COMODO
Creating Trust Online®

Comodo
Certificate Manager

Introducing the Certificate Dashboard

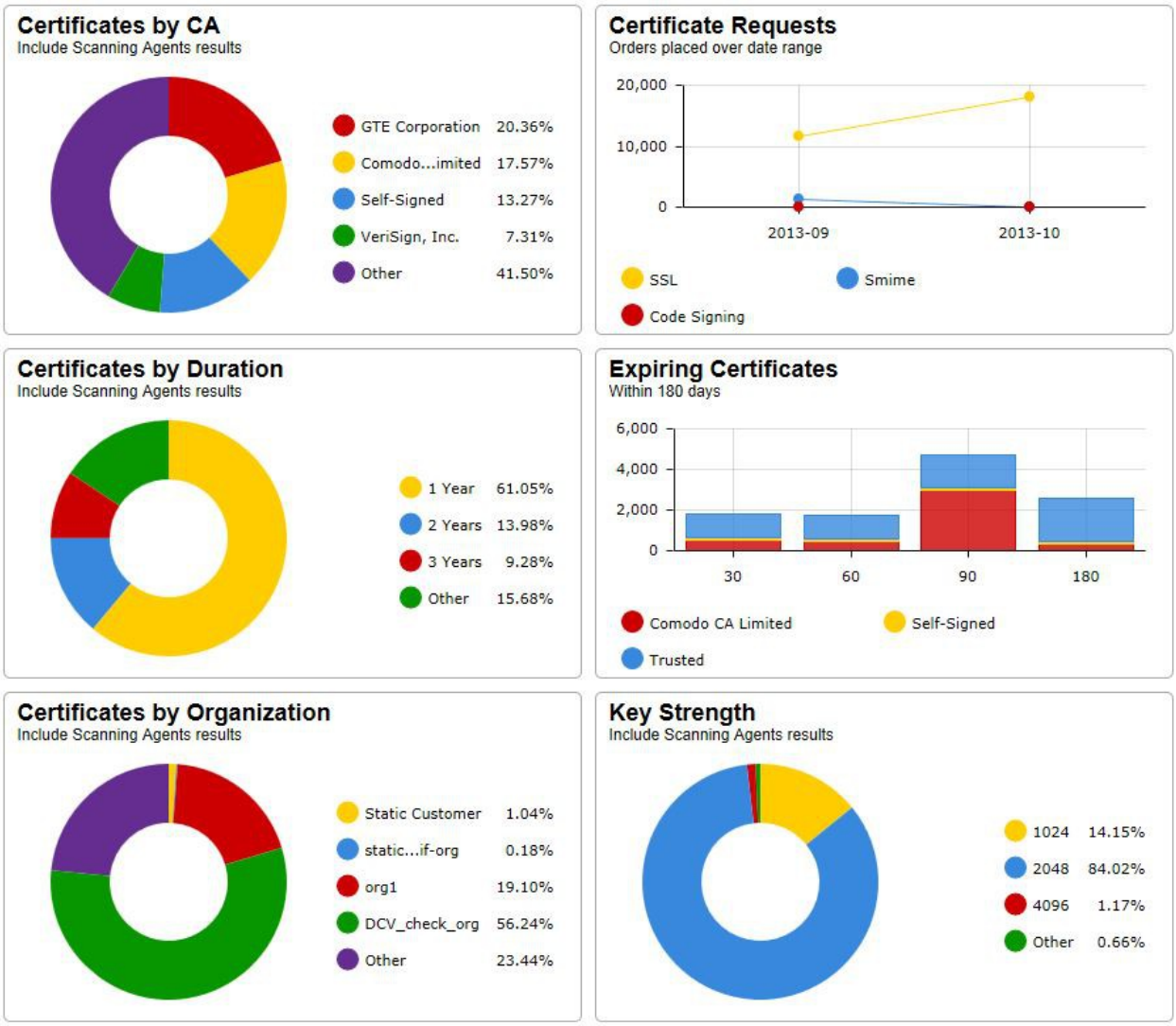
Comodo CA Limited,
3rd Floor, 26 Office Village, Exchange Quay,
Trafford Road, Salford,
Greater Manchester M5 3EQ,
United Kingdom.

Introducing the Certificate Dashboard

This document introduces the new graphical dashboard feature in Comodo **Certificate Manager** - a visually appealing heads-up-display which allows you to quickly gain an **overview of all SSL**, SMIME and code-signing certificates on your network.

