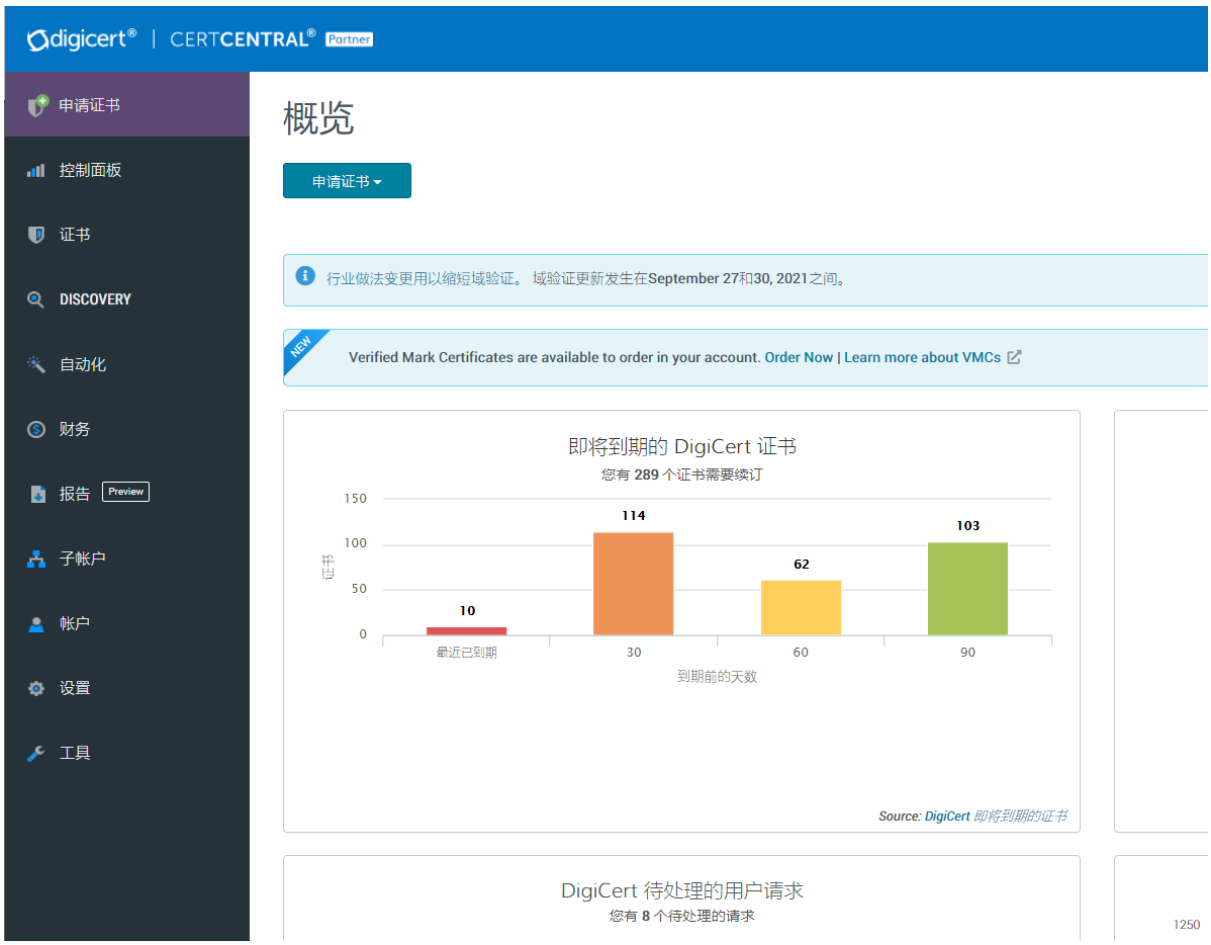
DigiCert®技术认证
CertCentral®专业学习指南

2021 v2



© 2021 DigiCert, Inc. 保留所有权利。DigiCert 是 DigiCert, Inc.在美国和其他地方的注册商标。所有其他商标和注册商标是其各自所有者的财产。

内容

简介 4
目标 5
SSL/TLS 证书产品 6
灵活证书 6
多年计划 7
安全网站证书的好处 7
DigiCert 智能标章 8
证书档案选项 9
代码签名证书 10
产品设置 10
域名和组织验证 11
域名控制验证(DCV) 11
组织验证 12
订单和证书的管理 12
证书批准 14
复制证书 15
补发证书 15
下载证书 15
自定义订单表单字段 16
更新通知 17
子账户和部门 18
部门划分 18
子账户 19
用户角色 20
用户访问/认证控制方法 22
密码 22
双因素认证 22
IP 限制 22
单点登录 22
来宾访问选项 23

来宾 URL 23
来宾访问 24
报告和通知 25
报告 25
通知 25
审核日志 26

简介

本学习指南旨在帮助您准备 DigiCert 技术认证：CertCentral 专业评估考试。考试将包括 50 道选择题，允许的最长时间为 1 小时。

本评估的目标受众是以技术角色（技术支持、SSL/TLS 管理员等）使用 DigiCert CertCentral 证书管理平台的任何人。

在尝试进行认证评估之前，你应该回顾以下目标。如果你认为你已经能够达到列出的所有目标，欢迎你安排一次评估。然而，如果有任何列出的目标，你可能需要额外的准备，你应该计划在安排评估之前详细研究这些主题。

