CertCentral® Public SSL/TLS Certificate CT Logging Guide

Version 1.3

Table of Contents

1 Logging Public SSL/TLS Certificates to Public CT Logs

As of February 1, 2018, DigiCert logs all newly issued public SSL/TLS certificates to public Certificate Transparency (CT) logs by default. This does not affect any OV certificates issued before February 1, 2018. Note that CT logging has been required for EV SSL Certificates since 2015.

DigiCert advocates CT logging because:

- It improves security across the web by providing early detection of misissued certificates.
- It checks the integrity of Certificate Authority (CA) practices.
- Most importantly, it provides you with a way to monitor all certificates issued for their domains, adding another layer of protection for your domains and customers.

References:

- DigiCert First CA Compatible with Google CT
- Google CT to Expand to All Public SSL/TLS Certificates
- Feb 1, DigiCert Logs All Public SSL/TLS Certificates to Public CT Logs

1.1 Will DigiCert Log All Certificates to Public CT Logs?

Since June 2015, DigiCert has been logging all EV SSL and EV Multi-Domain SSL Certificates to public CT logs. Starting February 1, 2018, DigiCert will log all **public** SSL/TLS certificates to CT logs. This includes the following certificate types:

- Standard SSL
- Multi-Domain SSL
- Wildcard SSL
- Extended Validation SSL
- EV Multi-Domain SSL
- Grid Host SSL
- Grid Host Multi-Domain SSL

The CT logging expansion doesn't affect your private SSL/TLS certificates. DigiCert will not log the following types of certificate to CT logs:

- Private SSL
- Private Multi-Domain SSL
- Private SSL Wildcard
- Client
- Code Signing
- EV Code Signing
- Document Signing

1.2 When and When Not to Log Public SSL/TLS Certificates

Before you decide whether to log a certificate to CT logs, it is important to understand that in the vast majority of situations, logging your certificates in public CT logs is the correct option.

However, we know that you may have internal domains you don't want made public in CT logs. These domains can be excluded from CT logs. Below is some information to help you make the right CT logging choice.

1. **When should I log my public SSL/TLS certificate?**

   If the certificate is protecting a public website, you should always log it in public CT logs.

   - The certificate information is already publicly available. A visitor to your site can click the lock icon to see certificate details; the same information available in public CT logs.
   - There is no benefit in not logging the certificate, just a downside – individuals using browsers with CT logging requirements (e.g., Chrome, Safari, etc.) to visit your site will see an **untrusted** warning and probably go somewhere else.

2. **When should I keep my SSL/TLS certificate information private?**

   If the certificate is protecting an internal or private site and you have organization and domain names that need to be kept private for branding privacy or network security reasons, you are probably okay not logging the certificate.

   The downside is that visitors using browsers with CT logging requirements (e.g., Chrome, Safari, etc.)to visit your site will see an **untrusted** warning. So, make sure you:

   - Really need to keep organization and domain names private.
   - Are prepared to manage the users who visit this site and get an **untrusted** warning.

1.3 Keeping SSL/TLS Certificates Out of Public CT Logs

We understand that you may want to keep specific public SSL/TLS certificates out of the CT logs. However, before you begin excluding certificates from the CT logs, make sure you understand the consequences of unlogged SSL/TLS certificates.

What Happens When You Don't Log SSL/TLS Certificates

Browsers with CT requirement policies will show an **untrusted** warning or a reduced security indicator on sites with unlogged SSL/TLS certificates.

- **For public-facing sites**, customers may be discouraged from using your site, causing losses in business, customer trust, and revenue.
- **For internal-facing sites**, people who come to your site may be scared off.

Google Chrome was the first browser to show warnings on sites with unlogged certificates issued after April 1, 2018. See Google CT to Expand to All Certificates Types.

Other browsers have begun to follow suit. Apple will show warning on sites with unlogged certificates issued after October 15, 2018. See Apple Announces Certificate Transparency Requirement.