The charts and graphs in the dashboard provide an essential combination of key life-cycle information (such as certificates approaching expiry, certificates issued/requested and DCV status) as well as important technical insights like how many servers have support for perfect forward secrecy, renegotiation and RC4 suites.

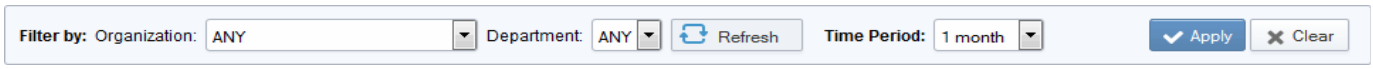
The dashboard will be displayed by default when an administrator first logs into the CCM interface and can be accessed at any time by clicking the 'Dashboard' tab at the top-left of the interface. Chart data is updated in real-time, so any modifications should be reflected in the dashboard near-instantly.



The area at the top of the dashboard displays a real-time summary of Active/Revoked certificates:

Active/Revoked Server Certificates	Active/Revoked Client Certificates	Active/Revoked Code Signing Certificates
9 / 2	**5 / 1**	**1 / 0**
+ 5 Since Last Month	+ 1 Since Last Month	+ 0 Since Last Month

The statistics displayed in the dashboard can be filtered based on the time period and by Organization/Department:

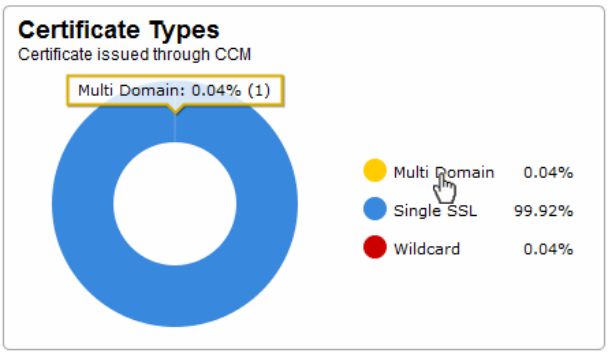


Charts available in first release. Click any link to view more details:

- **Certificates by Type** – Single Domain, Wildcard, Multi-Domain, UCC etc.
- **Certificates by Validation Level** – EV, DV, OV.
- **Certificates by Internal Type** – Certificates broken down by brand names like Instant SSL, Premium SSL etc.
- **Certificates by Issuer** – Comodo, VeriSign, GoDaddy, Thawte, self-signed etc.
- **Certificate Requests by Category of Certificate** – SSL requests, SMIME requests, Code signing requests
- **Certificate Requests versus Certificates Issued**
- **Certificates By Duration** – How many of your certificates are 1 year, 2 year, 3 year etc
- **Expiring Certificates by Issuer** – Comodo, self-signed and 'Other Trusted' certificates expiring within 180 days
- **DCV Status** – The current stage in the Domain Control Validation process held by your certificate-hosting domains
- **DCV Expiring Domains** – Domains for which Domain Control Validation will expire within 180 days
- **Certificates by Organization** - Certificates broken down by the Organizations they are issued to.
- **Certificates by Key Strength** - Certificates by the strength of key with which they were signed (1024 bit, 2048 bit etc)
- **Certificates by Public Key Algorithm** - Certificates broken down by encryption algorithm (RSA, DSA etc)
- **Certificates by Signing Algorithm** - Certificates by hashing and signing algorithms (e.g. SHA1withRSA)

Charts which are coming soon. Click any link to view more details:

- **EV Express Validation** – Organizations whose eligibility for accelerated EV validation will expire within 180 days.
- **Forward Secrecy** - The degree to which forward secrecy is supported on the web-servers hosting your certificates
- **Hosted by OS** - Details the server operating systems used to host your certificates (Windows, Linux etc)
- **RC4 Support -** The level of support for RC4 suites on the web-servers that host your certificates
- **Renegotiation Support** – The level of renegotiation support on the web-servers that host your certificates
- **Supported Protocols** – The types of encryption protocols supported by the web-servers that host your certificates
- **Certificates by port number** – The port numbers used for SSL traffic on the web-servers that host your certificates



