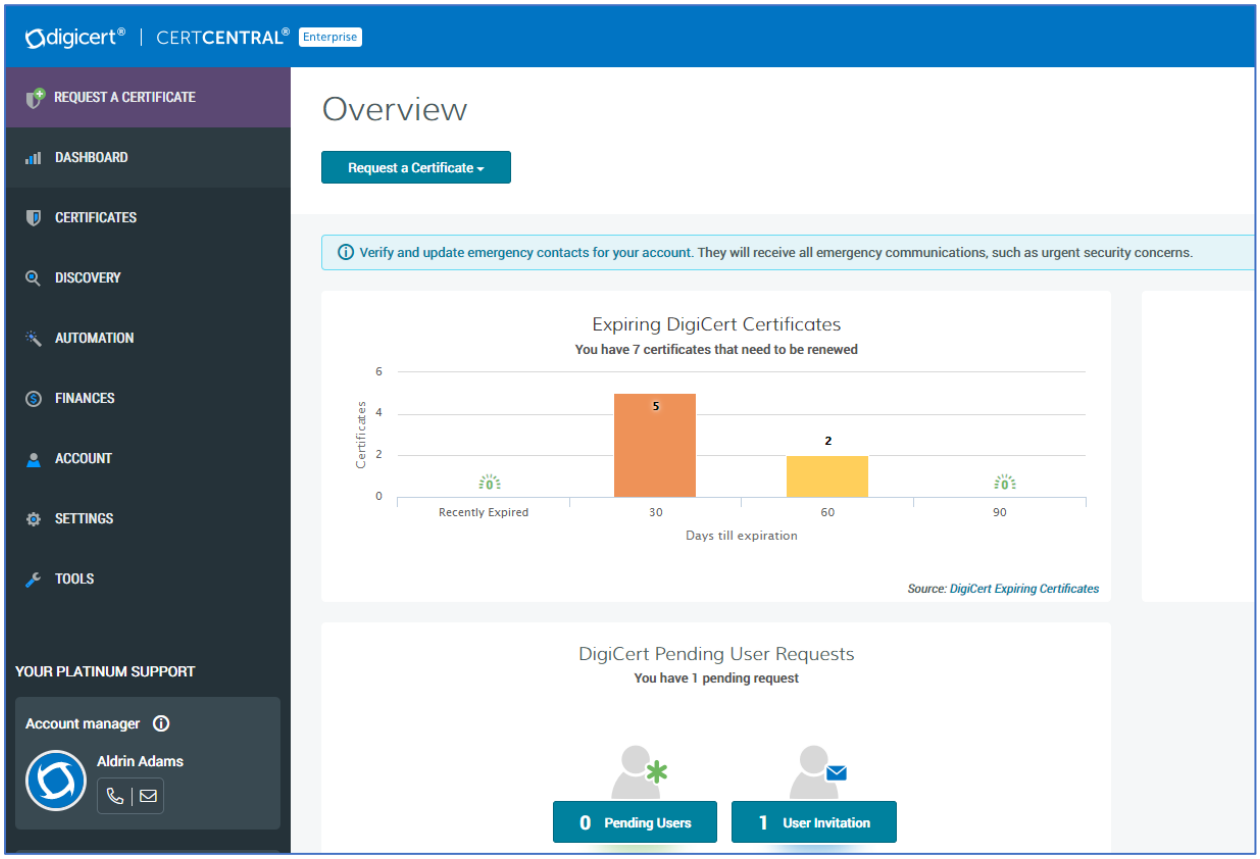
DigiCert® Technical Certifications CertCentral® Studienleitfaden

2021 v2



© 2021 DigiCert, Inc. alle Rechte vorbehalten. DigiCert ist eine eingetragene Marke von DigiCert, Inc. in den USA und anderswo. Alle anderen Marken und eingetragenen Marken sind das Eigentum ihrer jeweiligen Inhaber.

Contents

Einführung 4
Zielsetzungen 5
Produkte für SSL/TLS-Zertifikate 6
Flex-Zertifikate 6
Multi-year Plan 7
Vorteile des Secure Site-Zertifikats 7
DigiCert Smart-Siegel 9
Optionen für das Zertifikatsprofil 10
Produkte mit Code Signing-Zertifikat 11
Produkt-Einstellungen 12
Validierung von Bereichen und Organisationen 12
Validierung der Bereichskontrolle (DCV) 12
Validierung der Organisation 13
Verwaltung von Aufträgen und Zertifikaten 14
Genehmigung der Zertifikatsanforderung 16
Duplikate 17
Neuausstellung des Zertifikats 17
Herunterladen eines Zertifikats 17
Benutzerdefinierte Auftragsfelder 18
Renewal-Mitteilung 19
Unterkonten und Abteilungen 20
Abteilungen 20
Unterkonten 20
Benutzerrollen 21
Methoden zur Kontrolle des Benutzerzugangs/der Benutzerauthentifizierung 23
Passwörter 23
Zwei-Faktoren-Authentifizierung 23
IP-Beschränkungen 24
Einzelanmeldung 24
Optionen für den Gastzugang 25
Guest-URL 25
Guest Access 26
Berichte und Benachrichtigungen 27

Berichte 27
E-Mail-Benachrichtigungen 27
Audit-Protokollierung 28

Einführung

Dieses Studienhandbuch soll Ihnen helfen, sich auf die ‚DigiCert Technical Certification: CertCentral Professional Assessment-Prüfung' vorzubereiten. Die Prüfung besteht aus 50 Multiple-Choice-Fragen, für die maximal 1 Stunde Zeit zur Verfügung steht.

Dieses Trainingsprogramm richtet sich an alle, die mit der DigiCert CertCentral-Zertifikatsverwaltungsplattform arbeiten (technischer Support, SSL/TLS-Administrator usw.).

Bevor Sie am Certification Assessment teilnehmen, sollten Sie sich die unten aufgeführten Lerninhalte ansehen. Eine Teilnahme am Trainingsprogramm ist keine bindende Voraussetzung, um sich für die Prüfung anzumelden.

Es wird jedoch dringend empfohlen, sich mit allen Lerninhalten zu befassen, um sich vollständig auf die Prüfung vorzubereiten.

Weitere Informationen finden Sie im CertCentral Professional Training Guide, den Sie unter https://www.digicert.com/tls-ssl/tls-certification-program herunterladen können

Darüber hinaus bieten wir Ihnen die Möglichkeit, an einem DigiCert-Workshop teilzunehmen. Dieser Kurs beinhaltet ausführliche Informationen zu den Lerninhalten, um Sie optimal auf die Prüfung vorzubereiten. Bitte wenden Sie sich an Ihren DigiCert-Kundenbetreuer, um mehr darüber zu erfahren.

Zielsetzungen

Folgende Lerninhalte sind Bestandteil der ‚DigiCert Technical Certification: CertCentral Professional Assessment-Prüfung':

- Beschreiben der in DigiCert CertCentral Enterprise verfügbaren SSL/TLS- und Code Signing-Zertifikatsprodukte
- Beschreiben Sie die Produkteigenschaften für Business SSL-Zertifikate, z. B. CT-Protokollüberwachung, Malware-Scanning, DigiCert Smart Seal
- Beschreiben Sie die in DigiCert CertCentral verfügbaren Zertifikatsprofiloptionen, z. B. HTTP Signed Exchange
- Beschreiben Sie die Richtlinien und Methoden, die DigiCert für die Validierung von Domänen und Organisationen verwendet
- Beschreiben der Benutzerrollen in DigiCert CertCentral
- Verwaltung von Aufträgen, Zertifikaten, Organisationen und Domänen in DigiCert CertCentral
- Methoden zur Benutzerzugangs-/Authentifizierungskontrolle in DigiCert CertCentral, z. B. SAML, 2FA
- Verwendung von Unterkonten und Abteilungen in DigiCert CertCentral
- Beschreiben Sie die in DigiCert CertCentral verfügbaren Berichtsoptionen
- DigiCert CertCentral Guest Access Optionen: Guest URL und Guest Access Merkmale

Produkte für SSL/TLS-Zertifikate

Die meisten Unternehmen verwenden die DigiCert-Produktreihe der Business SSL-Zertifikate:

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

Diese Zertifikatsprodukte bieten zahlreiche Optionen und Vorteile:

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

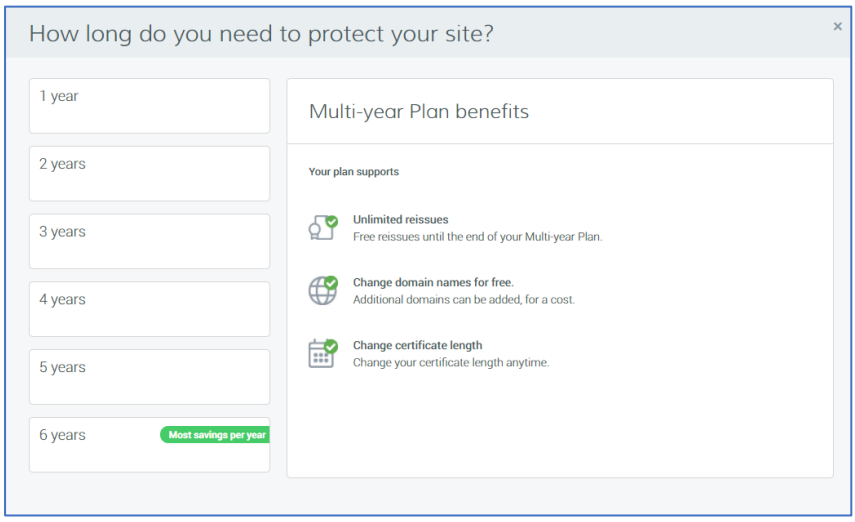
Flex-Zertifikate

DigiCert Secure Site- und Secure Site Pro-Zertifikate unterstützen jede Art von Domain-Konfiguration und können als Single-Domain- oder Multi-Domain-Zertifikate mit jedem gewünschten Domain-Namen (FQDN) und Wildcard-SANs bestellt werden.

Während der Laufzeit des Zertifikats können weitere SANs hinzugefügt, ohne dass Sie das Produkt wechseln müssen. Für diese Zertifikate gibt es keine speziellen Multi-Domain- oder Wildcard-Versionen, sondern Sie fügen diese Ihrem Zertifikat hinzu. Dies gibt Ihnen die Flexibilität, die Sie benötigen.

Weitere Informationen: https://docs.digicert.com/manage-certificates/flex-certificates/

Multi-year Plan



Der DigiCert Multi-year Plan ermöglichen es Ihnen, einen Preis für bis zu sechs Jahre SSL/TLS-Zertifikatsabdeckung zu zahlen. Bei den Mehrjahresplänen wählen Sie das SSL/TLS-Zertifikat, den gewünschten Zeitraum (bis zu sechs Jahre) und die Gültigkeit des Zertifikats. Bis zum Ablauf des Plans stellen Sie Ihr Zertifikat jedes Mal kostenlos neu aus, wenn es das Ende seiner Gültigkeitsdauer erreicht. Beachten Sie, dass die maximale Gültigkeitsdauer für ein öffentlich vertrauenswürdiges SSL/TLS-Zertifikat derzeit 397 Tage beträgt, so dass Sie ein solches Zertifikat während eines Mehrjahresplans möglicherweise mehrmals neu ausstellen müssen.

