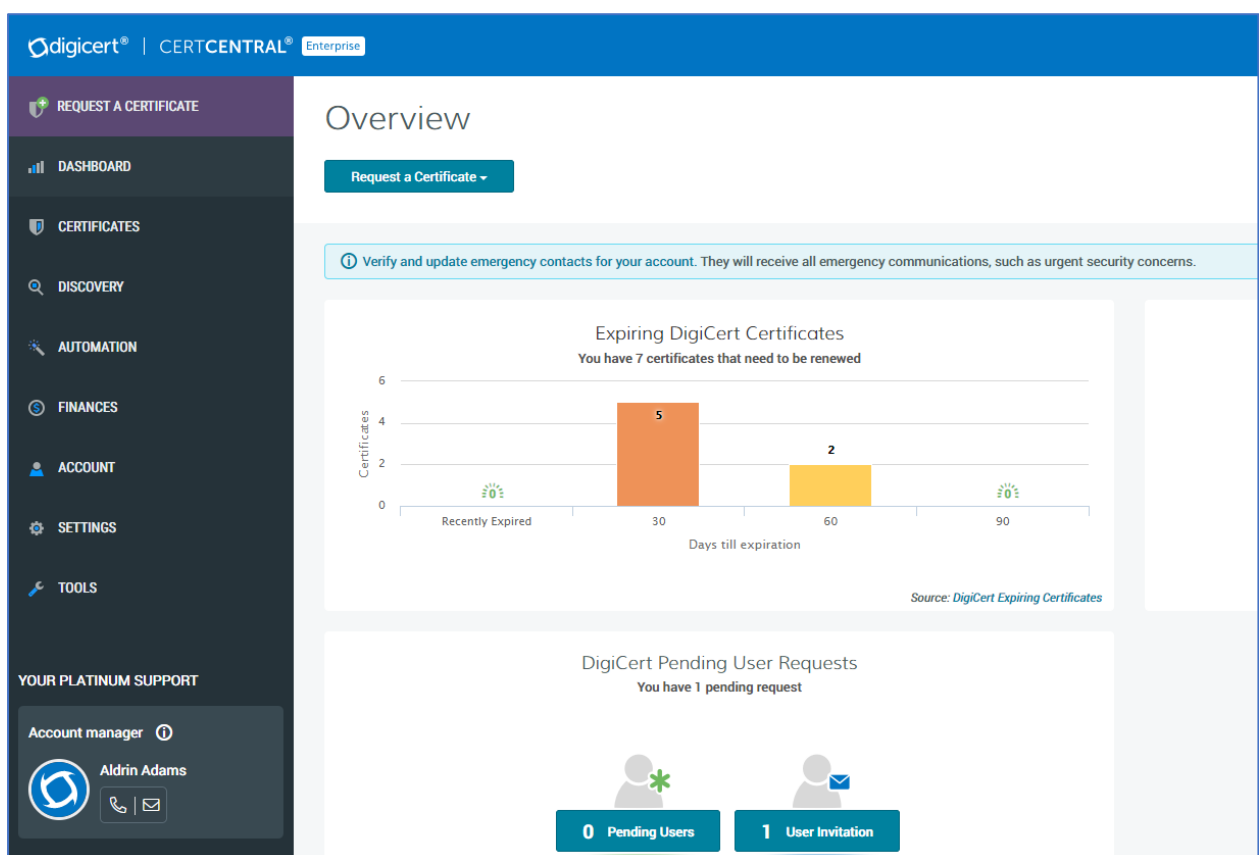


## DigiCert® Technical Certifications CertCentral® Professional Study Guide

2021 v2



© 2021 DigiCert, Inc. All rights reserved. DigiCert is a registered trademark of DigiCert, Inc. in the USA and elsewhere. All other trademarks and registered trademarks are the property of their respective owners.

## Contents

Introduction .....	4
Objectives .....	5
SSL/TLS certificate products.....	6
Flex certificates .....	6
Multi-year Plans .....	7
Secure Site certificate benefits .....	7
DigiCert Smart Seal .....	9
Certificate profile options .....	10
Code Signing Certificate Products.....	10
Product Settings.....	11
Domain and organisation validation.....	12
Domain Control Validation (DCV) .....	12
Organization validation.....	13
Management of orders and certificates .....	13
Certificate approval.....	15
Duplicate certificates .....	16
Certificate reissue .....	16
Downloading a certificate .....	16
Custom order fields.....	17
Renewal notification .....	18
Subaccounts and divisions .....	19
Divisions .....	19
Subaccounts.....	19
User roles .....	20
User access/authentication control methods.....	22
Passwords .....	22
Two-Factor Authentication .....	22
IP restrictions .....	22
Single Sign-On .....	22
Guest access options.....	23
Guest URL.....	23
Guest access.....	24
Reports & Notifications.....	25

Reports.....	25
Email Notifications .....	25
Audit logging .....	26

## Introduction

This study guide is designed to help you prepare for the **DigiCert Technical Certification: CertCentral Professional** assessment exam. The exam will consist of 50 multiple-choice questions with a maximum time allowed of 1 hour.

The intended audience for this assessment is anybody who works with the DigiCert CertCentral certificate management platform in a technical role (technical support, SSL/TLS administrator, etc).

Before attempting a certification assessment, you should review the objectives below. If you believe that you are already able to meet all the objectives listed, you are welcome to schedule an assessment. However, if there are any objectives listed where you may need additional preparation, you should plan to research these topics in detail prior to scheduling an assessment.

More information can be found in the **CertCentral Professional Training Guide** which can be downloaded from <https://www.digicert.com/tls-ssl/tls-certification-program>. Please note – these resources are just a starting point! It is strongly recommended that you do further research in order to be fully prepared for an assessment on all the objectives, including hands-on experience using DigiCert CertCentral.

In addition, it may be possible to attend a DigiCert instructor-based workshop which will give in-depth information on many of the assessment objectives. Please contact your DigiCert account manager if you would like to find out more.

## Objectives

Before attempting the **DigiCert Technical Certification: CertCentral Professional** assessment exam, you should be able to do the following:

- List and compare the SSL/TLS and Code Signing certificate products available in DigiCert CertCentral Enterprise
- Describe the Business SSL certificate entitlements, e.g. CT log monitoring, malware scanning, DigiCert Smart Seal
- Describe certificate profile options available in DigiCert CertCentral e.g. HTTP Signed Exchange
- Describe the policies and methods used by DigiCert for domain and organisation validation
- List and compare the user roles in DigiCert CertCentral
- Demonstrate the management of orders, certificates, organisations and domains in DigiCert CertCentral
- Explain and demonstrate the user access/authentication control methods in DigiCert CertCentral, e.g. SAML, 2FA
- Explain and demonstrate the use of subaccounts and divisions in DigiCert CertCentral
- Describe the reporting options available in DigiCert CertCentral
- Describe and demonstrate guest access options in CertCentral: Guest URL & Guest Access feature

# DIGICERT® CERTIFICATION PROGRAM

## SSL/TLS certificate products

Most Enterprises use the DigiCert range of Business SSL certificates:

- Secure Site Pro
- Secure Site Pro EV
- Secure Site EV
- Secure Site OV

These certificate products come with many options and benefits. These are described below.

