



## Release Notes

---

### ***Clavister CorePlus Version 9.00***

Clavister AB  
Torggatan 10  
SE-891 33 Örnsköldsvik  
SWEDEN

Phone: +46-660-299200  
Fax: +46-660-12250

[www.clavister.com](http://www.clavister.com)

Build: 9.00.02  
Published 2008-10-14  
Copyright © 2008 Clavister AB.

---

## **Release Notes Clavister CorePlus Version 9.00**

Published 2008-10-14  
Build: 9.00.02

Copyright © 2008 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 CorePlus 9.00.02 .....	4
2.2. New Features and Enhancements in CorePlus 9.00.01 .....	4
2.3. New Features and Enhancements in CorePlus 9.00.00 .....	4
3. Addressed Issues .....	5
3.1. Addressed Issues in CorePlus 9.00.02 .....	5
3.2. Addressed Issues in CorePlus 9.00.01 .....	7
4. Installation Instructions .....	9
4.1. Upgrading from a CorePlus 8.nn system .....	9
4.2. Upgrading a CorePlus 9.nn system .....	9
5. Known Issues .....	10
6. Compatibility .....	10
7. Licensing .....	11
8. Getting Help .....	11

---

# 1. Version Summary

The new Clavister CorePlus 9.00 release is centered on enhancements of the administration experience and ease-of-use for administrators. Apart from a new Web-based administration user interface (UI), the Clavister CorePlus 9.00 comes with an enhanced command-line interface (CLI) with extensive scripting capabilities, a built-in SSH server, a built-in SCP server and a completely new configuration file system.

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



## **Important**

**The Clavister CorePlus version 9.00 does not support centralized management! If you need centralized management you must use an earlier version of Clavister CorePlus with Clavister FineTune support (e.g. version 8.xx). Clavister CorePlus will as of next major release have full support for centralized management.**

## 2. New Features

The following sections detail new features and enhancements in Clavister CorePlus 9.00. For a complete list and description of all the features in Clavister CorePlus 9.00, refer to Clavister CorePlus Admin Guide 9.00.

### 2.1. New Features and Enhancements in CorePlus 9.00.02

*No new features were introduced in the 9.00.02 release.*

### 2.2. New Features and Enhancements in CorePlus 9.00.01

#### **IPsec status page**

The IPsec status page has been extended to show the same information as the ipsectunnels CLI command.

#### **PPPoE Interfaces**

It is now possible to configure the MTU (Maximum Transmission Unit) for PPPoE interfaces.

#### **PPTP/L2TP client interfaces**

It is now possible to configure the MTU (Maximum Transmission Unit) for PPTP/L2TP client interfaces.

### 2.3. New Features and Enhancements in CorePlus 9.00.00

#### **Web-based administration user interface**

Easy to use web-based administration with much simplified deployment. No need to use local console for initial setup anymore and no need to install any management software; just use your browser and you are good to go. Still retains the ability to do granular configuration, but presents a simpler and more intuitive user interface for first-time users. The new interface also rationalizes some aspects of the user interface and automates some complex task to further speed up the common administrative tasks.

#### **Command-line interface (CLI)**

Using the new command-line interface, you have access to all objects in a Clavister Security

---

Gateway configuration. This makes it a very powerful tool for anyone who wants to build custom administration interfaces, or interact with external tools and systems. The command-line interface also gives the administrator a powerful way of scripting changes to the configuration.

### **Built-in SSH Server**

Clavister CorePlus 9.00 has a built in SSH (Secure Shell) Server, which provides secure and remote access to the command-line interface (CLI).

### **Built-in SCP Server**

Clavister CorePlus 9.00 has a built-in SCP (Secure Copy) Server, which makes it easy to upload firmware in a more secure way. SCP can also be used to backup and restore the system.

### **Extensive Usability Enhancements**

A number of usability enhancements have been included to further aid administrators in their day-to-day tasks. One example of this is that routes now are created automatically for the interfaces, and another is that the "Advanced Settings" now have been more integrated into the administrative interface.

### **Simplified Backups**

It is now possible to take one-click backups of your configuration through the Web User Interface or automatically fetch backups using SCP.

### **Upgrade Wizard**

A purpose built upgrade wizard has been created to guide the administrator through the upgrade procedure. The Upgrade Wizard helps the administrator to backup the old system, convert the configuration and resolve configuration issues.