Wenn Sie Zertifikate für einen DigiCert Multi-year Plan neu ausstellen, haben Sie folgende Möglichkeiten:

- Legen Sie ein neues Ablaufdatum für das neu ausgestellte Zertifikat fest: Die maximale Gültigkeitsdauer für ein neu ausgestelltes Zertifikat entspricht der maximalen Zertifikatslaufzeit, die in den Basisanforderungen des CA/B-Forums festgelegt ist, oder dem Ende des DigiCert Multi-year Plan, je nachdem, was früher eintritt.
- Domains ändern oder entfernen: Das Entfernen und Ändern von Domains erfordert, dass DigiCert alle zuvor ausgestellten Zertifikate widerruft. DigiCert wartet 48-72 Stunden, bevor es das Originalzertifikat und alle vorhandenen Duplikate und Neuausstellungen widerruft.
- Domains hinzufügen: Das Hinzufügen von Domains kann zusätzliche Kosten verursachen. Die Preise für neue Domains werden anteilig berechnet auf Grundlage der Restlaufzeit des Multi-year Plan.

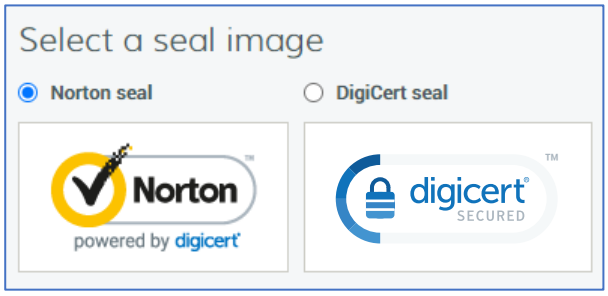
Weitere Informationen: https://docs.digicert.com/manage-certificates/multi-year-plans/

Vorteile des Secure Site-Zertifikats

Neben der 2048-Bit-Verschlüsselung bieten DigiCert Secure Site-Zertifikate zusätzliche Vorteile, wie z. B. einen priorisierten Support. Diese Vorteile gelten für die gesamte Laufzeit Ihrer Zertifikatsbestellung. Jedes Mal, wenn Sie die Bestellung des Secure Site-Zertifikats erneuern, werden Ihre Vorteile automatisch auf Ihre neue Bestellung übertragen.

- Priorisiert Validierung - Secure-Site-Bestellungen werden an den Anfang unserer Validierungswarteschlangen gestellt, damit unsere Mitarbeiter diese Bestellungen zuerst bearbeiten können.

- Prioritäts-Support - Secure Site-Zertifikate haben Zugang zu zwei Prioritäts-Support-Kanälen, damit unser Support-Team zuerst auf Ihre Bedürfnisse reagieren kann: Bestell- und Validierungsstatus sowie Installation und Konfiguration.
- Premium Site-Seals - Secure Site-Zertifikate werden mit den beiden anerkanntesten Vertrauenssiegeln im Internet ausgeliefert: DigiCert und Norton. Wählen Sie das Premium-Site-Seal, das Sie für Ihre Website verwenden möchten.



- CT (Certificate Transparency)-Log-Monitoring - Das CT-Log-Monitoring ermöglicht Ihnen die Überwachung der öffentlichen CT-Logs für SSL/TLS-Zertifikate, die für die Domänen auf Ihrem Secure Site Pro- oder Secure Site Pro EV-Zertifikat ausgestellt wurden. Nachdem Sie die CT Log-Überwachung für eine Secure Site Pro-Zertifikatsbestellung aktiviert haben, erhalten Sie zwei Arten von E-Mail-Benachrichtigungen: Tägliche CT Log-Zusammenfassung und bei Bedarf, dringende Benachrichtigungen. Diese werden an die Kontoverwalter gesendet, so dass sie die CT-Protokolle für ihre Domänen überprüfen können, ohne sich jeden Tag bei ihrem CertCentral-Konto anmelden zu müssen. Das CT-Log-Monitoring zeigt die entdeckten SSL/TLS-Zertifikate in Ihrem CertCentral-Konto, wo Sie Details zu den Zertifikaten einsehen können, um etwaige falsch ausgestellte Zertifikate für Ihre Domains schnell zu identifizieren. Sie können auch Kopien der Nicht-DigiCert-Zertifikate direkt von Ihrem CertCentral-Konto herunterladen. Weitere Informationen: https://docs.digicert.com/certificate-tools/ct-log-monitoring-service/
- Vulnerability Assessment - Secure Site EV-, Secure Site Pro SSL- und Secure Site Pro EV-Zertifikate beinhalten den Zugang zu einem Vulnerability Assessment. Dieser Dienst ermöglicht es Ihnen, Schwachstellen auf Ihrer Website zu erkennen und zu beseitigen. Weitere Informationen finden Sie unter https://docs.digicert.com/certificate-tools/vulnerability-assessment-service/.
- Malware-Check - Secure Site-Zertifikate werden mit einem Zugang zu einem VirusTotal-Malware-Check geliefert. Analysieren Sie Ihre öffentlichen Domains schnell mit mehr als 70 Antiviren-Scannern und URL/Domain-Blacklist-Diensten. Nutzen Sie die Scan-Ergebnisse, um Malware-Bedrohungen zu identifizieren, damit Sie Maßnahmen ergreifen können, um Ihre Website vor Blacklists zu schützen, die die Verfügbarkeit der Website und die Online-Einnahmen beeinträchtigen können.
- Post-Quantum-Kryptographie (PQC) - Kunden, die eine Secure Site Pro SSL oder Secure Site Pro EV SSL erwerben, haben Zugriff auf das Post-Quantum-Kryptographie-Toolkit (PQC) von DigiCert. Weitere Informationen: https://docs.digicert.com/certificate-tools/post-quantum-cryptography/
- Branchenführende Garantien - Secure Site-Zertifikate beinhalten Garantien, die Sie und Ihre Kunden schützen: eine $1,75 Mio. oder $2 Mio. Netsure Protection Warranty für Ihr Unternehmen und eine branchenweit führende $2 Mio. Relying Party Warranty für Ihre Kunden.

DigiCert Smart-Siegel

Das DigiCert Smart Seal ist ein neues dynamisches Website-Siegel, das Website-Besuchern die Gewissheit gibt, dass ihre Daten im Internet sicher sind. Echtzeit-Sicherheitsindikatoren, die durch verschiedene Mikrointeraktionen aktiviert werden, weisen die Besucher darauf hin, dass das Siegel aktiv auf der Seite vorhanden ist, die Website validiert wurde und durch ein aktives Zertifikat der weltweit vertrauenswürdigsten Zertifizierungsstelle geschützt ist.

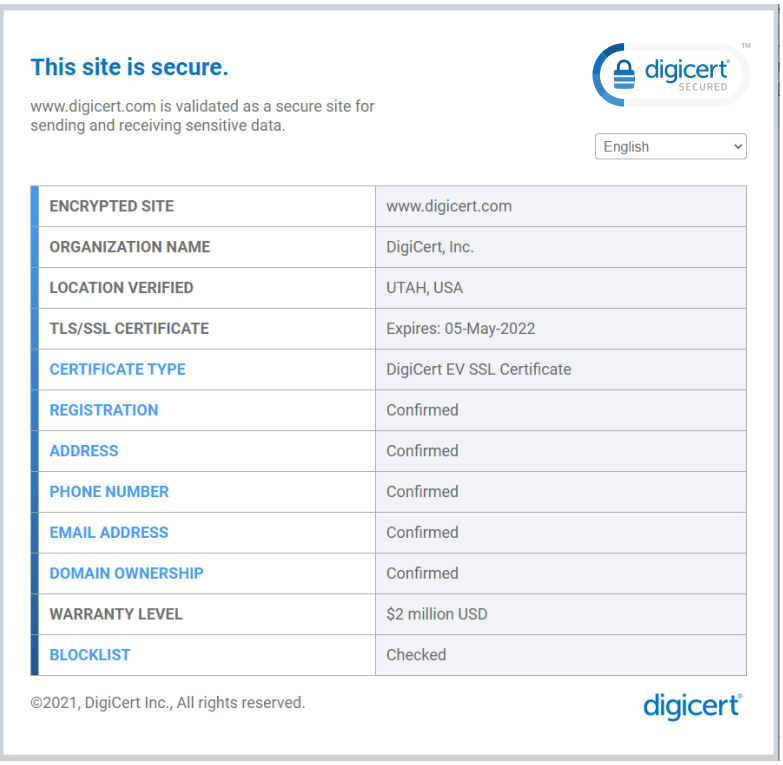
Wenn man mit dem Mauszeiger über das DigiCert Smart Seal fährt, erscheint das Logo des Unternehmens (sofern es hochgeladen und von DigiCert überprüft wurde) und nützliche Informationen über die Sicherheit der Website direkt auf dem Siegel. So müssen die Besucher der Seite diese nicht mehr verlassen, um die Legitimität einer Website zu überprüfen.

Das Smart Seal kann so konfiguriert werden, dass die folgenden Optionen auf der Informationsseite angezeigt werden:

Malware-Scan: Fügen Sie das Datum des zuletzt durchgeführten Malware-Scans hinzu. Website-Besucher können sehen, dass Sie Ihre Website auf Viren und Malware überwachen.

CT-Protokollüberwachung: Fügen Sie das Datum hinzu, an dem Sie die CT-Protokollüberwachung für die Domain Ihrer Website aktiviert haben. Website-Besucher können sehen, dass Sie die Transparenzprotokolle überwachen, so dass Sie schnell handeln können, wenn Betrüger ~~böser Akteur~~ unbefugt ein Zertifikat für Ihre Domain ausstellen. Diese Funktion ist nur für Secure Site Pro-Zertifikate verfügbar.

Blockliste: Fügen Sie eine Blocklistenprüfung hinzu. Website-Besucher können sehen, dass Ihr Unternehmen von staatlichen und länderspezifischen Sperrlisten befreit ist.



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.

PCI-Compliance-Scan: Fügen Sie das Datum des zuletzt durchgeführten PCI-Compliance-Scans hinzu. Website-Besucher können sehen, dass Sie Ihre Website überwachen, um sicherzustellen, dass diese mit den PCI DDS-Standards konform ist. Diese Funktion ist nur für Secure Site Pro- und Secure Site EV-Zertifikate verfügbar und setzt voraus, dass der Vulnerability Assessment Dienst für Ihre Zertifikatsbestellung aktiviert ist.

Verifizierter Kunde: Zeigt an, wie lange Sie bereits Kunde von DigiCert sind. Website-Besucher können sehen, wie lange Sie bereits einen der vertrauenswürdigsten Namen für TLS/SSL-Zertifikate zum Schutz Ihrer Websites verwenden.

Optionen für das Zertifikatsprofil

Zertifikatsprofile ermöglichen es Ihnen, Zertifikate an Ihre Anforderungen anzupassen, z.B. können Sie ein zusätzliches Feld in Ihr Zertifikat aufzunehmen, oder eine zusätzliche x.509-Erweiterung einzufügen.

