

Comodo Certificate Manager Certificate Management Problem Solved

Why SSL Certificates?

SSL certificates play a vital role in nearly all online transactions, ensuring a secure, trusted connection between a given browser and a given website. Ensuring the safe transmission of data, login information, and other key Internet-facilitated functionality, SSL certificates provide the foundation for online trust, and allow the Internet functionality for online banking, shopping and bill-paying that have become so ingrained into 21st century life.

The foundation for SSL-based security is encryption, an extremely reliable process when properly configured, but which can suffer from dangerous vulnerabilities if not effectively implemented or managed correctly. In fact, business security is too often compromised by a lack of automated certificate management tools. Attempts to manually track and monitor multiple certificates from various vendors will almost always result in error and mismanagement, leading to missed renewals and expired certificates, which, in turn, generally lead to insecure connections, lack of trust, and a tarnished brand, among other problems.

Effective enterprise certificate management protects against data breaches, failed audits and costly unplanned downtime. Just one expired certificate can lead to major outages, potentially costing tens of thousands of dollars to remediate and damaging brand integrity.

Why Comodo?

Comodo Certificate Manager, developed in partnership with several Fortune 500 companies, consistently and securely manages large volumes of digital certificates of all types and signature algorithms (SSL, ECC, RSA); CCM is the solution to these common – and potentially extremely costly – enterprise challenges.

Created by the world leader in SSL Certificates, Comodo Certificate Manager is an industry-leading, fully integrated automated enterprise solution designed to simplify digital certificate issuance and lifecycle management. Through its advanced capabilities, CCM provides businesses the ability to self-administer, instantly provision, and control all SSL certificates throughout their organization. Comodo leads the SSL certificate industry as an originator of the Certificate Authority/Browser (CA/B) Forum, a consortium of CAs and Internet browser providers that develop guidelines to govern the issuance and management of CAs. Comodo has been a pioneer in certificate management since the founding of the CA/B Forum in 2005 and issues more certificates than anyone else on earth, having surpassed Symantec (Verisign) in February, 2015, and has widened its lead over their nearest competitor by over 10% since then, currently holding over 41% of market share, and growing.

Comodo Certificate Manager is a robust, centralized certificate management solution designed to provide enterprise clients with a secure, reliable and consistent structure for the entire certificate lifespan, featuring streamlined but powerful tracking, management and compliance functionality for all of their SSL/PKI needs.

Comodo Streamlines Auto Discovery

Diving a little deeper, CCM's Auto Discovery feature simplifies the formerly arduous and error-prone manual discovery process. Rather than logging into various vendor portals to monitor each certificate's lifecycle, and manually collecting detailed information on SSL certificates purchased at different times from different CAs, Comodo Certificate Manager automates the process. After conducting a comprehensive scan of external (as well as internal) networks to discover every certificate regardless of the issuer, CCM automatically imports all relevant information, bringing the entire certificate inventory under central control and offering a comprehensive view of all certificates. CCM's Auto Discovery feature provides vital details about each certificate, including:

- The location of each SSL certificate (on both internal and external networks)
- The name of the CA that issued each SSL certificate
- The date each SSL certificate is set to expire
- Whether any certificates have weak keys (as of January 2014, keys must be 2048 bit or higher)
- Scheduling scans to run on a recurring basis.
- Providing the Signature Algorithm used to sign the certificate
- Identifying what ciphers are supported on the targets

“Since installing the Comodo Certificate Manager solution, it has become a major part of our IT management infrastructure, allowing us to update, add and delete thousands of digital certificates with a streamlined dashboard and email alert system.”

~ Craig Hurter, IT Security Manager,
University of Colorado at Boulder

WebTrust Certification

CCM is a proven, well-regarded and thoroughly trusted global solution for enterprise certificate management. Comodo's CA infrastructure is WebTrust certified by Ernst & Young. CCM creates an efficient, productive and secure business environment that allows organizations to issue SSL certificates for use within internal and external networks, websites, and email systems.

Quick, Easy and Cost-Effective

CCM offers scaled discounts from Comodo's already low prices on SSL certificates, enabling quick, easy and cost-effective fulfillment of multiple certificate requirements for distributed systems and personnel, as well as load balancing requirements.

