Centralized the Control of SecureAge Security Suite

SecureAge

What is SecureAge Management Server?

SecureAge Management Server provides a platform to centralize the control of all SecureAge Security Suite's components like SecureEmail and SecureData that are deployed in your organization. It helps your IT administrator to significantly streamline and reduce the time spent in managing the security configurations and policies for multiple SecureAge users.

How Does SecureAge Management Server Work?

SecureAge Management Server comprises of three key components:

1. Role-based Policy Server

The Role-based Policy Server of SecureAge Management Server helps system administrator to simplify the management of the security infrastructure of SecureAge Security Suite. It enables detailed online, offline and temporary security policies to be customized and managed for individual SecureAge users based on their user role. A more centralized access control management helps to protect sensitive data and applications against unauthorized use especially by users with restricted privileges or who have left the organization.

In a typical SecureAge SecureData deployment, system administrators can easily configure and centrally manage individual user's privileges within an organization via the policy wizard. Different policies can be defined for different users based on their functional role in an organization. For example, the permissions to transmit plain document to external parties or decrypt information on external storage media are assigned to specific roles that are created for various job functions. Changes can also be made to the same policy especially in cases when users may transfer to another department or assume another job function within the organization.

2. Log Server

The Log Server provides enterprises with a comprehensive visibility to individual user's data access and movement within the organization. It maintains records of all file access and security log entries for easy tracking and monitoring of file access activities including information on which application is accessing which file.

The Log Server helps organizations to view and log user activity with its administration and auditing capabilities which are configured to fulfill their strict internal auditing and policy management regulations. It also provides a centralized session management that controls user sign on and records their activity during the login time. When the corporate network is suspected to be under attack, such logs become extremely useful evidence to track down the malware activities. These logs can be sent to third party syslog server to analyze and trace unusual activity logs.

3. Key Management Server

The Key Management Server is another component of SecureAge Management Server which assumes the role of a Certificate Authority (CA) in managing the digital certificates and encryption keys for multiple SecureAge users. It unifies the control of all the setup, creation, management and revocation of user's digital certificates.

Apart from issuing digital certificate, the Key Management Server also provides other functionalities like Lightweight Directory Access Protocol (LDAP) directory, Certificate Revocation List (CRL) publishing, Online Certificate Status Protocol (OCSP) server as well as renewal and revocation of certificates. Its encryption key escrow capability enables administrator to back up and recover keys and key history when the users lost their keys or left the organization. This gives organizations peace of mind knowing that encrypted data will not be lost even if the users have lost or changed their keys.

Key Features

- Easy configuration of policy to support individual enterprise security requirements.
- User specific policy control to provide different security rights to different users.
- Provides full visibility to data access audit log for forensic analysis and historical trace purposes.
- Web-based console for policy update and log management.
- Supports PKCS #1, #5, #7, #8, #9, #10, #11, #12 standards.
- Supports MD5, SHA-1 and SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512) hash functions.
- Supports unlimited key length RSA, DSA, ECDH and ECDSA.
- Comprehensive certificate, CRL and OCSP support.
- Supports external PKI / CA for certificate based authentication and certificate validity checking.
- Provides full support for X.509 v3 and PKIX compliance extensions digital certificate format.
- Supports key and certificate import / export via PKCS #12, DER and PEM formats.
- Supports SecureAge CA and many other public and enterprise CAs.

Need More Information?

General Enquiry: contactus@secureage.com
Technical Support: support@secureage.com
Public Relations / Marketing: pr@secureage.com

www.secureage.com
www.lockcube.com

Asia Pacific
SecureAge Technology Pte Ltd
20, Ayer Rajah Crescent,
#09-13, Technopreneur Centre,
Singapore 139964

Japan
SecureAge K.K.
Barbizon 18, 7F
5-18-18 Shirokanedai
Minato-ku, Tokyo 108-0071
Japan

North America
SecureAge Technology Inc
3 Twin Dolphin Drive Suite 150
Redwood City CA 94065
U.S.A.