## **3. Addressed Issues**

The following sections detail the addressed issues in Clavister CorePlus 9.00 release.

COP items refer to issues in Clavister CorePlus.

### **3.1. Addressed Issues in CorePlus 9.00.02**

- **COP-4053:** Fixed issue with DHCP NAK reception during initial phase of reconfiguration
- **COP-4524:** Fixed issue in OSPF where an LSA could be incorrectly deleted after being reoriginated
- **COP-4848:** The interface listings for Marvell Yukon interfaces showed incorrect IRQ values.
- **COP-5630:** The amount of memory used by the IDP engine was too high. The memory consumption has now been reduced.
- **COP-5904:** E-mails from e-mail addresses in the whitelist were blocked if they were classified as spam messages. Now all e-mails sent from whitelisted addresses will be let through, even if they are classified as spam.
- **COP-6311:** Fixed leap year problem where leap year day was added to January instead of February
- **COP-6460:** The "add" CLI command no longer adds an object with errors, unless you specify the "-force" flag.

- 
- **COP-6513:** Fixed problem in HA where one of the cluster members could be in lockdown and prevent its member from going active.
  - **COP-6523:** Fixed missing icon for "Forcibly Log Out" user on the User Authentication Status
  - **COP-6546:** A configured external log receiver that does not accept log messages might send ICMP destination unreachable packets to the security gateway. These packets would trigger new log messages resulting in high CPU utilization. Logging is now connection-based and the sending rate of log messages will be decreased by the security gateway when it receives ICMP destination unreachable packets regarding log receiver connections.
  - **COP-6568:** Fixed problem resulting in the IDP/AV license being expired prematurely.
  - **COP-6569:** Updated the computation of WCF graph percentage values to correctly work for the IXP platform
  - **COP-6580:** The HA wizard sometimes failed to connect to the master during configuration of the slave.
  - **COP-6656:** Unnecessary DynDNS and HTTP-Poster re-posts were triggered during reconfigure. This is now avoided by always considering if the local interface IP address has been changed or if the HTTP-Poster/DynDNS configuration has been changed.
  - **COP-6711:** Add Virtual Routing to IPsec that was accidentally removed in the 9.0 release
  - **COP-6846:** Hardware accelerated IDS have sometimes ceased to work, at the same time filling up the logs with messages about "duplicate matches" and/or "invalid matches".
  - **COP-6855:** Broadcom Netextreme II NICs were not automatically detected.
  - **COP-6862:** It was not possible to enter an NTP server with a DNS name in the setup wizard. The NTP server can now be entered in the format "dns:server.example.com".
  - **COP-6917:** The identification of IPsec clients during reconfigure was not correct when they were behind NAT.
  - **COP-6920:** Saves the current command line so you can recover it by pressing the down arrow when viewing the last history item.
  - **COP-6947:** The description text for IP Pools incorrectly specified that IP Pools could be used by L2TP and PPTP.
  - **COP-6980:** The value of the advanced IP setting MulticastIPenetOnMismatch was ignored; Packets would be dropped and logged regardless of the configuration.
  - **COP-7047:** An internal buffer alignment error in the SIP-ALG could lead to a restart of the system.
  - **COP-7048:** Emails did not get forwarded by the SMTP-ALG. The sending client received an error message saying that the email could not be delivered.
  - **COP-7069:** Restoring backups with IDP configurations sometimes failed to restore the IDP rules.
  - **COP-7084:** HTTP Web Content Filter override functionality can cause an unexpected restart when timing out users that have clicked the override button. Users that have clicked the override button have access to blocked content for a specific amount of time. When this time expires, an unexpected restart may occur.
  - **COP-7101:** It was not possible to manually force media or duplex for Marvell Yukon interface types.
  - **COP-7124:** Pattern matching in the blacklist and whitelist in the SMTP-ALG has been extended to be more dynamic.