FEATURE	Secure Site OV	Secure Site EV	Secure Site Pro	Secure Site Pro EV
Wildcard Support	YES		YES	
SAN Limit	250	250	250	250
PQC Toolkit			YES	YES
CT Monitoring			YES	YES
Vulnerability Assessment		YES	YES	YES
Malware/Blacklist Check	YES	YES	YES	YES
Premium Site Seals	2	2	2	2
Priority Validation	YES	YES	YES	YES
Priority Support	YES	YES	YES	YES
Netsure Protection Warranty	\$1.75M	\$1.75M	\$2M	\$2M
Relying Party Warranty	\$2M	\$2M	\$2M	\$2M

## Flex certificates

DigiCert Secure Site and Secure Site Pro certificates support any type of domain configuration and can be ordered as single-domain or multi-domain certificates with any combination of fully qualified domain name (FQDN) and wildcard SANs.

This gives you the flexibility to order exactly what you want and add additional SANs during the lifetime of the certificate without needing to change products. These certificates do not have dedicated multi-domain or wildcard versions, instead you add those as you configure the base certificate.

More information: <https://docs.digicert.com/manage-certificates/flex-certificates/>

# DIGICERT® CERTIFICATION PROGRAM

## Multi-year Plans

The screenshot shows a web interface titled "How long do you need to protect your site?". On the left, there is a vertical list of options: "1 year", "2 years", "3 years", "4 years", "5 years", and "6 years". The "6 years" option is highlighted with a green border and a small green badge that says "Most savings per year". To the right of this list is a panel titled "Multi-year Plan benefits". Under the heading "Your plan supports", there are three items, each with a green icon and a title: 1. A lightbulb icon for "Unlimited reissues" with the subtext "Free reissues until the end of your Multi-year Plan." 2. A globe icon for "Change domain names for free." with the subtext "Additional domains can be added, for a cost." 3. A calendar icon for "Change certificate length" with the subtext "Change your certificate length anytime."

DigiCert Multi-year Plans allow you to pay a single price for up to six years of SSL/TLS certificate coverage. With Multi-year Plans, you pick the SSL/TLS certificate, the duration of coverage you want (up to six years), and the certificate validity. Until the plan expires, you reissue your certificate at no cost each time it reaches the end of its

validity period. Note that the maximum validity period for a publicly-trusted SSL/TLS certificate is currently 397 days, so you may need to reissue such as certificate multiple times during a Multi-year Plan.

When you reissue certificates for a Multi-year Plan, you can do the following:

- Set a new expiration date for the reissued certificate: The maximum validity period for a reissued certificate is the maximum certificate lifetime defined by CA/B Forum baseline requirements or the end of the Multi-year Plan, whichever is sooner.
- Change or remove domains: Removing and changing domains requires DigiCert to revoke all previously issued certificates. DigiCert waits 48-72 hours before revoking the original certificate and any existing duplicates and reissues.
- Add domains: Adding domains may result in additional costs. Prices for new domains are pro-rated and applied based on the remaining time in the Multi-year Plan.

More information: <https://docs.digicert.com/manage-certificates/multi-year-plans/>

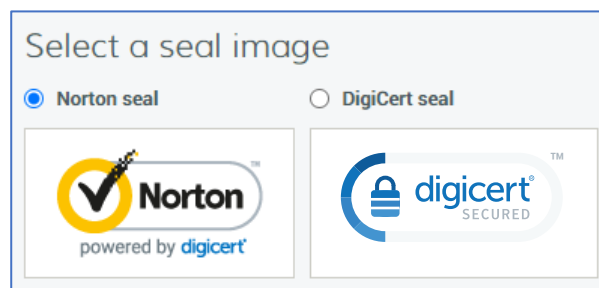
## Secure Site certificate benefits

In addition to industrial-strength 2048-bit encryption, DigiCert Secure Site certificates include additional benefits, such as priority support. These benefits are available during the life of your certificate order. Each time you renew the Secure Site certificate order, your benefits are automatically carried over to your new order.

- Priority validation— Secure Site orders are placed at the top of our validation queues so our agents can respond to these orders first.

# DIGICERT® CERTIFICATION PROGRAM

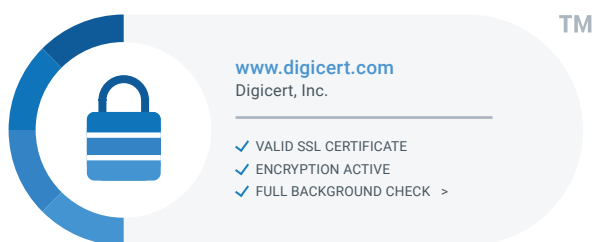
- Priority support – Secure Site certificates come with access to two priority support queues so our Support team can respond to your needs first: Order and validation status and Installation and configuration.
- Two premium site seals– Secure Site certificates come with the two most recognized trust marks on the web: DigiCert and Norton. Pick the premium site seal you want to use to display proof of trust on your site.
- CT (Certificate Transparency) Log Monitoring - The CT Log monitoring service allows you to monitor the public CT logs for SSL/TLS certificates issued for the domains on your **Secure Site Pro** or **Secure Site Pro EV** certificate. After you've enabled CT Log monitoring for a Secure Site Pro certificate order, you'll receive two types of email notifications: Daily CT log digest and if needed, Urgent notifications. Email notifications are sent to account admins allowing them to check the CT logs for their domains without signing in to their CertCentral account every day. The CT log monitoring service pulls the discovered SSL/TLS certificates into your CertCentral account, where you can view details about the certificates to quickly identify any miss-issued certificates for your domains. You can also download copies of the non-DigiCert certificates right from your CertCentral account. More information: <https://docs.digicert.com/certificate-tools/ct-log-monitoring-service/>
- Vulnerability assessment – **Secure Site EV, Secure Site Pro SSL, and Secure Site Pro EV** certificates include access to a vulnerability assessment service. This service allows you to identify and act against the most exploitable weaknesses on your website. To learn more, see <https://docs.digicert.com/certificate-tools/vulnerability-assessment-service/>
- Malware check– Secure Site certificates come with convenient access to a VirusTotal malware check. Quickly analyze your public domains with 70 plus antivirus scanners and URL/domain blacklist services. Use scan results to identify malware threats so you can take actions to keep your site off blacklists that can cripple site availability and online revenue.
- Post-quantum Cryptography (PQC) – Customers purchasing a **Secure Site Pro SSL or Secure Site Pro EV SSL** have access to DigiCert's post-quantum cryptographic (PQC) toolkit. More information: <https://docs.digicert.com/certificate-tools/post-quantum-cryptography/>
- Industry-leading warranties– Secure Site certificates include warranties to protect you and your customers: a \$1.75M or \$2M Netsure Protection Warranty for your business and an industry-best \$2M aggregate Relying Party Warranty for your customers.





# DIGICERT® CERTIFICATION PROGRAM

## DigiCert Smart Seal



The DigiCert Smart Seal is a new dynamic site seal that gives website visitors confidence that their information is secure on the web. Real-time security indicators enabled through various microinteractions alert visitors that the seal is actively present on the page, the site has been validated, and the site is protected by an active certificate from the world's most trusted

certificate authority.

