column width.
- **COP-21100:** IPsec tunnels used the IP address with the oldest lifetime when it tried to connect to an endpoint specified as an FQDN. It should now start with the latest IP address added instead.
- **COP-21109:** The WebUI configuration page showed an incorrect unit for the router priority of an OSPF interface.
- **COP-21134:** The SNMP value HOST-RESOURCES-MIB::hrSystemDate would be generated incorrectly when one of the time fields was zero resulting in partly invalid timestamp. The SNMP timestamp is now correctly formatted.
- **COP-21182:** If Route Monitoring failed on a route used for RADIUS authentication for an L2TP/PPTP Interface, unexpected system restarts could in some rare occasions occur.
- **COP-21212:** The WebUI dashboard Throughput graphs used interface receive data rate as source which is not always correct. The dashboard graphs have been changed to use interface send data rate to better reflect the current Throughput.
- **COP-21217:** Disabling DST did not stop the background service resulting in strange timezone offsets and time. The DST service is now properly stopped when the DST feature is disabled.

3.2. Addressed Issues in cOS Core 12.00.10

- **COP-20114:** The HTTP ALG handled HTTP responses for certain web pages incorrectly and made them unreachable. A system log about an 'invalid server http header received' was seen when trying to reach those pages.

-
- **COP-20170:** The WCF Log page would display a "No Logs" message even though the page contained WCF logs.
 - **COP-20177:** Multiple IKE SAs against the same peer with the same authentication method could cause issues with dropped traffic at rekey or HA failover. The peers of the tunnel could end up with different numbers of IKE/IPsec SAs if both peers initiated a negotiation at the same time. This could lead to packet loss for an extended time at rekey or failover until the peers detected and resolved the different states. The firewall is now more restrictive with multiple negotiations against the same peer to avoid any differences in state between the peers.
 - **COP-20241:** A security problem was present in the DNS subsystem.
 - **COP-20283:** Antivirus did not work as intended for singlepart messages when using POP3 or SMTP.
 - **COP-20412:** Email with very long padding just before end-of-email marker could cause a stall in SMTP and POP3 ALGs.
 - **COP-20649:** Upgrading a firewall firmware when running with configuration version 1 would bypass the strong password check resulting in that the admin user would be disabled and unable to login. The strong password feature is now disabled if initiating a firmware upgrade when the firewall is running a configuration with version 1 to prevent lockout.
 - **COP-20736,COP-20820:** The IPsec subsystem could in some rare occasions cause the system to restart unexpectedly.
 - **COP-20762:** The system sometimes restarted unexpectedly when mail was handled by the SMTP or IMAP ALG.
 - **COP-20768:** Removing an HA synced User could trigger unexpected behavior on the inactive node.
 - **COP-20831:** Using AutoEstablish on an IPsec tunnel could lead to duplicate IPsec SAs and/or negotiation failures.
 - **COP-20832:** The help text for "reset configuration" and "reset to factory" in the WebUI contained a reference to an incorrect default management interface on the E80B appliance model.
 - **COP-20871:** Certain rare setups with transparent mode could in rare occasions cause the firewall to make an unexpected restart.
 - **COP-20873:** DHCP Relay PPM limiting incorrectly applied to both requests and responses. Now it applies only to requests.
 - **COP-20874:** The distinction of IPv4 and IPv6 on the DNS client configuration page was missing.
 - **COP-20876:** The DHCP relay autosave timer was not used.
 - **COP-20895:** IPsec rekey were not triggered correctly by an HA cluster node that imported its SAs from its cluster peer.
 - **COP-20943:** Invalid memory access by the IPsec subsystem could in some rare cases occur during system shutdown.
 - **COP-20994:** The "authagentsnoop" CLI command could trigger unexpected behavior for certain packet types.
 - **COP-21137:** A typo in the IDP log message with ID 1300015 caused logs in InControl log format to miss a parameter.