- 
- **COP-7139:** Both members in the HA cluster did not log their change of state when roles were changed (active to passive and passive to active).
  - **COP-7140:** Very large configuration files could cause some web pages in the web user interface to not render completely.
  - **COP-7145:** It was not possible to select PPPoE interfaces as outer interface filter in PPTP/L2TP servers in the web user interface.
  - **COP-7152:** The SIP-ALG could in some scenarios cause instability of the system when running out of RAM. The issues have been addressed and fixed.
  - **COP-7194:** Fixed issue in TCPStack with stalling transfers with peers using a very small send window
  - **COP-7230:** Configuration objects were under certain conditions duplicated, causing configuration errors.
  - **COP-7238:** The SIP-ALG could in rare occasions fail to setup a call and generate a log message containing "M HEADER NOT FOUND". The issue has been corrected.
  - **COP-7302:** SNMP Trap messages could sometimes contain garbage characters.
  - **COP-7321:** The hardware accelerated IDP scanning caused "unexpected duplicate match" log messages under certain conditions.
  - **COP-7337:** The SNMP logger could in rare circumstances cause the system to malfunction.
  - **COP-7345:** Web Content Filtering functionality could fail if the WCF server used for URL lookups stopped responding to queries. The mechanism used for failing-over to secondary servers has been improved. WCF will connect to the second closest server if the primary server fails. If that server also fails, it will continue with the other servers. After 1 hour of using secondary servers, a new attempt will be made to contact the primary server in order to minimize latency.

## 3.2. Addressed Issues in CorePlus 9.00.01

- **COP-1549:** ICMP Destination Unreachable packets were not sent when UDP packets hit a Reject rule.
- **COP-2193:** Web authentication and wwwsrv connections were closed at reconfiguration.
- **COP-2231:** The DHCP Server did just send replies back on the receiving interface without regarding routing decisions. The DHCP Server now performs a route lookup if the reply is destined for a host address (i.e. not an IP broadcast).
- **COP-3346:** Eats TCP packets on the HA-node which was inactive when IDP was enabled, if fail-/handover occurs. HA for idpupdate now let active node download files. Timestamps are compared after reconfigure and signature files are synchronized between HA-nodes.
- **COP-4964:** Some services were using the private IP in HA setups for communicating. This is now changed to use the shared IP.
- **COP-5385:** The DNS lookup of the IP address to a remote gateway failed under certain circumstances.
- **COP-5847:** The CLI command for displaying updatecenter AV/IDP update status was not showing enough information. It has now been improved.
- **COP-6036:** The SMTP ALG could not tell the difference between the new Microsoft Office 2007 document file types and file type ZIP. This is because there is no difference that can be

---

easily discovered (the new Microsoft Office files are in fact ZIP files with a different extension). An ALG configured to make file integrity checks would therefore signal these files as invalid (wrong mime type, wrong file suffix...). The ALG will now identify Office 2007 files as ZIP files. Anti-virus checks will, if enabled, scan the contents of the new Office 2007 files just like it would with a regular ZIP file.

- **COP-6045:** IP address with suffixes .0 and/or .255 could incorrectly be assigned to IPsec config mode clients.
- **COP-6186:** Nested MIME bodies could in some scenarios be blocked by the SMTP-ALG. For example, the SMTP-ALG could block images inserted as 'inline' with an error message indicating base64 decoding error. The recipient received the email without the attached image but an error message saying: "The attachment xxxx has been blocked by the Security Gateway". The ALG has been updated with better support for nested MIME blocks.
- **COP-6209:** SMTP ALG statistics are now implemented both for RTM and SNMP and the Clavister MIB has been updated.
- **COP-6276:** When using the e1000 driver with an 82573-based MAC, link detection could sometimes fail under high load. This affects the SG3200-series appliances.
- **COP-6316:** Capture filters configured for the pcap functionality did not remain the same after a reconfigure.
- **COP-6338:** Default IPsec MTU is now 1420.
- **COP-6377:** IPsec tunnel setup could in some scenarios read from uninitialized memory and cause instability problems. The issue has been corrected and together with this fix, the memory used by the IPsec engine has been registered and can now be monitored using the 'memory' CLI command.
- **COP-6406:** DNS Blacklist CLI command showed wrong status of blacklist servers on inactive HA member. Inactive HA member does not perform any anti-spam inspection so the inactive node is unaware of the status of the blacklist servers.
- **COP-6460:** The "add" CLI command no longer adds an object with errors, unless you specify the "-force" flag.
- **COP-6503:** Attachments with very long file names could cause memory corruption.
- **COP-6512:** When restarting an interface using the yukon driver, there has been a theoretical possibility of memory corruption. This has been fixed.
- **COP-6516:** Will continue scanning even if an IDP hardware scanning error happens if AUDIT mode is used.
- **COP-6521:** In a scenario where one or more IPsec tunnels have been modified and needed to be reconfigured the unchecked use of an IPsec policy rule could cause the gateway to crash.
- **COP-6535:** Possible risk of crash, when doing a shutdown, is removed.
- **COP-6541:** Date and Time -popup dialog could not be used when inspecting logs logged in with auditor access.
- **COP-6610:** TCP connections with SYN relay were not synchronized correctly. In case of HA failover, traffic on these connections would freeze.
- **COP-6682:** Some H.323 messages were incorrectly disallowed by the ALG. The H.323 Status Enquiry message is now allowed to be forwarded through the H.323 ALG.
- **COP-6763:** The failmode setting in the HTTP ALG was not honored by the Dynamic Web Content Filtering.
- **COP-6773:** The log message for expired or no valid Web Content Filtering license did only