Remove Untrusted Warning

To remove this **untrusted** warning from an unlogged certificate, you must do the following:

- Reissue the certificate and allow us to log it.
- Replace the original certificate with the reissued, CT logged certificate.

1.4 Methods for Keeping SSL/TLS Certificates Out of CT Logs

We've provided two methods to keep SSL/TLS certificates out of these logs:

- **Per Certificate Order: Exclude from CT Log When Ordering a Certificate (Recommended)**

  This method is ideal if you only have a minimal number of certificates you don't want logged.

  In your DigiCert account, you can activate a feature that allows individuals to exclude an SSL/TLS certificate from CT logs on a per certificate basis. See How to Allow Users to Keep Certificates Out of CT Logs.

- **Per Account: Turn Off CT Logging for an Account (Use with Caution)**

  This method is ideal if you need to keep organization and domain information private within an entire account.

  To turn CT logging off for your DigiCert account, see How to Turn Off CT Logging for Your Account.

1.5 How to Allow Users to Keep Certificates Out of CT Logs

For your account, you can activate a feature that allows users to keep an SSL/TLS certificate from being logged to public CT logs. The feature is available when a user orders a new certificate, reissues a certificate, and renews a certificate.

Before you allow users to keep SSL/TLS certificates out of public CT logs when ordering certificates, make sure they understand the benefits of CT logging and understand the consequences of keeping SSL/TLS certificates out of these logs. See Keeping SSL/TLS Certificates Out of Public CT Logs and When and When Not to Log Public SSL/TLS Certificates.

1.5.1 CT Logging Certificate Detail Added

Because we are logging all SSL/TLS certificates to public CT logs by default, we are adding a new certificate detail to let users know that a certificate has been logged.

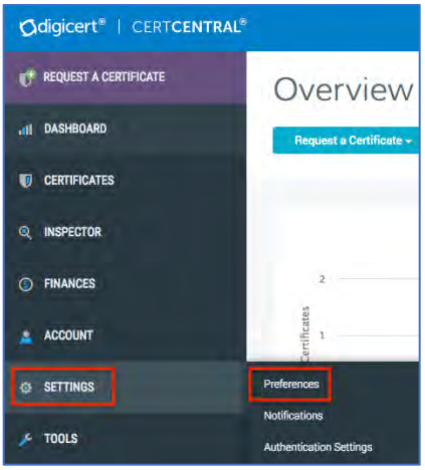
To see a certificate's details, go to the **Orders** page (**Certificates > Orders**), locate the certificate, and click the certificate's **Quick View** link. See How to See If a Certificate Was Logged to CT Logs.

Note: If you don't enable the CT log exclusion feature for your account, you will never see information about an SSL/TLS certificate not being logged. Note that this applies only to certificates issued as of February 1, 2018.

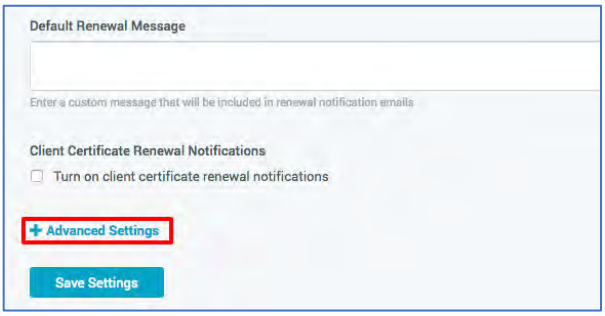
1.5.2 How to Enable the CT Log Exclusion Feature for Your Account

Use these instructions to activate a feature that allows users to keep SSL/TLS certificates out of public CT logs when ordering certificates (new, reissues, and renewals).

