Comodo Custom Client Certificates

Highly Secure Authentication of Customers and Employees

COMODO
ENTERPRISE™

www.instantssl.com
sales@comodo.com

Exponential rise of online fraud makes it essential for business to make sure resources are accessed only by authenticated personnel.

Conducting business online offers enormous benefits to an enterprise - but also creates enormous vulnerabilities. Recent high profile breaches of corporate databases and the theft of confidential customer data have been devastating to the reputation and long-term business prospects of many high street names. Hackers have evolved beyond simple phishing scams aimed at a broad cross section of the public into targeted, well planned attacks on specific organizations. Favored tactics include social engineering techniques, sophisticated cross-site scripting, spear-phishing and man-in-the-middle attacks – all designed to intercept customer and employee login data and gain access to confidential data. According to the research and analyst firm Gartner, nearly 30 percent of those who use online services say that publicized attacks have influenced their activities. Up to 75 percent of this group are logging on less often than they would if security were not a concern.

If your business supports remote login access to servers or web applications that contain vital corporate or customer data, the stakes are just too high to depend on passwords as gatekeepers. Businesses need stronger guarantees that the person accessing an online account or network resource is the genuine user – and not a hacker that has managed to steal a username and password. To safeguard vital customer information and avoid compliance violations, you really need to take a hard look at moving to two-factor authentication.

Password protection of online resources is no longer enough

Why is this? Online fraudsters have technologically outpaced the security measures that most institutions have put in place. Fraudsters are playing havoc with transactional safety in every aspect of the online experience. They can break into passwords and other ways consumers identify themselves, and they can build fake sites with authentic looking content to steal customers' private details without the customer knowing it. As a result, many businesses in highly regulated industries are paying close attention to two factor authentication solutions to ensure secure access to confidential services. It is this type of solution that enables enterprise to authenticate the user and also allow the user to authenticate the server as genuine.

Comodo Custom Client Certificates

Authentication of the user and the device from which they are accessing

At-a-glance Client Certificates

- True, two-factor authentication of users and employees
- Binds user and device identities with strong, PKI authentication
- Enables transparent log-on with no user inconvenience
- Very easy to roll out to employees or customer bases
- No costly physical tokens to distribute or replace
- Comodo Certificate Manager further simplifies deployment and management

Comodo client certificates help businesses achieve best practice levels of strong authentication by installing a digital certificate onto a user's PC which is used to authenticate the user every time they log into their account. Each certificate deploys proven and highly secure Public/Private Key Infrastructure (PKI) to prove a user's identity to a remote computer or server. Indeed, each certificate can only be used to authenticate one particular user because only that user's computer has the corresponding and unique private key needed to complete the authentication process. These client certificates are used as second factor user authentication, the first being user credentials such as login id and password.

A PKI based client certificate assures an enterprise that the person logging into a secure service is indeed one of their users by validating not only their User ID and Password, but their certificate as well. This type of solution can be delivered only by a Certification Authority such as Comodo because only a Certification Authority has the experience and expertise to manage the full life-cycle of these digital certificates - including issuance and revocation.

The Comodo Custom Client Certificate is highly customizable and:

- Allows full control over the contents of the "Subject" field of the certificate.
- Allows fully customizable web-pages, which can be hosted anywhere, for the certificate sign-up and collection/installation process.

How it Works – in brief

A Comodo X.509 Custom Client Certificate, once installed into the certificate store of the user's internet browser (e.g. Internet Explorer, FireFox, Opera), will be requested and verified every time the user logs into an enterprise's server and will authenticate them as the genuine account holder. Each client certificate contains two distinct yet equally important elements - the account holder's username and an encrypted public key that was generated by the

Comodo Certificate Manager - Features

- CCM's certificate life-cycle administration allows for the rapid enrollment, approval, issuance, revocation and renewal of Client Authentication certificates.
- Same day expiration. CCM allows administrators to control the term and expiration (day/month/year) of all issued certificates.
- Self-Enrollment. Web Interface for client certificate sign-up makes user enrollment and a simple and seamless process.
- Web-Interfaces can be localized and branded to maintain your corporate logo and image at all times.
- Certificates can be revoked by end-user and administrator
- Configurable email alerts for pending certificate requests, approvals, expiration 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.

end users computer during the enrollment process. This certificate is then digitally signed by the enterprise. (The enterprise will have been set up by Comodo as a sub-Certification Authority. A sub-CA is an entity entitled to sign their own user's authentication certificates from their own sub-CA certificate. In turn, the sub-CA's certificate is signed by Comodo - a trusted root CA). By signing the certificate, the sub-certification authority 'binds' the username to the public key. The presence of this certificate on the end users machine, along with the corresponding private key, is needed to complete the authentication process. This means that even if a hacker obtained an account holders username and password, they would still be denied access to the account because the enterprise's server would not detect the client certificate on the machine the hacker is connecting from.

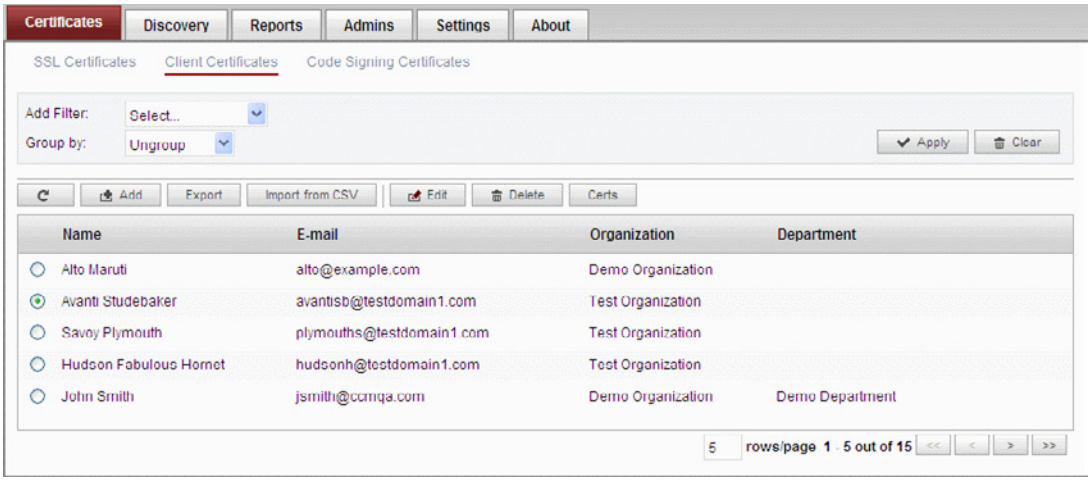
Comodo Certificate Manager

Easy-to-use web application to quickly deploy and manage client authentication certificates for employees and end-users

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 life-cycle 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 life-cycle management of 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 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. 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 your business can enjoy the security that you and your customers deserve.



Next Steps

To read more about Comodo solutions for enterprises, visit **http://www.instantssl.com**

To speak directly with a Comodo representative about client certificates or Comodo Certificate Manager, please contact us at the following:
Email: sales@comodo.com
Tel: Tel: +1 (888) 266-6361 / +1 (703) 581-6361

About Comodo

The Comodo companies provide 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.instantssl.com

Comodo CA Limited
3rd Floor, 26 Office Village,
Exchange Quay,
Trafford Road, Salford,
Manchester M5 3EQ,
United Kingdom
Tel: +44 (0) 161 874 7070
Fax: +44 (0) 161 877 7025

Comodo Group, Inc.
1255 Broad Street
Clifton, NJ 07013
United States

Tel: +1.(888).266.6361
Email: Sales@Comodo.com