---

show up once. The log message is now generated every 1 minutes, when HTTP request was parsed, and should be more noticeable to the administrator.

- **COP-6791:** The SMTP-ALG could in some scenarios cause instability to the system by losing track of SMTP state synchronization. The SMTP-ALG has been updated with improved state tracking and email syntax validation.
- **COP-6803:** The primary NBNS server for L2TP/PPTP server interfaces was not possible to configure in web user interface.
- **COP-6807:** SLB TCP monitoring did not increase TCP sequence number in reset packet sent to server in case of connection timeout. The sequence number is now increased by 1.
- **COP-6842:** SLB did not use All-To-One for port numbers, when using a range on the service the destination port would be the specified port + the offset from the low port number in the service.
- **COP-6897:** If the first message in the memlog was log ID 01800504, the memlog would display an empty table.
- **COP-6920:** Saves the current command line so you can recover it by pressing the down arrow when viewing the last history item.
- **COP-6947:** The description text for IP Pools incorrectly specified that IP Pools could be used by L2TP and PPTP.

## 4. Installation Instructions

### 4.1. Upgrading from a CorePlus 8.nn system

For a detailed instruction on how to upgrade from a CorePlus 8.nn version to 9.nn please refer to Chapter 2 of the Admin Guide for CorePlus 9.00



#### ***Important***

*Only versions from and including 8.60.01 upwards can be upgraded to 9.nn.*

### 4.2. Upgrading 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 your 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 is uploaded to the gateway you will be presented with a "Firmware upload complete." message and the system will restart.
- When the system is restarted you will be presented with the login screen and your system upgrade is completed.

---

## 5. Known Issues

- **HA: Transparent Mode won't work in HA mode** There is no state synchronization for Transparent Mode and there is no loop avoidance.
- **HA: No state synchronization for ALGs** No aspect of ALGs 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.
- **HA: 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.
- **HA: No state synchronization for L2TP, PPTP and IPsec tunnels** There is no state synchronization for L2TP, PPTP and IPsec 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.
- **HA: 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.
- **HA synchronization with a gateway using CorePlus version 8.81.01 is not supported.** Due to an interoperability problem in the High Availability protocol, HA synchronization with version 8.81.01 of CorePlus is not supported, and will cause stability issues.
- **IPsec: Pure IPsec between Windows Vista and Clavister CorePlus is not supported.**
- **The advanced setting PPTPBeforeRules is not obeyed in the current version of CorePlus.**

## 6. Compatibility

The following section outlines the direct compatibility considerations as of CorePlus 9.00.02.

The following appliance series are supported as of the Clavister CorePlus 9.00.02 release. Clavister does not guarantee compatibility with other appliances.

- SG10 Series
- SG50 Series
- SG3100 Series
- SG3200 Series
- SG4200 Series
- SG4400 Series

---

For software installations please refer to the Hardware Compatibility List on the Clavister website.

## 7. Licensing

Version 9.00 of Clavister CorePlus requires that you have a software subscription covering the **11th of March 2008**. Make sure that this is covered before trying to upgrade your system, otherwise the system will enter a "License Lockdown" mode.

## 8. Getting Help

### **Technical Assistance via Telephone or Email**

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

Clavister Technical Support  
Phone: +46 (0)660-29 77 55  
E-mail: [support@clavister.com](mailto:support@clavister.com)  
Web: <http://www.clavister.com/support/>