CertCentral® API
Public SSL/TLS Certificate Transparency Opt Out Guide

Version 1.4

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:

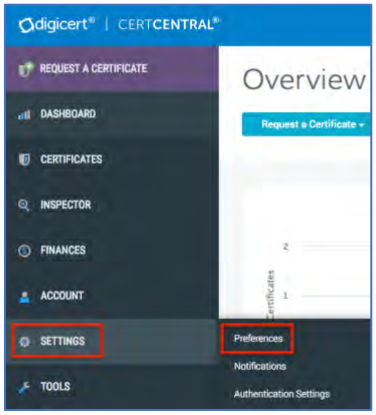
- Reissue the certificate and allow us to log it.
- Replace the original certificate with the reissued, CT logged certificate.

2 Enabling Account Users to Keep Certificates Out of CT Logs

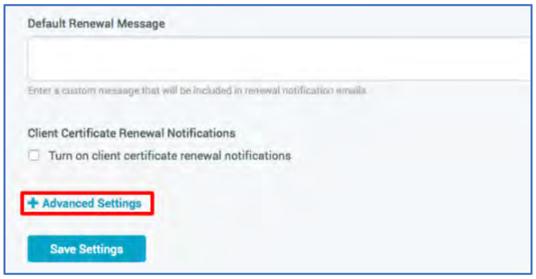
Use these instructions to activate a feature that allows users to keep SSL/TLS certificates out of public CT logs when ordering certificates (new, reissues, and renewals).

This step is a prerequisite to get the disable_ct field for the submit order endpoints to work properly (see 3.1 Prerequisites). It is also a prerequisite to get the new SSL Certificate CT-Status endpoint to work properly (see 4.1 Prerequisites).

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



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



Default Renewal Message

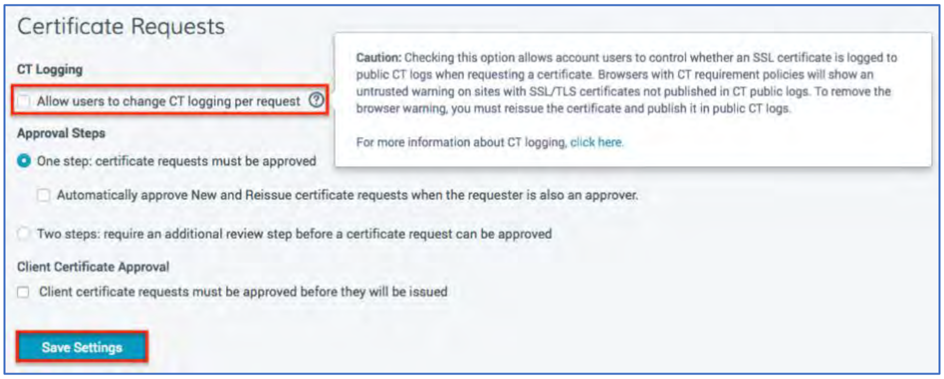
Enter a custom message that will be included in renewal notification emails

Client Certificate Renewal Notifications

☐ Turn on client certificate renewal notifications

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.



Certificate Requests

CT Logging

□ Allow users to change CT logging per request ⓘ

Approval Steps

● One step: certificate requests must be approved

□ Automatically approve New and Reissue certificate requests when the requester is also an approver.

○ Two steps: require an additional review step before a certificate request can be approved