When site visitors hover over the DigiCert Smart Seal, they see the company's logo (if uploaded and verified by DigiCert). They also view usable information about the site's security delivered right to the seal, so users do not have to leave the page to verify a site's legitimate identity.

The Smart Seal can be configured to show the following options on the information page:

**Malware scan:** Add the date of the most recently completed malware scan. Site visitors can see that you monitor your website for viruses and malware.

**CT log monitoring:** Add the date you enabled CT log monitoring for your website's domain. Site visitors can see you monitor the transparency logs allowing you to act quickly if a bad actor issues a fraudulent certificate for your domain. This feature is only available for Secure Site Pro certificates.

**Blocklist:** Add a blocklist check. Site visitors can see your business is clear from government and country-specific blocklists.

**This site is secure.**

www.digicert.com is validated as a secure site for sending and receiving sensitive data.

English

ENCRYPTED SITE	www.digicert.com
ORGANIZATION NAME	DigiCert, Inc.
LOCATION VERIFIED	UTAH, USA
TLS/SSL CERTIFICATE	Expires: 05-May-2022
CERTIFICATE TYPE	DigiCert EV SSL Certificate
REGISTRATION	Confirmed
ADDRESS	Confirmed
PHONE NUMBER	Confirmed
EMAIL ADDRESS	Confirmed
DOMAIN OWNERSHIP	Confirmed
WARRANTY LEVEL	\$2 million USD
BLOCKLIST	Checked

©2021, DigiCert Inc., All rights reserved.

digicert

**PCI compliance scan:** Add the date of the most recently completed PCI compliance scan. Site visitors can see that you monitor your website to ensure it is compliant with PCI DDS Standards. This feature is only available for Secure Site Pro and Secure Site EV certificates and requires the Vulnerability Assessment service to be enabled for your certificate order.

**Verified Customer:** Display how long you've been a DigiCert customer. Site visitors can see how long you've been using one of the most trusted names in

# DIGICERT® CERTIFICATION PROGRAM

TLS/SSL certificates to protect your sites.

## Certificate profile options

Certificate profiles allow you to do more with your certificates. Some options allow you to include an additional field in your certificate, while others allow you include in an additional x.509 extension.

- **OCSP Must-Staple:** Allows you to include the OCSP Must-Staple extension in OV and EV SSL/TLS certificates. Browsers with support for OCSP must-staple may display a blocking interstitial to users accessing your site. Ensure that your site is configured to properly and robustly serve stapled OCSP Responses before installing the certificate.
- **HTTP Signed Exchange:** Allows you to include the CanSignHTTPExchanges extension in an OV and EV SSL/TLS certificate. The HTTP Signed Exchange extension is under active development. There may be additional changes to the requirements as industry development continues.
- **Delegated Credentials:** Allows you to include the DelegationUsage extension in OV and EV SSL/TLS certificates. The Delegated Credentials for TLS extension is under active development within the Internet Engineering Task Force (IETF). There may be additional changes to the requirements as industry development continues.
- **Data Encipherment:** Allows you to include the Data Encipherment key usage extension in OV and EV SSL/TLS certificates. Useful when you want to use the public key in the certificate to encrypt user data and application data.

More information: <https://docs.digicert.com/manage-certificates/certificate-profile-options/>

## Code Signing Certificate Products

A DigiCert Code Signing Certificate increases trust by verifying the source and integrity of your application.

- Digitally signs a program to prove that it has not been altered or compromised
- Supports Microsoft Authenticode, Office VBA, Java, Adobe AIR, Apple's Mac OS, and Mozilla objects
- Avoids unnecessary warning messages and ensure your applications can be trusted

A DigiCert EV Code Signing Certificate increases trust by verifying the source and integrity of the application. It also helps users avoid warning messages when downloading the application.

- Combines the benefits of a standard Code Signing Certificate with a rigorous Extended Validation process
- Provides compatibility and grants immediate reputation with Windows 8 and Internet Explorer, eliminating warning messages
- Supports Microsoft Authenticode, Office VBA, Java, Adobe AIR, Apple's Mac OS, and Mozilla objects
- Extended Validation ensures additional organization vetting to protect your users and your reputation
- Includes two-factor authentication for enhanced security

A DigiCert EV Code Signing Certificate can be provisioned with the following options:

# DIGICERT® CERTIFICATION PROGRAM

- Preconfigured Hardware Token: DigiCert installs your EV CS certificate on a secure token and ships the token to you with instructions for how to activate it.
- Existing Token: After DigiCert issues your EV CS certificate, you need to install the certificate on your token.
- HSM: After DigiCert issues your EV CS certificate, install it on your HSM device. (Note: You must have a FIPS 140-2 Level 2 or Common Criteria EAL4+ compliant device.)

More information: <https://docs.digicert.com/manage-certificates/code-signing-certificate/>

## Product Settings

Role	Product	Product Settings	Settings
Administrator	Summary	Summary For Limited User	
Limited User	Private SSL OV	Product	
Finance Manager	Digital Signature Plus	Private SSL OV	1 Year
Manager	Premium	Digital Signature Plus	2 Years
Standard User	Code Signing	Premium	3 Years
	EV Code Signing	Code Signing	
	Document Signing - Organization (2000)	EV Code Signing	
	Document Signing - Organization (5000)	Document Signing - Organization (2000)	
	RapidSSL Standard DV	Document Signing - Organization (5000)	
	RapidSSL Wildcard DV	Document Signing -	

The Product Settings page allows you to configure which certificate products can be selected per account or per division. In addition, product options can also be configured by user role.

# DIGICERT® CERTIFICATION PROGRAM

## Domain and organisation validation

### Domain Control Validation (DCV)

#### Domain Control Validation (DCV)

**DCV Methods**

- ☒ Show DNS CNAME as an alternative DCV method when managing / adding domains
- ☒ Show HTTP Practical Demonstration as an alternative DCV method when managing / adding domains
- ☒ Show DNS TXT as an alternative DCV method when managing / adding domains

**By Default Send DCV Emails To**

Check All

- ☒ admin@newdomain.com
- ☒ administrator@newdomain.com
- ☒ webmaster@newdomain.com
- ☒ postmaster@newdomain.com
- ☒ hostmaster@newdomain.com
- ☒ Org/Tech/Admin contacts from Whois

When a domain is added to your account, you can limit where the DCV emails are sent by default.

Before DigiCert can issue an SSL/TLS certificate, you must demonstrate control over the domains and any SANs (Subject Alternative Names) on the order. We refer to this process as the Domain Control Validation (DCV) process.

DigiCert currently supports these DCV Methods:

- **Email Validation:** With this validation method, DigiCert sends three sets of DCV emails: WHOIS-based, constructed, and DNS TXT-based. To demonstrate control over the domain, an email recipient follows the instructions in a confirmation email sent for the domain. The confirmation process consists of visiting the link provided in the email and following the instructions on the page.
- **DNS CNAME Validation:** With this validation method, you add a DigiCert generated random value (provided for the domain in your CertCentral account) to the domain's DNS as a CNAME record. When DigiCert does a search for DNS CNAME records associated with the domain, we can find a record where the record's value includes the DigiCert random value.
- **DNS TXT Validation:** With this validation method, you add a DigiCert generated random value (provided for the domain in your CertCentral account) to the domain's DNS as a TXT record. When DigiCert does a search for DNS TXT records associated with the domain, we can find a record where the record's value includes the DigiCert random value.
- **File Validation (HTTP Practical Demonstration, also referred to as FileAuth):** With this validation method, you host a file containing a DigiCert generated random value (provided for the domain in your CertCentral account) at a predetermined location on your website: [domain]/.well-known/pki-validation/fileauth.txt. Once the file is created and placed on your site, DigiCert visits the specified URL to confirm the presence of our random value.