3.3. Addressed Issues in cOS Core 12.00.09

- **COP-13499:** OSPF did not send any updates for a period of time after a reconfigure, which could cause problems for other OSPF nodes.
- **COP-14569:** After HA failover Application Control connections could stop working because of faulty classifications. The Application Control binding is removed from connections on HA failover to prevent connections from being miss classified.
- **COP-20334:** Multiple IPsec rekeys were sometimes initiated when IPsecLifetimeKiloBytes was exceeded.
- **COP-20609:** ARPCache authenticated users were not listed in the mouse-over popup on the dashboard. The users were counted in the total value, which made the sum of all authentication methods not match with the total value.
- **COP-20653:** The firewall could on rare occasions make an unexpected restart after logging into the WebUI when receiving a large number of user authentication requests against the REST API.
- **COP-20679:** Some IPsec log messages used source_ip and dest_ip as parameter names, while most other subsystems use srcip and destip as parameter names. The parameter names have been updated to be more aligned with the rest of the system. IPsec log message ID 103, 110, 111, 112, 113, 114, 115, 116, 117, 118 and 119 have been updated. This change also makes the source and destination IPs be parsed in the correct columns in the web user interface system log page, instead of being shown in the general text part of the message.
- **COP-20681:** A security issue was found and fixed in the WebUI.
- **COP-20724:** The IPsec interface name was not shown in the interface column in the web user interface memlog. The interface name was instead shown in the general text line.
- **COP-20760:** IKEv1 could be vulnerable to a Bleichenbacher attack when used in IPsec tunnels configured with certificate authentication. Reference ID CVE-2018-8753.
- **COP-20894:** Memory corruption could in some rare occasions occur during an IPsec Informational message exchange.

3.4. Addressed Issues in cOS Core 12.00.08

- **COP-15449:** Sending fragmented IP packets into an IPsec transport mode tunnel, where the resulting ESP packets were fragmented again when going out on the Ethernet interface, would cause the packets to be dropped by the receiver. The packets couldn't be reassembled correctly by the receiver due to lost fragmentation information. All fragmented IP packets going into a transport mode IPsec tunnel are now reassembled before encryption.
- **COP-15765:** The BIOS version check for virtual firewalls didn't handle version prefixes correctly.
- **COP-18840:** When acting as an L2TP/Client, the IPsecTunnel was incorrectly required to be configured with "SetupSAPer" to "Host" to be able to negotiate the tunnel successfully.
- **COP-19841:** Using the ping CLI command would in some situations cause a disjointed command line prompt to appear.
- **COP-20004:** The way interface packet queues were flushed during reconfigure could cause unnecessary packets loss. It could result in packet loss when cOS core performs a reconfigure even when the system load was low.
- **COP-20182:** ID passed from the IKE negotiation to the RADIUS server was incorrectly

formatted when an IP address was used as ID.

- **COP-20243:** The IPReputation Graph on the status page could sometimes cause inaccurate values to appear.
- **COP-20274:** The simplified VPNClients object was set to use session timeout from the RADIUS server. Microsoft RADIUS server uses 60s as default session timeout which will cause the firewall to disconnect the clients after 60s in that case. The simplified tunnel has been changed to ignore session and idle timeout from the RADIUS server.
- **COP-20284:** DHCP server sent duplicate NAKs for some requests, occasionally with invalid options.
- **COP-20292:** A modification to a netobject configured on a user in a user local database didn't take effect until after a restart.
- **COP-20300:** DHCPv6 server and client did not treat the DUID as an opaque value and therefore did not work correctly with other devices using the newer UUID type.
- **COP-20301:** IKEv2 tunnels with failed negotiations could in some situations cause leakage of IKE SAs and eventually cause a max_ike_sa_reached log event. When this happens, no more IKE tunnels could be established.
- **COP-20313:** Some items in the MIB had incorrect variants of unsigned integer types.
- **COP-20337:** The High Availability Wizard had graphical errors which made it hard to select interfaces in the combobox controls.
- **COP-20343:** The system could in some rare occasions restart during an IPsec EAP negotiation.
- **COP-20357:** Entries in the neighbor cache could sometimes linger forever.
- **COP-20362:** On the W40 platform, the 8 port SFP module (NET81) was wrongly detected in both module slot 1 and 2 when only module slot 2 was used.
- **COP-20364:** There was no configuration warning when services dependent of IP Reputation were configured and no valid IP Reputation license was installed.
- **COP-20366:** The Neighbor Devices status page was not accessible by audit users.
- **COP-20371:** It was possible to authenticate multiple users on the same IP / Interface combination using different username. The IP / Interface is now enforced as unique identifier.
- **COP-20383:** In rare situations for High Availability setups, the firewall could make an unexpected restart with reference to NeighborCache. Affected models: SG60, E5 and E7.
- **COP-20385:** The calculation of the shared MAC address on Link Aggregation interfaces, when UseUniqueSharedMac is enabled, was using the same MAC address for all Link Aggregation interfaces.
- **COP-20407:** The Address column inside Address Folder objects only showed a single address for High Availability objects.
- **COP-20419:** Packet loss at rekey triggered an unnecessary tunnel deletion for IKEv2 tunnels.
- **COP-20483:** The firewall responded to a peer with no PFS, even though the peer was only suggesting one PFS group, if "None" was part of the configured PFS groups. Scenarios where cOS Core is used on both endpoints may fail after upgrade if only one is upgraded to this release. Upgrade both endpoints or make sure the PFS groups are configured with the same values on both peers to ensure a working tunnel after upgrade.

