Clavister cOS Core Release Notes

Version 11.00.00

Clavister AB
Sjögatan 6 J
SE-891 60 Örnsköldsvik
SWEDEN

Phone: +46-660-299200

www.clavister.com

Published 2015-07-03

Clavister cOS Core
Release Notes
Version 11.00.00

Published 2015-07-03

Copyright Notice

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

Clavister cOS Core 11.00.00 is the latest version of our award-winning network security operating system powering the Clavister Security Gateway Series, 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 11.00.00 requires InControl version 1.50.00 or later. We recommend always using the latest version.*

> ***Important***
> *Clavister cOS Core 11.00.00 requires a Clavister Security Subscription covering **July 1, 2015**. 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 11.00.00. For a complete list and description of all the features in Clavister cOS Core 11.00.00, refer to Clavister cOS Core Administration Guide 11.00.00.

2.1. New Features and Enhancements in cOS Core 11.00.00

- **Anti-SPAM for POP3 and IMAP**
  The system now supports Anti-SPAM for POP3 and IMAP, with fully configurable threshhold levels and usage of mechanisms such as Reply Address Domain Verification, DNS Blacklisting and Distributed Checksum Clearinghouses (DCC). Malicious Link Protection detects malicious links in e-mails and protects users from clicking on them by breaking the malicious link. E-mails identified as SPAM can be tagged by the system in both subject and headers to notify the end-users mail clients that the e-mail is identified as SPAM. Configurable whitelists and blacklists allow the administrator to statically decide how to treat e-mails to and from specific IP address and e-mail addresses, such as bypassing SPAM protection for certain IPs or e-mails.

- **IPv6 HA Support**
  The system now supports redundancy in a high availability setup while actively forwarding IPv6 traffic.

- **RADIUS Relay Improvements**
  RADIUS Relay now supports manual configuration of the interface where the user traffic is expected for authenticated users via the "Override User Data Interface" setting. This is needed if the interface used for the user data traffic is different from the interface where the RADIUS messages are sent to the system.

- **HTTP Content Inspection Improvements**
  A new lightweight HTTP ALG is now supported that more efficiently can handle content inspection of HTTP, such as web content filtering and client user-agent filtering. The new HTTP ALG is more efficient and requires less resources which leads to higher HTTP content inspection throughput capabilities.

- **Improved Support for Virtual Routing**
  The system now supports configuration of the source IP to use when communicating with RADIUS and LDAP for authentication, as well as configuration of the source IP to use when performing route monitoring. This is useful in virtual routing scenarios where the interface IP is not necessarily the correct IP to use as source IP for this communication.

- **Anti-Virus Support for Scanning of ZIP-in-ZIP Files**
  The system now supports antivirus scanning of nested ZIP files, i.e. ZIP within ZIP files, transported over HTTP or FTP, configurable to support up to 10 levels of ZIP-in-ZIP.

- **SHA-2 Signed Certificates for IKE Authentication**
  The system now supports use of SHA-2 signed certificates for IKE authentication, including SHA-256, SHA-384 and SHA-512 hashing algorithms.

- **Configurable Behavior for CRL Failures**
  The system now supports configuration of how the system should behave when a CRL for a certificate cannot be accessed on the CA server. A "conditional" option has been added to allow use of the certificate even if the CRL cannot be accessed.

- **Configurable CRL Distribution Points for Certificates**
  The system now supports configuration of the CRL distribution points (CDPs) to use with a certificate.

- **Configurable Differentiated Services field for IKE packets**
  The system now supports configuration of the value of the Differentiated Services (DSCP) field in the IP header of IKE packets sent by the system.

- **MIB File Download via WebUI or SCP**
  The system MIB files can now be downloaded directly from the device either via the web user interface or via SCP.

- **Improved SNMP Support**
  The system can now keep interface SNMP indexes and interface OIDs persistent during reconfigures and restarts.

- **Traceroute Support in CLI**
  A new "traceroute" CLI command has been added that can be used to perform traceroute towards domain names, IPv4 and IPv6 addresses.

