IdenTrust
part of HID Global

How to Renew a Digital Certificate

You must periodically renew your digital certificate. A renewal notification will be sent to your email address starting ninety (90) days before your certificate expires and periodically thereafter until you renew.

In this document, IdenTrust will provide answers to frequently asked questions about how to renew a digital certificate.

To begin, identify the type of certificate that you have and note these guidelines regarding certificate renewal:

- **GSA ACES** certificates expire two (2) years from the date of issuance. These certificates cannot be renewed after they expire. If your certificate has expired, you will need to apply for a new certificate.
- **DoD ECA** and **IdenTrust Global Common (IGC)** certificates expire one (1), two (2) or three (3) years from the date of issuance. These certificates cannot be renewed after they expire. If your certificate has expired, you will need to apply for a new certificate.
- **IdenTrust TrustID®** certificates expire one (1) year from the date of issuance (retrieval). These certificates may be renewed up to thirty (30) days after their expiration date(s).
- If you have a TLS/SSL certificate, please follow the instructions shown below for renewing this certificate type.
- For all other certificates, if your certificate has not expired and it is within ninety (90) days of expiration, simply login to your account in the **IdenTrust Certificate Management Center (CMC)** with your current digital certificate.

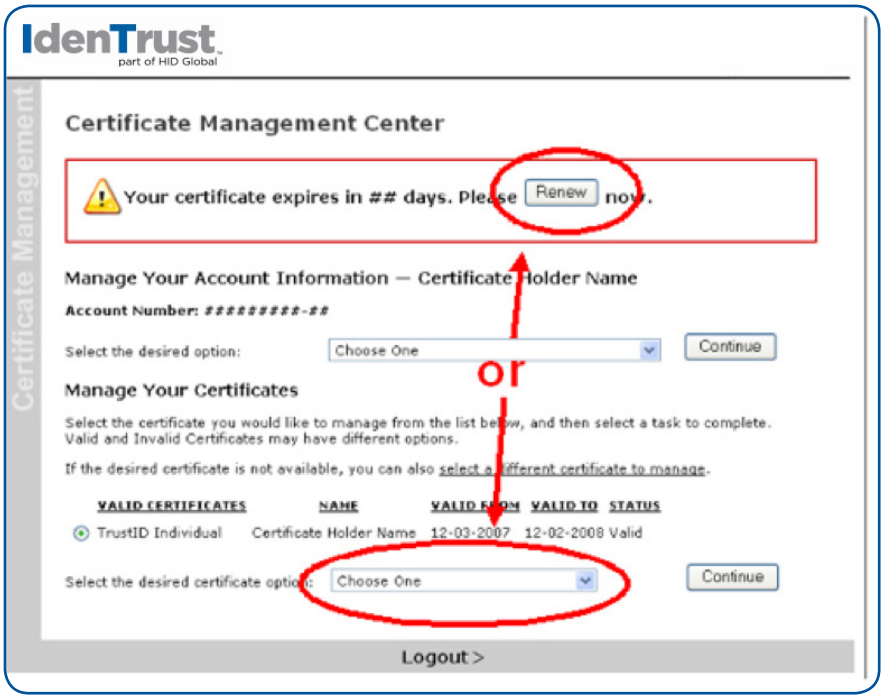
You can check your certificate expiration date(s) by going to **Manage My Certificate > Certificate Management Center (CMC) > Access My Account**. After logging in to your account with your digital certificate, your certificate(s) will be listed there, along with their status and expiration ("valid through") date(s). You will also receive email notifications 90, 60, 30 15, 7 and 1 day(s) before your certificate expires.

The renewal process usually takes three (3) to five (5) business days. Once we receive your renewal request, our Registration team reviews and approves the account. Once approved, a letter with instructions on how to retrieve the renewed certificate will be sent to you by U.S. mail.

To renew your digital certificate, please follow these instructions:

1. Go to **Manage My Certificate > Certificate Management Center (CMC) > Access My Account** and log in to your account with your digital certificate.