- OCSP Must-Staple: Ermöglicht es Ihnen, die OCSP Must-Staple-Erweiterung in OV- und EV SSL/TLS-Zertifikate aufzunehmen. Browser mit OCSP Must-Staple-Unterstützung können Benutzern, die auf Ihre Website zugreifen, ein blockierendes Interstitial anzeigen. Stellen Sie vor der Installation des Zertifikats sicher, dass Ihre Website so konfiguriert ist, dass sie OCSP-Antworten ordnungsgemäß und zuverlässig verarbeiten kann.
- HTTP Signed Exchange: Ermöglicht es Ihnen, die CanSignHTTPExchanges-Erweiterung in ein OV- und EV-SSL/TLS-Zertifikat aufzunehmen. Die Erweiterung HTTP Signed Exchange wird derzeit entwickelt. Im Zuge der Weiterentwicklung innerhalb der Branche kann immer wieder zu Anpassungen der Anforderungen kommen.
- Delegated Credentials: Ermöglicht die Erweiterung ‚DelegationUsage' in OV- und EV-SSL/TLS-Zertifikate. Die Delegated Credentials für TLS-Erweiterung wird derzeit von der Internet Engineering Task Force (IETF) aktiv entwickelt. Im Zuge der Weiterentwicklung innerhalb der Branche kann immer wieder zu Anpassungen der Anforderungen kommen.
- Data Encipherment: Ermöglicht es Ihnen, die EKU Data Encipherment in OV- und EV-SSL/TLS-Zertifikate aufzunehmen. Dies wird benötigt, wenn Sie den öffentlichen Schlüssel des Zertifikats zur Verschlüsselung von Benutzer- und Anwendungsdaten verwenden möchten.

Weitere Informationen: https://docs.digicert.com/manage-certificates/certificate-profile-options/

Produkte mit Code Signing-Zertifikat

Ein DigiCert Code Signing-Zertifikat erhöht das Vertrauen, indem es die Quelle und Integrität Ihrer Anwendung verifiziert.

- Signiert ein Programm digital, um zu beweisen, dass es nicht verändert oder kompromittiert wurde.
- Unterstützt Microsoft Authenticode, Office VBA, Java, Adobe AIR, Apples Mac OS und Mozilla-Objekte
- Vermeidet unnötige Warnmeldungen und stellt sicher, dass Ihren Anwendungen vertraut werden kann

Ein DigiCert EV Code Signing-Zertifikat bietet neben den Standard-Features folgende Vorteile.

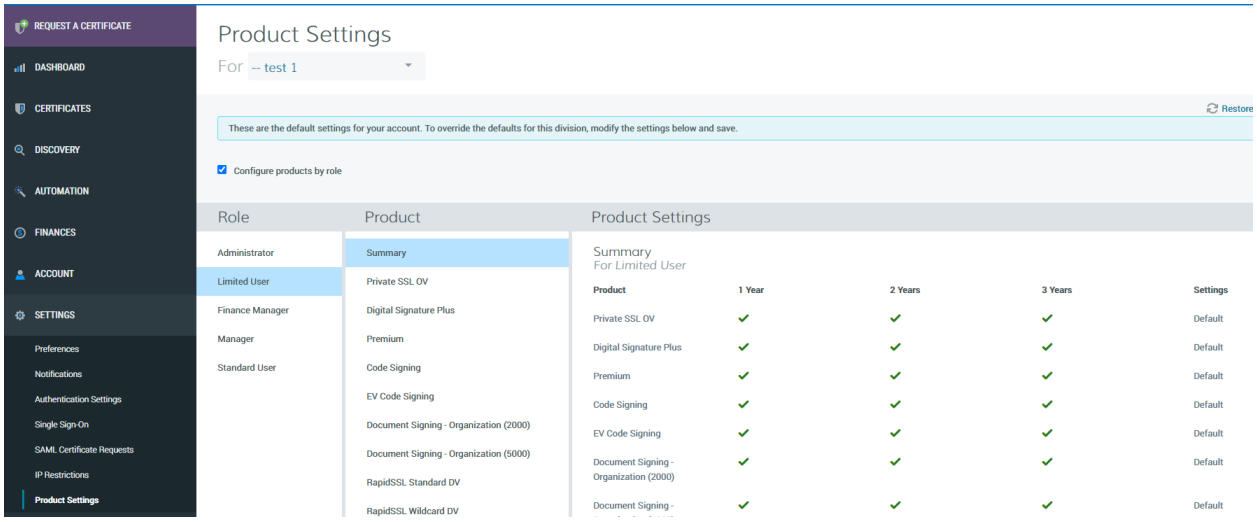
- Kombiniert die Vorteile eines Standard Code Signing-Zertifikats mit einem strengen Extended Validation-Prozess
- Bietet Kompatibilität und gewährt sofortige Reputation mit Windows-Betriebssytemen und beseitigt Warnmeldungen
- Unterstützt Microsoft Authenticode, Office VBA, Java, Adobe AIR, Apples Mac OS und Mozilla-Objekte
- Die erweiterte Validierung gewährleistet eine zusätzliche Überprüfung der Organisation, um Ihre Benutzer und Ihren Ruf zu schützen.
- Umfasst Zwei-Faktor-Authentifizierung für mehr Sicherheit

Ein DigiCert EV Code Signing-Zertifikat kann mit den folgenden Optionen bereitgestellt werden:

- Vorkonfigurierter Hardware-Token: DigiCert installiert Ihr EV CS-Zertifikat auf einem sicheren Token und sendet Ihnen diesen mit Anweisungen zur Aktivierung zu.
- Vorhandener Token: Nachdem DigiCert Ihr EV CS Zertifikat ausgestellt hat, müssen Sie das Zertifikat auf Ihrem Token installieren.
- HSM: Nachdem DigiCert Ihr EV CS-Zertifikat ausgestellt hat, installieren Sie es auf Ihrem HSM-Gerät. (Hinweis: Sie müssen ein FIPS 140-2 Level 2 oder Common Criteria EAL4+ konformes Gerät besitzen).

Weitere Informationen: https://docs.digicert.com/manage-certificates/code-signing-certificate/

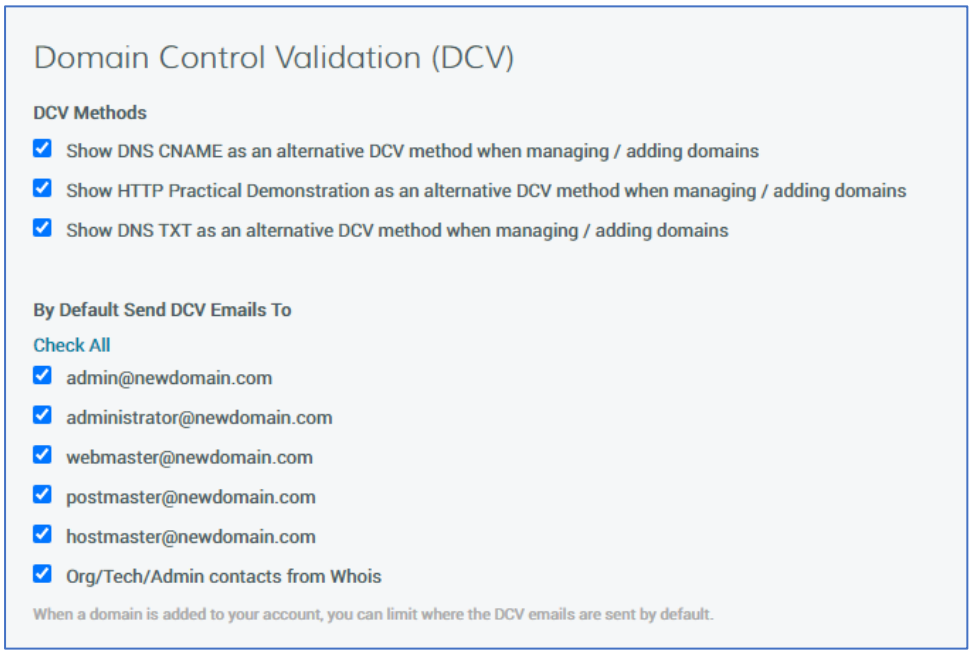
Produkt-Einstellungen



Auf der Seite Produkteinstellungen können Sie konfigurieren, welche Zertifikatsprodukte pro Konto oder pro Abteilung ausgewählt werden können. Darüber hinaus können die Produktoptionen auch nach Benutzerrolle konfiguriert werden.

Validierung von Bereichen und Organisationen

Validierung der Bereichskontrolle (DCV)



Bevor DigiCert ein SSL/TLS-Zertifikat ausstellen kann, müssen Sie die Kontrolle über die Domains und alle SANs (Subject Alternative Names) auf der Bestellung nachweisen. Wir bezeichnen diesen Prozess als Domain Control Validation (DCV) Prozess.

DigiCert unterstützt derzeit diese DCV-Methoden:

- E-Mail-Validierung: Bei dieser Validierungsmethode sendet DigiCert drei Sätze von DCV-E-Mails: WHOIS-basiert, Alias-Adressen (admin@, administrator@, postmaster@, hostmaster@, webmaster@) und DNS-TXT-basiert. Um die Kontrolle über die Domäne zu demonstrieren, befolgt ein E-Mail-Empfänger die Anweisungen in einer für die Domäne gesendeten Bestätigungs-E-Mail. Der Bestätigungsprozess besteht darin, den in der E-Mail angegebenen Link aufzurufen und den Anweisungen auf der Seite zu folgen.
- DNS CNAME-Validierung: Bei dieser Validierungsmethode fügen Sie einen von DigiCert generierten Zufallswert (der für die Domain in Ihrem CertCentral-Konto bereitgestellt wird) als CNAME-Eintrag in das DNS der Domain ein, damit dieser Wert von DigiCert abgerufen werden kann.
- DNS-TXT-Validierung: Bei dieser Validierungsmethode fügen Sie einen von DigiCert generierten Zufallswert (der für die Domain in Ihrem CertCentral-Konto bereitgestellt wird) als TXT-Eintrag in das DNS der Domain ein, damit dieser Wert von DigiCert abgerufen werden kann.
- Dateivalidierung (HTTP-Praxisdemonstration, auch als FileAuth bezeichnet): Bei dieser Validierungsmethode hosten Sie eine Datei mit einem von DigiCert generierten Zufallswert (der für die Domäne in Ihrem CertCentral-Konto bereitgestellt wird) an einem vorgegebenen Ort auf Ihrer Website: [Domäne]/.well-known/pki-validation/fileauth.txt. Sobald die Datei erstellt und auf Ihrer Website platziert ist, wird dieser durch DigiCert geprüft.

Hinweis: Für DV-Zertifikate in CertCentral unterstützt DigiCert derzeit die folgenden DCV-Methoden: WHOIS-basierte E-Mail, konstruierte E-Mail, E-Mail an DNS-TXT-Kontakt, DNS-TXT und Dateivalidierung.

Weitere Informationen: https://docs.digicert.com/manage-certificates/organization-domain-management/managing-domains-cc-guide/domain-pre-validation-domain-control-validation/

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

Validierung der Organisation

Um eine Organisation zu validieren, prüft DigiCert zunächst, ob die Organisation, die ein Zertifikat beantragt, einen guten Ruf genießt. Dazu kann auch die Bestätigung des guten Rufs und der aktiven Registrierung in Unternehmensregistern gehören. Dabei kann auch überprüft werden, ob die Organisation nicht in Datenbanken für Betrug, Phishing, staatlich eingeschränkte Stellen und Terrorismusbekämpfung aufgeführt ist.