更多信息可在 CertCentral 专业培训指南中找到，可从 https://www.digicert.com/tls-ssl/tls-certification-program 。请注意--这些资源只是一个起点！我们强烈建议你做进一步的研究，以便为所有目标的评估做好充分准备，包括使用 DigiCert CertCentral 的实践经验。

此外，还可以参加以 DigiCert 教员为基础的研讨会，该研讨会将深入介绍许多评估目标。如果您想了解更多信息，请联系您的 DigiCert 客户经理。

目标

在尝试参加 DigiCert 技术认证：CertCentral 专业评估考试之前，你应该能够做到以下几点。

- 列出并比较 DigiCert CertCentral Enterprise 中的 SSL/TLS 和代码签名证书产品
- 描述商业 SSL 证书的特性，如 CT 日志监控、恶意软件扫描、DigiCert 智能标章等。
- 描述 DigiCert CertCentral 中可用的证书档案选项，例如 HTTP 签名交换。
- 描述 DigiCert 用于域名和组织验证的政策和方法
- 列出并比较 DigiCert CertCentral 中的用户角色
- 展示在 DigiCert CertCentral 中对订单、证书、组织和域名的管理。
- 解释并演示 DigiCert CertCentral 中的用户访问/认证控制方法，例如 SAML、2FA。
- 解释并演示 DigiCert CertCentral 中的子帐户和部门的使用。
- 描述 DigiCert CertCentral 中可用的报告选项
- 描述并演示 CertCentral 中的来宾访问选项：来宾 URL 和来宾访问功能

SSL/TLS 证书产品

大多数企业使用 DigiCert 的商业 SSL 证书系列。

- 安全网站专业版
- 安全网站专业版 EV
- 安全网站 EV
- 安全网站 OV

这些证书产品有许多选择和好处, 请看以下的介绍:

Features	Secure Site OV	Secure Site EV	Secure Site Pro	Secure Site Pro EV
通配符	✓		✓	
SAN 限制	250	250	250	250
PQC 工具包			✓	✓
CT 日志监控服务			✓	✓
漏洞评估服务		✓	✓	✓
恶意软件检查	✓	✓	✓	✓
网站标章	2	2	2	2
优先验证支持	✓	✓	✓	✓
优先技术支持	✓	✓	✓	✓
Netsure 安全担保	$1.75M	$1.75M	$2M	$2M
信赖方赔付保障	$2M	$2M	$2M	$2M

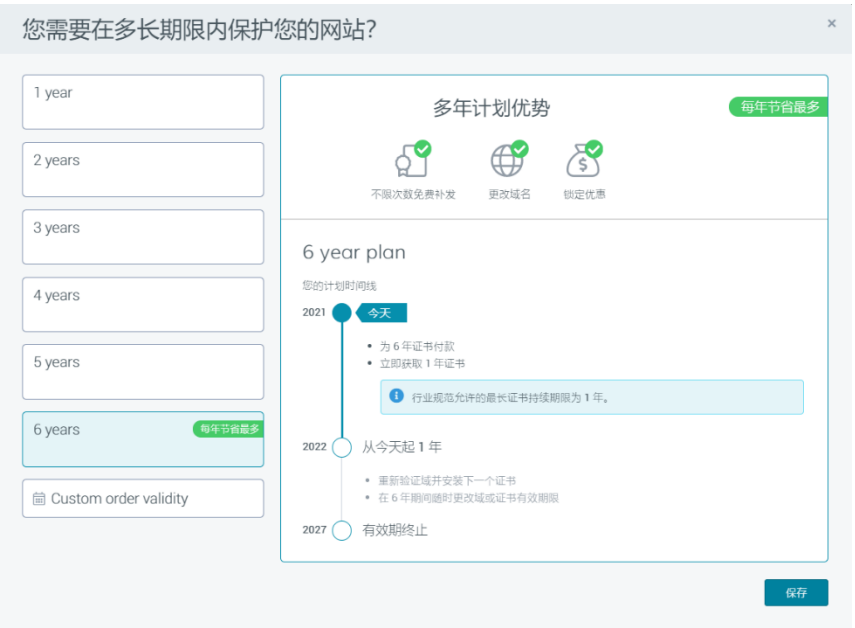
灵活证书

DigiCert Secure Site 和 Secure Site Pro 证书支持任何类型的域配置，并可作为单域或多域证书订购，具有完全合格域名（FQDN）和通配符 SAN 的任何组合。

这使你可以灵活地订购你想要的东西，并在证书的有效期内增加额外的 SAN，而不需要更换产品。这些证书没有专门的多域名或通配符版本，而是在配置基本证书时添加这些内容。

更多信息：https://docs.digicert.com/zh-cn/manage-certificates/flex-certificates/

多年计划



DigiCert 多年计划允许你以单一价格支付长达 6 年的 SSL/TLS 证书保障。通过多年计划，你可以选择 SSL/TLS 证书、你想要的覆盖时间（最长 6 年）以及证书的有效期。在该计划到期之前，每次当你的证书达到有效期时，你都可以免费重新签发。请注意，目前公开信任的 SSL/TLS 证书的最长有效期是 397 天，所以你可能需要在多年计划中多次重新签发证书。