1. In your CertCentral account, in the sidebar menu, click **Settings > Preferences**.



2. On the **Division Preferences** page, scroll down and click **+Advanced Settings**.

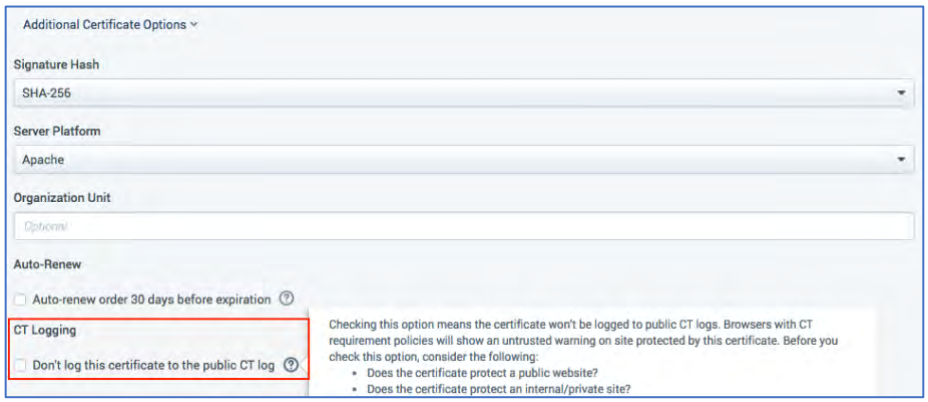


3. In the **Certificate Request section**, under **CT Logging**, check **Allow users to change CT logging per request**.

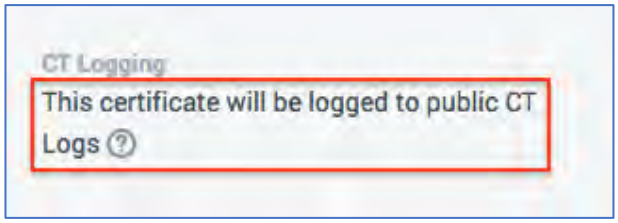
Note: Before you save your changes, make sure you understand the consequences of keeping certificates out of the CT logs.

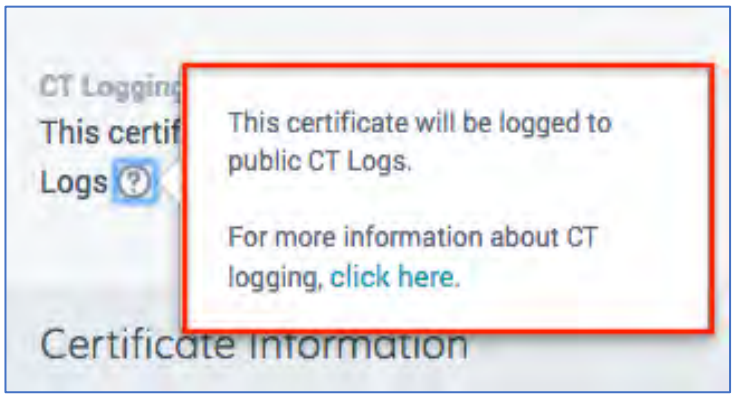
4. Click **Save Settings**.
5. Congratulations! When ordering a certificate (new, reissue, and renewal orders), account users will see an option under **Additional Certificate Options** that allows them to keep an SSL/TLS certificate out of public CT logs.

   Note: Make sure those who can order certificates understand the consequences of keeping certificates out of the CT logs.