Außerdem überprüfen wir, ob die Organisation, die ein Zertifikat beantragt, tatsächlich die Organisation ist, für die das Zertifikat ausgestellt werden soll. Wir überprüfen auch den Kontakt der Organisation.

Das Hinzufügen von Organisationen zu Ihrem CertCentral-Konto und deren Validierung ist eine Voraussetzung für die Validierung Ihrer Domänen. Eine vorab validierte Organisation beschleunigt den Prozess der Zertifikatserteilung.

Bei der Verwaltung von Organisationen geht es in der Regel darum, eine Organisation hinzuzufügen und sie zur Validierung zu übermitteln. Sie können auch eine nicht mehr benötigte Organisation deaktivieren.

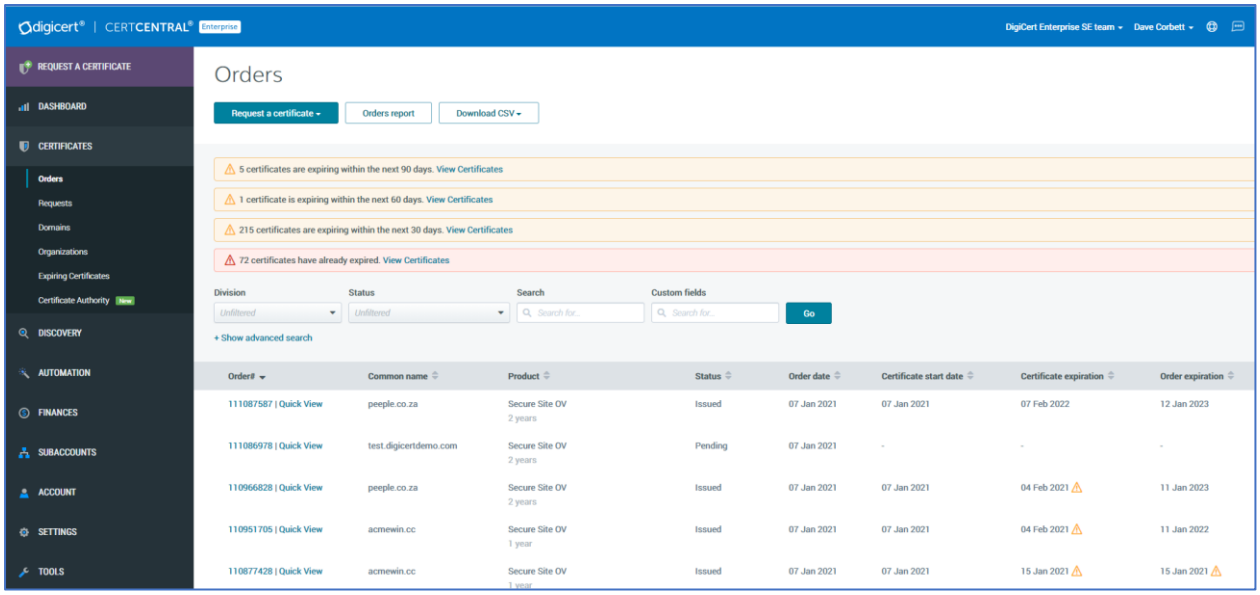
Weitere Informationen: https://docs.digicert.com/manage-certificates/organization-domain-management/manage-organizations/

Nachdem Sie Ihre Organisationen zur Validierung eingereicht haben, können Sie beginnen, Domänen zur Validierung einzureichen und die Art der Berechtigung anzugeben, für die die Domäne validiert werden soll.

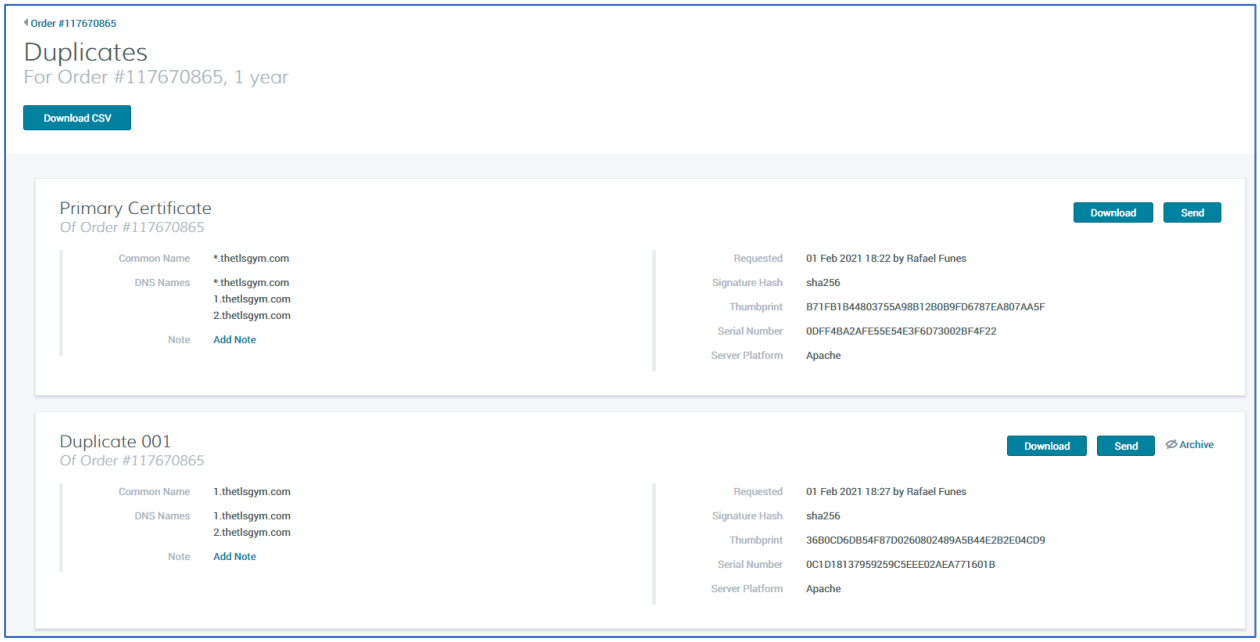
Weitere Informationen: https://docs.digicert.com/manage-certificates/organization-domain-management/managing-domains-cc-guide/

In der Regel ist es besser, Domänen und Organisationen vor der Beantragung von Zertifikaten zu validieren. Es ist jedoch auch möglich, neue Domänen und Organisationen bei der Beantragung eines Zertifikats hinzuzufügen.

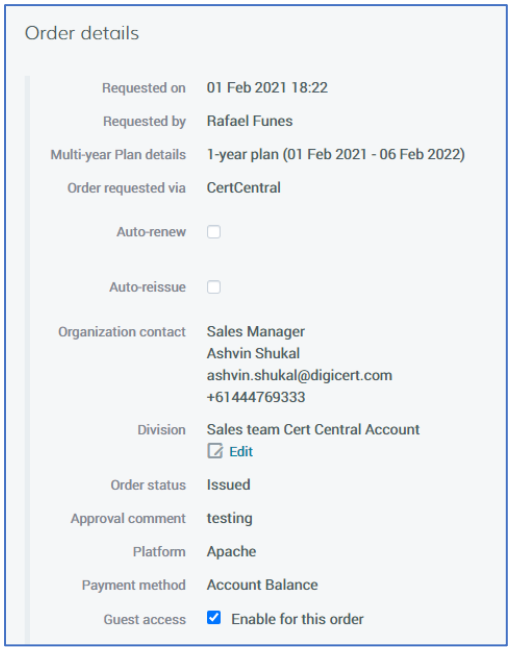
Verwaltung von Aufträgen und Zertifikaten



Bestellungen und Zertifikate können direkt über die CertCentral-Plattform verwaltet werden.



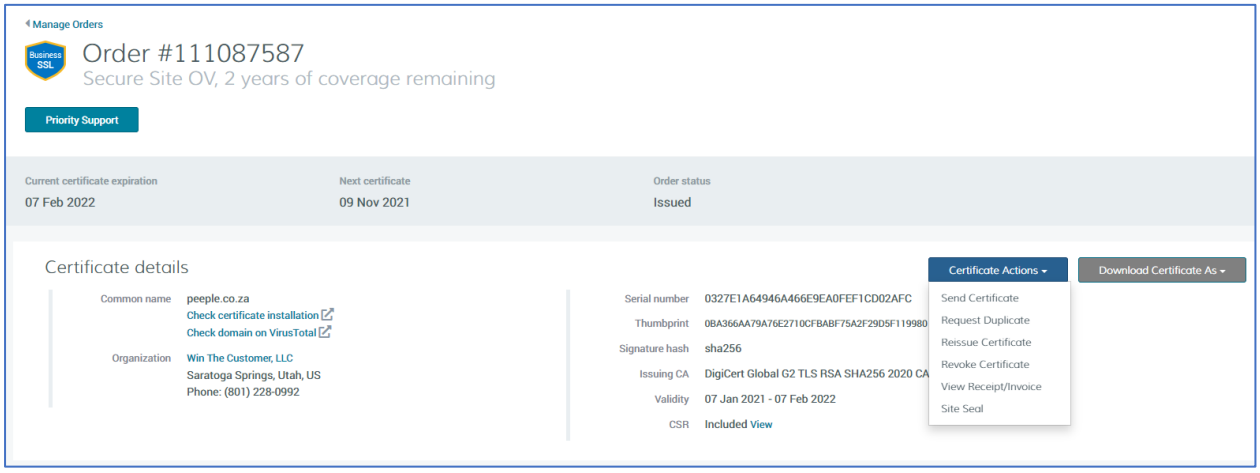
Ein Auftrag bezieht sich auf den gewählten Multi-year Plan. Ein Zertifikat gehört zu einem Auftrag und kann während der Laufzeit des Auftrags mehrmals neu ausgestellt werden. Wichtige Optionen für eine Bestellung sind:



Automatisch verlängern: Verlängert den Multi-year Plan automatisch 30 Tage vor Ablauf des aktuellen Plans.

Automatische Neuausstellung: Stellt 30 Tage vor Ablauf des aktuellen Zertifikats automatisch ein neues Zertifikat aus.

Beachten Sie, dass ein Zertifikat nicht mit einem Enddatum ausgestellt werden kann, das über das Enddatum des Auftrages hinaus geht.



Die Zertifikatsverwaltung umfasst die folgenden Aktionen:

- Zertifikat anfordern
- Zertifikatsantrag genehmigen
- Duplikat des Zertifikates anfordern
- Zertifikat neu ausstellen
- Zertifikat widerrufen
- Website-Seal Code erhalten

Genehmigung der Zertifikatsanforderung

Standardmäßig müssen Zertifikatsanträge genehmigt werden, bevor sie an DigiCert zur Ausstellung von Zertifikaten weitergeleitet werden. Nachdem ein Benutzer ein Zertifikat angefordert hat, muss ein Administrator, ein Manager, ein EV-geprüfter Benutzer, ein CS-geprüfter Benutzer oder ein EV-CS-geprüfter Benutzer die Zertifikatsanforderung genehmigen. Anschließend wird der Antrag an DigiCert gesendet, um zu überprüfen, ob alle Voraussetzungen für die Vorvalidierung erfüllt sind.