当你为一个多年计划重新签发证书时，你可以做以下事情。

- 为重新签发的证书设置一个新的到期日：重新签发的证书的最大有效期是 CA/B 论坛基线要求所定义的最大证书寿命或多年计划的结束，以较早者为准。
- 更改或删除域名：删除和更改域名需要 DigiCert 吊销所有以前签发的证书。DigiCert 等待 48-72 小时后才会吊销原始证书和任何现有的复制和重新签发的证书。
- 添加域名：添加域名可能会导致额外的费用。新域名的价格是按比例计算的，并根据多年计划的剩余时间适用。

更多信息：https://docs.digicert.com/zh-cn/manage-certificates/multi-year-plans/

安全网站证书的好处

除了工业强度的 2048 位加密外，DigiCert 安全网站证书还包括其他好处，如优先支持。这些好处在你的证书订单有效期内都可以享受。每次你更新安全网站证书订单时，你的利益都会自动转入新的订单。

- 优先验证 - 安全网站的订单被放在我们验证队列的顶端，因此我们的代理可以优先处理这些订单。
- 优先支持 - 安全网站证书可以进入两个优先支持队列，因此我们的支持团队可以优先处理你的需求：订单和验证状态以及安装和配置。
- 两个高级网站标章--安全网站证书带有网络上两个最公认的信任标志：DigiCert 和 Norton。挑选你想使用的高级网站标章，在你的网站上显示信任证明。

- CT（证书透明度）日志监控 - CT 日志监控服务允许你监控 Secure Site Pro 或 Secure Site Pro EV 证书上域名的公共 CT 日志。在你为 Secure Site Pro 证书订单启用 CT 日志监控后，你会收到两种类型的电子邮件通知：每日 CT 日志摘要和紧急通知。电子邮件通知将会发送到帐户管理员，允许他们检查域名的 CT 日志，而无需每天登录 CertCentral 帐户。CT 日志监控服务将发现的 SSL/TLS 证书拉到您的 CertCentral 账户中，在那里您可以查看证书的细节，以快速识别任何错误签发的证书。你也可以从你的 CertCentral 帐户中直接下载非 DigiCert 证书的副本。更多信息：https://docs.digicert.com/zh-cn/certificate-tools/ct-log-monitoring-service/
- 漏洞评估 - Secure Site EV、Secure Site Pro SSL 和 Secure Site Pro EV 证书包括漏洞评估服务。这项服务使你能够识别你的网站上最容易被利用的弱点并采取行动。要了解更多信息，请参阅 https://docs.digicert.com/zh-cn/certificate-tools/vulnerability-assessment-service/
- 恶意软件检查--安全网站证书附带方便的 VirusTotal 恶意软件检查。通过 70 多个反病毒扫描器和 URL/域名黑名单服务，快速分析你的公共域名。因为黑名单会削弱网站的可用性和在线收入，使用扫描结果来识别恶意软件的威胁，这样你就可以采取行动，使你的网站远离黑名单。
- 后量子密码学（PQC）--购买 Secure Site Pro SSL 或 Secure Site Pro EV SSL 的客户可以使用 DigiCert 的后量子密码学（PQC）工具包。更多信息：https://docs.digicert.com/zh-cn/certificate-tools/post-quantum-cryptography/
- 行业领先的保证--安全网站证书包括保护您和您的客户的保证：为您的企业提供 175 万美元或 200 万美元的 Netsure 安全担保，为您的客户提供行业最佳的 200 万美元的总信赖方保障。

DigiCert 智能标章

DigiCert 智能标章是一个新的动态网站标章，让网站用户相信他们的信息在网上是安全的。通过各种微互动实现的实时安全指标提醒用户，标章在页面上积极存在，网站已被验证，并且网站受到世界上最值得信赖的证书机构的有效证书的保护。

当网站用户将鼠标悬停在 DigiCert 智能标章上时，他们会看到该公司的标志（如果上传并经 DigiCert 验证）。他们还可以看到关于网站安全的可用信息，这些信息直接传递到封条上，因此用户不必离开页面来验证一个网站的合法身份。

智能标章可以被配置为在信息页面上显示以下选项。

恶意软件扫描：添加最近完成的恶意软件扫描的日期。网站用户可以看到你监控你的网站是否有病毒和恶意软件。

CT 日志监控：添加网站域名启用 CT 日志监控的日期。网站用户可以看到你监控的透明度日志，允许不良行为者为你的域名签发欺诈性证书时迅速采取行动。该功能仅适用于 Secure Site Pro 证书。

封锁名单：增加一个封锁名单检查。网站用户可以看到你的业务没有受到政府和特定国家的封锁名单的影响。

PCI 合规性扫描：添加最近完成的 PCI 合规性扫描的日期。网站用户可以看到，你对你的网站进行了监控，以确保其符合 PCI DDS 标准。该功能仅适用于 Secure Site Pro 和 Secure Site EV 证书，并且需要启用漏洞评估服务。

