Comodo Certificate Manager

Centrally Managing Enterprise
Security, Trust & Compliance

COMODO
ENTERPRISE™

SSL Certificate Management - PKI

With an ever-increasing abundance of web-enabled, collaborative and mobile applications, as well as netaccessible data and email, today's enterprises are responsible to protect more on-line business transactions and personally sensitive digital information than ever before. Our customers, business partners and government agencies rightfully expect and mandate the security of critical business, financial and personal information. At the same time, digital threats and data breaches are escalating in frequency, complexity and magnitude, and are causing security and remediation costs to skyrocket. Sound familiar?

SSL certificates protect digital information assets and identities by supporting data encryption while at rest or intransport.Certificates enable user authentication and endpoint device access rights, and are employed to digitally sign and authenticate media objects such as web content, documents, files, email messages and software programs. PKI technologies help you to effectively meet these security and regulatory challenges by providing for the rapid deployment and reliable management of Enterprise Security,Trust and Compliance.

Although some smaller organizations may be able to control a limited number of certificates, larger organizations find that certificate administration becomes burdensome and expensive as the number of users, endpoints and compliance policies increase. Dynamic security applications and policy requirements make the availability of a robust PKI certificate management application an important and essential IT asset.

Comodo has repeatedly helped businesses around the globe to address their unique requirements, and to achieve the benefits of sound PKI management solutions. By providing a capability to organize and streamline SSL certificate administration, Comodo enables significant cost savings in addition to important administrative reporting, security, management and compliance improvements. Through its' advanced certificate lifecycle management capability, Comodo Certificate Manager (CCM) provides your business the ability to self-administer, instantly provision and control all SSL certificates and certificate enabled users or devices. CCM significantly reduces administrative obstacles and security deployment times, producing clear and immediate improvements to your security infrastructure and costs.

With Comodo's Certificate Authority (CA) infrastructure that'sWebTrust certified by KPMG there's no need for you to invest in expensive hardware, software or CA expertise. Comodo is able to rapidly empower and deploy enterprise-wide PKI management structures using widely recognized, flexible and highly secure digital certificate solutions. Comodo offers the industry's broadest array of digital certificate types and terms, excellent browserrecognition of its own root-keys, fully-featured certificate management utilities, and attractive pricing. Certificates can be immediately issued through a secure web console, enabling network servers, users, applications, objects and devices to be secured in minutes rather than days. Additionally, Certificate Manager can web-enable and automate the enrollment process for requesting and issuing SSL, client authentication and S/MIME certificates.

Comodo Certificate Manager

Instant security for your web operations, internal and external networks, users and email

Comodo Certificate Manager (CCM) is a core component of Comodo's Identity, Trust and Security product portfolio. CCM provides a flexible and reliable system for digital certificate issuance and lifecycle management. By automating and centralizing the management of cryptographic keys and digital certificates, organizations are able to more easily deploy and scale the security of their e-business applications and services. CCM streamlines the lifecycle management of SSL, S/MIME and Client Authentication certificates through a unified and secure web interface. CCM is fully integrated with the Comodo Certificate Authority operation that ensures a highly secure and rapid certificate

management capability, functionality that reduces certificate administration and thus creates an efficient, productive and secure business environment.

Comodo provides the convenience and controls needed to easily and fully administer an extensive portfolio of SSL, S/MIME and Client Authentication certificates. Through its multi-tiered administrative capabilities, CCM can be easily configured to comply with your organizational authority structure(s) and security policies. Microsoft Active Directory integration, and CSV file upload utilities enable the rapid automation of client certificate tasks such as enrollment, issuance and revocation while Key Management Services

with protected key storage, enables your organization to recover valuable data encrypted by the original user.

CCM was designed to significantly reduce the administrative complexity, time and costs of operating PKI based security solutions. More time, less costs, so that you can enjoy the security that you and your customers deserve.

Assure customers and partners of your identity

Assuring customers of your identity is an essential factor for successful online business. Certificates and Trustmarks issued through Comodo assure customers of your online and email identity. Further, Comodo's support for digital certificate industry standards such as X.509v3 and International Domain Naming (UTF-8 encoding that enables internationalization of domain names and certificate content) ensures their ubiquity and widespread acceptance. Comodo also applies its patent-pending certificate deployment and EV enhancement Instant security for your web operations, internal and external networks, users and email Assure customers and partners of your identity Comodo Certificate Manager Creating Trust OnlineTM tools to speed your deployments and to extend certificate recognition, all factors that serve to increase user confidence and trust in your brand and identity. Through CCM's user-friendly interface you can issue digital certificates to web servers, internal servers, employees and partners with certificates that in turn represent the identities and credentials of their owner. Comodo helps you achieve trust and confidence within an environment where trust and confidence is essential.