Nachdem ein Benutzer ein Zertifikat angefordert hat, kann jeder Administrator, Manager, EV Verified User, CS Verified User oder EV CS Verified User die Zertifikatsanforderung bei Bedarf auch ablehnen. Zum Beispiel, wenn der Nutzer ein falsches Zertifikat bestellt hat.

Standardmäßig sind die CertCentral-Konten für die Genehmigung von Zertifikatsanträgen in einem Schritt konfiguriert. Ein Kontoadministrator muss einen Zertifikatsantrag genehmigen, bevor DigiCert mit der Bearbeitung der Bestellung beginnen kann (Validierung der Organisation usw.). Sie können jedoch den Genehmigungsschritt aus den Arbeitsabläufen zur Ausstellung von OV/EV-SSL-Zertifikaten für Ihre CertCentral-Administratoren, Manager und Finanzmanager entfernen. Die Genehmigungsanforderungen können auf der Seite Einstellungen/Präferenzen von CertCentral konfiguriert werden.

Duplikate

Alle DigiCert-Zertifikate werden mit einer unbegrenzten Anzahl von kostenlosen Duplikaten ausgeliefert. Um die Sicherheit zu erhöhen und die Installation des Zertifikats auf mehreren Servern zu erleichtern, generieren Sie eine neue CSR und erstellen Sie für jeden Server ein Duplikat des Zertifikats.

Die Angaben im Dublikat sind genau dieselben wie im Original. Bei Duplikaten muss DigiCert vorherige Kopien Ihres Zertifikats nicht widerrufen.

Weitere Informationen: https://docs.digicert.com/manage-certificates/duplicate-ssltls-certificate/

Neuausstellung des Zertifikats

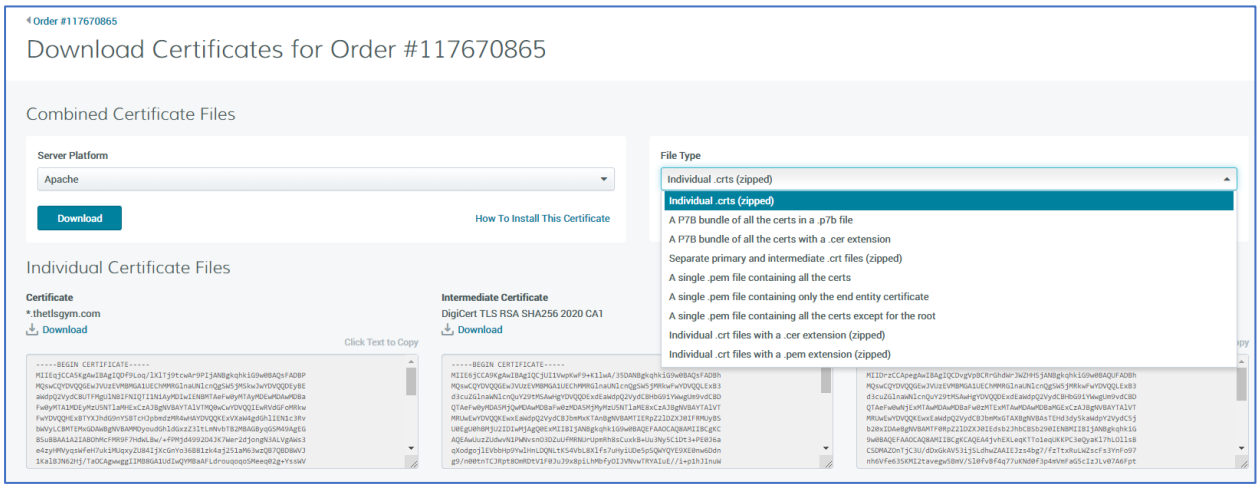
Alle DigiCert-Zertifikate können kostenlos und unbegrenzt neu ausgestellt werden. Der Prozess der Neuausstellung von Zertifikaten ermöglicht es Ihnen, ein ausgestelltes Zertifikat anzupassen. Einige Änderungen ermöglichen es Ihnen, auf dem ursprünglichen Zertifikat aufzubauen, was zu zwei oder mehr Versionen dieses Zertifikats führt. Wenn Sie zum Beispiel ein Zertifikat neu ausstellen, können Sie dem ursprünglichen Zertifikat Domänen hinzufügen. Durch das Hinzufügen von Domänen zu einem Zertifikat wird das ursprüngliche Zertifikat nicht widerrufen.

Wenn Sie jedoch Änderungen vornehmen, wie z.B. das Entfernen von SANs oder das Ändern von SANs in einem Multi-Domain-Zertifikat, wird ein neues Zertifikat erstellt und DigiCert wird das ursprüngliche Zertifikat sowie alle Neuausstellungen und Duplikate widerrufen.

Weitere Informationen: https://docs.digicert.com/manage-certificates/reissue-ssltls-certificate/

Herunterladen eines Zertifikats

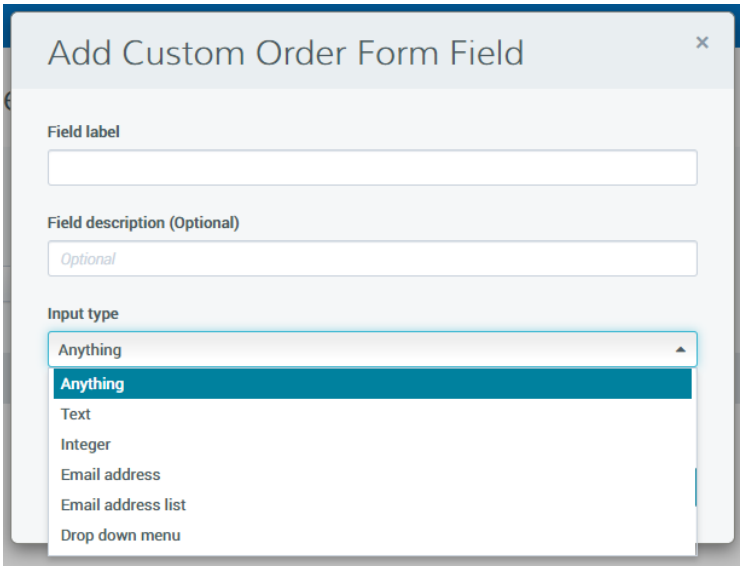
Nachdem DigiCert Ihr Zertifikat ausgestellt hat, können Sie das Zertifikat direkt auf den Server herunterladen, auf dem die Zertifikatsanforderung erstellt wurde (d. h. auf den Server mit dem passenden öffentlichen Schlüssel des Zertifikats).



CertCentral bietet eine Reihe von Dateiformaten an. Sobald Sie die entsprechende Serverplattform ausgewählt haben, wird eine Auswahl an Dateitypen angeboten. Sie können das Zertifikat, das Zwischenzertifikat und das Stammzertifikat auch direkt als .pem-Dateien herunterladen.

Benutzerdefinierte Auftragsfelder

CertCentral ermöglicht es Ihnen, benutzerdefinierte Felder zu Ihren Zertifikatsbestellformularen hinzuzufügen. Die Metadaten des benutzerdefinierten Feldes können verwendet werden, um Zertifikate und Aufträgen zu suchen oder zu sortieren, die den Suchkriterien der Metadaten entsprechen.



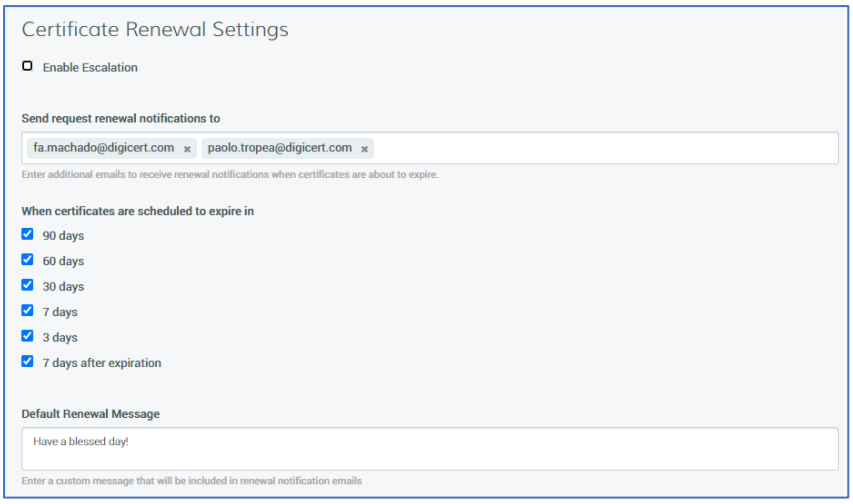
Features:

- Können auf zukünftige und aktuelle Anfragen angewendet werden: Wenn Sie benutzerdefinierte Felder hinzufügen, wird das Feld auch zu ausstehenden Anfragen hinzugefügt. Wenn das Feld als erforderlich gekennzeichnet ist, können die anhängigen Anträge erst genehmigt werden, wenn das Feld ausgefüllt ist.
- Auf das gesamte Konto anwenden: Wenn Sie benutzerdefinierte Felder hinzufügen, werden diese Felder auf die Bestellformulare für das gesamte Konto angewendet. Benutzerdefinierte Felder können nicht pro Abteilung festgelegt werden.
- Auf alle Zertifikatstypen anwenden: Wenn Sie benutzerdefinierte Felder erstellen, werden die Felder zu den Bestellformularen für alle Zertifikatstypen (SSL, Client, Code Signing usw.) hinzugefügt. Sie können den Bestellformularen keine benutzerdefinierten Felder nur für SSL-Zertifikatstypen usw. hinzufügen.
- Auf Gast-URLs anwenden: Wenn Sie benutzerdefinierte Felder für Bestellformulare hinzufügen, werden diese Felder zu den Zertifikaten hinzugefügt, die direkt über Ihr CertCentral-Konto bestellt werden, sowie zu allen Gast-URLs, die Sie verschickt haben.
- Auswahl verschiedener Typen: Es können unterschiedliche Arten von Feldern hinzugefügt werden, z. B. einzeilige und mehrzeilige Textfelder, E-Mail-Adressen und E-Mail-Adressenlistenfelder usw.
- Erforderlich oder optional: Wenn Sie benutzerdefinierte Felder hinzufügen, können Sie diese als erforderlich oder optional festlegen. Die erforderlichen Felder müssen ausgefüllt werden, bevor die Bestellung genehmigt werden kann. Optionale Felder können leer gelassen werden.
- Deaktiviert oder aktiviert: Nachdem Sie ein benutzerdefiniertes Feld hinzugefügt haben, können Sie das Feld nach Bedarf deaktivieren (entfernen) und aktivieren (wieder hinzufügen). Felder, die Sie deaktivieren, werden aus ausstehenden Anfragen, aber nicht aus erteilten Aufträgen entfernt. Felder, die Sie aktivieren, werden den ausstehenden Anfragen hinzugefügt. Wenn das Feld erforderlich ist, muss es ausgefüllt werden, bevor der Antrag genehmigt werden kann.