经过验证的客户：显示你成为 DigiCert 客户的时间。网站用户可以看到你使用 TLS/SSL 证书中最值得信赖的名称之一来保护你的网站有多长时间。

证书档案选项

证书档案允许你对你的证书做更多的事情。一些选项允许你在证书中加入一个额外的字段，而其他选项则允许你加入一个额外的 x.509 扩展。

- OCSP 装订：允许你在 OV 和 EV SSL/TLS 证书中包括 OCSP 装订扩展。网站服务器将自行查询 OCSP 服务器并缓存响应结果，然后在与浏览器进行 TLS 连接时返回给浏览器，这样浏览器就不需要再去查询了。如果客户端不支持 OCSP 扩展字段，则功能无法生效。
- HTTP 签名交换：允许你在 OV 和 EV SSL/TLS 证书中包括 CanSignHTTPExchanges 扩展。HTTP Signed Exchange 扩展正在积极开发中。随着行业的不断发展，这些要求可能会有更多变化。
- 授权证书：允许你在 OV 和 EV SSL/TLS 证书中包括 DelegationUsage 扩展。TLS 扩展的授权凭证正在互联网工程任务组（IETF）内积极开发。随着行业的不断发展，这些要求可能会有更多变化。
- 数据加密：允许你在 OV 和 EV SSL/TLS 证书中包括数据加密密钥使用扩展。当你想使用证书中的公开密钥来加密用户数据和应用程序数据时，这很有用。

更多信息：https://docs.digicert.com/zh-cn/manage-certificates/certificate-profile-options/

代码签名证书

DigiCert 代码签名证书通过验证你的应用程序的来源和完整性来增加信任。

- 对一个程序进行数字签名，以证明它没有被改变或被破坏
- 支持微软的 Authenticode、Office VBA、Java、Adobe AIR、苹果的 Mac OS 和 Mozilla 对象。
- 避免不必要的警告信息，确保你的应用程序可以被信任

DigiCert EV 代码签名证书通过验证应用程序的来源和完整性来增加信任。它还帮助用户在下载应用程序时避免警告信息。

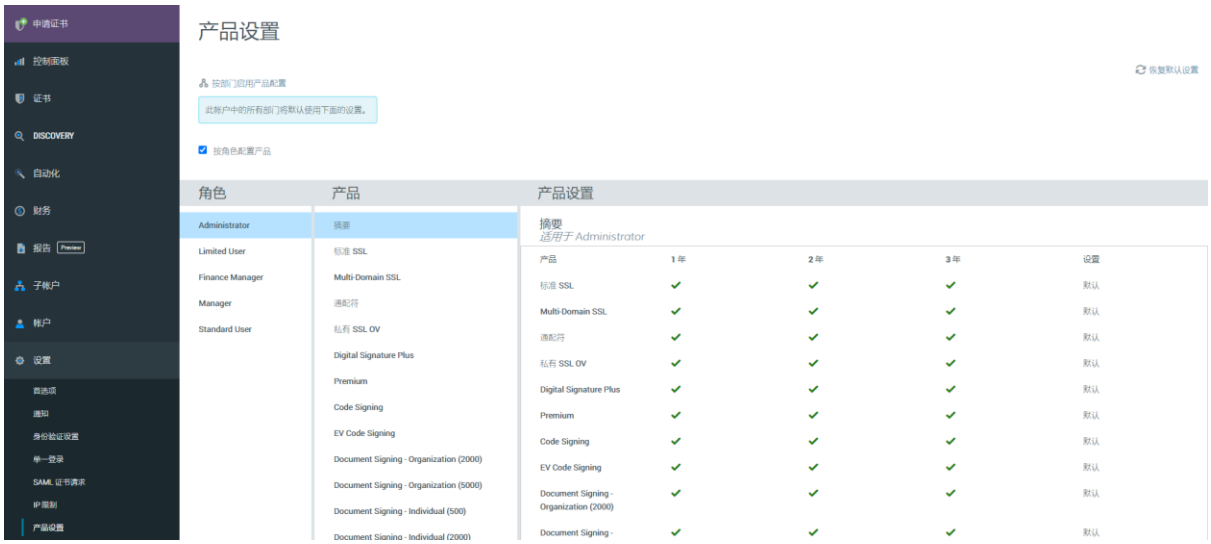
- 将标准代码签名证书的优点与严格的扩展验证过程相结合
- 提供兼容性，并授予 Windows 8 和 Internet Explorer 的即时信誉，消除了警告信息
- 支持微软的 Authenticode、Office VBA、Java、Adobe AIR、苹果的 Mac OS 和 Mozilla 对象。
- 扩展验证确保额外的组织审查，以保护你的用户和你的信誉
- 包括双因素认证以增强安全性

DigiCert EV 代码签名证书可以通过以下选项进行配置。

- 预先配置的硬件令牌 (USB key)：DigiCert 将你的 EV CS 证书安装在一个安全令牌上，并将令牌寄给你，并说明如何激活它。
- 现有令牌(USB key)：在 DigiCert 签发你的 EV CS 证书后，你需要在你的令牌上安装该证书。
- 加密硬件令牌（HSM): 在 DigiCert 签发你的 EV CS 证书后，将其安装在你的 HSM 设备上。(注意：你必须有一个符合 FIPS 140-2 级别或通用标准 EAL4+的设备。)