-
- **COP-20484:** Application rule dialog had no scrollbar when the window had been resized to be very small.
 - **COP-20548:** The extended connection information e.g. data usage and identified application was not visible when printing IPv6 connections using the "connections" CLI command.
 - **COP-20565:** An IPsec EAP negotiation using a UserAuthRule with RADIUS as agent, could in some rare occasions lead to memory corruption if the negotiation happened at reconfiguration.
 - **COP-20570:** CLI command to force blacklist unblocking would sometimes remove wrong entries or all entries.
 - **COP-20575:** A large number of authenticated users would in certain scenarios lead to high CPU load on the firewall when used in High Availability cluster.
 - **COP-20606:** The LW-HTTP engine did not allow connections through the system if the Web Content Filtering servers could not be reached. E.g. due to a failing DNS server. A new Fail Mode parameter has been added to the IP Policy Web Profile to control this behavior. A fix was also made to the WCF subsystem that minimizes the delay of resuming WCF Lookups once the DNS servers are reachable again.
 - **COP-20624:** Gratuitous ARP queries was not correctly forwarded in transparent mode.
 - **COP-20625:** Radius protocol packet field for NAS-Identifier incorrectly sent a null termination character in the value string.
 - **COP-20668:** The system could sometimes restart unexpectedly when processing specially crafted HTTP headers.

3.5. Addressed Issues in cOS Core 12.00.07

- **COP-14583:** If SSH remote management was configured for a specific interface, the SSH server could only be accessed using the core IP address for that specific interface. The behavior of SSH remote management is now changed to allow access from an interface using any core IP address, consistent with how HTTP remote management works.
- **COP-19299:** DIGEST-MD5 authentication for SMTP was not fully supported.
- **COP-19982:** IPsec could leak memory on hardware models using Cavium accelerators. Affected models: W5, SG4300 and SG4500.
- **COP-20028:** Downloads of IP Reputation databases could stall with the error message "download_start_failure". This error occurred if the system reconfigured more than once during an IP Reputation database update.
- **COP-20090:** Updating the IP Reputation database could in some scenarios result in an unwanted HA failover when the new database was installed.
- **COP-20123:** Threshold rules could trigger on connections opened by an ALG even when it shouldn't.
- **COP-20124:** IP Reputation queries could sometimes stall if the connection to the server failed. The system will now automatically switch to another server in case of communication failure.
- **COP-20166:** The DHCP Client did not handle link down event correctly. The client could enter the discovery state without completely resetting previous values.
- **COP-20176:** Some options were not selectable on an SSH client key object.