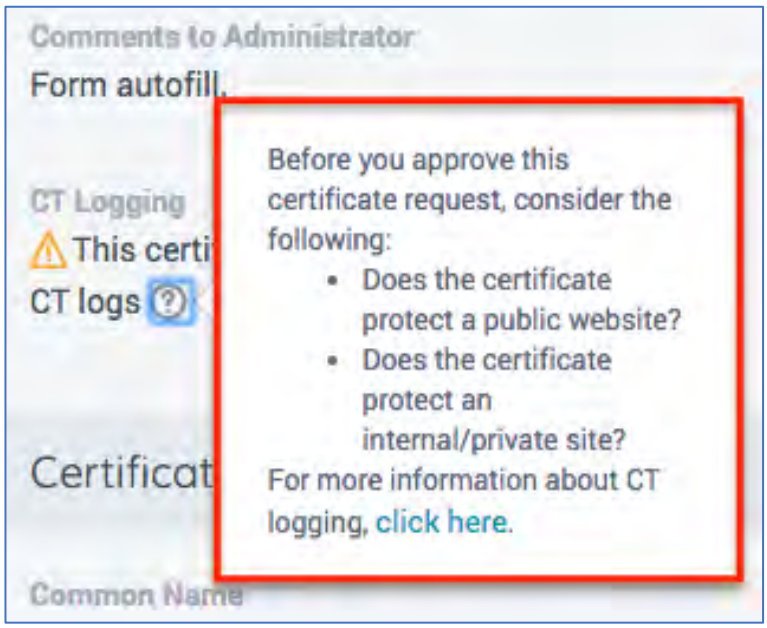


6. In addition, before someone approves an SSL/TLS certificate request, they can see (and make the final decision on) whether the certificate will be logged to CT logs.
   a. Logged to CT Logs





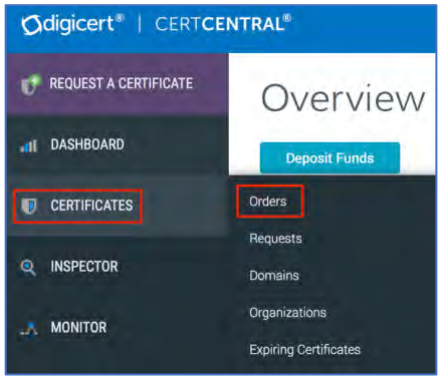
b. Not Logged to CT Logs



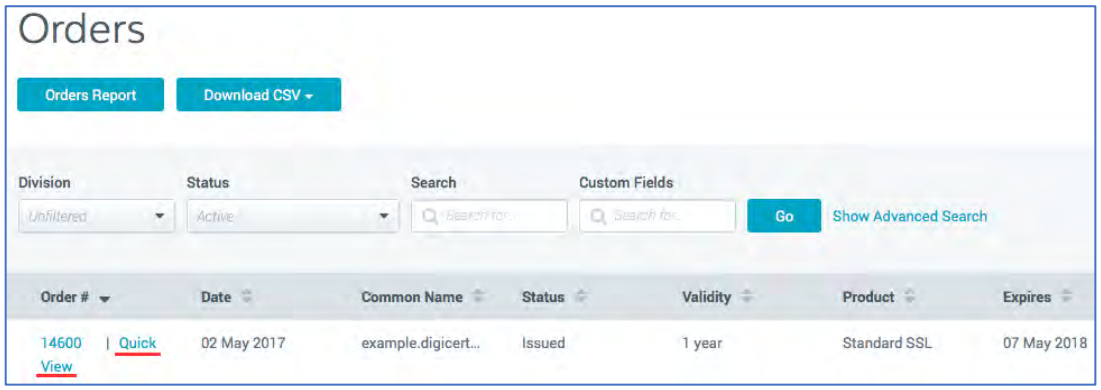
1.5.3 How to See If a Certificate Was Logged to CT Logs

Use these instructions to find out if a certificate has been logged to public CT logs. This certificate detail only appears if you've enabled the account feature that lets users opt out of logging certificates to CT logs.

1. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.



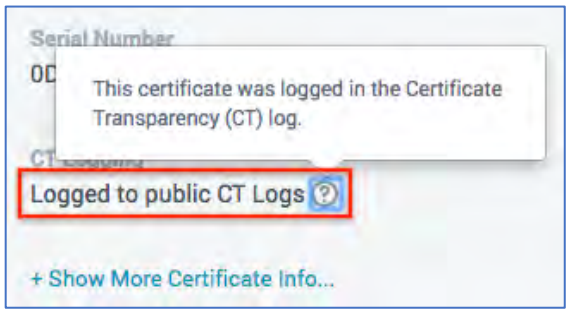
2. On the **Orders** page, find the certificate with the CT logging details you need to check.