Note: For DV certificates in CertCentral, DigiCert currently supports the following DCV Methods: WHOIS-based Email, Constructed Email, Email to DNS TXT contact, DNS TXT, and File Validation.

More information: <https://docs.digicert.com/manage-certificates/organization-domain-management/managing-domains-cc-guide/domain-pre-validation-domain-control-validation/>

# DIGICERT® CERTIFICATION PROGRAM

<https://docs.digicert.com/manage-certificates/dv-certificate-enrollment/domain-control-validation-dcv-methods/>

## Organization validation

To validate an organization, DigiCert first verifies that the organization requesting a certificate is in good standing. This may include confirming good standing and active registration in corporate registries. It may also include verifying that the organization is not listed in any fraud, phishing, or government restricted entities and anti-terrorism databases.

Additionally, we verify that the organization requesting a certificate is, in fact, the organization to which the certificate will be issued. We also verify the organization contact.

Adding organizations to your CertCentral account and getting them validated is a prerequisite for getting your domains validated. Validating organizations as soon as possible quickens the certificate issuance process.

Managing organizations typically involves adding an organization and submitting it for validation. You can also deactivate a no longer needed organization.

More information: <https://docs.digicert.com/manage-certificates/organization-domain-management/manage-organizations/>

After you've submitted your organizations for validation, you can begin submitting domains for validation and the type of authorization for which the domain should be validated.

More information: <https://docs.digicert.com/manage-certificates/organization-domain-management/managing-domains-cc-guide/>

It is usually preferable to validate domains and organizations before requesting certificates, however it is also possible to add new domains and organizations when requesting a certificate.

## Management of orders and certificates

The screenshot shows the DigiCert CertCentral Enterprise interface. The left sidebar contains navigation links: REQUEST A CERTIFICATE, DASHBOARD, CERTIFICATES, Orders, Requests, Domains, Organizations, Expiring Certificates, Certificate Authority, DISCOVERY, AUTOMATION, FINANCES, SUBACCOUNTS, ACCOUNT, SETTINGS, and TOOLS. The main content area is titled 'Orders' and includes buttons for 'Request a certificate', 'Orders report', and 'Download CSV'. Below these are four warning banners: '5 certificates are expiring within the next 90 days', '1 certificate is expiring within the next 60 days', '215 certificates are expiring within the next 30 days', and '72 certificates have already expired'. A search bar and filters for 'Division' and 'Status' are present. The table below lists several orders with their details.

Order#	Common name	Product	Status	Order date	Certificate start date	Certificate expiration	Order expiration
111087587   Quick View	people.co.za	Secure Site OV 2 years	Issued	07 Jan 2021	07 Jan 2021	07 Feb 2022	12 Jan 2023
111086978   Quick View	test.digicertdemo.com	Secure Site OV 2 years	Pending	07 Jan 2021	-	-	-
110966828   Quick View	people.co.za	Secure Site OV 2 years	Issued	07 Jan 2021	07 Jan 2021	04 Feb 2021	11 Jan 2023
110951705   Quick View	acmewin.cc	Secure Site OV 1 year	Issued	07 Jan 2021	07 Jan 2021	04 Feb 2021	11 Jan 2022
110877428   Quick View	acmewin.cc	Secure Site OV 1 year	Issued	07 Jan 2021	07 Jan 2021	15 Jan 2021	15 Jan 2021

# DIGICERT® CERTIFICATION PROGRAM

Orders and certificates can be managed directly from the CertCentral platform.

Order #117670865

## Duplicates

For Order #117670865, 1 year

[Download CSV](#)

### Primary Certificate

Of Order #117670865

[Download](#) [Send](#)

Common Name	*.thetlsigym.com
DNS Names	*.thetlsigym.com 1.thetlsigym.com 2.thetlsigym.com
Note	<a href="#">Add Note</a>

Requested	01 Feb 2021 18:22 by Rafael Funes
Signature Hash	sha256
Thumbprint	B71FB1B44803755A98B12B0B9FD6787EA807AA5F
Serial Number	0DFF4BA2AFE5E54E3F6D73002BF4F22
Server Platform	Apache

### Duplicate 001

Of Order #117670865

[Download](#) [Send](#) [Archive](#)

Common Name	1.thetlsigym.com
DNS Names	1.thetlsigym.com 2.thetlsigym.com
Note	<a href="#">Add Note</a>

Requested	01 Feb 2021 18:27 by Rafael Funes
Signature Hash	sha256
Thumbprint	36B0CD6D854F87D0260802489A5B44E2B2E04CD9
Serial Number	0C1D18137959259C5EE02AEA771601B
Server Platform	Apache

An order relates to the chosen multi-year plan. A certificate belongs to an order and may be reissued many times during the lifetime of the order. Important options for an order include:

### Order details

Requested on	01 Feb 2021 18:22
Requested by	Rafael Funes
Multi-year Plan details	1-year plan (01 Feb 2021 - 06 Feb 2022)
Order requested via	CertCentral
Auto-renew	<input type="checkbox"/>
Auto-reissue	<input type="checkbox"/>
Organization contact	Sales Manager Ashvin Shukal ashvin.shukal@digicert.com +61444769333
Division	Sales team Cert Central Account <a href="#">Edit</a>
Order status	Issued
Approval comment	testing
Platform	Apache
Payment method	Account Balance
Guest access	<input checked="" type="checkbox"/> Enable for this order


**Auto-renew:** Automatically renew the multi-year plan 30 days before expiration date of the current plan.

**Auto-reissue:** Automatically issue a new certificate 30 days before expiration date of the current certificate.

Note that a certificate cannot be issued with an end-date which is later than the end date of the corresponding order.

# DIGICERT® CERTIFICATION PROGRAM

[Manage Orders](#)

 **Order #111087587**  
Secure Site OV, 2 years of coverage remaining

[Priority Support](#)

Current certificate expiration	Next certificate	Order status
07 Feb 2022	09 Nov 2021	Issued

**Certificate details**

**Common name** people.co.za  
[Check certificate installation](#)  
[Check domain on VirusTotal](#)

**Organization** Win The Customer, LLC  
Saratoga Springs, Utah, US  
Phone: (801) 228-0992

**Serial number** 0327E1A64946A466E9EA0FEF1CD02AFC

**Thumbprint** 0BA366AA79A76E2710CFB8F75A2F2905F119980

**Signature hash** sha256

**Issuing CA** DigiCert Global G2 TLS RSA SHA256 2020 CA

**Validity** 07 Jan 2021 - 07 Feb 2022

**CSR** Included [View](#)

**Certificate Actions**

[Send Certificate](#)  
[Request Duplicate](#)  
[Reissue Certificate](#)  
[Revoke Certificate](#)  
[View Receipt/Invoice](#)  
[Site Seal](#)

[Download Certificate As](#)

Certificate management includes the following actions:

- Request certificate
- Approve certificate request
- Request duplicate certificate
- Reissue certificate
- Revoke certificate
- Get site seal code

## Certificate approval

By default, certificate requests require approval before they are submitted to DigiCert for certificate issuance. After a user requests a certificate, an Administrator, a manager, an EV Verified User, a CS Verified User, or an EV CS Verified User must approve the certificate request. Next, the request is sent to DigiCert to verify that all the pre-validation requirements have been met.