-
- **COP-20186:** Changing cluster ID on an HA cluster could cause the state synchronization to fail between the cluster members until a restart of the member.
 - **COP-20236:** The file extension lists in the File Control profile could not handle long lists of file extensions.
 - **COP-20246:** HTTP protocol upgrade to e.g. websockets was not allowed when using an IP Policy with a Web Profile. Protocol upgrade is now allowed as per default.
 - **COP-20294:** Running the techsupport or dconsole commands could in some rare occasions cause an unexpected system restart.
 - **COP-20311:** The web user interface DHCP Server status page could render incorrectly if special characters were used in the DHCP hostname.
 - **COP-20335:** A list containing Neighbor Devices could in some situations become incorrect and cause an unexpected restart.

3.6. Addressed Issues in cOS Core 12.00.06

- **COP-20336:** Downloads of IP Reputation updates could in some special scenarios cause corruption of the file system. A unit with a corrupt file system will fail to boot up, and the unit would in that case have to be sent to Clavister for RMA.

3.7. Addressed Issues in cOS Core 12.00.05

- **COP-18448:** The system incorrectly allowed configurations of RemoteManagementSSH objects where neither RSA or DSA were configured as host key. It was also possible to store configurations with neither password or public key as authentication method.
- **COP-18453:** Several CLI commands that could modify the state of the system did not require administrator privileges. The following CLI commands can no longer be executed as auditor: arp - flush, nd -flush, time - set, route -flushl3cache, zonedefense -blockip/blockenet, ike -delete, dhcp -lease renew/release, dhcp6 -lease renew/release, ha -activate/deactivate and ldap -reset.
- **COP-18644:** Log messages containing special characters could prevent the WebUI System log page to render correctly. System log page has been updated to better handle special characters.
- **COP-19022:** Removing the COMPort object on virtual firewalls was not correctly written down in the configuration.
- **COP-19683:** IPsec throughput graphs in the WebUI were reset at every reconfigure even though the IPsec interfaces hadn't changed.
- **COP-19809:** Users were unable to choose whether to send upper or lower cased Ethernet addresses for MAC/ARP authentication in user auth rules.
- **COP-19852:** When loading a specific address in the WebUI, the firewall could make an unexpected reboot.
- **COP-19922:** The reported SNMP value type for "HStatusRole", "HStatusState" and "HStatusTimeWithinState" used the wrong datatype. The reported SNMP values have been updated to the correct datatype Integer.
- **COP-19987:** It was possible to delete COMPort objects from the configuration on hardware appliances.

-
- **COP-20089:** Users were unable to test a ZoneDefense switch with an address inside of an address folder.

3.8. Addressed Issues in cOS Core 12.00.04

- **COP-9969:** If the previous "shutdown reason" could not be determined, the initial startup and the "stats" command would use unnecessarily amount of CPU resources.
- **COP-14555:** The ICMP service for IPv6 service was named IPv6-ICMP. It has now been renamed to ICMPv6 which is the name used in eg the RFC.
- **COP-18457:** The description for Netcon idle timeout was misleading.
- **COP-18783:** Excluding ipa files from antivirus scanning resulted in all ZIP files being excluded from scanning.
- **COP-19125:** Some configurations made it impossible to set Local and Remote Networks on an IPsec tunnel with IKEv2.
- **COP-19265:** IPsec tunnel setup failed with reason "out of memory".
- **COP-19499:** The DHCP Relay function could in some situations fail to relay DHCP messages.
- **COP-19551:** It was not possible to disconnect an IPv6 session using the sessionmanager CLI command.
- **COP-19617:** There was a memory leak when using HTTP ALG and NAT.
- **COP-19691:** Adding a new authenticated user through the REST API with space or new line characters at the end of the group list would make the authentication fail.
- **COP-19730:** Uploaded DER certificate could cause failure to activate IPsec configuration.
- **COP-19782:** The userauth REST API limits the num variable to max 9999. The max limit has been increased to 1000000000.
- **COP-19783:** Re-authenticating user using the REST API didn't update the "idle_timeout" property.
- **COP-19821:** The "userauth -list" CLI command could cause traffic interruption when large amount of users were authenticated even though only a few were shown. The CLI command has been optimized to only process the users shown by the command.
- **COP-19824:** Reconfiguring with an IPsec tunnel with tunnel monitoring enabled could lead to unexpected behavior.
- **COP-19825:** CLI command "hostmon" with the flag "num" printed one session short of the number specified by the user.
- **COP-19827:** If both peers of an IPsec tunnel initiated IKE SA setup at the same time, one endpoint could end up with duplicate IPsec and IKE SAs causing issues with traffic through the tunnel.
- **COP-19831:** IPsec rekey could fail if the tunnel was configured as a config mode client and remote network was set to something other than all nets.
- **COP-19834:** When the IP Reputation license expired or when the ipreputation -stop CLI command was given, the system could unexpectedly restart.
- **COP-19867:** It was not possible to specify more than one interface when issuing the CLI's command "pcapdump".

