

Product Data Sheet



Clavister Secure Access Gateway 3000 Series

Clavister SSP™ Security Services Platform

firewall • VPN termination • intrusion prevention • anti-virus
anti-spam • content filtering • traffic shaping • authentication

CLAVISTER®

Protecting Values



- Increased Productivity
- Lowers IT Overhead and Total Cost of Ownership
- Secure Application Delivery
- Multi-Factor Authentication
- Single Sign-On
- Comprehensive Access Control
- Adaptive Client User Interface
- Built-In Web Portal
- Integrated Support for Leading Portal Solutions
- Web-Based Administration
- Clavister Remote Assistance™
- Advanced Virtualization
- Dynamic Load Balancing and High Availability

Clavister Secure Access Gateway 3000 Series

Today's global economy forces organizations to reevaluate their business processes to optimize and streamline the way they do business. The importance of accurate information in a responsive and timely fashion is pivotal for any organization's ability to execute and reach its target business goals.

By making mission-critical information easily accessible to more people, organizations can gain competitive advantages fast. However, before setting up a remote access solution it is important to consider potential security risks, workforce deployment and administration. There are a number of factors that can prevent a successful deployment of a corporate remote access solution, such as authentication, access control, auditing, etc.

The Clavister Secure Access Gateway 3000 Series enables organizations to rapidly deploy a powerful and cost-effective solution for secure remote access. Users can access network resources, including corporate data resources, applications and files residing on file shares, using any standard Web browser. The Clavister Secure Access Gateway is designed to utilize the TLS/SSL protocol; the security and encryption protocol used by most standard Web browsers. By using TLS/SSL as the transport mechanism there is no need to install any clients that would require time-consuming administration.

Multi-Factor Authentication (MFA)

Clavister Secure Access Gateway offers a multitude of different authentication methods, ranging from single factor authentication methods, such as username/password, Web-based token, to multi-factor authentication methods, such as SMS token and hardware tokens, including EMC/RSA SecurID and VASCO DIGIPASS. It is also possible to use an external RADIUS authentication server for authentication. Your users can use the most secure and convenient authentication method for authentication, without fear of identity theft or unauthorized access.

Single Sign-On (SSO)

Clavister Secure Access Gateway provides a comprehensive Single Sign-On environment with support for internal systems based on group membership, authentication method, IP address, and client encryption level. This enables users to interact with multiple corporate data resources and applications without having to re-authenticate every time, thus creating a seamless, transparent workflow.

Advanced Virtualization

Clavister Secure Access Gateway has full support for virtual hosts. This means that you can set up and host several different solutions, each with its own directory service, using the same Clavister Secure Access Gateway.

Features and Benefits

Increased productivity. Clavister Secure Access Gateway 3000 Series enables organization to easily set up a secure remote access solution. This solution enables their mobile workforce access to corporate data resources and applications, regardless where they are and which device they are using. Always correct and timely information when your workforce needs it.

Lowers IT overhead and total cost of ownership. Clavister Secure Access Gateway 3000 lowers IT costs by enabling network administrators to deploy and manage a remote access solution, which extends remote access via SSL VPN to all network resources. Clavister Secure Access Gateway requires no client installation which reduces management overhead and lowers your support calls.

Comprehensive access control. Clavister Secure Access Gateway supports differentiated access control, based on group membership, authentication method, IP address, and client encryption level. This enables you to set up precise and fine-tuned access controls for all your users that match their needs and credential levels.

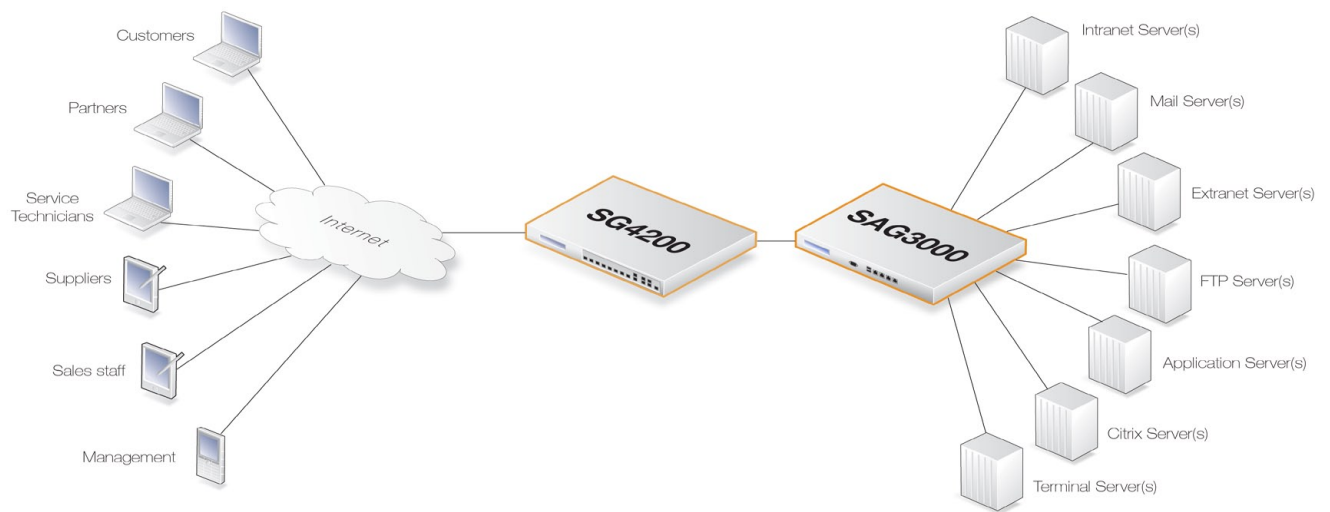
Adaptive device user interface model. Clavister Secure Access Gateway supports an innovative adap-