After a user requests a certificate, any Administrator, manager, EV Verified User, CS Verified User, or EV CS Verified User can also reject the certificate request, if needed. For example, if the user ordered the wrong type of certificate.

**Approval Steps**

☐ Skip approval step: remove the approval step from your certificate order processes [?](#)

☒ 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

**DV Certificate Approval**

☐ DV certificate requests must be approved before they will be issued

**Client Certificate Approval**

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

By default, CertCentral accounts are configured for one-step certificate request approvals. An account admin must approve a certificate request before DigiCert can start processing the order (validating the organization, etc.). However, you can remove the approval step from the OV/EV SSL certificates issuance workflows for

your CertCentral administrators, managers, and finance managers. Approval requirements can be configured in the Settings/Preferences page of CertCentral.

# DIGICERT® CERTIFICATION PROGRAM

## Duplicate certificates

All DigiCert certificates come with unlimited free duplicate issues. To increase security and make it easier to install the certificate on multiple servers, generate a new CSR and create a duplicate certificate for each server.

The details in the duplicate certificate will be exactly the same as in the original certificate. Duplicate certificates never require DigiCert to revoke previous copies of your certificate.

More information: <https://docs.digicert.com/manage-certificates/duplicate-sslts-certificate/>

## Certificate reissue

All DigiCert certificates come with unlimited free reissues. The certificate reissue process allows you to modify an issued certificate. Some modifications allow you to build upon the original certificate, resulting in two or more versions of that certificate. For example, when reissuing a certificate, you can add domains to the original certificate. Adding domains to a certificate doesn't revoke the original certificate.

Other modifications allow you to create a new version of the certificate and require DigiCert to revoke the original certificate and any certificate reissues and duplicates. For example, removing SANs or changing SANs on a multi-domain certificate creates a new version of the certificate and revokes the original certificate and any previous reissues and duplicate copies.

More information: <https://docs.digicert.com/manage-certificates/reissue-sslts-certificate/>

## Downloading a certificate

After DigiCert issues your certificate, you may want to download the certificate directly to your server where the certificate signing request was created (in other words the server with the certificate's matching public key).

Order #117670865

### Download Certificates for Order #117670865

Combined Certificate Files

Server Platform: Apache

Download

How To Install This Certificate

Individual Certificate Files

Certificate: \*.thetlsym.com

Download

Intermediate Certificate: DigiCert TLS RSA SHA256 2020 CA1

Download

Click Text to Copy

File Type

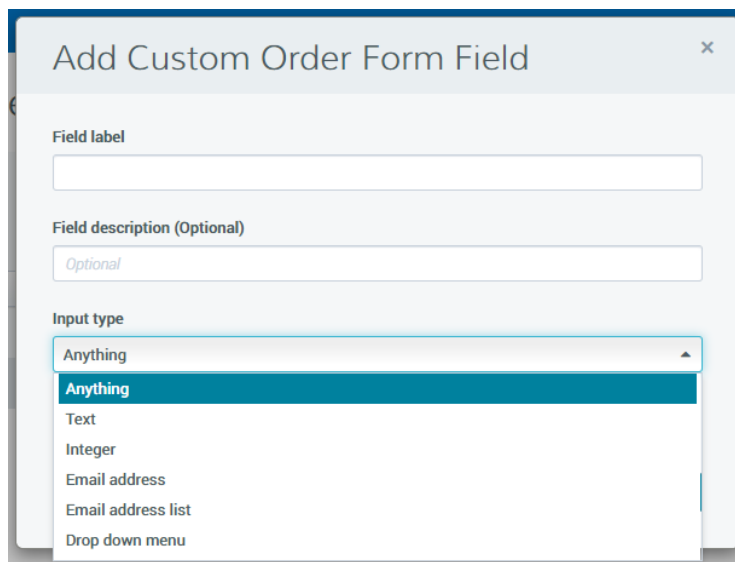
- Individual .crt (zipped)
- Individual .crt (zipped)
- A P7B bundle of all the certs in a .p7b file
- A P7B bundle of all the certs with a .cer extension
- Separate primary and intermediate .crt files (zipped)
- A single .pem file containing all the certs
- A single .pem file containing only the end entity certificate
- A single .pem file containing all the certs except for the root
- Individual .crt files with a .cer extension (zipped)
- Individual .crt files with a .pem extension (zipped)

CertCentral offers a choice of file formats. Once you select the appropriate server platform, a choice of file types will be offered. You can also download the certificate, intermediate certificate and root certificate directly as .pem files.



## Custom order fields

CertCentral allows you to add custom fields to your certificate order forms. The custom field metadata can be used to search or sort a set of certificate orders that match the metadata search criteria.



Custom order forms fields features:

- **Apply to Future and Present Requests:** When you add custom order form fields, the field is also added to pending requests. If the field is required, the pending requests cannot be approved until the field is completed.
- **Apply to Entire Account:** When you add custom order form fields, the fields are applied to the order forms for the entire account. Custom order form fields cannot be set per Division.
- **Apply to All Certificate Types:** When you create custom order form fields, the fields are added to the order forms for all certificate types (SSL, Client, Code Signing, etc.). You cannot add a custom order form field to the order forms for only SSL certificate types, etc.
- **Apply to Guest URLs:** When you add custom order form fields, these fields are added to the certificates ordered from directly inside your CertCentral account as well as from any guest URLs you have sent out.
- **Different Types to Choose From:** When you create custom order form fields, different types of fields can be added such as single line and multiple line text boxes, email address and email address list boxes, etc.
- **Required or Optional :** When you add custom order form fields, you can make them required or optional. Required fields must be completed before the order can be approved. Optional fields can be left blank.
- **Deactivated or Activated:** After you have added a custom order form field, you can deactivate (remove) and activate (add back) the field as needed. Fields that you deactivate are removed from pending requests but not from issued orders. Fields that you activate are added to pending requests. If the field is required, it must be completed before the request can be approved.

Custom field data can be edited at any time before or after a certificate is issued.

More information: <https://docs.digicert.com/manage-account/customize-your-certificate-request-forms/managing-custom-order-form-fields/>

# DIGICERT® CERTIFICATION PROGRAM

## Renewal notification

Certificate Renewal Settings

☐ Enable Escalation

Send request renewal notifications to

fa.machado@digicert.com x paolo.tropea@digicert.com x

Enter additional emails to receive renewal notifications when certificates are about to expire.

When certificates are scheduled to expire in

- ☒ 90 days
- ☒ 60 days
- ☒ 30 days
- ☒ 7 days
- ☒ 3 days
- ☒ 7 days after expiration

Default Renewal Message

Have a blessed day!