-
- **COP-19870:** IP reputation leaked memory when connecting to the update servers.
 - **COP-19872:** The antivirus advisory link seen in virus found memlog entries could sometimes point to the wrong URL.

3.9. Addressed Issues in cOS Core 12.00.03

- **COP-17330:** When issuing the 'rules' CLI command when having more than 1000 rules or policies defined, the index column would display '...' for indexes larger than 999.
- **COP-17568:** The SSH server only supported AES ciphers in CBC mode, not in CTR mode.
- **COP-17927,COP-19536,COP-18914:** The SIP ALG could in some scenarios leak memory.
- **COP-18120:** An error message related to antivirus was displayed although antivirus was not in use.
- **COP-18126:** The date-time picker in the WebUI could malfunction when using non-English languages.
- **COP-18136:** In rare occasions, configuring an SMTP ALG could lead to an unexpected restart.
- **COP-18574:** The HTTP ALG could block certain file types that use ZIP format.
- **COP-18877:** The check for max password length when configuring users in the Local User Database displayed an incorrect message if the entered password exceeded the max supported length.
- **COP-19003:** The CLI command to list current DNS queries printed incorrect addresses.
- **COP-19121:** The 'blacklist' CLI command did not have a default action. Now, the "show" argument is the default action.
- **COP-19123:** An administrator using the default password could be locked out when changing the first configuration through the command line.
- **COP-19277:** It was not possible to retrieve statistics via encrypted SNMP (SNMPv3 in AuthPriv mode) on models SG60, E5 and E7.
- **COP-19308:** SNMP trap sometimes reported an incorrect value for "ifOperStatus".
- **COP-19320:** Sending IKE/ESP packets into another IPsec tunnel caused the packets to be dropped.
- **COP-19348:** ZoneDefense switch verification did not work in cOS Core 11.04.01 and 11.20.01.
- **COP-19349:** Assigning a static client IP to a user from the Local User Database did not work as intended.
- **COP-19401:** IP Pool could not be used with IPsec interfaces and config mode.
- **COP-19626:** It was not possible to use more than 512 FQDN addresses.
- **COP-19627:** LACP was not compatible with implementations that produce Protocol Data Units that are longer than the standard specification dictates they should be.
- **COP-19654:** Emails could not be sent through the IMAP ALG for some email clients that were set to save a copy of the mail in the sent folder.
- **COP-19656:** There was no warning printed when using an Email profile with Domain Verification and no DNS server was configured.

-
- **COP-19677:** The idle CPU load increased very slightly after each reconfigure.
 - **COP-19704:** There could be erroneous logs for 'out of memory' in rare occasions when antivirus was used.
 - **COP-19712:** There was a memory leak in the Whitelist/Blacklist feature of an Email Profile.
 - **COP-19716:** There was a memory leak in the SMTP, POP3 and IMAP ALGs.
 - **COP-19717:** Established connections were not closed when blacklisted by an IDP Rule Action or Threshold Action if the setting to only block connections with the same service was enabled.
 - **COP-19737:** The pre-configured time synchronization interval was too high. The interval has been changed from every week to every day.
 - **COP-19738:** The system could unexpectedly reboot during IPsec tunnel setup if a previously non-responding CA server used for CRL lookup started responding again.
 - **COP-19753:** The firewall could make an unexpected restart under heavy traffic load. Affected models SG60, E5 and E7.
 - **COP-19759:** The DCC Anti-spam feature did not work for SMTP due to incorrectly formatted DCC packets sent to the DCC servers.
 - **COP-19764:** The Update Center WebUI page showed an incorrect time for "Next Update" on systems without a valid IP Reputation license.
 - **COP-19765:** The CLI command for ZoneDefense displayed incorrect data in certain scenarios.
 - **COP-19793:** Some rare emails could make the system unstable.