Certificate Types

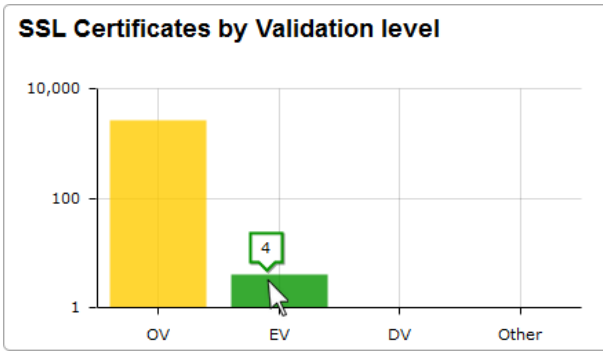
The 'Certificate Types' pie chart summarizes the different types of SSL certificates installed on servers in your network. (single domain, wildcard, multi-domain etc). This chart covers only 'managed' certificates issued through CCM.

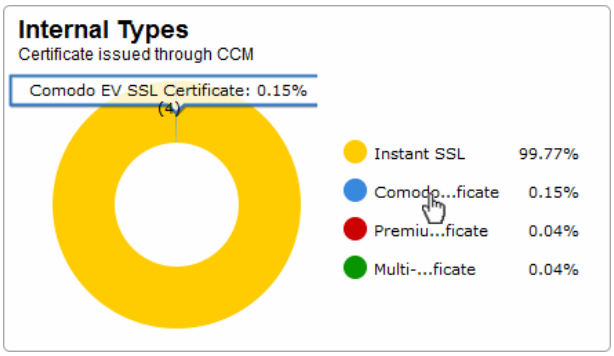
Hovering your mouse cursor over a legend item or section displays additional details such as the actual quantity of certificates of that type.

SSL Certificates by Validation level

Displays the composition of your certificate portfolio according to certificate validation level. This includes the number of Domain Validated, Organization Validated and Extended Validation certificates on your network.

Hovering the mouse cursor over a bar displays the exact number of certificates in that category.





Internal Types

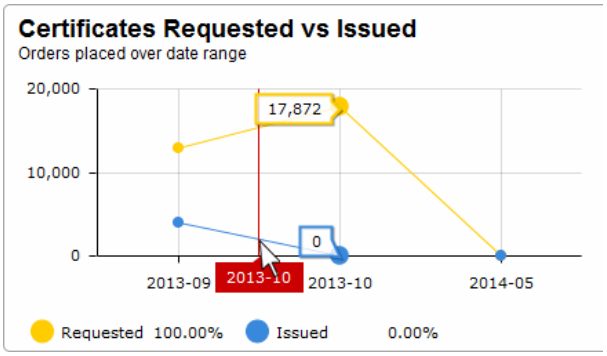
The 'Internal Types' chart details the quantities of SSL certificates issued by CCM according to certificate brand name.

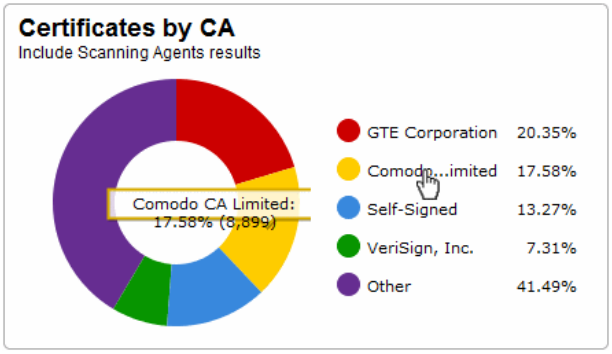
Hovering your mouse over a legend or sector displays additional details.

Certificates Requested Vs Issued

The 'Certificates Requested Vs Issued' graph allows you to view certificate issuance against certificate requests over time.

Placing the mouse cursor over the graph nodes displays more details about the number of certificates that were requested and issued on that date.





Certificates by CA

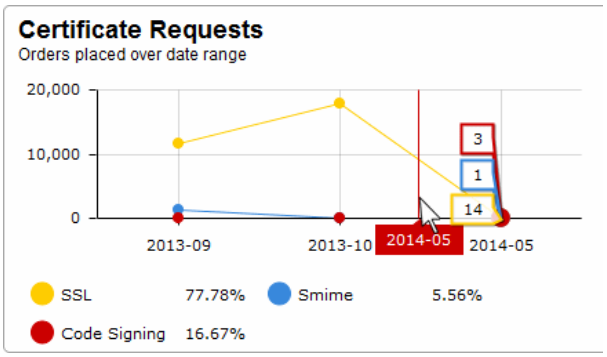
The 'Certificates by CA' chart allows you to determine what % of your certificates are publicly trusted by providing a break-down of certificates by signer. This includes all certificates signed by Certificate Authorities (CA) and those which are self-signed. It also highlights certificates from other CA's which you may want to replace with Comodo equivalents in order to benefit from CCM's management capabilities.