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

By default, CertCentral sends certificate renewal notifications 90, 60, 30, 7, and 3 days before a certificate expires and 7 days after a certificate expires. You may want to configure your Certificate Renewal Settings to determine when renewal notifications are sent and which email addresses receive the notifications.

You can configure certificate renewal notifications or escalation renewal notifications:

- **Certificate Renewal Settings:** Allows you to send renewal notifications to the same email addresses at every stage as certificates gets closer to expiration or after they have expired.

Certificate Renewal Settings

☒ Enable Escalation

Days before expiration	Additional email addresses or distribution lists
<input checked="" type="checkbox"/> 90 days	
<input checked="" type="checkbox"/> 60 days	
<input checked="" type="checkbox"/> 30 days	
<input checked="" type="checkbox"/> 7 days	
<input checked="" type="checkbox"/> 3 days	
<input checked="" type="checkbox"/> 7 days after expiration	

Default Renewal Message

Have a blessed day!

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

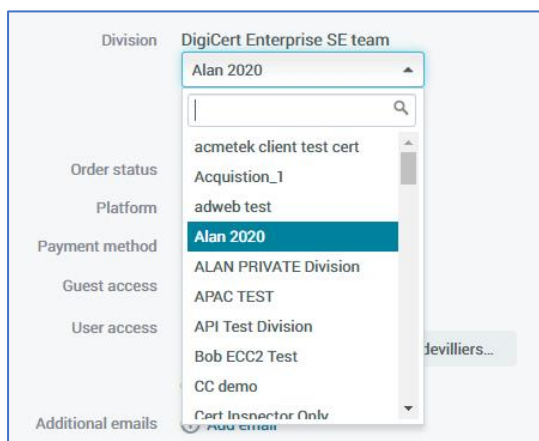
- **Escalation Renewals Settings:** Allows you to determine which email addresses will receive which renewal notifications at each stage as certificates get closer to expiring or after they have expired.

# DIGICERT® CERTIFICATION PROGRAM

## Subaccounts and divisions

### Divisions

Divisions are a feature in CertCentral for restricting users and organizations. You can add users at your organization to your CertCentral account and control their account access through user permissions.



You can provide a division as much freedom as you want, controlling their ability to create and manage users, permissions, domains, and organizations. Unlike subaccounts, you have total visibility and control over the users, orders, settings, and activity of divisions in your account.

Additionally, divisions can share account funds, or each division can have their own funds and pay for only their certificates.

Note that certificate orders can be reassigned to a different division at any time.

More information: <https://docs.digicert.com/manage-account/division-management/>

### Subaccounts

Subaccounts are CertCentral accounts linked to and managed by a top-level 'parent' CertCentral account. Subaccounts let resellers or other organizations give users individual control over a CertCentral account and their certificate management process, while still allowing you, the 'parent' account, to control the product pricing and billing.

Subaccounts are specifically designed for customer-business relationships or other relationships where you need to control the product pricing or billing of orders made by the subaccounts. There are four types of subaccounts:

- Retail
- Enterprise
- Partner
- Managed (usually API only access).

Each account type comes with a different set of CertCentral features available to them. Managed subaccounts are API only accounts intended for integration into an existing user portal and provide the parent with some additional controls such as the ability to download certificates.

Subaccounts can go 3 levels deep, i.e. Parent, child and grandchild.

More information: <https://docs.digicert.com/manage-account/subaccounts-management/>

<https://docs.digicert.com/manage-account/subaccounts-management/creating-and-configuring-subaccount/>

# DIGICERT® CERTIFICATION PROGRAM

## User roles

User access

Username

☐ Only allow this user to log in through SAML SSO

☐ Restrict this user to specific divisions

Role

☒ Standard User  
Access to place and manage orders, with changes being approved by a manager or administrator

☐ Limit to placing and managing their own orders

☐ Manager  
Access to manage finances, create and approve requests, manage orders and domains, and to view and edit users

☐ Finance Manager  
Access to manage finances, and to place and manage orders

☐ Administrator  
Full administrative access, including access to create divisions and users, and to manage user access

Account administrators do not assign individual permissions to a user. Instead, they assign each user a role:

- Administrator
- Standard User
- Limited User
- Finance Manager
- Manager

The role assigned to the user determines which account features they can access.

The main roles are:

- Standard User: Access to place and manage orders, with changes being approved by a manager or administrator
- Manager: Access to manage finances, create and approve requests, manage orders and domains, and to view and edit users
- Finance Manager: Access to manage finances, and to place and manage orders
- Administrator: Full administrative access, including access to create divisions and users, and to manage user access

To create a Limited User role, select Standard User and check the box “Limit to placing and managing their own orders”.

More details are given below.

<b>Administrator</b>	Full CertCentral account access with these permissions: <ul style="list-style-type: none"><li>• Access and manage Discovery.</li><li>• Manage divisions (create and edit) and account users (create, delete, and edit).</li><li>• Manage organizations (add new organizations), domains (add or deactivate), guest requests, and API access.</li><li>• View all certificate requests and certificate orders, request certificates, approve certificate requests, and run order reports.</li><li>• Manage account finance settings and finances (view balance history, run spending reports, deposit funds, and more).</li><li>• Manage account settings (authentication settings, IP access restrictions, product restrictions, and more), audit settings, and audit logs.</li></ul>
<b>Standard User</b>	Account users with these permissions:

# DIGICERT® CERTIFICATION PROGRAM

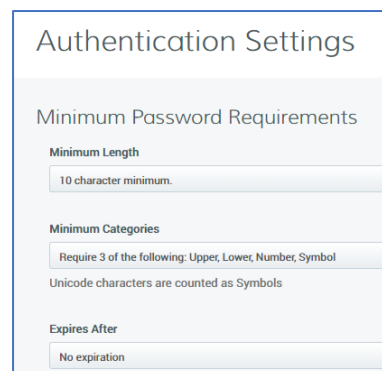
	<ul style="list-style-type: none"> <li>• Request certificates.</li> <li>• Monitor certificate requests and orders (their own and others).</li> <li>• A manager or administrator must approve changes.</li> </ul>
<b>Limited User</b>	<p>Account users with these permissions:</p> <ul style="list-style-type: none"> <li>• Request certificates.</li> <li>• Monitor their own certificate requests and orders.</li> <li>• A manager or administrator must approve changes.</li> </ul>
<b>Finance Manager</b>	<p>Limited account users whose primary role is to manage account finances. Includes these permissions:</p> <ul style="list-style-type: none"> <li>• View balance history, spending reports, and account pricing.</li> <li>• Manage purchase orders and deposit funds.</li> <li>• Manage order reports.</li> <li>• Request certificates.</li> <li>• Monitor their own certificate requests and orders.</li> </ul>
<b>Manager</b>	<p>Limited account users whose primary role is to help manage the account. Includes these permissions:</p> <ul style="list-style-type: none"> <li>• Access and manage Discovery.</li> <li>• View divisions and manage account users (edit).</li> <li>• View organizations and manage domains (add or deactivate).</li> <li>• View all certificate requests and certificate orders, request certificates, approve certificate requests, and run order reports.</li> <li>• Manage account finance settings and finances (view balance history, run spending reports, deposit funds, and more).</li> <li>• Manage audit settings and audit logs.</li> </ul>

All user roles can be restricted to working with certificates in specified divisions.

