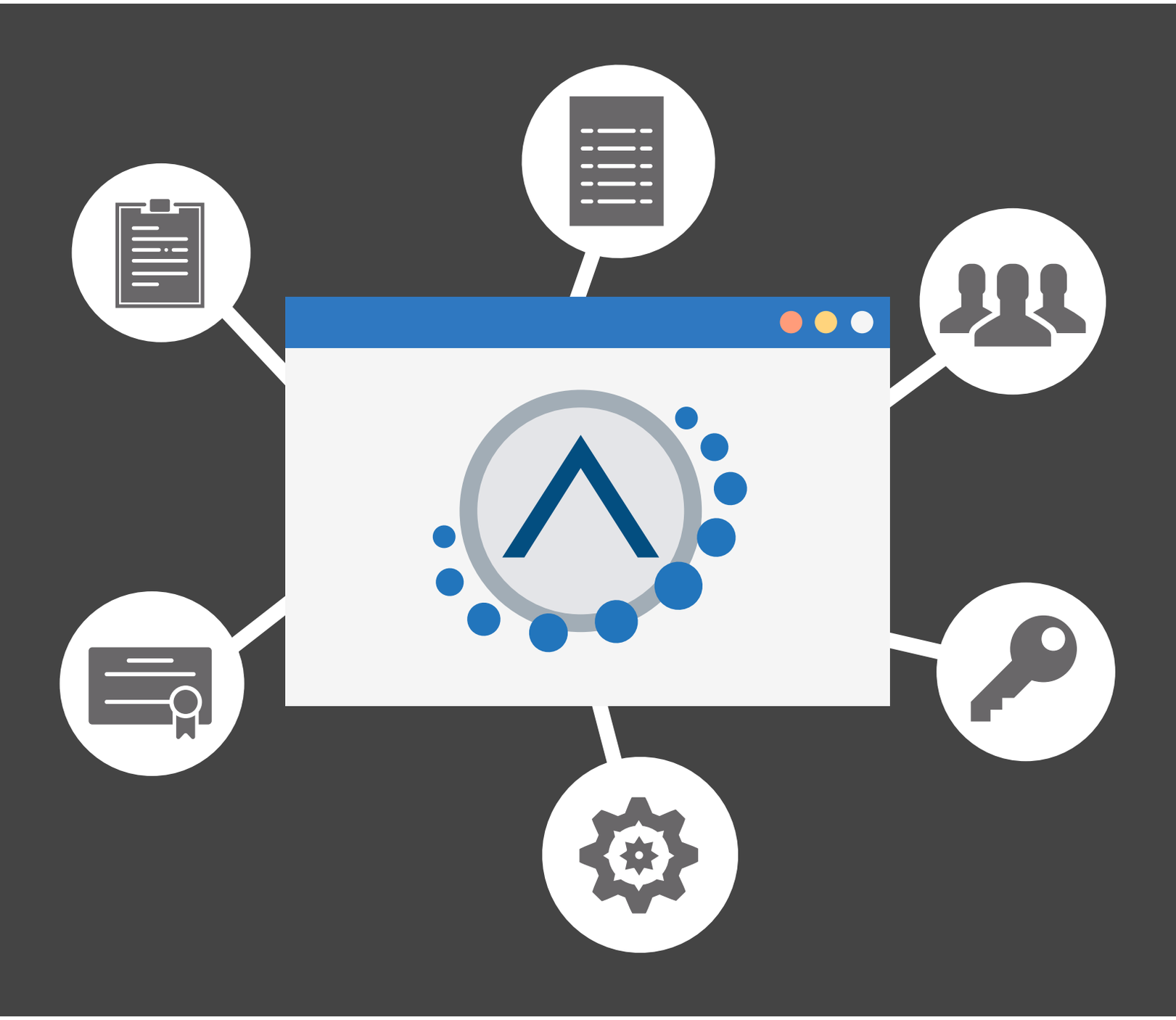
SecureAge

Security Management Server



Unified Large-Scale Centralized Security Management

What is Security Management Server?