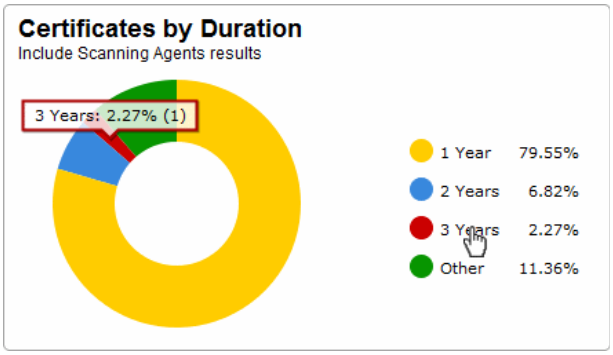
Placing your mouse cursor over a legend or sector displays the number of certificates by that signer and their % of the total certificates.

Certificate Requests

The 'Certificates Requests' graph displays the number of CCM orders placed over time for SSL, SMIME and Code Signing certificates.

Hovering the mouse cursor over the nodes on the graph displays the exact number of certificates that were requested.





Certificates by Duration

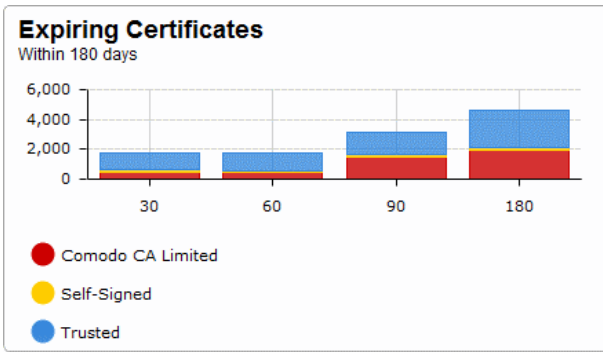
The 'Certificates by Duration' pie chart is a break-down of your certificates by term length.

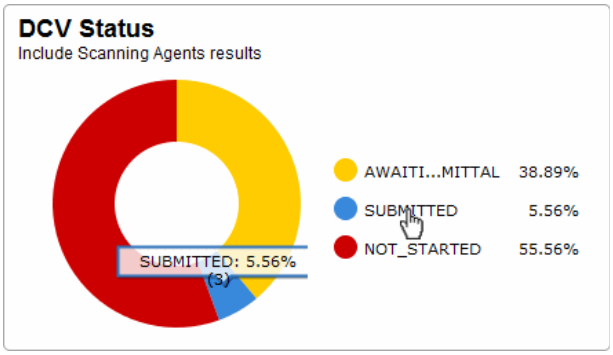
Hovering your mouse cursor over a legend or section displays the exact number of certificates with that term length and their percentage of the total.

Expiring Certificates

The 'Expiring Certificates' bar graph shows the number of certificates expiring within the next 30, 60, 90 and 180 days. Expiring certificates are further broken down according to signer. 'Trusted' certificates are those from other CAs which you may want to replace with Comodo certificates in order to benefit from CCM's management capabilities.

Hovering the mouse cursor over a legend or graph displays the number of certificates in each category.





DCV Status

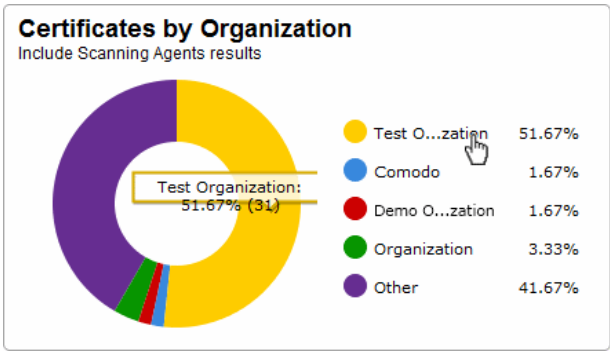
Summarizes the Domain Control Validation status of certificates on your network. DCV is required in order for Comodo to issue certificates to your domains and sub-domains. We advise customers to first pass DCV on their high level domain (e.g. domain.com). Once the HLD has passed DCV then future applications will be faster because all sub-domains, including wildcards, will be considered passed.