tive device user interface model, which adapts its look and feel based on available bandwidth and Web browser support. Your users will be able to access and use required corporate data resources and applications depending on the ability of the device.

Integrated support for leading portal solutions. For customer who demand even more flexibility, Clavister Secure Access Gateway offers integrated support for leading Web portal solutions, such as EPI Server's EPI Server Content Management Server, Microsoft SharePoint Portal Server and Senselogix's SiteVision.

Dynamic load balancing and high availability. Clavister Secure Access Gateway comes with sophisticated load balancing features and high availability support. You will be able to set up clustered, load balanced solutions in matter of minutes, giving your users reliability and confidence that they will be able to access corporate data resource without interruptions.

Clavister xPansion Lines™ Flexible Licensing. The Clavister Secure Access Gateway comes with the Clavister xPansion Lines™ licensing, which lets you start with the model that matches your current needs and allows scaling to match your growing needs.



This virtualization capability makes it possible for Managed Security Service Providers (MSSP) and other types of service providers to provision remote access solutions to multiple customers using the same infrastructure thereby decreasing costs for both equipment and administration.

Built-In Web Portal

Clavister Secure Access Gateways offers a sophisticated and customizable user portal right out-of-the-box. The Clavister Access Portal can be used both as your extranet for partners as well as your intranet for employees. The Clavister Access Portal can be set up to present only the resources that the visitor need and should see. The Clavister Access Portal can also be configured to present different resources based on how strong authentication method the visitor currently uses. This gives you as an administrator a very fine-granular level of administration at the same time as it allows you to raise the overall security in your network. The Clavister Secure Access Gateway does not require any infrastructure changes or software client installation which makes deployment fast and effortless.

Web-Based Administration

Clavister Secure Access Gateway offers fast, centralized and dynamic Web-based administration interface, enabling administrators to easily manage all aspects of their remote access installation.

Feature Highlights

Mobile Workforce

All users, based on the existing IT security policy, can gain secure access to all types of internal systems and information - anywhere, at any time. All you need is a computer connected to the Internet and a standard web browser. Since no client software is required on the connecting computer, Clavister offers a very high level of mobility for your mobile workforce.

High Security

Clavister Secure Access Gateway provides secure authentication, including One-Time Passwords (OTP) that can be distributed to the user by Short Message Service (SMS). You can also use several well-known external authentication methods, such as VASCO DIGIPASS, EMC/RSA SecurID and any external RADIUS-compliant authentication server.

No trace or history data is left behind on the connecting client computer, when the session terminates, which ensures that no other user of the client computer can gain access to the information afterwards.

Secure Application Delivery

By allowing secure clientless access to most IT environments, Clavister Secure Access Gateway offers full flexibility. A connection can be made to

Web pages, Web-based applications, and TCP and UDP/IP-based applications with advanced protocols that are not Web-based. Some examples of protocols managed by the Clavister Secure Access Gateway are Citrix Metaframe, Microsoft Terminal Services, SSH, VNC, pcAnywhere, RemotelyAnywhere, FTP, and Microsoft Windows network disks.

Cost Effective Solution

Through central administration, no client software, and no need for reconfiguration of existing internal target systems, Clavister Secure Access Gateway offers you a comprehensive and cost-effective solution. The connection to existing user administration, such as Microsoft Active Directory and Novell eDirectory, entails even less administration.

Thanks to the high level of scalability, Clavister Secure Access Gateway is the perfect choice for small as well as larger organizations. It is easy to customize the solution to fit your current needs.

