



# Enterprise Public Key Infrastructure (EPKI) Manager

Version 3.5

For issuance & management of Enterprise - wide SSL Certificates &  
Secure Email (S/MIME) Certificates

**COMODO**  
Creating Trust Online®

## Introduction:

Comodo's EPKI Manager is a web-based certificate management application that allows your nominated administrator(s) to manage all your company's SSL and email certificates from a single, centralized console.

The EPKI Manager allows you to issue bulk numbers of:

- SSL Certificates for use on domain names owned by your company
- Secure Email Certificates (S/MIME) for use by employees of your company

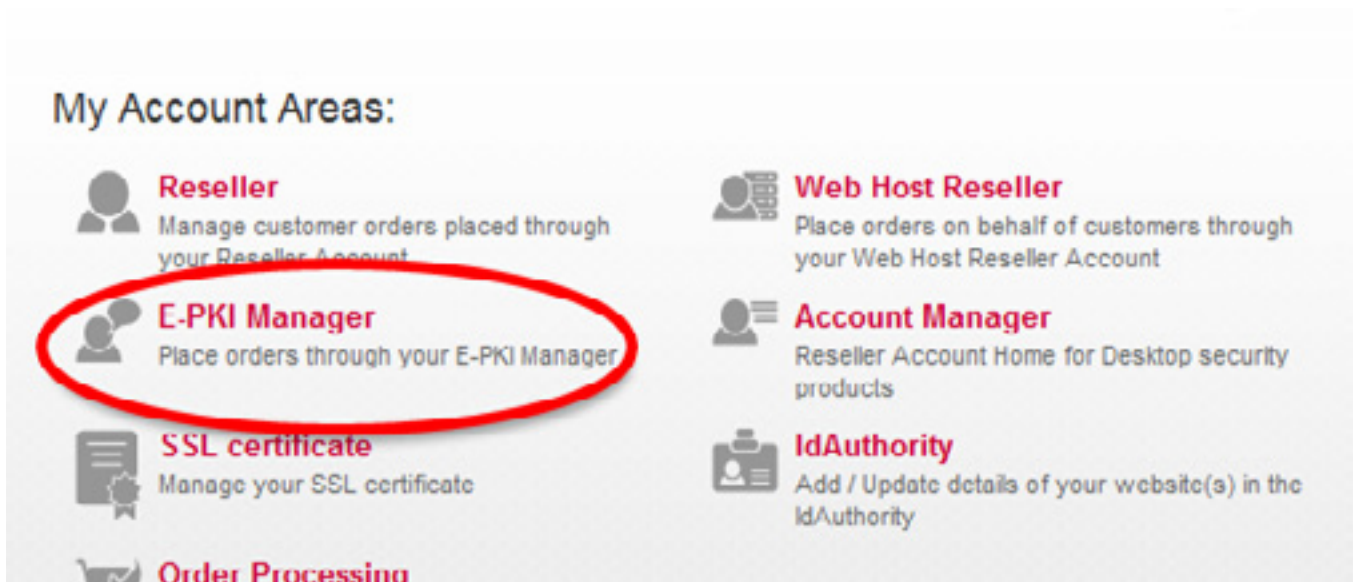
Additional certificates may be purchased through the console in minutes - ensuring new servers and employee email may be secured in minutes rather than days. You may use the 'User Management' facility to create new users for your EPKI account and specify permissions for users on a granular basis, including certificate issuance, revocation and reporting permissions.

## Logging into EPKI Manager

Please find your login details in the email sent by your Comodo account manager. Should you need reminding of your login details please contact [support@comodo.com](mailto:support@comodo.com). To login to your Comodo account, visit <https://www.comodo.com/login/comodo-members.php> and enter your username and password at the 'Comodo Certificate Authority' area.

## Using EPKI Manager

Once logged in, click the 'E-PKI Manager' link from the 'My Account Account Areas'.