Benutzerdefinierte Felddaten können jederzeit vor oder nach der Ausstellung eines Zertifikats bearbeitet werden.

Weitere Informationen: https://docs.digicert.com/manage-account/customize-your-certificate-request-forms/managing-custom-order-form-fields/

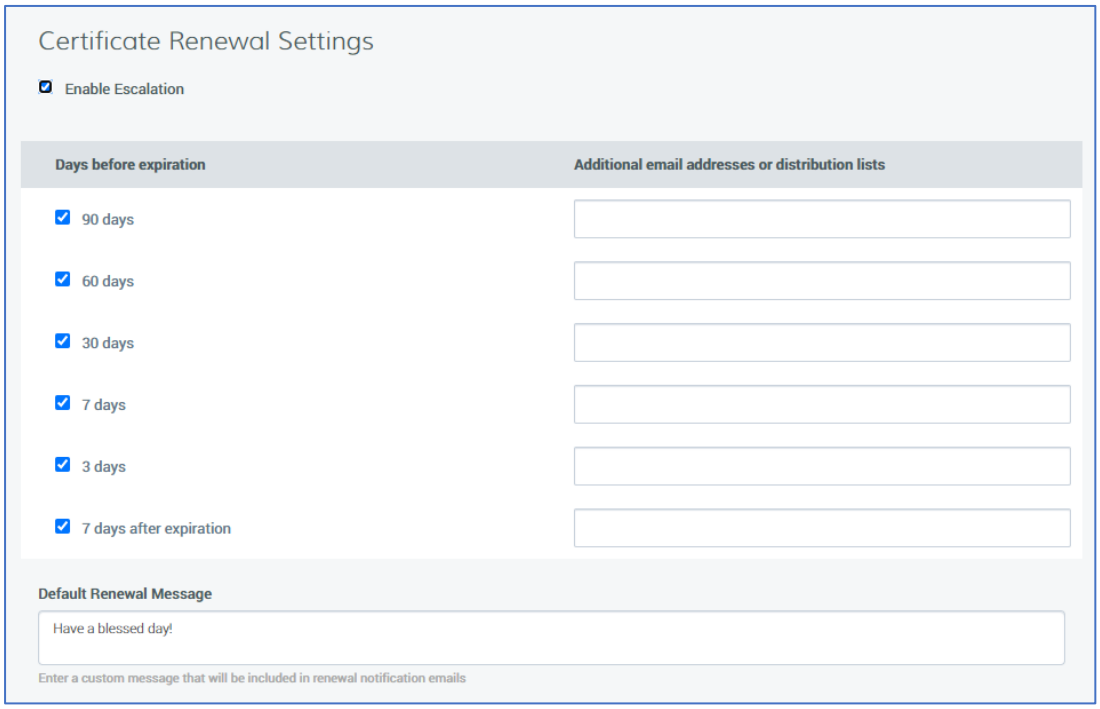
Renewal-Mitteilung



Standardmäßig sendet CertCentral Benachrichtigungen zur Zertifikatserneuerung 90, 60, 30, 7 und 3 Tage vor Ablauf eines Zertifikats und 7 Tage nach Ablauf eines Zertifikats. Sie können Ihre Zertifikatserneuerungseinstellungen konfigurieren, um festzulegen, wann Erneuerungsbenachrichtigungen gesendet werden und welche E-Mail-Adressen die Benachrichtigungen erhalten.

Sie können Benachrichtigungen zur Zertifikatserneuerung oder zur Eskalation konfigurieren:

- Einstellungen für die Zertifikatserneuerung: Hier legen Sie fest wann an welche E-Mail-Adresse eine Benachrichtigung gesendet wird.

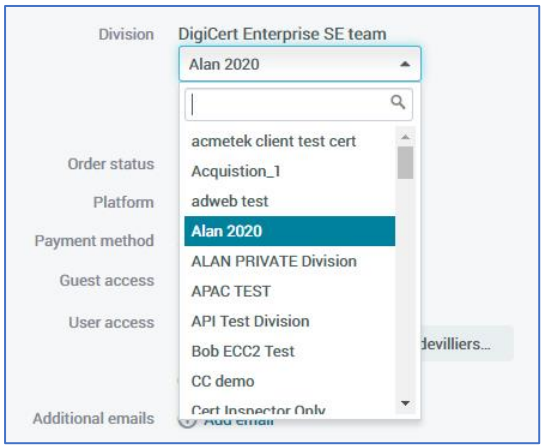


- Einstellungen für die Eskalation von Verlängerungen: Hier können Sie festlegen, welche E-Mail-Adressen welche Verlängerungsbenachrichtigungen in den einzelnen Phasen erhalten, wenn die Gültigkeit von Zertifikaten näher rückt oder sie bereits abgelaufen sind.

Unterkonten und Abteilungen

Abteilungen

Abteilungen sind eine Funktion in CertCentral zur Einschränkung von Benutzern und Organisationen. Sie können Benutzer in Ihrer Organisation zu Ihrem CertCentral-Konto hinzufügen und den Zugriff auf ihr Konto durch Benutzerberechtigungen kontrollieren.



Sie können einer Abteilung bestimmte Berechtigungen zuweisen, um damit deren Möglichkeiten zur Erstellung und Verwaltung von Benutzern, Berechtigungen, Domänen und Organisationen kontrollieren. Im Gegensatz zu Unterkonten haben Sie volle Einsicht und Kontrolle über die Benutzer, Bestellungen, Einstellungen und Aktivitäten der Abteilungen in Ihrem Konto.

Darüber hinaus können sich die Abteilungen ein gemeinsames Konto teilen, oder jede Abteilung kann ihr eigenes Konto haben und nur für ihre Zertifikate bezahlen.

Zertifikatsaufträge können jederzeit einer anderen Abteilung zugewiesen werde.

Weitere Informationen: https://docs.digicert.com/manage-account/division-management/

Unterkonten

Unterkonten sind CertCentral-Konten, die mit einem übergeordneten CertCentral-Konto verbunden sind und von diesem verwaltet werden. Mit Unterkonten können Wiederverkäufer oder andere Organisationen den Benutzern individuelle Kontrolle über ein CertCentral-Konto und ihren Zertifikatsverwaltungsprozess geben, während Sie als "übergeordnetes" Konto weiterhin die Produktpreise und die Rechnungsstellung kontrollieren.

Unterkonten sind z.B. für Kunden-Geschäftsbeziehungen, bei denen Sie die Produktpreise oder die Fakturierung der von den Unterkonten getätigten Bestellungen kontrollieren müssen. Es gibt vier Arten von Unterkonten:

- Einzelhandel
- Unternehmen
- Partner
- Verwaltet (normalerweise nur API-Zugang).

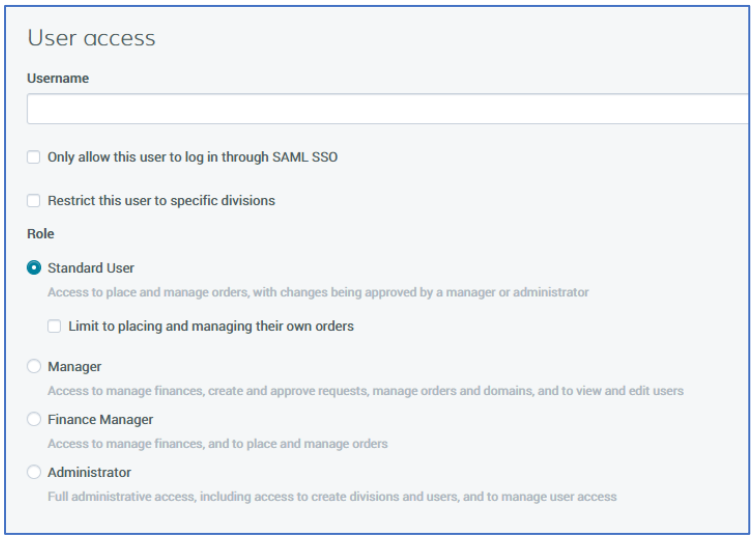
Jeder Kontotyp verfügt über einen anderen Satz von CertCentral-Funktionen, die ihm zur Verfügung stehen. Verwaltete Unterkonten sind reine API-Konten, die für die Integration in ein bestehendes Benutzerportal vorgesehen sind und dem übergeordneten Konto einige zusätzliche Kontrollmöglichkeiten bieten, wie z.B., um Zertifikate herunterzuladen.

Unterkonten können bis zu 3 Ebenen umfassen.

Weitere Informationen: https://docs.digicert.com/manage-account/subaccounts-management/

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

Benutzerrollen



Kontoverwalter weisen einem Benutzer keine individuellen Berechtigungen zu. Stattdessen weisen sie jedem Benutzer eine Rolle zu:

- Administrators
- Standard Benutzer
- Eingeschränkter Benutzer
- Finanzmanager
- Manager

Die dem Benutzer zugewiesene Rolle bestimmt, auf welche Kontofunktionen er zugreifen kann.

Die Hauptrollen sind:

- Standardbenutzer: Zertifikate bestellen und die Verwaltung von Bestellungen, Änderungen von einem Manager oder Administrator genehmigt werden müssen
- Manager: Zugang zur Finanzverwaltung, Erstellen und Genehmigen von Anträgen, Verwaltung von Aufträgen und Domänen, Ansicht und Bearbeitung von Benutzern
- Finanzmanager: Zugang zur Finanzverwaltung und zur Platzierung und Verwaltung von Aufträgen
- Administrator: Vollständiger administrativer Zugriff, einschließlich der Möglichkeit, Abteilungen und Benutzer zu erstellen und den Benutzerzugriff zu verwalten

Um die Rolle "Eingeschränkter Benutzer" zu erstellen, wählen Sie "Standardbenutzer" und aktivieren Sie das Kontrollkästchen "Nur eigene Bestellungen aufgeben und verwalten".

Berechtigungsdetails:

Administrator	Vollständiger CertCentral-Kontozugang mit diesen Berechtigungen: • Zugriff und Verwaltung von Discovery. • Abteilungen erstellen und bearbeiten und Kontonutzer erstellen, löschen und bearbeiten. • Verwalten der Organisationen (neue Organisationen hinzufügen), Domänen (hinzufügen oder deaktivieren), Gastanfragen und API-Zugang. • Zugriff auf alle Zertifikatsanforderungen und -aufträge, Beantragen von Zertifikaten, Genehmigen der Zertifikatsanforderungen und Ausführen von Reports. • Verwalten der Finanzeinstellungen und Finanzen Ihres Kontos (Saldoübersicht, Ausgabenberichte, Einzahlungen, etc.). • Verwalten der Kontoeinstellungen (Authentifizierungseinstellungen, IP-Zugriffsbeschränkungen, Produktbeschränkungen usw.), Prüfeinstellungen und Prüfprotokolle.
Standard Benutzer	Kontonutzer mit diesen Berechtigungen können: • Zertifikate anfordern. • Zertifikatsanträge und -aufträge (eigene und fremde) überwachen. • Ein Manager oder Administrator muss die Änderungen genehmigen.
Eingeschränkter Benutzer	Kontonutzer mit diesen Berechtigungen können: • Zertifikate anfordern. • ihre eigenen Zertifikatsanträge und -aufträge überwachen. • Ein Manager oder Administrator muss die Änderungen genehmigen.
Finanzmanager	Benutzer mit eingeschränktem Konto, deren Hauptaufgabe darin besteht, die Finanzen des Kontos zu verwalten, haben folgende Berechtigungen: • Anzeige des Kontostandes, der Ausgabenberichte und Kontopreise. • Verwaltung von Bestellungen und Einzahlung von Geldern. • Verwalten der Auftragsberichte. • Zertifikate anfordern. • Überwachen eigener Zertifikatsanträge und -aufträge.
Manager	Begrenzte Kontonutzer, deren Hauptaufgabe darin besteht, bei der Verwaltung des Kontos zu helfen, haben folgende Berechtigungen: • Zugriff und Verwaltung von Discovery. • Anzeigen von Abteilungen und Verwalten von Kontonutzern (bearbeiten). • Organisationen anzeigen und Domänen verwalten (hinzufügen oder deaktivieren).