更多信息：https://docs.digicert.com/zh-cn/manage-certificates/code-signing-certificate/

产品设置



产品设置页面允许你配置每个账户或每个部门可以选择哪些证书产品。此外，产品选项也可以按用户角色进行配置。

域名和组织验证

域名控制验证(DCV)

在 DigiCert 签发 SSL/TLS 证书之前，你必须证明对订单上的域名和任何 SAN（多域名）的控制。我们把这个过程称为域名控制验证（DCV）过程。

DigiCert 目前支持这些 DCV 方法。

- 电子邮件验证：通过这种验证方法，DigiCert 发送三套 DCV 电子邮件：基于 WHOIS 的，构建的，以及基于 DNS TXT 的。为了证明对域名的控制，电子邮件收件人按照为该域名发送的确认电子邮件中的指示行事。确认过程包括访问电子邮件中提供的链接，并遵循页面上的指示。
- DNS CNAME 验证：使用这种验证方法，您将 DigiCert 生成的随机值（在您的 CertCentral 帐户中为该域名提供）作为 CNAME 记录添加到该域名的 DNS。当 DigiCert 对与该域名相关的 DNS CNAME 记录进行搜索时，如果找到了正确的记录，该验证被视为成功。
- DNS TXT 验证：使用这种验证方法，您将 DigiCert 生成的随机值（在您的 CertCentral 帐户中为该域提供）作为 TXT 记录添加到该域的 DNS。当 DigiCert 对与该域名相关的 DNS TXT 记录进行搜索时，如果找到了正确的记录，该验证被视为成功。
- 文件验证（HTTP 实际演示，也称为 FileAuth）：使用这种验证方法，你在你的网站上预定的位置添加一个包含 DigiCert 生成的随机值（在你的 CertCentral 帐户中为域名提供）的文件：[域名]/.known/pki-validation/fileauth.txt。一旦文件被创建并放在你的网站上，DigiCert 会访问指定的 URL，以确认我们的随机值的存在。

注意：对于 CertCentral 中的 DV 证书，DigiCert 目前支持以下 DCV 方法：基于 WHOIS 的电子邮件、构建的电子邮件、电子邮件到 DNS TXT 联系、DNS TXT 和文件验证。

更多信息：https://docs.digicert.com/zh-cn/manage-certificates/organization-domain-management/managing-domains-cc-guide/domain-pre-validation-domain-control-validation/

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

组织验证

为了验证一个组织，DigiCert 首先会验证申请证书的组织是否有良好的信誉。这可能包括确认良好的信誉和在公司登记处的积极注册。它还可能包括核实该组织没有被列入任何欺诈、网络钓鱼或政府限制实体和反恐怖主义数据库。

此外，我们核实申请证书的组织实际上是将被签发证书的组织。我们还核实了该组织的联系人。

在您的 CertCentral 账户中添加机构并使其得到验证是使您的域名得到验证的先决条件。尽快验证组织可以加快证书的颁发过程。

管理组织通常涉及添加一个组织，并提交给它进行验证。你也可以停用一个不再需要的组织。

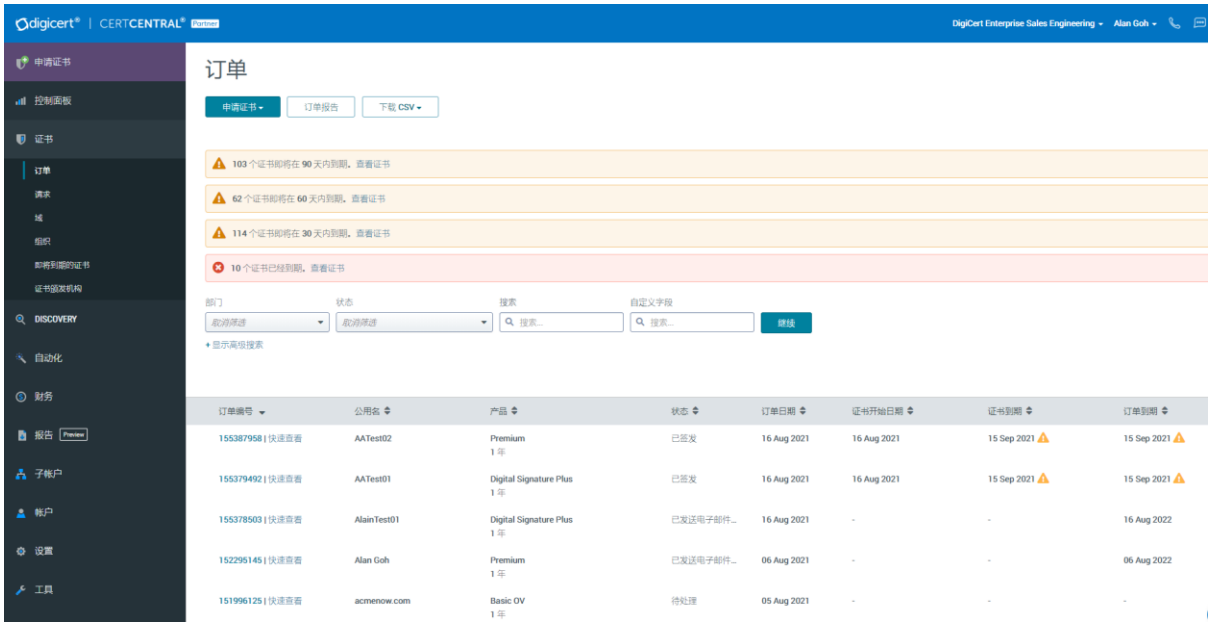
更多信息：https://docs.digicert.com/zh-cn/manage-certificates/organization-domain-management/manage-organizations/