You will be presented with the EPKI hub page. From here you can purchase SSL and email certificates, manage EPKI users, deposit additional funds and run reports on your orders:

The screenshot shows the Comodo E-PKI Manager interface in a Microsoft Internet Explorer browser window. The page title is 'E-PKI Manager' and it includes a 'Welcome!' message. The main content area is divided into several sections:

- Account Actions:** 'Your Current Credit is: \$44.24', 'Deposit additional funds', and 'View your account Buy Prices'.
- Using your E-PKI Manager:** 'E-PKI Manager pages'.
- Customer Order Options:** A list of certificate types including InstantSSL, PremiumSSL, and PlatformSSL certificates, along with a 'Corporate Secure Email Certificate'.
- Management Facilities:** 'User Management'.
- Reporting Facilities:** 'Run report on your Orders'.

Red annotations on the left side of the screenshot point to these sections with the following text:

- 'Account actions: Deposit funds & view buy prices' points to the Account Actions section.
- 'Get Support' points to the 'E-PKI Manager pages' link.
- 'Placing a customer order: Available products' points to the 'Customer Order Options' section.
- 'Manage EPKI Manager Users and their permissions' points to the 'User Management' link.
- 'Run reports on orders placed' points to the 'Run report on your Orders' link.

Other elements on the page include a 'Can We Help?' contact box at the top right, a 'Please do not use your browser's BACK and FORWARD buttons' warning, and a 'Latest News' section on the right side.

## Applying for a Certificate

You can use your EPKI Manager to apply for SSL and S/MIME Certificates for your organization.

To apply for an SSL Certificate, first select the type of SSL Certificate you want from the list under 'Customer Order Options'. This will open the first stage of the application process, 'Provide Your CSR':

**COMODO**  
Enterprise SSL

Can We Help ?  
Tel: + 1-888-256-2608  
Tel: + 1-703-637-9361  
enterprisesolutions@comodo.com

Please do not use your browser's BACK and FORWARD buttons

**EliteSSL Certificate**

Welcome:

Step 1: Provide a CSR

You must generate a Certificate Signing Request (CSR) on your webserver. [Click here](#) for help generating your CSR.

**NOTE:** Please ensure that the Common Name (CN) in your CSR is ONE of the following:

- your Fully Qualified Domain Name (e.g. "secure.yourdomain.com")
- your Public IP address (e.g. "202.144.8.10")
- the Full Server Name of your internal server (e.g. "techserver")
- your Private IP address (e.g. "192.168.0.1")

After you have generated a CSR using your server software **copy and paste** the CSR text using an **ASCII text editor** into the CSR box below: Your CSR should look something like this:

```
-----BEGIN CERTIFICATE REQUEST-----  
MEUDDCCANCAQAwfTEWMBIGGA1UEAxMNSGVzZC50Z3N0LmVudGV0eSMBAGATUECMMJ  
TWYya2V0dW5wMREwDwYDVGQKEThwZ3N0eS5yZzEzMBAGATUEEwMUV0Vz3CDBAQRS  
(more encoded data)-----  
Rq=8Lr5X3i0dzyf1pLqPIMckSve1eCzSR8CekGSRno7ow4TVyxAF6J6ozDaw7e  
GwQ2w40VLT04GvK2X0H5SRFQBWYTOcTRPnkG8BwV  
-----END CERTIFICATE REQUEST-----
```

1. Copy and paste your CSR into this box:

2. Select the server software used to generate the CSR: Select from list

3. Select the validity period for your Certificate:

- 1 year
- 2 years
- 3 years
- 4 years
- 5 years

Note: You will be licensed to use this Certificate on an unlimited number of servers.

4. Free Upgrade to EV?

Total Cost: **\$331.12**

Please note: Data on this company will be retrieved from IdAuthority where available to assist you with the signup.