3.10. Addressed Issues in cOS Core 12.00.02

- No addressed issues included in this release.

3.11. Addressed Issues in cOS Core 12.00.01

- No addressed issues included in this release.

3.12. Addressed Issues in cOS Core 12.00.00

- **COP-8489:** Disabled objects were shown in the available list in the WebUI group controller.
- **COP-17810:** The system sometimes restarted unexpectedly after a configuration deployment.
- **COP-18268:** When using InControl to deploy a configuration including a lot of comment groups, there was a long delay to finish the deployment.
- **COP-18613:** Adding an Interface with a configured DHCP client to a Link Aggregation group failed with a strange error message. Now the DHCP client is not initiated, instead the DHCP client must be configured on the Link Aggregation interface if DHCP should still be used.
- **COP-18648:** The error and warning count on the system overview page in the WebUI would show incorrect numbers.
- **COP-18847:** The "Download Logs" button was shown for the logging pages in the WebUI for Microsoft Edge even though the browser does not support this feature.

-
- **COP-18900:** When having an IDP rule with a drop rule on the "Invalid hex encoding" setting, certain emails would not be let through depending on the segmentation of the TCP traffic.
 - **COP-18905:** Certain rare DNS problems where DNS lookup had failed could cause an FQDN Address to stop being updated by the DNS cache.
 - **COP-18908:** ZoneDefense log events were incorrectly generated at the start of the firewall.
 - **COP-18924:** The word "shutdown" was removed from reconfiguration events, since it caused confusion.
 - **COP-18935:** It was possible to use the same name for an IPPolicy in multiple rule sets.
 - **COP-18940:** Rekey could fail in scenarios with multiple networks set as LocalNetwork or RemoteNetwork on an IPsecTunnel. This caused packets to be dropped during the recreation of IPsec SAs.
 - **COP-18960,COP-18961:** In certain cases email headers were not interpreted correctly and blacklisted IP addresses could be missed.
 - **COP-18966:** Application Control was only enforced on IPv6 TCP packages. Now it is possible to use Application Control for all types of IPv6 packages.
 - **COP-18987:** IPsec tunnels using FQDN endpoints could be taken down unexpectedly if the DNS Cache got a response from the DNS server indicating an error even though there were valid IP addresses in the cache.
 - **COP-19028:** In rare circumstances, the diagnostic console page returned an error and was not able to show the logs.
 - **COP-19052:** Traffic could halt if an IPPolicy using an ALG positioned before the active IPPolicy in the rule list was added, enabled, deleted or disabled.
 - **COP-19060:** The Distributed Checksum Clearinghouses (DCC) license could expire prematurely in some rare cases.
 - **COP-19106:** MAC address formatting was previously inconsistent across several features, some used uppercase while others used lowercase. Now all of them use uppercase.
 - **COP-19107:** When downloading an empty log file the received file contained the source code of the web page and was simply named "Logs.txt". Now the file contains the text "Empty log" and is named with date and time in the same way as log files that contain log data.
 - **COP-19109:** There was unusually high CPU load when scanning some emails for viruses.
 - **COP-19114:** When using an FQDN address as remote endpoint for an IPsec tunnel, the tunnel was not taken down if the address failed to resolve.
 - **COP-19134:** The firewall could become unresponsive if an entry in the dynamic blacklist timed out after a reconfiguration.
 - **COP-19140:** Log entries were generated on each load/save of the blacklist file during reconfigure.
 - **COP-19155:** When performing antivirus inspection of emails transported with IMAP, some emails could make the mail connection stall.
 - **COP-19157:** The clvUserAuthIDAwareUsers SNMP stat value was only registered if one or more User Authentication Rules was defined. It is now always possible to read the clvUserAuthIDAwareUsers SNMP stat value.