Comodo Certificate Manager Feature Summary

- Secure, multi-tiered administrative web interface to the Comodo Certificate Authority operations. Flexible organizational alignment of administrative domains and responsibilities easily adjusts to your business model.
- Two-Factor Authentication and/or IP address validation for highly secure administrative account access protection.
- Local or Comodo secure site hosting options provide flexible security and reliability choices for this turn-key solution. Comodo secure site(s) meet the highest levels of security and resiliency.
- Certificate Lifecycle administration for Comodo's extensive portfolio of SSL, S/MIME and Client Authentication certificates that allows for the rapid enrollment, approval, issuance, revocation and renewal of all certificates.
- Same day expirations; CCM allows administrator to control the term and expiration (day/month/year) of all issued certificates.
- Client Key Management Services; escrow and recovery of private keys enabling a protected (policy driven) restoration of user encrypted data.
- Auto-Enrollment; Web Interface for corporate SSL requests from functional owners (non-admins) facilitates an easy to acquire certificate enrollment request.
- Self-Enrollment; Web Interface for Client (user) certificate requests and deployment programs makes enrollment and distribution of user keys seamless.
- Web-Interfaces can be localized and branded to maintain your corporate logo and image at all times.
- Auto-Deployment; Microsoft Active Directory or CSV file upload utilities for rapid client certificate distribution and management achieves tight integration with many types of directory-based employee/device management systems.
- Configurable email alerts for pending certificate requests, approvals, expirations and revocations allows administrator to be notified about requests, or to enable certificate owners and administrators to receive expiration notices in advance.
- Report sub-system produces detailed certificate and administrative status and activity logs.
- Quick implementation and set-up, expert technical assistance and thorough User Guides.
- Real-Time Status Checking; Being able to verify the validity of certificates is extremely important to the integrity of a certificate management system. Comodo real-time Online Certificate Status Protocol (OCSP) eliminates the time lag during which users could log on and gain access to the system after their certificate has been revoked – thereby helping to eliminate the threat of security breaches from non-valid certificates.

Comodo Certification Authority Operations

More than 200,000 businesses use and rely upon Comodo for their Internet Identity, Security, Trust and Brand Assurance. On a day to day basis Comodo provides services which are certified to provide the highest possible levels of trust and integrity. To meet such requirements Comodo has invested heavily in providing both physical and logical security for the Certification Authority operations using high availability and redundant server systems deployed across diverse geographic locations.

Comodo Secure Operations Overview

Comodo employs policies and practices that have been designed to meet or exceed the requirements of the AICPA/ CICA WebTrust Program for Certification Authorities, ANSI X9.79:2001 PKI Practices and Policy Framework, and other industry standards related to the operation of CAs. Comodo's global compliance with these stringent security and reliability standards has been repeatedly certified by KPMG.

To date, Comodo has issued hundreds of thousands of "validated" SSL and email digital certificates through our secure Certification Authority operation. The advanced physical and logical security and validation practices ensure that all Comodo certificates are highly trusted.

Use of Hardware Security Modules for Key Protection and Certificate Generation

Comodo securely generates and protects its own private key(s), using a trustworthy system (IBM 4758 accredited to FIPS PUB 140-1 level 4), and takes necessary physical and logical precautions to prevent the compromise or unauthorized usage of such devices. All digital certificates issued are issued using IBM 4758 hardware security modules.

Access to the secure part of Comodo facilities is limited through the use of physical access control and is only accessible to appropriately authorized individuals (known as Trusted Personnel). Card access systems are in place to control, monitor and log access to all areas of the facility. Access to the Comodo CA physical machinery within the secure facility is protected with locked cabinets and logical access control.

The secure facilities are protected from fire and smoke damage (fire protection is made in compliance with local fire regulations) and flood and water damage. Comodo secure facilities have a primary and secondary power supply and ensure continuous, uninterrupted access to electric power. Heating / air ventilation systems are used to prevent overheating and to maintain a suitable humidity level. Comodo employs a redundant CAsystem to ensure uninterrupted service levels.