By default, Administrators and Managers do not have permission to approve EV Certificate, EV Code Signing Certificate, or Code Signing Certificate requests. To approve these types of requests, the manager must be assigned the appropriate subroles.

More information: <https://docs.digicert.com/manage-account/certcentral-user-roles-account-access/roles-account-access/>

## User access/authentication control methods



Authentication Settings

Minimum Password Requirements

Minimum Length

10 character minimum.

Minimum Categories

Require 3 of the following: Upper, Lower, Number, Symbol

Unicode characters are counted as Symbols

Expires After

No expiration

### Passwords

Minimum password requirements can be set from the CertCentral portal.

### Two-Factor Authentication

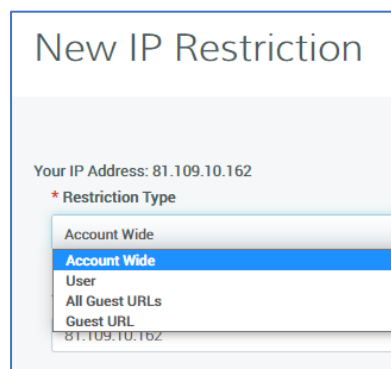
To add a second form of identity verification to your sign in process, you need to configure the two-factor authentication requirements for your account. You can configure a requirement for all users and for individual users as needed.

In addition to the User ID/Password requirement, users can be required to use one of the following factors:

- One-Time Password (OTP): Applying this rule will require users to initialize their OTP app or device and generate a one-time password the next time they sign in. OTP authentication requires the use of any mobile app that supports the Time-Based One-Time Password (TOTP) protocol.
- Client Certificate: Applying this rule will require users to generate a client certificate in their browser the next time they sign in. Internet Explorer (Windows) and Safari (Mac) are the only browsers that support client certificate generation.

More information: <https://docs.digicert.com/manage-account/certcentral-two-factor-authentication/configure-two-factor-authentication-requirements/>

### IP restrictions



New IP Restriction

Your IP Address: 81.109.10.162

\* Restriction Type

Account Wide

Account Wide

User

All Guest URLs

Guest URL

81.109.10.162

For increased security, DigiCert offers the ability to restrict your account so that it can only be accessed from certain IP addresses. These can be set:

- Account Wide
- Per User
- Per Guest URL
- For all Guest URLs

### Single Sign-On

Remove the need for multiple passwords and use SAML Single-Sign-On (SSO) to connect your identity provider (IdP) with CertCentral.

Once you've configured the SAML-to-CertCentral connection, your CertCentral users can use their SSO credentials to sign in. They will access the SSO account sign in page via a service provider initiated custom SSO URL that DigiCert provides or an IDP initiated SSO URL that you provide.

More information: <https://docs.digicert.com/manage-account/saml-single-sign-on-admin-guide/>

# DIGICERT® CERTIFICATION PROGRAM

## Guest access options

### Guest URL

The screenshot displays the Digicert CertCentral Enterprise web interface. On the left is a dark sidebar with navigation links: REQUEST A CERTIFICATE, DASHBOARD, CERTIFICATES, DISCOVERY, AUTOMATION, FINANCES, REPORTS (with a 'Preview' button), SUBACCOUNTS, ACCOUNT, Users, Divisions, Guest Access (highlighted), Audit Logs, and User Invitations. The main content area is titled 'Guest access' and includes a sub-section 'Guest URLs' with the description 'Allow your users to request certificates without a CertCentral account' and an 'Add Guest URL' button. Below this is a table with columns 'Name' and 'OV cert 1 year', containing entries 'test2' and 'test'. A modal window titled 'Add Guest URL' is open on the right. It contains the following fields: 'Name' (text input), 'Division' (dropdown menu), 'Default language' (dropdown menu set to 'English'), 'Allowed certificate types' (dropdown menu), and 'Certificate validity periods' (dropdown menu). A light blue information box states: 'At the time an order is placed, certificate availability and validity periods will be subject to industry standards for each certificate type, as well as your account's Product Settings.' Below the modal, the text 'When requesting a certificate via this guest URL:' is followed by a 'Transaction summary' section with a checked checkbox for 'Hide contract information' and a 'Domains' section with unchecked checkboxes for 'Hide existing domains' and 'Hide domain control validation (DCV) methods'.

A Guest URL lets you provide a guest user with the ability to request a certificate without adding them to your account. Guest URLs only give users access to a specific certificate request page within the account. The user cannot access anything else within the account.

Guest URLs are configured with the following details:

- Name
- Division
- Allowed Certificate Types
- Certificate Validity Periods

More information: <https://docs.digicert.com/manage-account/managing-guest-urls/>

# DIGICERT® CERTIFICATION PROGRAM

## Guest access

The screenshot shows the 'Guest access' settings page. At the top, it says 'Guest access' and 'Allow your users to access orders without a CertCentral account.' Below this, there is a 'Guest access link' field containing the URL 'https://www.digicert.com/account/guest-access/?c=s/m4c' and a status 'Enabled'. Under 'Guest access settings', there are four checkboxes, all of which are checked: 'Enable', 'Organization contact', 'Technical contact', 'Guest URL requester (subscriber)', and '"Additional emails" listed on order'. A 'Save Settings' button is at the bottom.

Guest access allows a person to manage their order without a CertCentral login. With their email address and order number (or FQDN in the certificate), they can download, reissue, or revoke their certificate. Guest access can be

enabled for all orders across your account, or on individual orders.

You can control what order contacts are eligible for Guest access by enabling or disabling the Organization contact, Technical contact, Guest URL requester (subscriber) (the email address that placed the order), and "Additional emails" listed on order checkboxes.

Your CertCentral account has a unique Guest access login page. To confirm your person's identity, an authentication email is sent by CertCentral that provides access for two hours.

The screenshot shows the Digicert Guest portal login page. The header includes the Digicert logo, a phone number '1.801.701.9600', and links for 'Support' and 'English'. The main content area has a large blue shield icon with a checkmark and the text 'View and manage your orders.' To the right, it says 'Welcome to the guest portal' and 'Manage existing orders without a CertCentral account.' Below this are two input fields: 'Email address' and 'Order ID or common name/SAN'. A 'Continue' button is below the second field. At the bottom, there is a link: 'Have a CertCentral account? Sign in'.

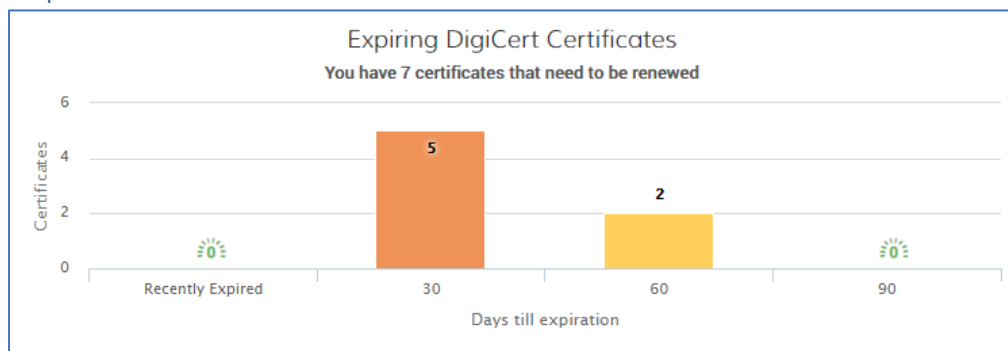
More information: <https://docs.digicert.com/manage-account/guest-access/>



# DIGICERT® CERTIFICATION PROGRAM

## Reports & Notifications

### Reports



CertCentral provides dashboards and reports within the console or via APIs.