Client Certificate Approval

□ Client certificate requests must be approved before they will be issued

Save Settings

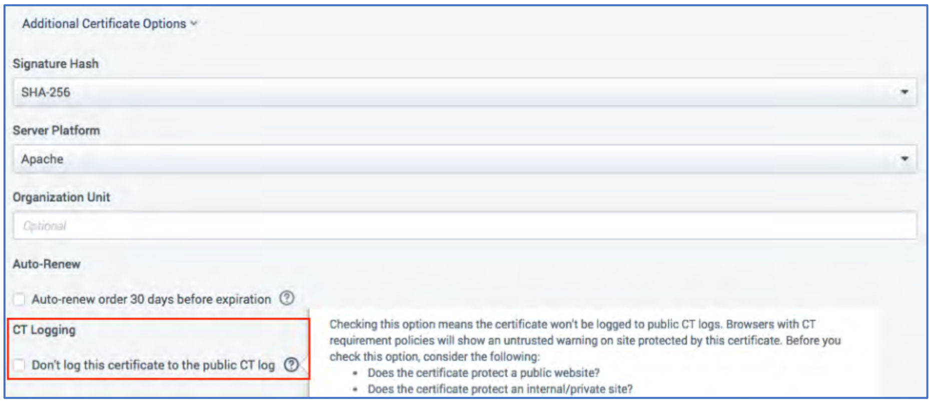
Caution: Checking this option allows account users to control whether an SSL certificate is logged to public CT logs when requesting a certificate. Browsers with CT requirement policies will show an untrusted warning on sites with SSL/TLS certificates not published in CT public logs. To remove the browser warning, you must reissue the certificate and publish it in public CT logs.

For more information about CT logging, click here.

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.



Additional Certificate Options ˅

Signature Hash

SHA-256

Server Platform

Apache

Organization Unit

Optional

Auto-Renew

□ Auto-renew order 30 days before expiration ⓘ

CT Logging

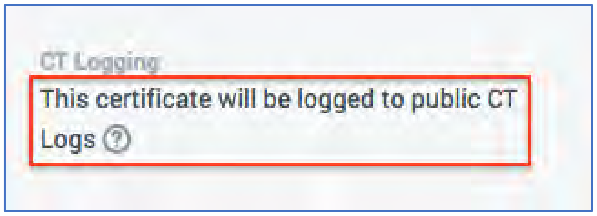
□ Don't log this certificate to the public CT log ⓘ

Checking this option means the certificate won't be logged to public CT logs. Browsers with CT requirement policies will show an untrusted warning on site protected by this certificate. Before you check this option, consider the following:

- Does the certificate protect a public website?
- Does the certificate protect an internal/private site?

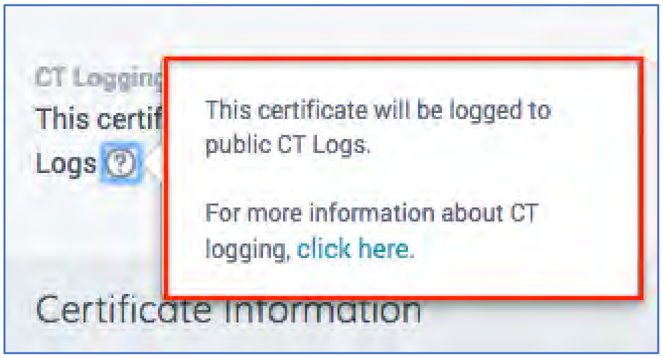
6. In addition, before someone approves an SSL/TLS certificate request, they can see (and make the final decision on) whether the certificate will be logged to CT logs.

   a. Logged to CT Logs



CT Logging

This certificate will be logged to public CT Logs ⓘ



CT Loggin

This certif

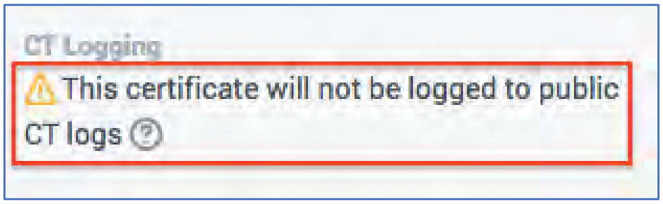
Logs

This certificate will be logged to public CT Logs.

For more information about CT logging, click here.