-
- **COP-19183:** The firewall running under the Hyper-V advisor could fail to restart in some cases.
 - **COP-19194:** Some emails would stall the fetching through IMAP when using Anti-Spam.
 - **COP-19195:** MOBIKE notification was sent to the peer when initiating a tunnel setup even though cOS Core doesn't support changing local endpoint address of the tunnel at runtime.
 - **COP-19200:** Using an IPsec tunnel to assign clients IP addresses taken from a RADIUS server could cause unexpected behavior if a RADIUS accounting server was used as well.
 - **COP-19227:** Some specific emails stalled the IMAP transfer.
 - **COP-19275:** Mobile IKE clients not behind a NAT were disconnected after changing IP.
 - **COP-19323:** Traffic through NATed IPsec client could stop when the NAT changed port of the UDP encapsulated ESP packets. Affected models: Wolf Series W5 and Security Gateway Series SG4300 and SG4500.
 - **COP-19361:** There was a memory leak in the LW-HTTP ALG that could cause problems with certain situations.
 - **COP-19367:** Hyper-V could cause watchdog reboot on Windows 10.
 - **COP-19409:** Traceroute for IPv6 did not work as intended.
 - **COP-19476:** Sessions created with the newest Netcon version never timed out.
 - **COP-19502:** Reconfiguring an IPsec interface that had an ongoing IKE SA negotiation could lead to unexpected behavior.

4. New Features SSL VPN client

4.1. New Features and Enhancements in SSL VPN client 1.1.3

- **OpenSSL update**
The OpenSSL library has been updated to the latest version.

4.2. New Features and Enhancements in SSL VPN client 1.1.2

- **OpenSSL update**
The OpenSSL library has been updated to the latest version.

5. Addressed issues SSL VPN client

5.1. Addressed Issues in SSL VPN Client 1.1.3

- **SSL-150:** Installation of the client failed on Windows 10 when Secure Boot was enabled on the PC, starting with Windows 10 Anniversary Update (1607).
- **SSL-151:** Windows 10 could choose to use a default GW with higher metric value when the connection to the default GW of the lower metric value, in this case the SSLVPN tunnel, was bad. Made the SSLVPN service remove all default routes, except the SSLVPN tunnel, when tunnel is created.

6. Installation Instructions

6.1. Upgrade Considerations

This section covers considerations to take into account when upgrading to the latest cOS Core version, such as configuration aspects related to changes in features or behavior of the system after upgrade.

- **Centralized Management via InControl**
Centralized management via InControl of cOS Core 12.00.00 and later, requires that InControl version 1.83.00 or later is used.
- **L2TP/IPsec client**
As of cOS Core 10.20.00 and the addition of virtual routing support for IPsec, the L2TPv2 client configuration has been extended with a setting for the IPsec interface to use as outer tunnel. This will bypass routing for L2TP packets and send them directly over the configured IPsec interface, avoiding potential routing loops that could occur otherwise. If IPsec is to be used for the L2TP client tunnel, the L2TP client configuration **MUST** be updated with the correct IPsec interface for the L2TP client to work after upgrade to 10.20.00 or later.
- **L2TP/IPsec server**
As of cOS Core 10.20.00 and the addition of virtual routing support for IPsec, after upgrade a configuration warning may trigger, notifying that addition of routes dynamically for the IPsec tunnel used by an L2TP server as outer interface filter is ignored. These routes are no longer necessary since packets to/from the L2TP server are routed directly to the configured IPsec interface without consulting the routing table. Addition of dynamic routes over the IPsec interface would cause a routing loop. The upside of this change is that only L2TP traffic is routed through the IPsec tunnel and other traffic is routed according to the routing table. Earlier versions of cOS Core routed all matching traffic into the IPsec tunnel, not only L2TP.

- **IPsec in transport mode without L2TP**

As of cOS Core 10.20.00 and the addition of virtual routing support for IPsec, using the same PBR table for the Outer PBR table as for the PBR table of the interface itself, will end up in a routing loop. To prevent routing loops, make sure that the IPsec interface is configured with different PBR tables for the Outer PBR table and the PBR table of the interface itself.