3. Next to the certificate's **Order #**, click the **Quick View** link for the certificate you want CT log details about.

4. In the **Order #** details pane (on the right), in the **Certificate Details** section, under **CT logging**, you will see one of the following messages:

   - Logged to CT Logs



   - Not Logged to CT Logs

1.6 How to Turn Off CT Logging for Your Account

Before you ask us to turn off CT logging for your account, make sure you understand the importance of logging SSL/TLS certificates to public CT logs and the consequences of keeping certificates out of these logs. See Keeping SSL/TLS Certificates Out of Public CT Logs.

Ideally, you should dedicate an entire account to ordering certificates you want kept out of public CT logs. You can then use multiple accounts to manage logged and not logged SSL/TLS certificates.

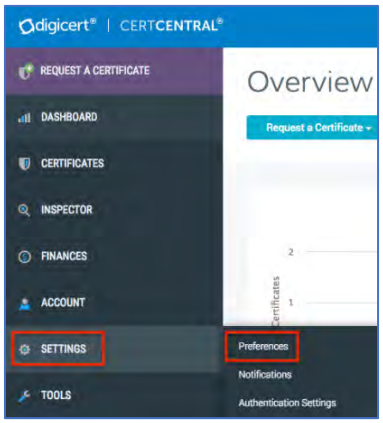
We don't recommend doing this if you only have a single account. This set up doesn't provide a good workflow for issuing a certificate to CT logs when the time comes.

Caution: If CT logging is turned off for your only account, the only way to log an SSL/TLS certificate into the CT logs is to contact your Sales/Account representative and have them turn CT logging back on for your account. Only then can you reissue/renew the certificate, allow it to be logged to public CT logs, and then install it.

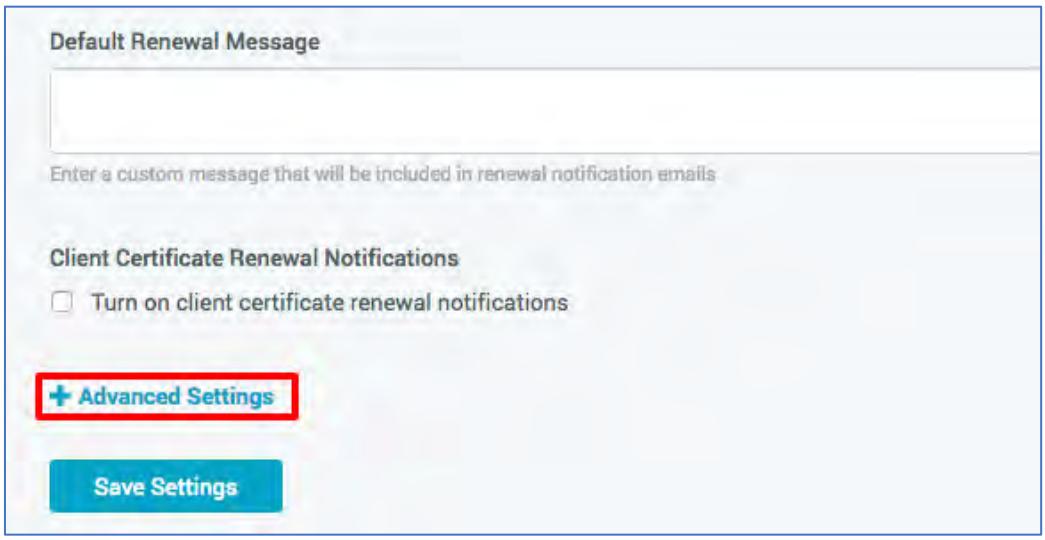
To turn CT logging off for your account, contact your Sales/Account representative.