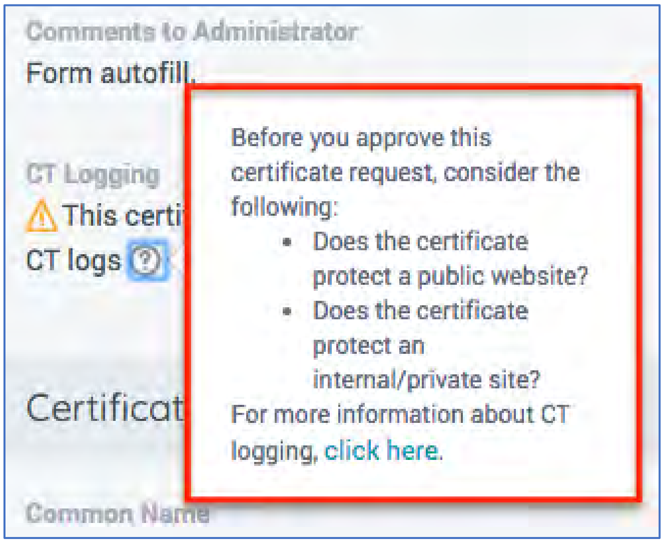
Certificate Information

b. Not Logged to CT Logs



CT Logging

⚠ This certificate will not be logged to public CT logs



Comments to Administrator

Form autofill.

CT Logging

⚠ This certi

CT logs

Certificat

Common Name

Before you approve this certificate request, consider the following:

- Does the certificate protect a public website?
- Does the certificate protect an internal/private site?

For more information about CT logging, click here.

3 CT Logging Exclude/Include Feature for Submit Order Endpoints

Before you configure the API Submit Order endpoints, we've added an optional field: "disable_ct". During the public SSL certificate order process, this field provides users with the option to keep a certificate from being logged to public CT logs.

3.1 Prerequisites

In CertCentral, the disable_ct optional field allows users to keep SSL certificates from being logged public CT logs. Before this optional field will work, you must first enable the CT log exclusion feature in your CertCentral account. See Enabling Account Users to Keep Certificates Out of CT Logs.

Note: If CT logging was disabled for your account, you will receive an error code. See CT Logging Errors.

3.2 Example: Configure the Order Standard SSL Certificate Endpoint

Request Endpoint

Method	URL
POST	https://www.digicert.com/services/v2/order/certificate/ssl_plus

Request Body

The request body for this endpoint must be in one of the following formats

- application/json
- application/xml

3.3 JSON Request Parameters

Parameter Name	Req/Opt	Allowed Values	Default	Description
Certificate	**Required**	**[object]**		
common_name	Required	[string]		The name to be secured in the certificate
csr	Required	[string]		Certificate Signing Request. To create a CSR from you server, visit the DigiCert website (https://www.digicert.com/csr-creation.htm)
organization_units	Optional	[array]	[blank]	The OU field for the certificate.
server_platform	Optional	Reference:	-1	The server platform type defaults to *other*.
id	Required	[int]		The id of the server platform

Parameter Name	Req/Opt	Allowed Values	Default	Description
signature_hash	Required	sha256, sha384, sha512 (sha1 accepted on private certs)		The certificate's signing algorithm hash. For Code Signing certificates only sha256 is supported.
organization	**Required**	**[object]**		
id	Required	[int]		The organization's identifier
validity_years	Required	[int]		Number of years that certificate is valid
custom_expiration_date	Optional	[date]		A custom expiration date that overrides the standard validity period. Date must be formatted in format YY-MM-DD.
comments	Optional	[string]	[string]	Comments about this request that the approver will see.
disable_renewal_notifications	Optional	[bool]	false	If this is true, then no renewal notifications will be sent for the certificate.
renewal_of_order_id	Optional	[int]		If this order is a renewal of a previous order, add the previous order's id to this parameter.
payment_method	Optional	balance, card profile	balance	How to pay for the certificate. If there is a default payment profile, it will default to "profile"; otherwise, it will default to "balance".

Parameter Name	Req/Opt	Allowed Values	Default	Description
disable_ct	Optional	[bool]	0	If the certificate is to be kept out of public CT logs. By default, all public SSL certificates are logged to public CT logs. • 0 = certificate will be logged in CT logs • 1 = certificate will not be logged in CT logs

3.4 JSON Response Parameters

Request Status Response Parameters

Parameter Name	Data Type	Description
id	[int]	The order’s identifier
requests	[array]	
id	[int]	
status	[string]	Statuses: pending, approved, rejected

3.5 Sample Request

Endpoint

https://www.digicert.com/services/v2/order/certificate/ssl_plus

Headers

X-DC-DEVKEY: Your-API-Key-Generated-In-Your-Account
Content-Type: application/json