SecureAge Security Management Server (SMS) enables enterprises to centrally control all SecureAge software deployment and oversight from a single web console. SMS offers central policy control, audit logs, application whitelisting, and key management for the SecureAge Security Suite, which includes SecureData, SecureEmail and SecureAPlus.

Keep IT Simple with 4 Core Components

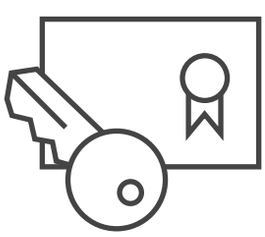
Policy Server

Security Management Server helps the system administrator to simplify deployment and management of the SecureAge Security Suite through the customization and management of detailed online, offline and temporary security configuration policies for each SecureAge user based on their role.

Log Server

By maintaining records of all file access and security log entries, Security Management Server tracks and monitors individual user data access and movement throughout the security environment, including information on which application is accessing which file.

In addition, administrators can view log records of current and previous scan activities and actions taken for all running applications, proving useful in the event of malware and ransomware attacks.



Key Management Server

The Key Management Server takes on the role of Certificate Authority (CA) in managing and issuing digital certificates and encryption keys for SecureAge client machines. It unifies the control of the setup, creation, management and revocation of user keys and digital certificates.

Whitelist Management

The Security Management Server ensures standardized client system configurations by managing and enforcing a whitelist, which allows only trusted and authorized applications to run on the user machine. Protection from malware happens both by enforcing the whitelisted applications while building and filtering a blacklist of unwanted or unauthorized applications.

Security Management Server At A Glance

Relevant Admin functions are grouped as major tabs across the top of the window for maximum visibility and ease of access to security controls

Management: Configure and manage policies, user groups, users, machines, whitelists and blacklists

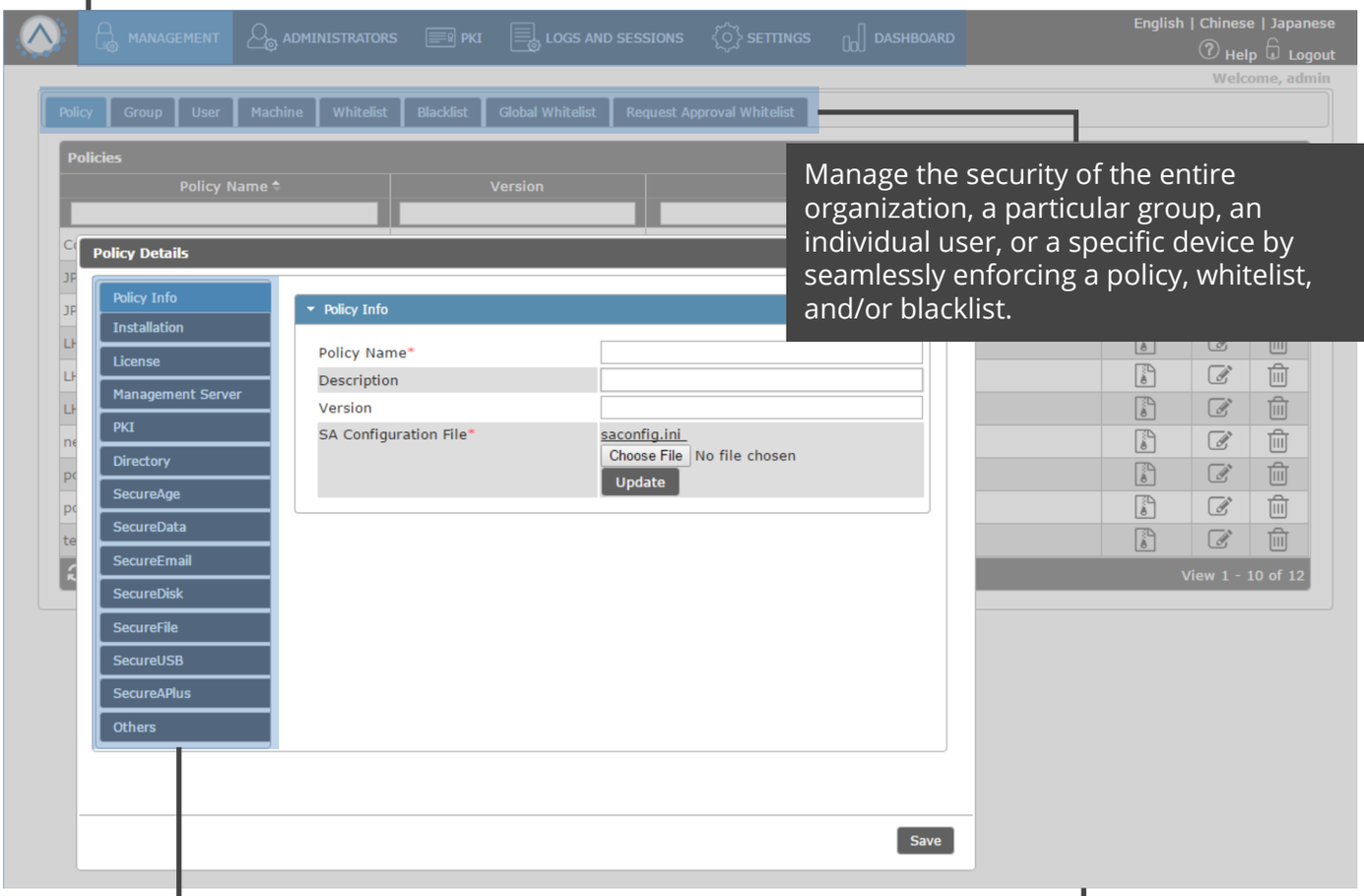
Administrators: Manage administrator and role permissions