	• Zugriff auf alle Zertifikatsanforderungen und -aufträge, Beantragen von Zertifikaten, Genehmigen der Zertifikatsanforderungen und Ausführen von Reports. • Verwalten der Finanzeinstellungen und Finanzen Ihres Kontos (Saldoübersicht, Ausgabenberichte, Einzahlungen, etc.). • Verwalten Sie Audit-Einstellungen und Audit-Protokolle.

Allen Benutzerrollen kann der Zugriff auf Zertifikate in bestimmten Abteilungen eingeschränkt werden.

Standardmäßig haben Administratoren und Manager nicht die Berechtigung, EV-Zertifikat-, EV Code Signing-Zertifikat- oder Code Signing-Zertifikat-Anforderungen zu genehmigen. Um diese Anträge zu genehmigen, müssen dem Manager die entsprechenden Unterrollen zugewiesen werden.

Weitere Informationen: https://docs.digicert.com/manage-account/certcentral-user-roles-account-access/roles-account-access/

Methoden zur Kontrolle des Benutzerzugangs/der Benutzerauthentifizierung

Passwörter

Die Mindestanforderungen für Passwörter können über das CertCentral Portal festgelegt werden.

Zwei-Faktoren-Authentifizierung

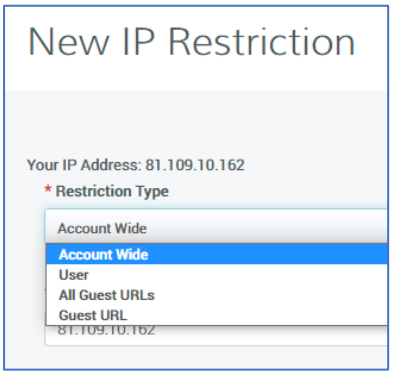
Um eine zweite Form der Identitätsüberprüfung zu Ihrem Anmeldevorgang hinzuzufügen, müssen Sie die Anforderungen für die Zwei-Faktor-Authentifizierung für Ihr Konto konfigurieren. Sie können eine Anforderung für alle Benutzer oder für einzelne Benutzer konfigurieren.

Zusätzlich zu der Anforderung Benutzer-ID/Passwort können Benutzer aufgefordert werden, einen der folgenden Faktoren zu verwenden:

- Einmaliges Passwort (OTP): Bei Anwendung dieser Regel müssen die Benutzer ihre OTP-App oder ihr Gerät initialisieren und bei der nächsten Anmeldung ein einmaliges Passwort generieren. Für die OTP-Authentifizierung muss eine beliebige mobile App verwendet werden, die das TOTP-Protokoll (Time-Based One-Time Password) unterstützt.
- Client-Zertifikat: Wenn Sie diese Regel anwenden, müssen die Benutzer bei der nächsten Anmeldung ein Client-Zertifikat in ihrem Browser generieren. Internet Explorer (Windows) und Safari (Mac) sind die einzigen Browser, die die Erstellung von Client-Zertifikaten unterstützen.

Weitere Informationen: https://docs.digicert.com/manage-account/certcentral-two-factor-authentication/configure-two-factor-authentication-requirements/

IP-Beschränkungen



Um die Sicherheit zu erhöhen, bietet DigiCert die Möglichkeit, Ihr Konto so einzuschränken, dass nur von bestimmten IP-Adressen aus darauf zugegriffen werden kann. Diese können eingestellt werden:

- Konto weit
- Pro Benutzer
- Pro Gast-URL
- Für alle Gast-URLs

Einzelanmeldung

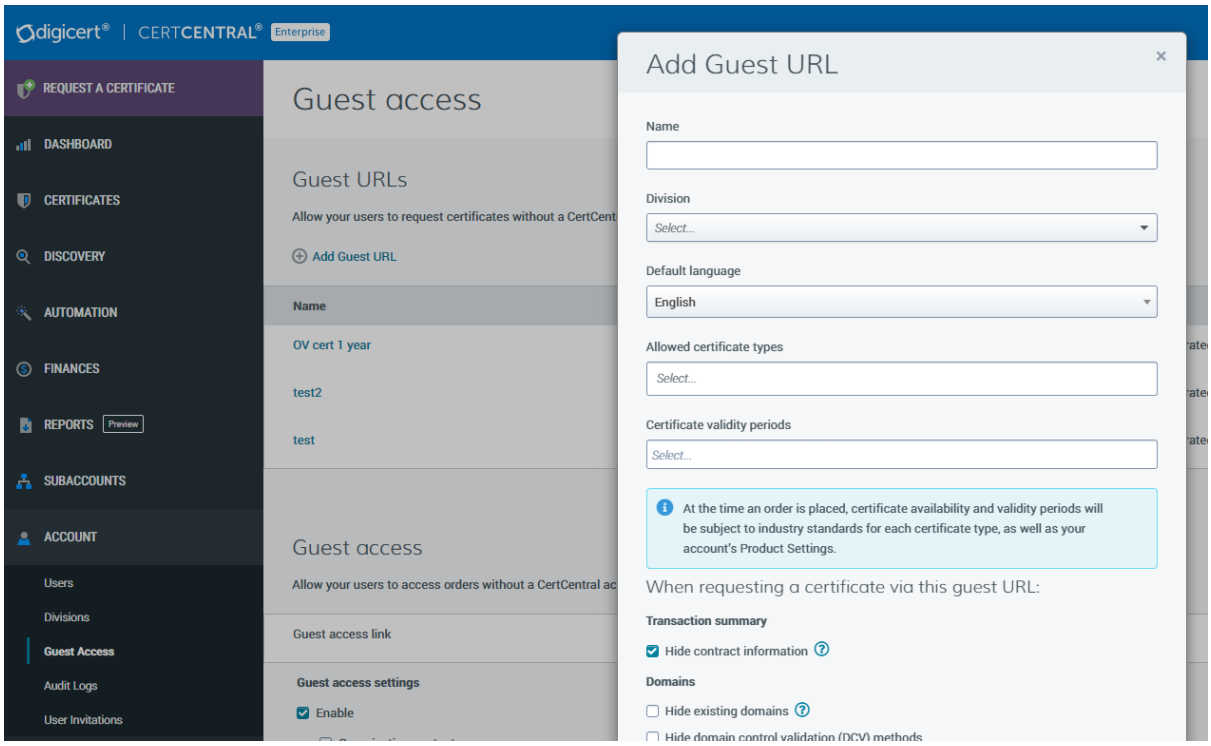
Machen Sie Schluss mit mehreren Passwörtern und verwenden Sie SAML Single-Sign-On (SSO), um Ihren Identitätsanbieter (IdP) mit CertCentral zu verbinden.

Sobald Sie die SAML-zu-CertCentral-Verbindung konfiguriert haben, können sich Ihre CertCentral-Benutzer mit ihren SSO-Anmeldedaten anmelden. Sie greifen auf die Anmeldeseite für das SSO-Konto über eine vom Dienstanbieter initiierte benutzerdefinierte SSO-URL zu, die DigiCert bereitstellt, oder über eine von Ihnen bereitgestellte IDP initiierte SSO-URL.

Weitere Informationen: https://docs.digicert.com/manage-account/saml-single-sign-on-admin-guide/

Optionen für den Gastzugang

Guest-URL



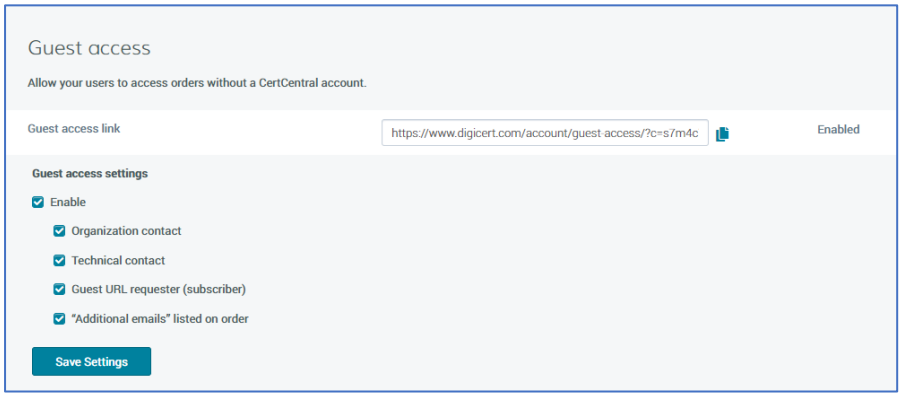
Mit einer Gast-URL können Sie einem Gastbenutzer die Möglichkeit geben, ein Zertifikat anzufordern, ohne ihn zu Ihrem Konto hinzuzufügen. Über Gast-URLs erhalten Benutzer ausschließlich Zugriff auf eine bestimmte Zertifikatsanforderungsseite innerhalb des Kontos.

Gast-URLs werden mit den folgenden Details konfiguriert:

- Name
- Abteilung
- Erlaubte Zertifikatstypen
- Gültigkeitszeiträume der Zertifikate

Weitere Informationen: https://docs.digicert.com/manage-account/managing-guest-urls/

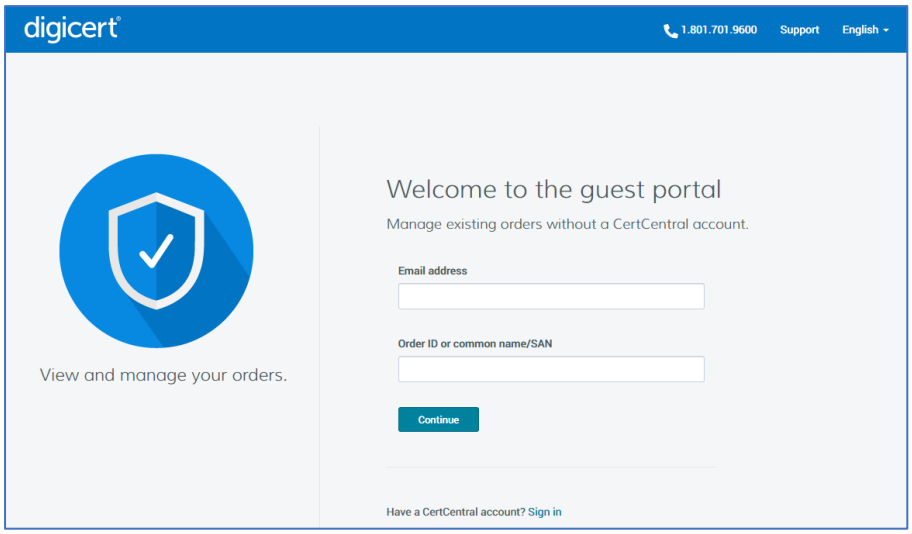
Guest Access



Der Gastzugang ermöglicht es einer Person, eine Bestellung ohne einen CertCentral-Login zu verwalten. Mit der E-Mail-Adresse und Bestellnummer (oder dem FQDN im Zertifikat) kann das Zertifikat heruntergeladen, neu ausgestellt oder widerrufen werden. Der Gastzugang kann für alle Bestellungen in Ihrem Konto oder für einzelne Bestellungen aktiviert werden.