Hovering your mouse cursor over a legend or section displays the quantity of domains with a particular status and their percentage of the total domains.

DCV Expiring Domains

Indicates how many of your domains are within 30, 60, 90 and 180 days of DCV (domain control validation) expiry. DCV validity lasts for one year so It is possible DCV might be approaching expiry even though your certificate is not. If DCV is allowed to expire, it will not mean your certificate becomes invalid/stops functioning. However, your next application for that domain will need to pass DCV again.

Placing the mouse cursor over a legend or graph displays a tool-tip showing the number of domains within that time-frame.



Certificates by Organization

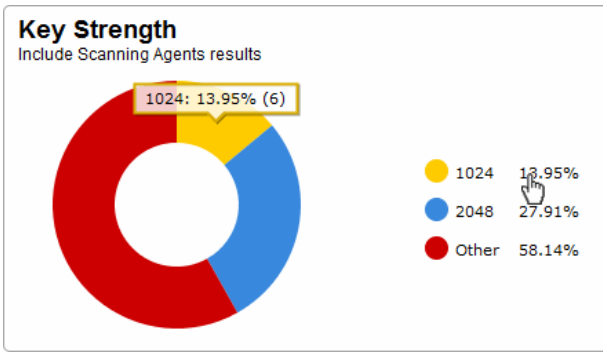
The 'Certificates by Organization' chart shows how many certificates have been issued to each Organization in your CCM account.

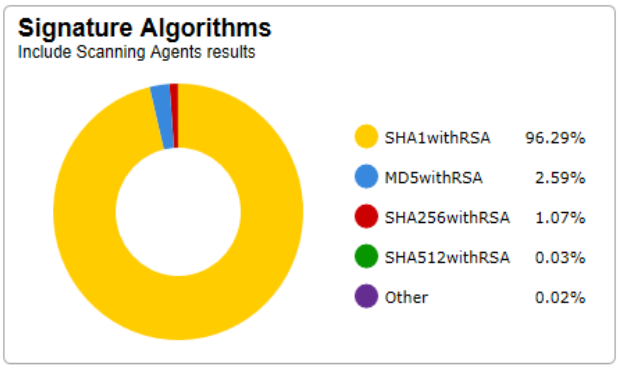
Hovering your mouse cursor over a legend or section displays the precise number and percentage of total certificates issued to to a particular Organization.

Key Strength

The 'Key Strength' chart shows the composition of your certificate portfolio based on the size of their signature. This can be useful for identifying certificates which need to replaced in order to be compliant with National Institute of Standards (NIST) recommendations. NIST has stated that all certificates issued after 1st January 2014 should be of at least 2048 bit key length

Placing your mouse cursor over a legend or sector displays the exact number of certificates with a particular signature size and their percentage of the total certificates.





Signature Algorithms

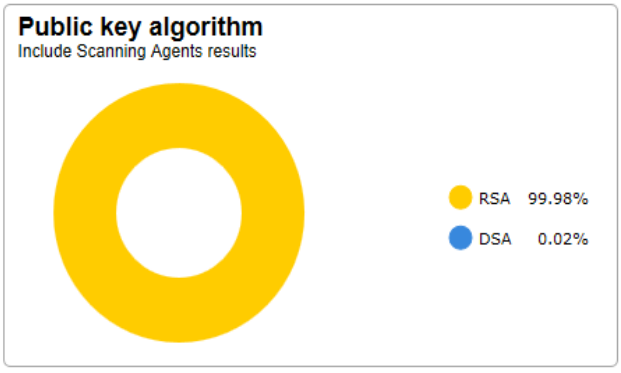
Provides an overview of the algorithms used by your certificates to hash and sign data. This chart can be useful for identifying certificates using weaker algorithms which may need to be replaced before their expiry dates. Comodo recommends SHA-256 and upwards. MD5 has been proven insecure and Microsoft has stated its products will stop trusting SHA-1 code-signing and SSL certificates in 2016 and 2017 respectively.