Fast, Customer-Focused Rollout

CCM's Software-as-a-Service (SaaS) architecture enables PKI management within hours. CCM significantly reduces administrative obstacles and time delays. SSL certificates can be issued immediately through a secure web console, thus enabling network servers, users, applications, objects and devices to be secured quickly. CCM also automates the enrollment process for requesting and issuing SSL, client authentication, code signing and S/MIME certificates.

Multiple Administrative Tiers

CCM facilitates granular user management, enabling a master administrator to assign specific permissions to various personnel. Business sectors can be delegated in such a way that management of the certificate assets of a particular department, network, domain or subdomain can be assigned in whatever way is most beneficial to the organization, even to a specific person.

Maximize Certificate Management with Minimal Resource Expenditure

Comodo safeguards businesses against the interruptions associated with manual CA management. CCM discovers all certificates in the trust chain (root, intermediate and end-entity) and provides details of each individual certificate including its issuing authority and expiration date. In addition, the “Important Messages” panel displays any certificate or server vulnerabilities.

Features

Certificate Lifecycle Administration

Extensive portfolio of SSL, Code-Signing, S/MIME and client authentication certificates that allows for the rapid enrollment, approval, issuance, revocation and renewal of all certificates.

Internal and External Discovery Scanning - Administrators can track and see all the details of each certificate purchased from different vendors.

Secure, Multi-Tiered Administrative Web Interface - Flexible organizational alignment of administrative domains that easily adjusts to your business model.

Configurable Email Notifications - Allows the administrator to be notified about requests, approvals, expirations or revocations and enables certificate owners and administrators to receive expiration notices in advance.

Same-Day Expirations - Administrators control the term and expiration (day/month/year) of all issued certificates.

Dashboards - Provides one common, intuitive dashboard to view.

Reporting - Produce detailed reports, certificate and administrative status, and activity logs.

Client Key Management Services - Escrow and recovery of private keys enable a protected (policy-driven) restoration of user encrypted data.

Automatic Deployment with Microsoft Active Directory or CSV File Upload - Rapid client certificate distribution and management achieve tight integration with many types of directory-based employee/device management systems.

Automatic CSR Generation and Private Key Management - Escrow and recovery of private keys for SSL certificates in a secure and redundant way simplifying key management and protecting certificate assets from human error and data loss.

Server Auto Installation, Enrollment and Renewal – [Corporate SSL requests from functional owners facilitates an easy-to-acquire certificate enrollment request, allowing for the scheduled enrollment of certificates on Apache, Tomcat or IIS.](#)

Self-Enrollment Web Interface – Provides a secure and fluid workflow for requestors to enroll for SSL or client certificates, making enrollment and distribution of certificates seamless.

Customized Web Interfaces - Can be customized with your corporate logo and images to help maintain your brand identity.

Reliable OCSP - Comodo real-time Online Certificate Status Protocol (OCSP) is distributed worldwide to maintain high availability.

Code Signing on Demand – Rapid code-signing service that gives enterprises the ability to give their development teams a centrally managed platform to sign their code. This allows them to manage which users can sign code, what code has been signed, and which code-signing certificate was used to sign it, as well as the status of those [code-signing certificates](#).

Two-Factor Authentication and/or IP Address Validation - Highly secure administrative account access protection.

Hosted Private CA – CCM's 'Private CA' feature allows companies to seamlessly and expertly issue and manage privately trusted certificates without the associated setup and management costs.

Assured Compliance – Comodo will automatically keep Private CAs in compliance with any changes to certificate regulations.

Web Service API's- API's are available for the enrollment, renewal and revocation for SSL and Client Certificates.

Quick Implementation and Setup – Featuring fast and efficient auto enrollment and auto installation.

Conclusion

For effective, efficient and automated certificate management throughout the certificate lifecycle, look no further than Comodo Certificate Manager to automatically for SSL and PKI Management to save time, money, effort, brand reputation, and potentially crushing remediation costs.

About Comodo

The Comodo organization is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Building on its unique position as the world's largest certificate authority, Comodo authenticates, validates and secures networks and infrastructures from individuals, to mid-sized companies, to the world's largest enterprises. Comodo provides complete end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats, both known and unknown. With global headquarters in New Jersey and branch offices in Silicon Valley, Comodo has 12 international offices across Europe and Asia.

Comodo and the Comodo brand are trademarks of the Comodo Group Inc. or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. The current list of Comodo trademarks and patents is available at comodo.com/repository