Sie können festlegen, welche Bestellkontakte für den Gastzugang in Frage kommen, indem Sie die Kontrollkästchen für den Organisationskontakt, den technischen Kontakt, den Gast-URL-Anforderer (Abonnent) (die E-Mail-Adresse, die die Bestellung aufgegeben hat) und "Zusätzliche E-Mails" in der Bestellliste aktivieren oder deaktivieren.

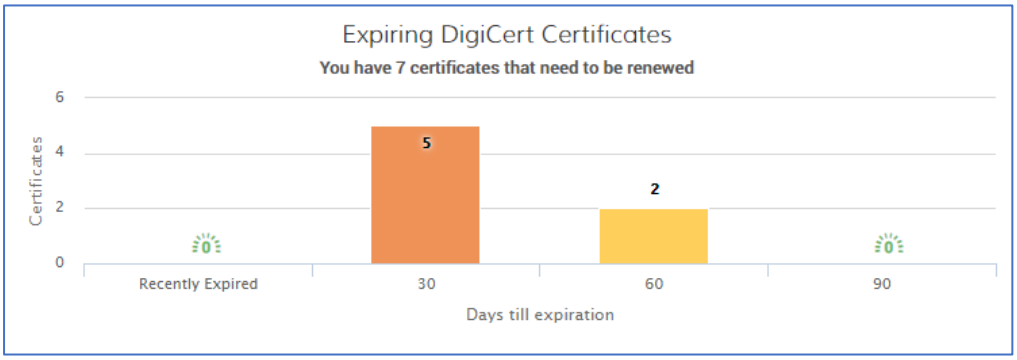
Ihr CertCentral-Konto hat eine eigene Anmeldeseite für den Gastzugang. Um die Identität der Person zu bestätigen, sendet CertCentral eine Authentifizierungs-E-Mail, die den Zugang für zwei Stunden ermöglicht.



Weitere Informationen: https://docs.digicert.com/manage-account/guest-access/

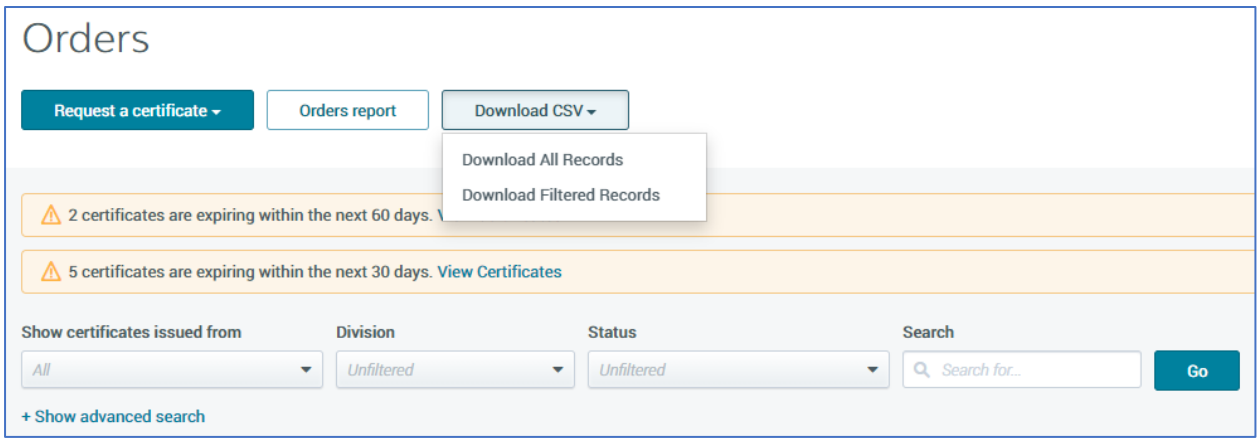
Berichte und Benachrichtigungen

Berichte



CertCentral bietet Dashboards und Berichte innerhalb der Konsole oder über APIs.

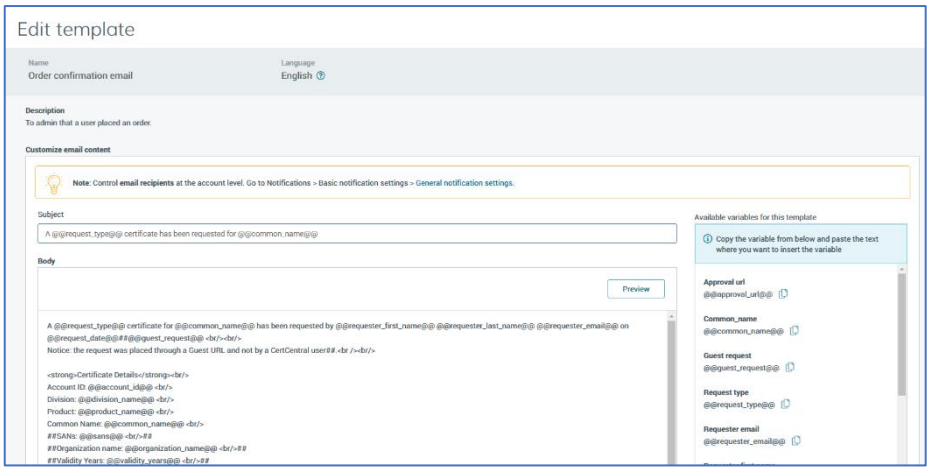
Dashboard: Eine grafisch organisierte Ansicht Ihrer Zertifikate, einschließlich auslaufender Zertifikate und ausstehender Anträge.



Auftragsbericht: Hier finden Sie alle ausgestellten Zertifikate und können nach einem beliebigen Feld gesucht werden.

E-Mail-Benachrichtigungen

CertCentral sendet während des gesamten Bestell-/Genehmigungsprozesses und bei Ablauf eines Zertifikats E-Mails an die Benutzer. Sie können diese E-Mail-Vorlagen gemäß Ihren Anforderungen selbst anpassen.

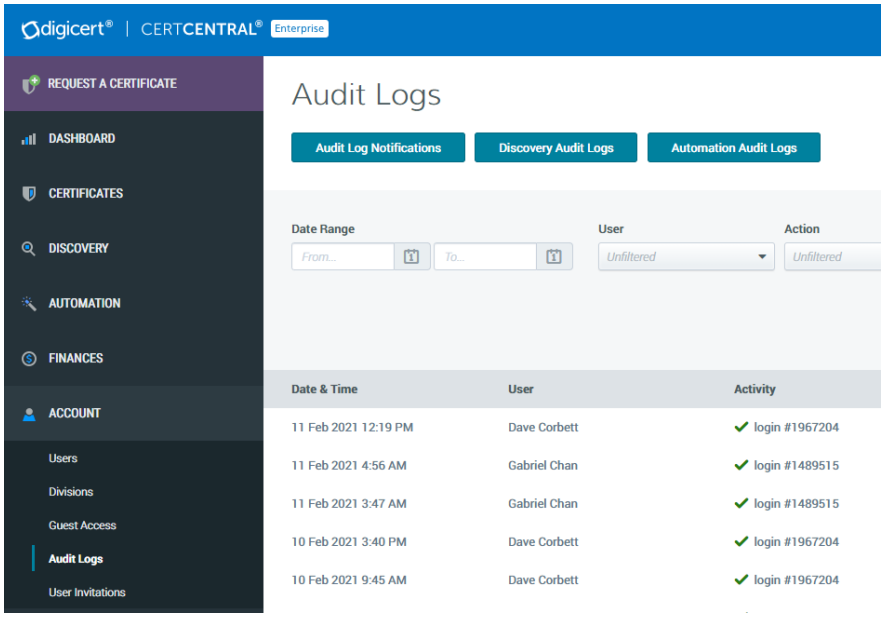


In den ***Grundeinstellungen*** für Benachrichtigungen können Sie die E-Mail-Empfänger und die E-Mail-Sprache festlegen.

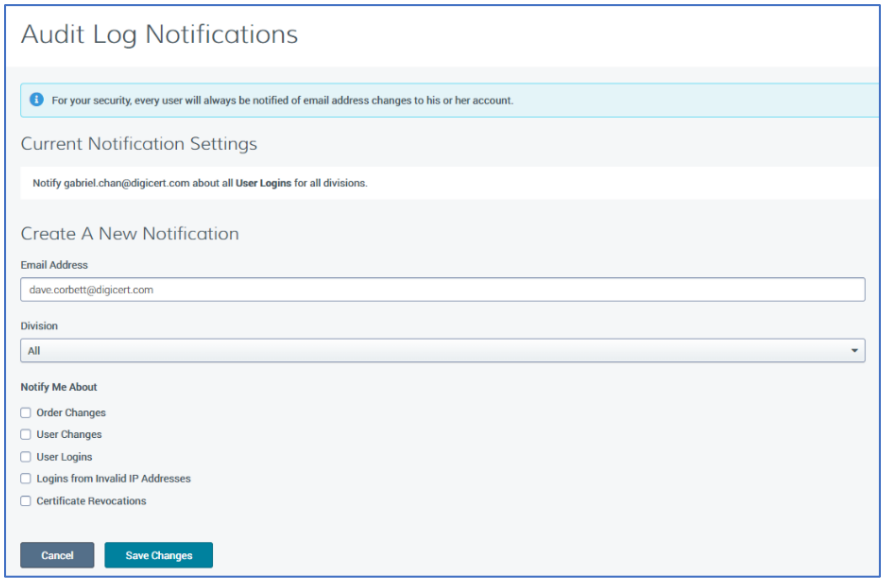
Mit ***benutzerdefinierten E-Mail-Vorlagen*** können Sie die Standard-E-Mail-Vorlagen bearbeiten.

Weitere Informationen: https://docs.digicert.com/manage-account/account-notifications/customize-email-templates/

Audit-Protokollierung



Audit-Protokolle zeigen eine Historie aller Aktionen in Ihrem Konto. CertCentral führt automatisch Prüfprotokolle, die mehr als 50 verschiedene Aktionen in Ihrem Konto aufzeichnen (einschließlich Anmeldungen, Zertifikatsanforderungen und Widerrufe), zusammen mit dem Zeitstempel und dem Benutzer, der die Aktion durchgeführt hat. Um die Audit-Protokolle in Ihrem Konto einzusehen, gehen Sie auf die Seite ***Audit-Protokolle.***



Klicken Sie auf ***Audit Log Notifications***, um E-Mail-Benachrichtigungen für bestimmte Ereignisse zu erstellen.