- **Improved Ping CLI Command**
  The "ping" CLI command has been improved to support ping towards IPv6 addresses and domain names.

- **Improved Statistics for IKE/IPsec**
  The statistical counters available via SNMP for IKE/IPsec has been improved to include a wide range of statistical values useful for troubleshooting or monitoring.

3. Addressed Issues

The following sections detail the addressed issues in Clavister cOS Core 11.00.00 release.

3.1. Addressed Issues in cOS Core 11.00.00

- **COP-8871:** The setting "Local Console Timeout" under "Remote Management Settings" had an unclear name. It has now been renamed to "SSH Idle Timeout".

- **COP-10794:** Log Message Exceptions ID numbers typed with leading zeroes were incorrectly changed to a different numerical value in the table.

- **COP-11208:** Input fields for IPv4 addresses in the web user interface were too small. The text box size has now been increased.

- **COP-12024:** The 'rules' CLI command would in some cases output incomplete information to save screen space, even with the -verbose flag set. Its output format has been redesigned to improve readability across the board, and to never omit any information when -verbose is specified.

- **COP-12700:** After closing an IPsec tunnel used for L2TPv3 traffic, the Security Gateway in some rare occasions rebooted unexpectedly.

- **COP-12721:** Tab completion for CLI commands with branching options did not work correctly.

- **COP-12813:** The titles of the Application Control Statistics in the web user interface dashboard had unclear names.

- **COP-13518:** The pcapdump tool erroneously captured IPsec traffic when the Ethernet Address filter was used.

- **COP-13592:** Some Application Control attributes never produced any logging output, due to problems with the underlying data type. The log system now supports more data types and logging is no-longer possible to enable for data types that cannot be logged.

- **COP-13656:** The web user interface control for service groups incorrectly made it possible to include a group as a member of itself.

- **COP-13701:** When using "script -create" on a Security Gateway with global domain objects, not all global domain objects were created.

- **COP-13769:** Configuring a static ARP or ND entry on an interface group would result in a confusing error.

- **COP-14039:** No error message was shown when an SSL VPN interface was added and no HTTPS certificate was configured in the system.

- **COP-14154:** Crypto accelerator statistics were missing from the SNMP MIB file.

- **COP-14346:** The encapsulation mode property on IPsec interfaces didn't work correctly when it was configured to use both tunnel mode and transport mode. E.g transport mode IPsec SAs could be negotiated successfully but no packets could be routed through the tunnel. The properties local/remote network and local/remote endpoint could also be configured in a way that contradicted the encapsulation mode property. The encapsulation mode option 'Both' has been removed. A tunnel is now only allowed to be either tunnel mode or transport mode. Any configuration using the setting 'Both' will be converted to 'Tunnel' when upgrading. Please configure your IPsec interfaces to use either tunnel mode or transport before upgrading to make sure your IPsec interfaces still work after upgrade.

- **COP-14698:** There was no log when an IPRule or IPPolicy was changed.
- **COP-14717:** When the Security Gateway logged what applications were found in an Application Control Rule, the name of the corresponding IPRule was not logged.
- **COP-14858:** When configuring the Security Gateway using the WebUI, it sometimes failed to add correct IPv6 addresses for recent versions of Mozilla Firefox. Now correct IPv6 addresses may be added to both old and recent versions of Firefox.
- **COP-14889:** Under certain circumstances the Security Gateway would show unexpected behavior when the SIP module handled a non answered incoming call.
- **COP-15105:** Under some circumstances, L2TPv3 tunnels could stop operating after reconfiguring the Security Gateway.
- **COP-15238:** Under certain situations HTML Page Parameter %REDIRHOST% for WebAuth could cause the Security Gateway to render unprintable symbols in the HTTP banners.
- **COP-15275:** The log message generated by the authentication system when a user logged in did not include configured authentication source.
- **COP-15302:** The system could unexpectedly restart if a reconfigure failed due to configuration errors within the interface configuration.
- **COP-15308:** IPsec SA log event details differed between High Availability nodes.
- **COP-15317:** In some circumstances the Security Gateway needed to be restarted in order to retry a failed HTTP POSTER request.
- **COP-15330:** Memory used by the Anti-Virus engine when inspecting compressed files was not included in the memory statistics.
- **COP-15337:** There was a small memory leak related to POP3 email processing.
- **COP-15414:** Not possible to get Ethernet link when forcing speed and duplex on Ethernet device. Affected models: Eagle Series E80, Wolf Series W20 and W30.
- **COP-15444:** Time sync operations performed after startup of the system could fail continously if the time drift of the system clock was larger than the configured maximum allowed time drift. To mitigate this problem, the maximum time drift protection is not enabled for the first ten minutes after startup of the system, allowing the time synchronization procedure to correct the system time after startup even if time drift is larger than the configured maximum time drift.
- **COP-15587:** Synchronization of ESP sequence numbers between cluster peers could during some circumstances be done with wrong sequence numbers which lead to packet loss after HA fail over.
- **COP-15620:** Some POP3 ALG features did not work as intended for certain rare messages.
- **COP-15655:** The system did not require that the configured local ID on an IPsec tunnel strictly matched the received remote ID on the remote tunnel endpoint.