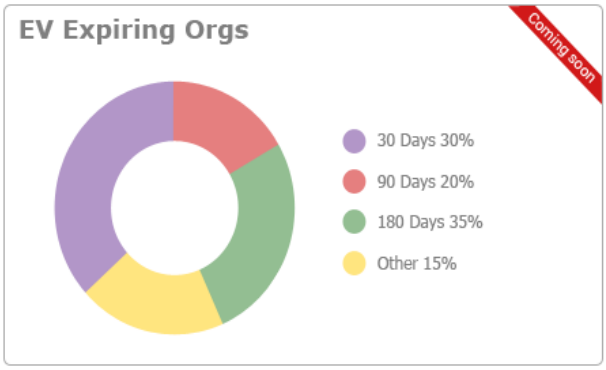
For more details, see **http://www.comodo.com/e-commerce/SHA-2-transition.php**

Public Key Algorithm

This chart provides an overview of the algorithms used to encrypt data by certificates on your network. Example algorithms include RSA, DSA and ECC.

Placing your mouse cursor over a legend or sector displays the exact number of certificates using a particular signature algorithm and their percentage of the total certificates.



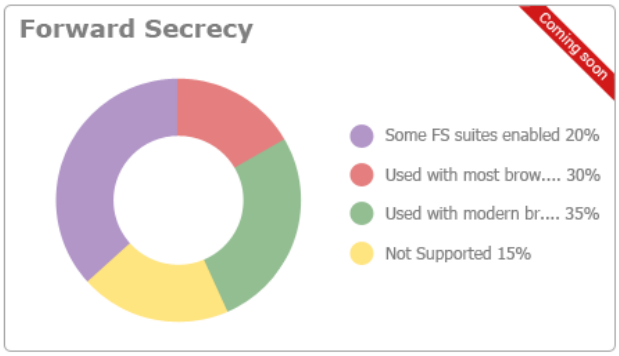


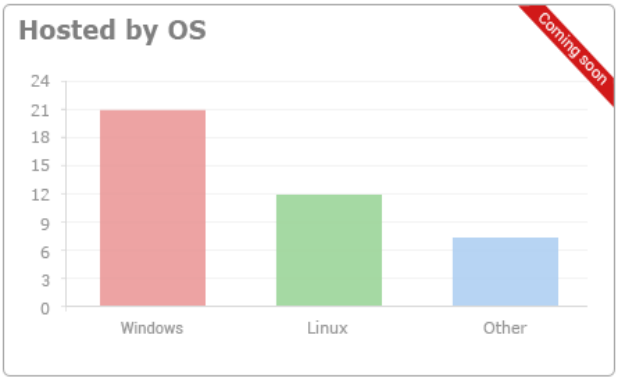
EV Express Validation – coming soon

Displays the percentage of Organizations for which accelerated validation of one or more EV certificates will expire within 30, 90 and 180 days. Once an EV certificate has been validated for the high level domain (e.g. domain.com) it qualifies for EV Express and subsequent EV applications for that domain and it's sub-domains will be issued much more quickly (assuming address and contact details are not changed). EV Express status lasts for 13 months before it must be renewed by re-validating the details of the certificate on the high level domain.

Forward Secrecy Enabled – coming soon

Displays the percentage of certificates which are hosted on web-servers which have perfect forward secrecy fully or partially enabled. Forward secrecy prevents encrypted data from previous sessions from being decrypted in the event that the private key of the certificate is compromised.



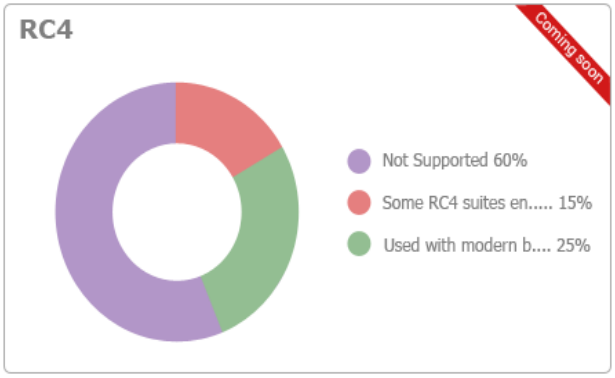


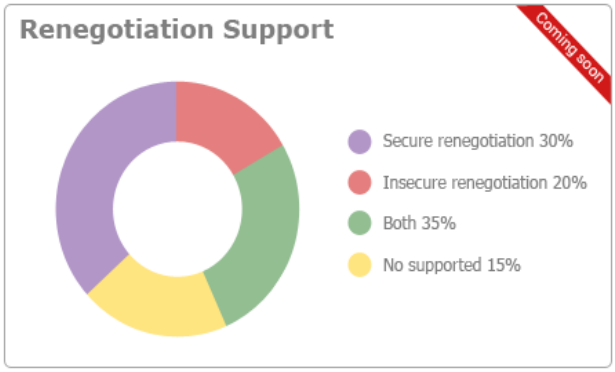
Hosted by OS – coming soon

Provides a visual break-down of the server operating systems used to host your certificates.