Dashboard: A graphically

organized view of your certificates, including expiring certificates and pending requests.

Orders

Request a certificate ▾ Orders report Download CSV ▾

Download All Records  
Download Filtered Records

⚠ 2 certificates are expiring within the next 60 days. View Certificates

⚠ 5 certificates are expiring within the next 30 days. View Certificates

Show certificates issued from Division Status Search

All Unfiltered Unfiltered Search for... Go

+ Show advanced search

Orders Report: Find all certificates issued and filter by any field.

### Email Notifications

CertCentral sends out emails to users throughout the order/approval process, and when a certificate is expiring or has expired. You can customize these email templates so they suit your account or organization's needs.

Edit template

Name: Order confirmation email Language: English

Description: To advise that a user placed an order

Customize email content

Note: Control email recipients at the account level. Go to Notifications > Basic notification settings > General notification settings.

Subject: A @request\_type@ certificate has been requested for @common\_name@

Body: A @request\_type@ certificate for @common\_name@ has been requested by @requester\_first\_name@ @requester\_last\_name@ @requester\_email@ on @request\_date@. Notice: the request was placed through a Guest URL and not by a CertCentral user. <br /> <strong>Certificate Details</strong> <br /> Account ID: @account\_id@ <br /> Division: @division\_name@ <br /> Product: @product\_name@ <br /> Common Name: @common\_name@ <br /> #PSANs: @psans@ <br /> #Organization name: @organization\_name@ <br /> #Validity years: @validity\_years@

Preview

Available variables for this template

Copy the variable from below and paste the text where you want to insert the variable

Approval url: @approval\_url@

Common name: @common\_name@

Guest request: @guest\_request@

Request type: @request\_type@

Requester email: @requester\_email@

**Basic notification settings** allows you to specify the email recipients and the email language.

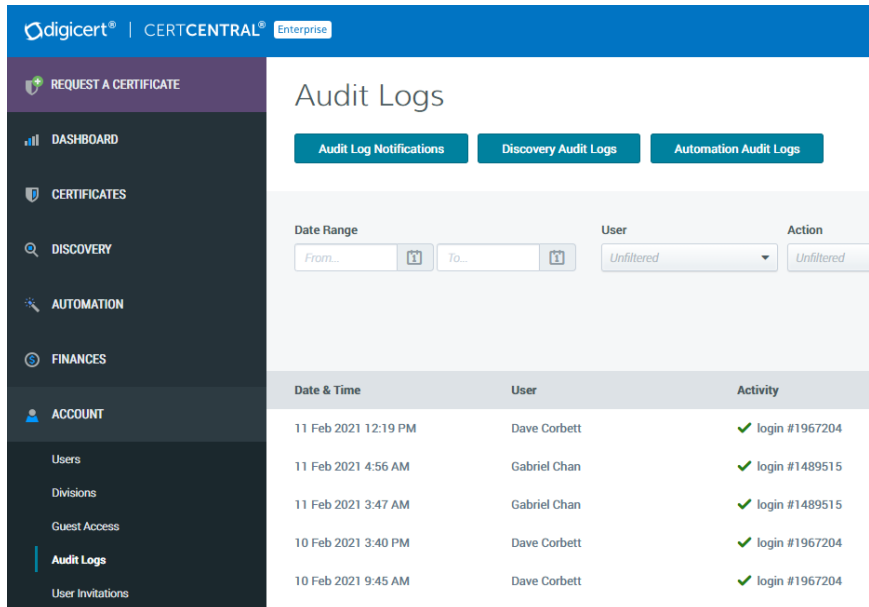
**Custom email templates** allows you to edit the standard email templates.

More information:

<https://docs.digicert.com/manage-account/account-notifications/customize-email-templates/>

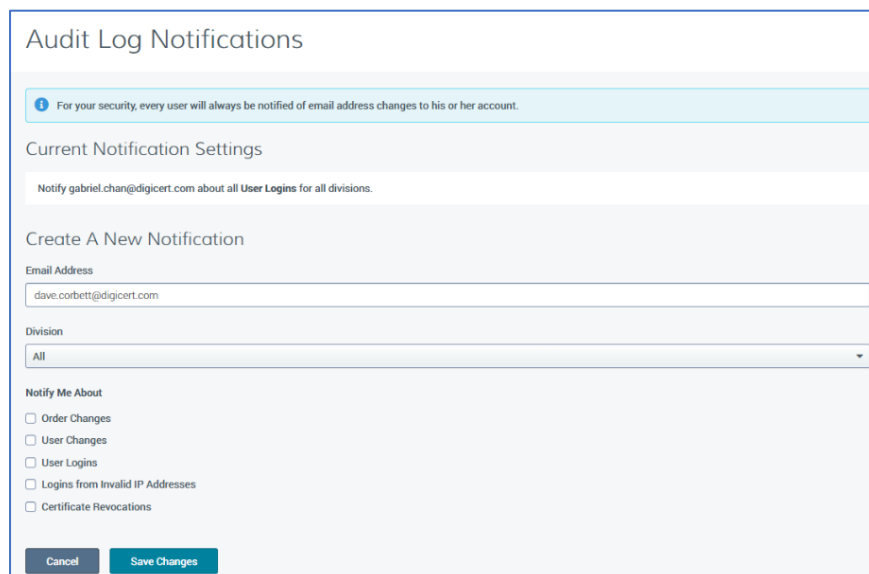
# DIGICERT® CERTIFICATION PROGRAM

## Audit logging



Date & Time	User	Activity
11 Feb 2021 12:19 PM	Dave Corbett	✓ login #1967204
11 Feb 2021 4:56 AM	Gabriel Chan	✓ login #1489515
11 Feb 2021 3:47 AM	Gabriel Chan	✓ login #1489515
10 Feb 2021 3:40 PM	Dave Corbett	✓ login #1967204
10 Feb 2021 9:45 AM	Dave Corbett	✓ login #1967204

Audit logs are a history of actions that occur in your account. CertCentral automatically keeps audit logs that record more than 50 different actions in your account (including sign ins, certificate requests, and revocations), along with the time stamp and user who performed the action. To see the audit logs in your account, visit the Audit Logs page.



**Audit Log Notifications**

For your security, every user will always be notified of email address changes to his or her account.

**Current Notification Settings**

Notify gabriel.chan@digicert.com about all User Logins for all divisions.

**Create A New Notification**

Email Address: dave.corbett@digicert.com

Division: All

**Notify Me About**

- ☐ Order Changes
- ☐ User Changes
- ☐ User Logins
- ☐ Logins from Invalid IP Addresses
- ☐ Certificate Revocations

Cancel Save Changes

Clicking on **Audit Log Notifications** to create email notifications for specific events.