2. Select **"I would like to renew my account"** from the pull-down menu.
3. Follow the on-screen instructions.



If your digital certificate has expired:

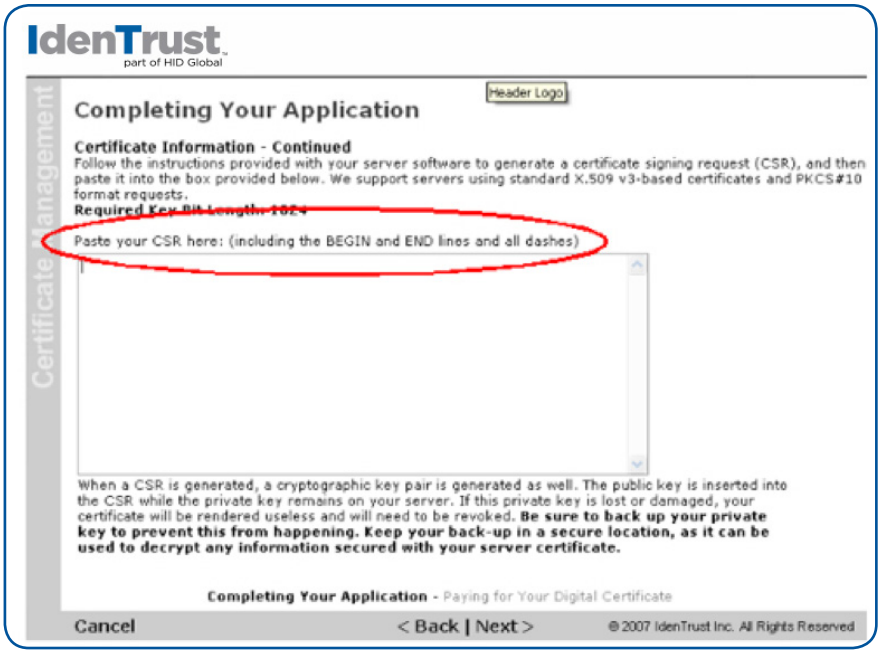
1. Go to **Manage My Certificate > Certificate Management Center (CMC) > Access My Account** and login with your account number and IdenTrust passphrase. To do this, when you are asked to authenticate with your certificate, click **"Cancel"**.
2. When prompted, enter the **"Account Number"** that was sent to you in a letter when your account was originally approved. Then, enter your IdenTrust **"Passphrase"**; this is the password you chose online when you applied for the certificate.
3. Under the heading **"Valid Certificates"** there should only be one (1) option. Choose **"All my certificates are expired, and I want to request a renewal"**. Then click **"Continue"** and follow the on-screen instructions.

To renew a TLS/SSL server certificate, please follow these instructions:

A server certificate is renewed like any other certificate, with the following changes:

1. Before starting the renewal process, you will need to create a Certificate Signing Request (CSR).
2. Go to **Manage My Certificate > Certificate Management Center (CMC) > Access My Account** . You will login using your account number and passphrase (instead of using a certificate).
3. Once you have created a Certificate Signing Request (CSR) and are logged on to the CMC, select **"I would like to renew my certificate"** from the pull-down menu. Verify your information and make any necessary changes.

4. You will then be asked to provide a CSR; copy and paste it into the provided field.
5. Follow the remaining on-screen directions to complete the renewal process.



Other helpful tips associated with the renewal process are as follows:

- If you are having **trouble logging into the Certificate Management Center (CMC)**:
  - Please make sure your browser is not blocking pop-ups for this site.
  - If you have forgotten your passphrase, you will need to reset your passphrase. You should then be able to access the Certificate Management Center and complete your certificate renewal.
- If you are trying to renew your certificate and get a message that says **"I need to login to the Certificate Management Center with my certificate"**, you must be renewing your certificate before it expires and you must be on the computer that currently holds your certificate. When you login to the Certificate Management Center, a box will appear with your name in it. You must highlight your name and click **"OK"**. If your name is not in the box, it means that your certificate is not on the computer you are using.
  - If your certificate is on another computer, please renew it from that computer.
  - If your certificate is no longer on any computer, you will need to **replace your certificate** first and then renew it.
- **If personal information that goes into the certificate has changed** (or will change soon), you should update that information while renewing. In most cases, the personal information in a certificate is your name and email address.
  - Please note that the only time you can change the information embedded in a certificate is during renewal. If this information changes at any other time, you must apply for a new certificate that reflects the changes.

- If you renew your certificate and the receive any email saying that you need to **send in notarized forms**, the following is applicable:
  - For GSA ACES and TrustID certificates, if your name, your company name, the company headquarters address or your email address has changed, you will need to resubmit the notarized forms. Otherwise the original forms you submitted are good for six (6) years.
- During the renewal process, **you will be asked if you want to change your IdenTrust passphrase**. Remember that this is not the same as the password you use when using your certificate (although you may have chosen the same code for both the passphrase and password).
  - Unless you are confident that you will remember a new passphrase, you should not change it.
  - Changing this passphrase will not change the password for using your certificate.

For more information on passphrases and passwords, see the IdenTrust FAQ about passphrases and passwords.

2018-01-04-identrust-renew-digi-cert-en