Paste your CSR in this field.  
If you need help with this, click the highlighted link to see a list of support documentation

Select the type of server used to generate your CSR (e.g. Apache, IIS, nginx etc)

Select certificate term. Discounts are available for multi-year terms

Certificate cost as per your current buy prices. Payment will be debited from your available funds.

### To apply for a certificate

- Generate a CSR for your domain using your web-server software. Help documents are available at [https://support.comodo.com/index.php?\\_m=knowledgebase&\\_a=view&parentcategoryid=33&pcid=1&nav=0,96,1](https://support.comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=33&pcid=1&nav=0,96,1)
- Copy and paste the CSR into the space provided
- Select the type of SSL certificate you want

- Select from server software you used to create the CSR
- Select the validity period. This will range from between 1 – 5 years depending on certificate type

The product type and validity period will affect the price charged for the certificate. Please refer to your pricing band for your actual buy prices as set by your account manager.

### Applying for a Corporate Secure E-Mail Certificate (S/MIME)

As the EPKI administrator, you will apply for a Secure Email Certificate on behalf your employee then your employee will collect and install it on their machines. In brief, the process is as follows:

- Administrator completes the application form providing employee name, email address and selects relevant security policies.
- Comodo email the employee with a link to begin the certificate enrollment process. The enrollment must take place on the same PC on which the certificate will be used.
- After enrollment, Comodo issue the certificate and it will be automatically installed onto the employees PC
- The employee is redirected to the support pages for configuration and usage instructions

The screenshot shows the Comodo Corporate Secure Email Certificate application form. The browser title is "Comodo Security Services - Microsoft Internet Explorer". The page header includes the Comodo logo, contact information (Tel: +1 888 246 6361, Tel: +44 (0) 151 874 7170, Email: sales@comodogroup.com), and a "Can We Help?" section. A warning message states: "Please do not use your browser's BACK and FORWARD buttons".

The main content area is titled "Corporate Secure Email Certificate" and includes a "Welcome:" message. The user's current credit is shown as \$44.24. The "User Details" section contains the following fields:

- 1. Email Address: A dropdown menu with a warning message: "You may only apply for Corporate Secure Email Certificates containing domain names for which your right of use has been validated. If your required domain name does not appear in the above list, you may submit it for validation by clicking [here](#) to register an iSAuthority Website."
- 2. First Name: A text input field.
- 2. Last Name: A text input field.

Below the name fields is a checkbox with the text: "I confirm that the above individual is an employee / authorized representative of \_\_\_\_\_ and is permitted to use the above email address for email communication."

The "Advanced Security Options" section includes:

- 4. Cryptographic Service Provider: A dropdown menu set to "Microsoft Base Cryptographic Provider v1.2".
- 5. Is Private Key User-Protected?: A checkbox (unchecked).
- 6. Is Private Key Exportable?: A checkbox (checked).

The "Certificate validity period" section includes:

- 7. Select the validity period for your Certificate: A dropdown menu with options "1 year", "2 years", and "3 years".

The total cost is displayed as \$4.50. At the bottom of the form are "Cancel" and "Submit" buttons. The footer contains copyright information (©Copyright 2006. All rights reserved.), a "Using S/MIME (S/MIME)" section with a "Learn More" link, and the date "Thursday, November 24, 2005".



## Email certificate application – more details

First, click 'Corporate Secure Email Certificate' from 'Customer Order Options':

### Corporate Secure Email Certificate

#### Step 1: Set up a Validated Domain Name (if you haven't done so already)

Corporate Secure Email Certificates may only be applied for on domain names which have been registered with Comodo. If the domain drop down in stage 1 of 'User details' does not contain the domain you want to use, it is likely you need to register your domain with us. This is a one time process. Once your domain is registered, you can apply for as many email certificates for that domain as required.