Body

JSON (application/json)

```
{
    "certificate": {
    "common_name": "digicert.com",
    "csr": "------ [CSR HERE] ------",
    "organization_units": [
     "Developer Operations"
    ],
    "server_platform": {
     "id": 45
    },
    "signature_hash": "sha256",
    "profile_option": "some_ssl_profile"
     },
    "organization": {
    "id": 117483
    },
     "validity_years": 2,
    "custom_expiration_date": "2018-04-24",
    "comments": "Comments for the approver",
    "disable_renewal_notifications": false,
    "renewal_of_order_id": 314152,
    "payment_method": "balance",
    "disable_ct": 1
}
```

3.6 Sample Response

Status Code: 201

Headers

Content-Type: application/json

Body

JSON (application/json)

```
{
       "id": 1234567,
       "requests": [
         {
              "id": 1234567,
        "status": "pending"
     }
    ]
}
```

4 CertCentral Public SSL Certificate CT Status Endpoint

We’ve added a new endpoint that allows those using the DigiCert Services API to manage Certificate Transparency (CT) logging status for issued SSL/TLS certificates in their CertCentral account.

The ct-status endpoint lets you change the CT logging status for an issued certificate from **Don’t Log to CT Logs** to **Log to CT Logs** or from **Log to CT Logs** to **Don’t Log to CT Logs**. The certificate CT logging status change doesn’t take effect until the certificate is reissued and installed.

Caution: Before you start using this endpoint to change the CT logging status for issued certificates, make sure you have a process in place to reissue these certificates immediately and automatically. Make sure the process mitigates confusion and can guarantee that a certificate’s CT logging status is in sync with latest version of the issued certificate. Note that once a certificate is in public CT logs, it doesn’t come out. You can reissue the certificate and keep the reissued version out of CT logs but the original or previously issued version of the certificate will remain there.

4.1 Prerequisites

In CertCentral, the ct-status endpoint allows you to change the CT logging status of issued SSL certificates. Before this endpoint will work, you must first enable the CT log exclusion feature in your CertCentral account. See Enabling Account Users to Keep Certificates Out of CT Logs.

Note: If CT logging was disabled for your account, you will receive an error code. See CT Logging Errors.

4.2 Endpoint Details

With this endpoint, you can change the CT logging status of an issued certificate (CT Logging <--> Not CT Logging).

ct-status Endpoint

Method	URL
PUT	https://www.digicert.com/services/v2/order/certificate/:order_id/ct-status

Request Body

The request body for this endpoint must be in one of the following formats

- application/json

- application/xml

4.3 Sample Request

Endpoint

https://www.digicert.com/services/v2/order/certificate/1234567/ct-status

Headers

X-DC-DEVKEY: Your-API-Key-Generated-In-Your-Account
Content-Type: application/json

Body

0 = certificate will be logged in CT logs
1 = certificate will not be logged in CT logs

JSON (application/json)

```
{
        "disable_ct": 0
}
```

5 CT Logging Errors

Before you begin using the new ct-status endpoint or the new "disable_ct" field, make sure of the following:

- Per certificate order feature has been activated for your account. See Enabling Account Users to Keep Certificates Out of CT Logs.
- CT logging has not been turned off for your account. See the CertCentral® Public SSL/TLS Certificate CT Logging Guide.

Error	Description
Code: ct_logging_disabled **Message:** CT Logging has been disabled for this account.	CT logging has been disabled for your CertCentral account. An administrator must turn it back on for the new ct-status endpoint or disable_ct field to work. See the CertCentral® Public SSL/TLS Certificate CT Logging Guide.
Code: cert_transparency_ turned_off_for_account **Message:** Cert Transparency logging has been turned off for your account.	CT logging has been disabled for your CertCentral account. An administrator must turn it back on for the new ct-status endpoint or disable_ct field to work.

Error	Description
Please contact your administrator with any questions.	See the CertCentral® Public SSL/TLS Certificate CT Logging Guide.
Code: not_allowed_to_change_ct_setting_per_order **Message:** Per order Cert Transparency logging has not been enabled. Please contact your administrator with any questions.	The per certificate order feature has not been activated for your CertCentral account. An administrator must active this feature for the new ct-status endpoint or disable_ct field to work. See Enabling Account Users to Keep Certificates Out of CT Logs.

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