4. Installation Instructions

4.1. 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 11.00.00 and later, requires that InControl version 1.50.00 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.

- **IPsec keep-alive function removed**
  As of cOS Core 10.20.00 and the addition of virtual routing support for IPsec, IPsec interfaces can be used as any other interface when monitoring routes. The need for keep-alive on IPsec tunnels in order to improve fail-over times are no longer needed, thus removed as a feature. To be able to always keep a tunnel up a new setting has been introduced for the IPsec tunnel, called 'Auto Establish' that forces automatic establishment of the tunnel if it is down.

4.2. Upgrading from a CorePlus 8.nn system

For a detailed instruction on how to upgrade from a CorePlus 8.nn version to cOS Core 10.nn please refer to Chapter 2 of the Admin Guide for cOS Core 11.00.00

Important

Only versions from and including CorePlus 8.60.01 upwards can be upgraded to cOS Core 10.nn.

4.3. Upgrading from a CorePlus 9.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 CorePlus admin guide.

To upgrade Clavister CorePlus 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.

4.4. Upgrading from a cOS Core 10.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.

5. Known Limitations

- **IMAP ALG: IMAP protocol specification support.** The IMAP ALG has not yet been fully validated to support all aspects of the IMAP protocol specification, which means that some IMAP mail clients may experience problems when fetching mail via the IMAP ALG. Support for the full IMAP specification will be validated in upcoming maintenance releases.
- **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: 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, 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 and PPTP tunnels.** There is no state synchronization for L2TP and PPTP 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.

6. Compatibility

The following section outlines the direct compatibility considerations as of cOS Core 11.00.00.

The following hardware appliances are supported as of the Clavister cOS Core 11.00.00 release. Clavister does not guarantee compatibility with other hardware appliances.

- Clavister Security Gateway SG60 Series
- Clavister Security Gateway SG3200 Series
- Clavister Security Gateway SG4300 Series
- Clavister Security Gateway SG4500 Series
- Clavister Security Gateway Eagle Series E5
- Clavister Security Gateway Eagle Series E7
- Clavister Security Gateway Eagle Series E80
- Clavister Security Gateway Lynx Series X8
- Clavister Security Gateway Wolf Series W3
- Clavister Security Gateway Wolf Series W5
- Clavister Security Gateway Wolf Series W20
- Clavister Security Gateway Wolf Series W30

For software installations, please refer to the Hardware Compatibility List on the Clavister web site.
Note that only existing software maintenance deals are supported, as Clavister Software Series is declared End Of Sales.

7. Licensing

Clavister cOS Core 11.00.00 requires a Clavister Security Subscription covering **July 1, 2015**. Make sure that this is covered before trying to upgrade the system, otherwise the system will enter a "License Lockdown" mode.

8. 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®

Clavister AB
Sjögatan 6 J
SE-891 60 Örnsköldsvik
SWEDEN

Phone: +46-660-299200

www.clavister.com