To do this:

1. Click the link in the application form to open to the domain registration screen
2. Type your domain in 'Location of Website' field
3. Click the 'Register Website' button
4. Comodo will validate your ownership of the domain. This may take up to 2 working days.
5. After validation is complete, the domain will become available in the domain drop-down in 'User Details'

**User Details**

1. Email Address  ▼

*Example: username@*

You may only apply for Corporate Secure Email Certificates containing domain names for which your right of use has been validated. If your required domain name does not appear in the above list, you may submit it for validation by clicking [here](#) to register an IdAuthority Website.

**Register another Website**

Location of Website

**Register Website**

Examples:  
yourdomain.com or \*.yourdomain.com/ - use this format if your website spans the entire 'yourdomain.com' domain.  
www.yourhost.com/yourcompany/ - use this format if your website is hosted under your webhost's name, and your company name is a subdirectory.

| Website             | Homepage URL                    | Date Registered | Credentials                         | Primary Site                                  | Status              |
|---------------------|---------------------------------|-----------------|-------------------------------------|---|---------------------|
| anothertestsite.com | http://www.anothertestsite.com/ | 04-SEP-12       | <input type="button" value="Edit"/> | <input type="button" value="Set as Primary"/> | Awaiting Validation |
| anothertestsite.com | http://www.anothertestsite.com/ | 04-SEP-12       | <input type="button" value="Edit"/> | <input type="button" value="Primary Site"/>   | Valid               |

## Step 2: Entering Employee Details to be included in the Certificate

Once validated, your domain name can be selected in the 'Email Address' drop down. Complete the employee's full email address and first/last name then confirm the individual is an employee or authorized representative of your company.

### User Details

|                                     |  |
|-------------------------------------|--|
| 1. Email Address                    | joe.bloggs@ anothertestsite.com  |
| Example: username@                  | You may only apply for Corporate Secure Email Certificates containing domain names for which your right of use has been validated.<br>If your required domain name does not appear in the above list, you may submit it for Company by clicking <a href="#">here</a> to register an IdAuthority Website. |
| 2. First Name                       | Joe  |
| 3. Last Name                        | Bloggs   |
| <input checked="" type="checkbox"/> | I confirm that the above individual is an employee / authorized representative of testtestest and is permitted to use the above email address for email communication.   |

## Step 3: Selecting Security Options for the employee's Certificate

You will be asked to specify the security options for the employee's certificate.

### Advanced Security Options

(Only applicable if the User will obtain their Certificate using Internet Explorer)

|                                     |  |
|-------------------------------------|--|
| 4. Cryptographic Service Provider   | Microsoft Enhanced Cryptographic Provider v1.0 |
| 5. Is Private Key 'User-Protected'? | <input type="checkbox"/>                       |
| 6. Is Private Key 'Exportable'?     | <input checked="" type="checkbox"/>            |

#### Cryptographic Service Provide (CSP):

The CSP is the software responsible for generating the cryptographic keys on your employees machine. Select from the drop down list which CSP is to be used when the employee enrolls for their Corporate Secure Email Certificate. If the Certificate is to be generated on a placed on a smart card or other security device, ensure you select the relevant CSP from the list.

Please note that the CSP you select MUST be present on the employee's PC. For Window's machines, the default 'Microsoft Enhanced Cryptographic Provider' will be OK.

#### Private Key User Protected:

Place a tick in this check box to place additional protection on the use of the private key (signing key) associated with the employee's Certificate. Additional protection will challenge to the employee to OK the use of the Certificate every time the private key is used.

#### Private Key Exportable:

Leave the check-mark in this box if the private key associated with the employee's certificate should be exportable. For example, if you wish to be able to back up the certificate or if the user needs to be able to install this certificate on more than one machine, then you need to make sure it is exportable. If you do not allow exportability and the certificate is lost, all emails encrypted for the employee will no longer be accessible.

#### Step 4: Select Validity Period



Submit the form and the issuance process will begin.