Public Key Infrastructure (PKI): Manage encryption keys and digital certifications

Logs and Sessions: View audit logs for the server & client and login sessions for administrator & users

Settings: Configure clients' functional product settings for Network, SSL, Log, & PKI

Dashboard: Graphical overview of managed security information



Manage the security of the entire organization, a particular group, an individual user, or a specific device by seamlessly enforcing a policy, whitelist, and/or blacklist.

Policy Details

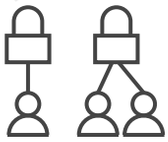
Each tab contains a comprehensive list of customizable configurations for SecureAge applications. Saving a customized policy lets IT Admins manage and easily deploy settings that match a particular enterprise environment.

Single Web Console

Simplify endpoint security with unified security configuration and management. Access to the web console can be done using either a password or a smart card.

Core Security Management Server Features

Policy Management
Easy configuration and management of policies to support individual enterprise security requirements



User Management
Create and group administrators and users according to security rights

Key Management
Create, issue, manage and store encryption keys and digital certificates for all users

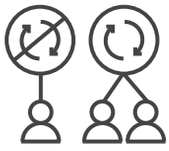
Public Key Cryptography Standards
Supports PKCS #1, #5, #7, #8, #9, #10, #11, #12 standards

Supporting Hashing Algorithm for Certificate Signing & Revocation
Supports SHA-1 and SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512) hash functions

Advanced Cryptographic Algorithm Support
Supports unlimited key length RSA, DSA, ECDH and ECDSA

Whitelist Management
Specify which users or groups are permitted or restricted to run particular applications

Audit Log Collection
Full data visibility access to server and centralized client log for forensic analysis, historical trace, and incident response

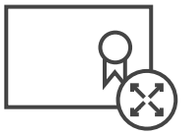


Assigned Software Update Push
Push installation of software updates for SecureAge Security Suite to particular groups and individuals

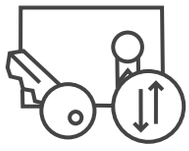
Web Console User Interface
Administrators can access the web portal to manage security on any machine connected to the network

Certificates Support
Comprehensive certificate, CRL and OCSP support

Integrate with External Certificate Authority
Supports external PKI / CA for authentication and certificate validity checking



Digital Certificates Format Support
Provides full support for X.509 v3 and PKIX compliance extensions for digital certificate format



Digital Certificate and Key Import & Export
Supports key and certificate import / export via PKCS #12, DER and PEM formats

Need More Information?

www.SecureAge.com contactus@secureage.com