6.2. Upgrading from a cOS Core 10.nn or 11.nn system

This section describes how to upgrade the system using the Web User Interface. For a detailed description on how to upgrade the system using SCP please refer to the Clavister cOS Core admin guide.

To upgrade Clavister cOS Core using the Web user interface, follow these simple steps:

- Browse to the Web User Interface and log in as a user with full administrative rights.
- From the "Maintenance" menu select "Upgrade".
- Click the "Browse..." button and select the .upg file which contains the upgrade.
- Click the "Upload firmware image" button to upload the image and start the upgrade procedure.
- When the file has been uploaded to the gateway, the message "Firmware upload complete." will be presented and the system will restart.
- When the system has been restarted the login screen will appear and the system upgrade is complete.

7. Known Limitations

- **High Availability: Transparent Mode does not work in HA mode.** There is no state synchronization for Transparent Mode and there is no loop avoidance.
- **High Availability: (Point-to-Point Protocol over Ethernet) PPPoE is not supported in HA mode.**
- **High Availability: No state synchronization for Application Layer Gateways.** No aspect of Application Layer Gateways are state synchronized.
This means that all traffic handled by ALGs will freeze when the cluster fails over to the other peer. If, however, the cluster fails back over to the original peer within approximately half a minute, frozen sessions (and associated transfers) should begin working again. Note that such failover (and consequent fallback) occurs each time a new configuration is uploaded.
- **High Availability: Tunnels unreachable from inactive node.** The inactive node in an HA cluster cannot communicate over IPsec, SSL VPN, PPTP, L2TP and GRE tunnels, as such tunnels are established to/from the active node.
 - Inactive HA member cannot send log events over tunnels.
 - Inactive HA member cannot be managed / monitored over tunnels.
 - OSPF: If the cluster members do not share a broadcast interface so that the inactive node can learn about OSPF state, OSPF failover over tunnels uses normal OSPF failover rather than accelerated (<1s) failover. This means 20-30 seconds with default settings, and 3-4 seconds with more aggressively tuned OSPF timings.
- **High Availability: No state synchronization for L2TP, PPTP and SSL VPN tunnels.** There is no state synchronization for L2TP, PPTP and SSL VPN tunnels. On failover, incoming clients

will re-establish their tunnels after the tunnels are deemed non-functional. This timeout is typically in the 30 -- 120 seconds range.

- **High Availability: No state synchronization for IDP signature scan states.** No aspects of the IDP signature states are synchronized. This means that there is a small chance that the IDP engine causes false negatives during an HA failover.

8. Compatibility

The following section outlines the direct compatibility considerations as of cOS Core 12.00.11.

The following hardware appliances are supported as of the Clavister cOS Core 12.00.11 release. Clavister does not guarantee compatibility with other hardware appliances.

- Clavister Next Generation Firewall E5
- Clavister Next Generation Firewall E10
- Clavister Next Generation Firewall E20
- Clavister Next Generation Firewall E80
- Clavister Next Generation Firewall X8
- Clavister Next Generation Firewall W3
- Clavister Next Generation Firewall W5
- Clavister Next Generation Firewall W20
- Clavister Next Generation Firewall W30
- Clavister Next Generation Firewall W40
- Clavister Next Generation Firewall W50

9. Licensing

Clavister cOS Core 12.00.11 requires a Clavister subscription covering **Sept 1, 2018**. Make sure that this is covered before trying to upgrade the system, otherwise the system will enter a "License Lockdown" mode.

10. Getting Help

Technical Assistance via Web or Telephone

We offer timely and rapid response to customer inquiries and service requests via our web based support tool or telephone. Do not hesitate to contact us if you have any questions regarding the upgrade or installation procedure.

Clavister Technical Support
<https://www.clavister.com/my-clavister/help-desk/>



CLAVISTER®

CONNECT . PROTECT

Clavister AB
Sjögatan 6J
SE-89160 Örnsköldsvik
SWEDEN

Head office/Sales: +46-(0)660-299200
Customer support: +46-(0)660-297755

www.clavister.com