Clavister CorePlus 9.30

Release Highlights

FEATURE SUMMARY

- IPv6 support
- Improved SSL/TLS support
- MAC address authentication
- Increased number of IDP Signatures
- Password Caching Prevention
- New and improved HTTP Poster

Introducing Clavister CorePlus 9.30

Clavister CorePlus 9.30 is our latest version of our award-winning network security operating system powering the Clavister Security Gateway Series, our premium enterprise unified threat management (UTM) security solution.

The Clavister CorePlus 9.30 features support for IPv6, improved SSL/TLS support, new MAC address authentication, increased number of IDP Signatures, prevent login passwords to be saved in Web browsers and a new implementation of the HTTP Poster.

The new release enables network administrators to gain even more benefits from their Clavister Security Gateways and improve their overall infrastructure.

New Features

IPv6 support

Clavister CorePlus 9.30 includes support for the new IP address standard IPv6. The new standard is designed to succeed the existing IPv4 standard. There are numerous advantages of using IPv6, for example, a larger number of available global IPv6 addresses. This means that NAT is no longer required to share a limited number of public IPv4 addresses.

The following Clavister CorePlus areas support IPv6 in this release: Ethernet and VLAN interfaces (static IPv6 address assignment), IP Rules ALLOW, DROP and REJECT, Routing, Policy-Based Routing, ICMPv6 and Neighbor Discovery, which replaces ARP in IPv6.

For more information about IPv6 support, please see the **Clavister CorePlus 9.30 Administration Guide**.

Improved SSL/TLS support

The SSL/TLS implementation has been improved in Clavister CorePlus 9.30. The major new improvement supports TLS Renegotiation for SSL/TLS as described in RFC5746 – SSL and TLS Renegotiation Vulnerability. The TLS Application Layer Gateway (ALG), SSL VPN, web authentication using HTTPS and the Clavister Web Management administration interface using HTTPS, all benefit from these security improvements.

For more information about SSL VPN support, please see the **Clavister CorePlus 9.30 Administration Guide**.

WE ARE NETWORK SECURITY

MAC address authentication

Clavister CorePlus 9.30 also support MAC address authentication enabling HTTP/HTTPS clients to use the MAC address of the connecting client's Ethernet interface for automatic authentications. This means that authentication is based only on the identity of the client hardware.

MAC address authentication is useful when administrators wants to ensure simple access for a particular device and not requiring the user to type in their credentials.

For more information about MAC address authentication, please see the **Clavister CorePlus 9.30 Administration Guide**.

Increased number of IDP Signatures

The number of Intrusion Detection and Prevention (IDP) Signatures for the Clavister Security Gateway 3200 Series has been increased to support up to 22,000 IDP Signatures.

For more information about Intrusion Detection and Prevention, please see the **Clavister CorePlus 9.30 Administration Guide**.

Password Caching Prevention

Clavister CorePlus 9.30 will prevent user login passwords to be saved in the Web browser to avert the possibility of malicious use. This feature is supported in the Clavister Web Management administration interface, as well as for SSL VPN logins.

For more information about password caching prevention, please see the **Clavister CorePlus 9.30 Administration Guide**.

New and improved HTTP Poster

The HTTP Poster has been completely rewritten and supports a number of new enhancements, including settings for individual time-outs, the possibility to post after each reconfiguration and greatly improved number of posters. The new HTTP Poster also fixed numerous defects and reporting time-out issues.

For more information about the new HTTP Poster, please see the **Clavister CorePlus 9.30 Administration Guide**.

Availability

Clavister CorePlus 9.30 is available for download for customers with active Clavister Software Maintenance Agreement. Please visit www.clavister.com/support/downloads/clavister-coreplus for download information (registration required).

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/).
This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

About Clavister

For over a decade, Clavister has been delivering leading network security solutions, providing commercial advantage to businesses worldwide. The Clavister family of Carrier Telecom Security Systems, unified threat management (UTM) appliances and remote access solutions provide innovative and flexible network security with world-class management and control. Clavister is a recognized pioneer in virtualization and cloud security. This compliments its portfolio of hardware appliances delivering customers the ultimate choice of network security products. Clavister products are backed by Clavister's award-winning support, maintenance and training program. Clavister boasts an unprecedented track record in pioneering network security solutions including the two largest deployments of Virtual Security Gateways in the world to date.

Clavister's solutions are sold through International sales offices, distributors, and resellers throughout EMEA and Asia.

To learn more, visit www.clavister.com.

Clavister Contact Information

Sales Offices
www.clavister.com/about-us/contact-us/worldwide-offices

General Contact Form
www.clavister.com/about-us/contact-us/contact-form

CID: clavister-dts-clavister-coreplus-9-30 (2011/09)

WE ARE NETWORK SECURITY

Clavister AB, Sjögatan 6 J, SE-891 60 Örnsköldsvik, Sweden
Phone: +46 (0)660 29 92 00 | Fax: +46 (0)660 122 50 | Web: www.clavister.com