Clavister Remote Assistance™

Clavister Secure Access Gateway also supports Clavister Remote Assistance™, enabling administrators to remotely access users devices and assist users in need.

Specifications

	Clavister SAG3010	Clavister SAG3015	Clavister SAG3025	Clavister SAG3050
Performance				
Concurrent users	Support for up to 10 concurrent users	Support for up to 15 concurrent users	Support for up to 25 concurrent users	Support for up to 50 concurrent users
Hardware				
Form Factor	1U rack-mount	1U rack-mount	1U rack-mount	1U rack-mount
Dimensions	16,7" W x 1,1" H x 10,6" D (426 mm W x 44,4 mm H x 270 mm D)	16,7" W x 1,1" H x 10,6" D (426 mm W x 44,4 mm H x 270 mm D)	16,7" W x 1,1" H x 10,6" D (426 mm W x 44,4 mm H x 270 mm D)	16,7" W x 1,1" H x 10,6" D (426 mm W x 44,4 mm H x 270 mm D)
Weight	6 kg (13,2 lbs)	6 kg (13,2 lbs)	6 kg (13,2 lbs)	6 kg (13,2 lbs)
Network	Four 10/100/1000Base-T Ethernet	Four 10/100/1000Base-T Ethernet	Four 10/100/1000Base-T Ethernet	Four 10/100/1000Base-T Ethernet
I/O Interfaces	DB9 RS-232 x 1, USB 2.0 x 2*	DB9 RS-232 x 1, USB 2.0 x 2*	DB9 RS-232 x 1, USB 2.0 x 2*	DB9 RS-232 x 1, USB 2.0 x 2*
Power				
Input	AC 90~264V@47Hz~63Hz	AC 90~264V@47Hz~63Hz	AC 90~264V@47Hz~63Hz	AC 90~264V@47Hz~63Hz
Power supply	220W	220W	220W	220W
Environmental				
Operating temperature	0° to 40° C (32° to 104 F)	0° to 40° C (32° to 104 F)	0° to 40° C (32° to 104 F)	0° to 40° C (32° to 104 F)
Humidity	5% ~ 95%, non condensing	5% ~ 95%, non condensing	5% ~ 95%, non condensing	5% ~ 95%, non condensing
Regulatory Approvals				
Approvals and Compliance	FCC, CE	FCC, CE	FCC, CE	FCC, CE
Key Features				
Security				
Encryption	Configurable session length, Ciphers: DES, 3DES, RC4, AES, Hashes: MD5, SHA			
Authentication methods	Clavister Web Token, Clavister SMS Token, Username/Password, EMC/RSA SecurID (using RADIUS), VASCO DIGIPASS (using RADIUS), external RADIUS authentication server			
Directories	Microsoft Active Directory, Novell eDirectory, OpenLDAP, RADIUS; Dynamic groups based on LDAP/AD queries, Certificate revocation lists (CRL)			
Password management	Notification of password expiration and password change from the Clavister Access Portal (CAP) portal Direct support for directory service password changes			
Access control options	User and group, Source IP and network, Destination network, Service/Port Define resources by destination URL, host name or IP address, IP range, subnet and domain, Day, date, time and range, Browser encryption key length, File system access controls			
Access and Application Support				
Supported applications/protocol	Web pages, Web-based applications, and TCP and UDP/IP-based applications; Citrix Metaframe, Microsoft Terminal Services, SSH, VNC, pcAnywhere, RemotelyAnywhere, FTP, and Microsoft Windows network disks			
Management and Administration				
Management	Clavister Management Console (CMC): centralized Web-based management for all access options, access control policies and Clavister Access Portal (CAP) configuration, support for Clavister Remote Assistance™			
Virtual Hosts	Support for Clavister Virtual Hosts, license for 2 virtual hosts are included with option to purchase more			
Auditing	RADIUS auditing and accounting integration			
Monitoring and Logging	User connection monitoring, event alarms, view logs via the Clavister Management Console (CMC)			
High Availability				
High Availability	Support for high-availability two-node cluster with built-in load-balancing and stateful authentication failover			
Clustering	Support for load-balanced array using standard external load balancers			
Warranty	All products in the Clavister Secure Access Gateway 3000 Series come with a two (2) years standard RMA warranty and ninety (90) days Software Subscription covering all major and minor software releases counting from the Start Date. Start Date means the earlier of Product registration or ninety (90) days following shipment from Clavister.			

* Reserved for future use.

NOTE: For product license options and support SKUs please visit: www.clavister.com.

CLAVISTER®

Protecting Values

Clavister AB, Torggatan 10, SE-891 28 Örnköldsvik, Sweden
Phone: +46 (0)660 29 92 00 | Fax: +46 (0)660 122 50 | Web: www.clavister.com | Email: info@clavister.com