1.7 How to See If CT Logging Is Disabled for Your Account

1. In your CertCentral account, in the sidebar menu, click **Settings > Preferences**.

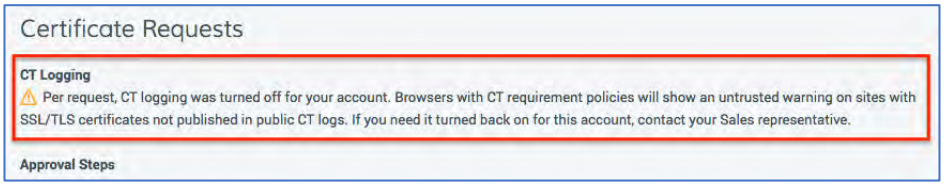


2. On the **Division Preferences** page, scroll down and click **+Advanced Settings**.

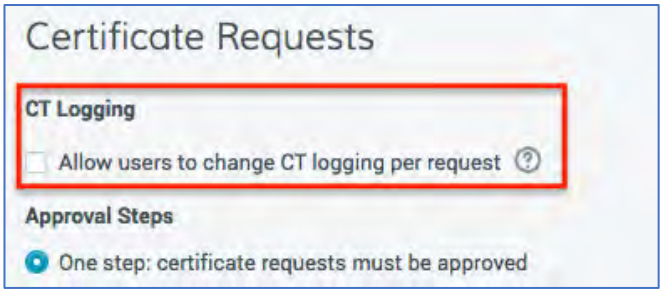


3. In the **Certificate Request section**, look under **CT Logging**.

    a. If CT logging was turned off for your account, you see the **Per request, CT logging was turned off for your account** message.



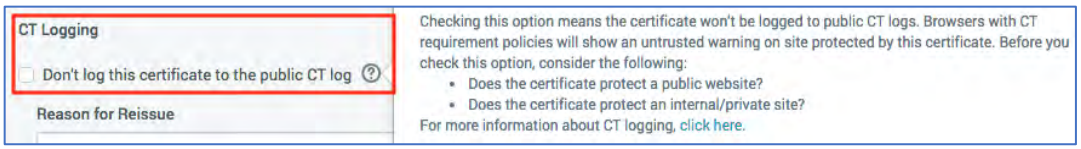
    b. If CT logging is turned on for your account, you see **Allow users to change CT logging per request**.



1.8 How to Add an Unlogged SSL/TLS Certificate to Public CT Logs

Once a certificate is published to public CT logs, you can't remove it from the logs. However, if you chose to keep a certificate out of public CT logs and then discover that you need it logged, you can fix the situation.

To get an unlogged public SSL/TLS certificate into public CT logs, reissue the certificate and uncheck the **Don't log this certificate to public CT logs** check box so we can log it. After we reissue the certificate, the resulting reissued certificate will be logged in CT logs. The browser warnings will go away once the CT-logged certificate has been installed.



Changes to Reissued Certificates Don't Affected Previously Issued Certificates (Original and Reissues)

When you reissue a certificate, any changes that you make to the reissued certificate don't affect the original certificate (or previously reissued certificates). Changes only affect that reissued certificate and all reissued certificates going forward.

For example, if you order an SSL/TLS certificate and you choose to keep it out of public CT logs, the original certificate will never be logged to CT logs. However, if you reissue the certificate and allow it to be logged the reissued certificate will be logged to CT logs. Additionally, all reissued certificates going forward will be logged to CT logs, unless you specifically choose to have that reissued certificate kept out.

Note: To get a duplicate certificate with a different CT logging setting, reissue the certificate and change the CT logging setting on the reissue certificate form.

About DigiCert

DigiCert is a premier provider of security solutions and certificate management tools. We have earned our reputation as the **security industry leader** by building innovative solutions for SSL Certificate management and emerging markets.

DIGICERT
2801 NORTH THANKSGIVING WAY STE. 500
LEHI, UTAH 84043
PHONE: 801.701.9690