在你提交了你的组织进行验证后，你可以开始提交域名进行验证，以及域名应被验证的授权类型。

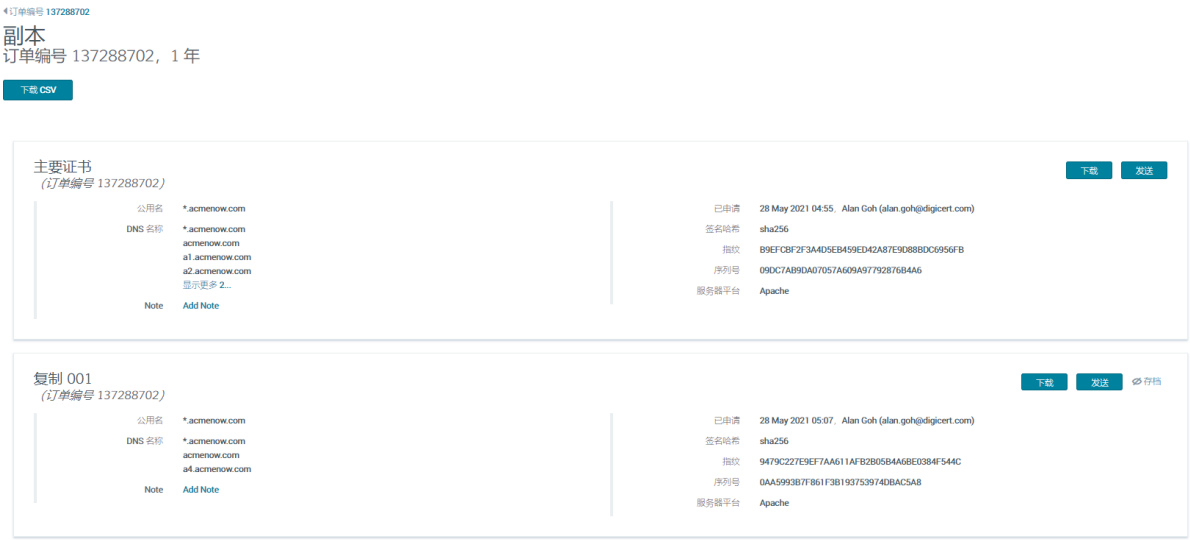
更多信息：https://docs.digicert.com/zh-cn/manage-certificates/organization-domain-management/managing-domains-cc-guide/