#### Step 5: Required Employee Actions

And email will be sent to the employee containing a link to the certificate collection page. This page will automatically generate a Corporate Secure Email Certificate request and submit this request to Comodo Certification Authority. It is important that the employee keep the browser window open at this point. The certificate, when issued, will be automatically be installed. The browser will then automatically redirect to the support pages to assist the employee in configuration and usage.

For support on configuration and installation please view:

[http://www.comodo.com/support/products/email\\_certs/index.php](http://www.comodo.com/support/products/email_certs/index.php)

#### Paying for Certificates

Your account will be debited with the value of the certificate product type and validity period selected upon application of the certificate. Providing that the certificate application contains no invalid or conflicting data, the certificate will usually be issued within 1 hour.

### IMPORTANT - Your Responsibilities when using the EPKI Manager

In order to make the Certificate issuance process as fast and seamless as possible, the organization has a number of responsibilities. It is your responsibility to ensure the following:

- You have the right to use the domain name contained in the SSL application. You must only make applications for domain names you own.
- The named individual in the Corporate Secure Email Certificate application is a bona-fide employee / representative of your company.

Making an illegitimate certificate application could affect the warranty provided by Comodo and your EPKI Manager Account and is a breach of the EPKI Manager Subscriber Agreement.

### Managing Users

Your EPKI Manager Administrator (Super User) has the ability to conduct all EPKI Manager functions (purchase products, deposit funds, run reports on all transactions) and may add additional users on a discretionary basis. Adding a user prompts the Super User to complete the new user details. By default, the new user will inherit the Super User's company address unless a different address is required.

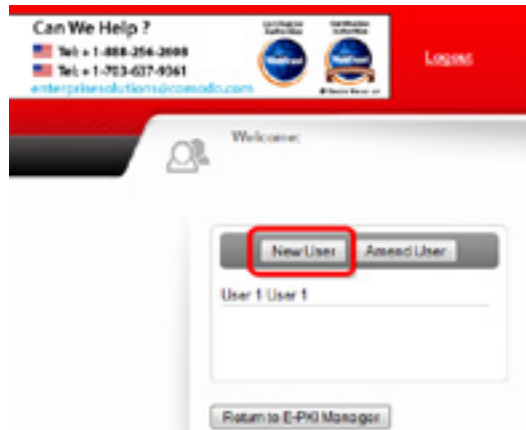


## To Add a New User

Click 'User Management' on the main EPKI menu screen...

### Management Facilities: [User Management](#)

...then click 'New User' in the management area:

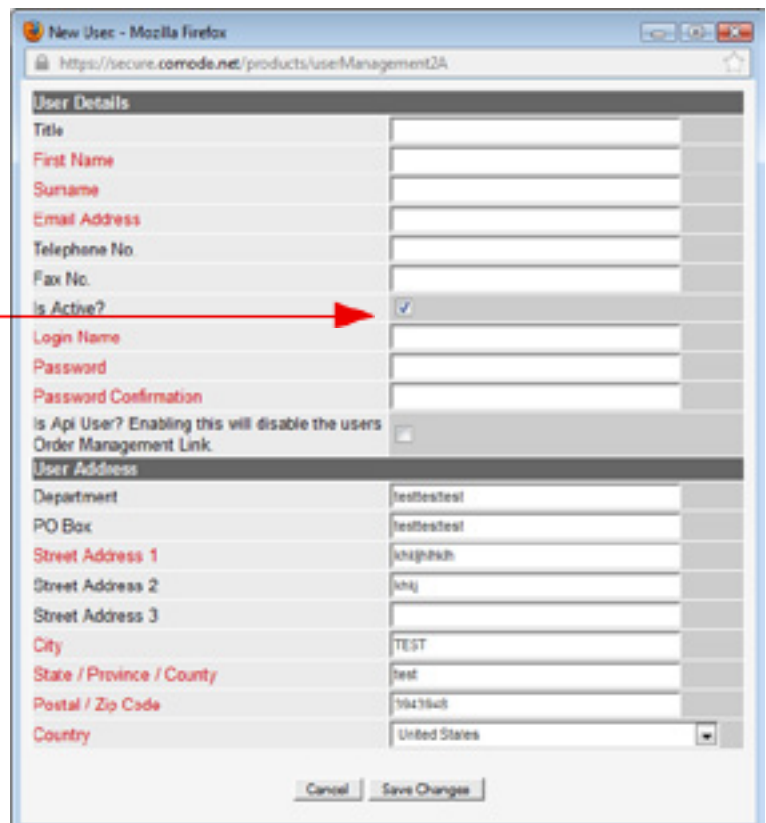


Fields with red text are mandatory. The user cannot be created until these are complete.

Uncheck the 'Is Active?' box to disable the login for this user

Click 'Save Changes' to create the new user

**Amend User:** Once a user has been added, they will be displayed in the user list. Select the user from the user list and click 'Amend User' to change user details.



| User Details   |                                     |
|--|-------------------------------------|
| Title  |                                     |
| First Name   |                                     |
| Surname  |                                     |
| Email Address  |                                     |
| Telephone No.  |                                     |
| Fax No.  |                                     |
| Is Active?   | <input checked="" type="checkbox"/> |
| Login Name   |                                     |
| Password   |                                     |
| Password Confirmation  |                                     |
| Is Api User? Enabling this will disable the users Order Management Link. | <input type="checkbox"/>            |

| User Address              |               |
|---------------------------|---------------|
| Department                | testtest      |
| PO Box                    | testtest      |
| Street Address 1          | shighsh       |
| Street Address 2          | shj           |
| Street Address 3          |               |
| City                      | TEST          |
| State / Province / County | test          |
| Postal / Zip Code         | 10478-0       |
| Country                   | United States |

Cancel Save Changes

## Managing User's Permissions

Clicking on the user's name from list of users will display the that user's permissions.

**E-PKI Manager User Permissions for User 2 User 2**

Click the corresponding permission box to toggle between allowed (tick) and deny (blank box). Remember to Save any changes you make.

|                                    | Purchase                 | Revoke                              | View Others                         |
|------------------------------------|--------------------------|-------------------------------------|-------------------------------------|
| SSL Certificate                    | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Corporate Secure Email Certificate | <input type="checkbox"/> | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| Deposit Funds                      | <input type="checkbox"/> |                                     | <input checked="" type="checkbox"/> |

Buttons: New User, Amend User, Return to E-PKI Manager

### Purchase:

Place a tick in the 'Purchase' column next to each product type (SSL Certificates, Corporate Secure Email Certificates, Deposit Funds) that you wish the user to be able to buy.

### Revoke:

Placing a tick in the Revoke column determines whether the user may revoke SSL certificates or email certificates.

Note that a revocation of deposited funds is not available.

### View Others:

By default, the user may only run reports on the product type he/she has purchased. Placing a tick in the 'View Others' column for each product type (SSL Certificates, Corporate Secure Email Certificates, Deposit Funds) allows the user to run reports on all product types made by all Users.

## Refunds:

Please contact Comodo directly should you require a refund on a certificate.

## Your Buy Prices

Click the "View your Current Buy Prices" to display a summary table containing your current buy prices as set by your account manager.

## Depositing Additional Funds:

Your EPKI account operates on a prepayment system. You may top up your account at any time with additional funds by selecting "Deposit Additional Funds". Unless you have sufficient funds in your account you will not be able to authorize Orders.

## Getting Help:

Should you have any questions regarding your account, please do not hesitate to contact our support department, we will be happy to assist you in any matter.

# 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.comodo.com](http://www.comodo.com)

#### **Comodo Group Inc.**

1255 Broad Street  
Clifton, NJ 07013  
United States

#### **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

Tel : +1.888.266.6361

Email : [sales@comodo.com](mailto:sales@comodo.com)