The secure facilities are protected from fire and smoke damage (fire protection is made in compliance with local fire regulations) and flood and water damage. Comodo secure facilities have a primary and secondary power supply and ensure continuous, uninterrupted access to electric power. Heating / air ventilation systems are used to prevent overheating and to maintain a suitable humidity level. Comodo employs a redundant CAsystem to ensure uninterrupted service levels.
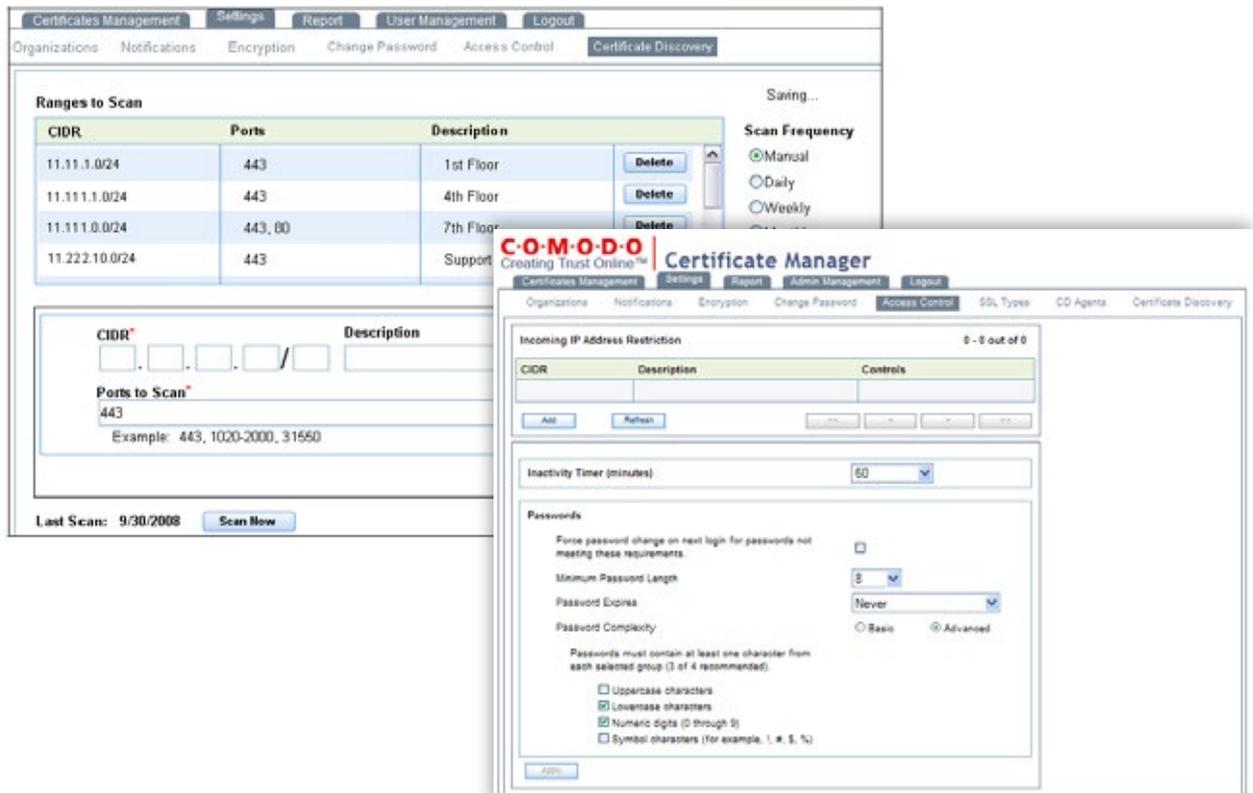
About Comodo

The Comodo companies create the infrastructure that is essential in enabling e-merchants, other Internet-connected companies, software companies, and individual consumers to interact and conduct business via the Internet safely and securely. The Comodo companies offer PKI SSL, Code Signing, Content Verification and Email Certificates; award winning PC security software; vulnerability scanning services for PCI Compliance; secure email and fax services. Continual innovation, a core competence in PKI, and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo secures and authenticates online transactions and communications for over 200,000 business customers and 10,000,000 users of our desktop security products.

For additional information on Comodo – Creating Trust Online™ visit www.comodo.com