通常最好在申请证书之前验证域名和组织，但是在申请证书时也可以添加新的域名和组织。

订单和证书的管理



订单和证书可以直接从 CertCentral 平台管理。

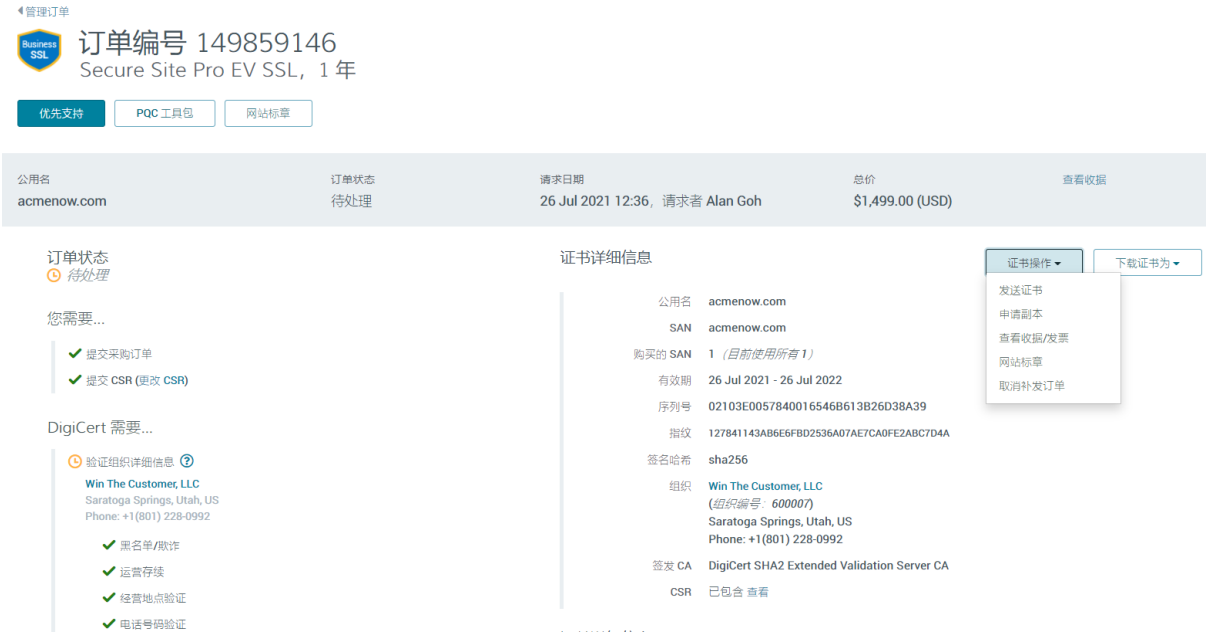


一个订单与所选择的多年计划有关。证书属于一个订单，在订单有效期内可能会被多次重新签发。一个订单的重要选项包括。

自动续订：在当前计划到期前 30 天自动续订多年计划。

自动补发：在当前证书到期日前 30 天自动签发新证书。

请注意，签发的证书的结束日期不能晚于相应订单的结束日期。



证书管理包括以下行动。

- 申请证书
- 批准证书申请
- 申请副本
- 补发证书
- 吊销证书
- 网站标章

证书批准

在默认情况下，证书请求在提交给 DigiCert 签发证书之前需要得到批准。用户申请证书后，管理员、经理、EV 验证用户、CS 验证用户或 EV CS 验证用户必须批准证书申请。接下来，该请求被发送到 DigiCert，以验证所有的预验证要求都已得到满足。

在用户申请证书后，如果需要，任何管理员、经理、EV 验证用户、CS 验证用户或 EV CS 验证用户也可以拒绝证书申请。例如，用户订购了错误的证书类型。

默认情况下，CertCentral 帐户被配置为一步到位的证书请求审批。在 DigiCert 开始处理订单（验证组织等）之前，账户管理员必须批准证书请求。然而，您可以为您的 CertCentral 管理

员、经理和财务经理从 OV/EV SSL 证书签发工作流程中移除审批步骤。审批要求可在 CertCentral 的设置/首选项页面中配置。

复制证书

所有 DigiCert 证书都有无限次的免费重复颁发。为了提高安全性并使其更容易在多个服务器上安装证书，生成一个新的 CSR 并为每个服务器创建一个副本。

副本证书中的详细信息将与原始证书完全相同。DigiCert 不会吊销你以前的证书副本。

更多信息：https://docs.digicert.com/zh-cn/manage-certificates/duplicate-ssltls-certificate/

补发证书

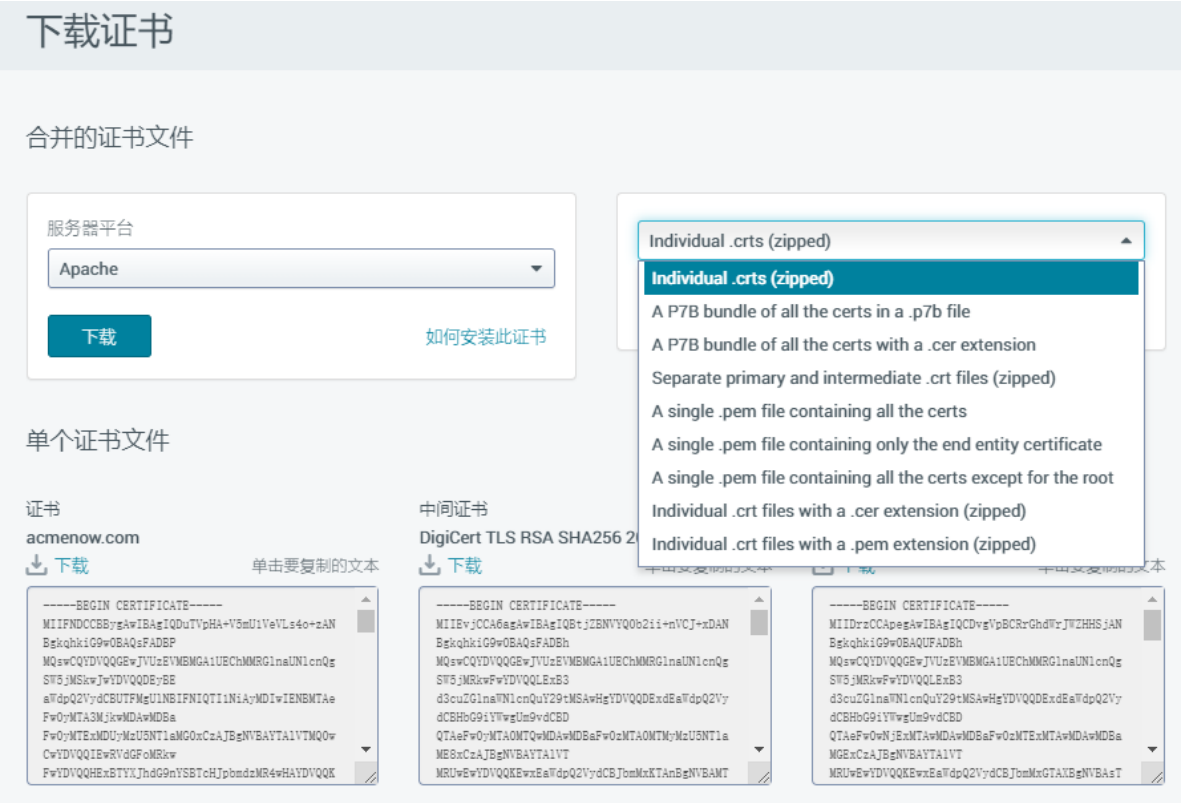
所有 DigiCert 证书都有无限次的免费补发。证书补发程序允许你修改已签发的证书。有些修改允许你在原始证书的基础上，形成该证书的两个或多个版本。例如，在补发证书时，你可以在原证书上添加域。在证书上添加域并不会吊销原始证书。