RC4 Support – coming soon

Indicates the degree to which the RC4 streaming cipher is supported by servers hosting your certificates. If your environment can operate without RC4, it is best practice to disable it.





Renegotiation Support – coming soon

Renegotiation is a feature that makes it possible to adjust the parameters of an SSL connection without disrupting the user experience by requiring an entirely new session. Take, for example, the case of an anonymous user browsing an e-commerce website who adds some products to the shopping cart then decides to login and purchase. Renegotiation allows the data from the 'anonymous' session to be transposed in a fluid and secure fashion. Unfortunately, security flaws were discovered in renegotiation in TLS 1 / SSL 3 which required a patch to fix. Unpatched web servers are shown here as 'Insecure renegotiation'.

Supported Protocols – coming soon

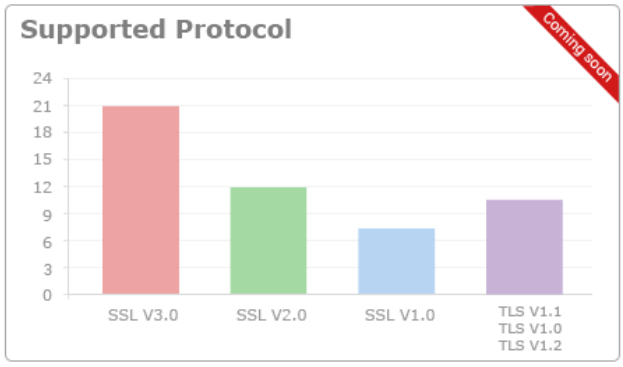
Shows the support for various cryptographic protocols on the web servers which are used to host your certificates. While we recommend each customer to investigate the precise impact of disabling a given protocol by analyzing the browsers used by their visitors, Comodo would recommend the following:

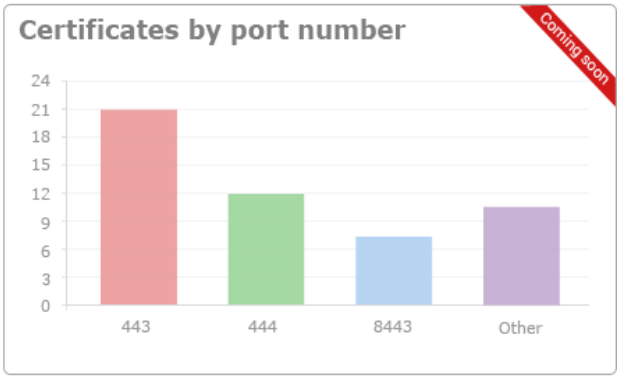
TLS 1.0, 1.1, 1.2 – Enable

SSL 3.0 – Discretionary. Disable preferred *

SSL 1.0. 2.0 – Disable

* SSL 3.0 is needed mainly for Windows XP / Internet Explorer 6.0 users. Microsoft have discontinued support for these systems and their use by the public has waned significantly. However, CCM customers *may* want to retain support in the short-medium term if widely supported by their user base.





Certificates by port number – coming soon

Shows the port numbers that are used for secure connections on web-servers that host your certificates.

About Comodo CA

Comodo Certificate Authority is one of the world's largest providers of SSL certificates by volume having issued over 91 million certificates and serving over 200,000 customers across 150 countries. The company provides a full suite of certificate products spanning all validation levels for website certificates, certificates for code-signing and email-signing, and the Comodo Certificate Manager (CCM) platform. Comodo CA has its US headquarters in New Jersey and international offices in the United Kingdom, Ukraine and India.

Comodo CA Limited

3rd floor, Office Village Exchange Quay

Trafford Road, Manchester, M5 3EQ

United Kingdom

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767