其他修改允许你创建一个新版本的证书，但是 Digicert 会废止原始证书和任何复制证书。例如：删除多域证书上的 SAN 或改变 SAN。

更多信息：https://docs.digicert.com/zh-cn/manage-certificates/reissue-ssltls-certificate/

下载证书

在 DigiCert 签发你的证书后，你可能想把证书直接下载到创建证书签名请求的服务器上（换句话说，就是拥有证书匹配密钥的服务器）。



CertCentral 提供了一种文件格式的选择。一旦你选择适当的服务器平台，将提供文件类型的选择。你也可以直接下载证书、中级证书和根证书的.pem 文件。

自定义订单表单字段

CertCentral 允许您在您的证书订单表中添加自定义字段。自定义字段元数据可用于搜索或排序一组符合元数据搜索标准的证书订单。

自定义订货单字段的功能。

- 适用于未来和现在的请求：当你添加自定义订单字段时，该字段也会被添加到未决请求中。如果该字段是必需的，在该字段完成之前，待批的申请不能被批准。

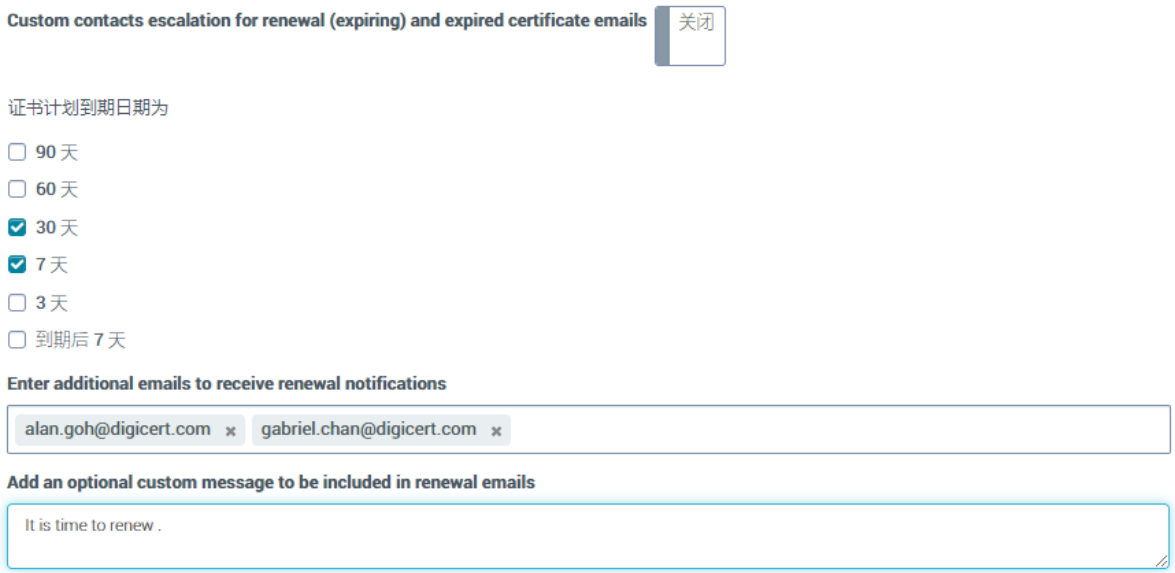
- 应用于整个账户：当您添加自定义订单字段时，这些字段将应用于整个账户的订单。自定义订单字段不能按部门设置。

- 适用于所有证书类型：当你创建自定义订单字段时，这些字段将被添加到所有证书类型（SSL、客户端、代码签名等）的订单中。你不能为只有 SSL 证书类型的订单添加自定义订单字段，等等。
- 适用于来宾 URL：当您添加自定义订单字段时，这些字段会添加到您的 CertCentral 账户内以及从您发出的任何客人 URL 中订购的证书上。
- 不同类型的选择：当你创建自定义订单字段时，可以添加不同类型的字段，如单行和多行文本框，电子邮件地址和电子邮件地址列表框，等等。
- 必填或可选：当你添加自定义订单字段时，你可以使它们成为必填或可选。在订单被批准之前，必须填写必要的字段。可选字段可以留空。
- 停用或激活：在您添加了一个自定义订单字段后，您可以根据需要停用（删除）和激活（重新添加）该字段。您停用的字段会从待处理的申请中删除，但不会从已发出的订单中删除。你所激活的字段会被添加到待处理的请求中。如果该字段是必填的，在申请被批准之前必须填写。

自定义字段数据可以在签发证书之前或之后的任何时候进行编辑。

更多信息：https://docs.digicert.com/zh-cn/manage-account/customize-your-certificate-request-forms/managing-custom-order-form-fields/

更新通知

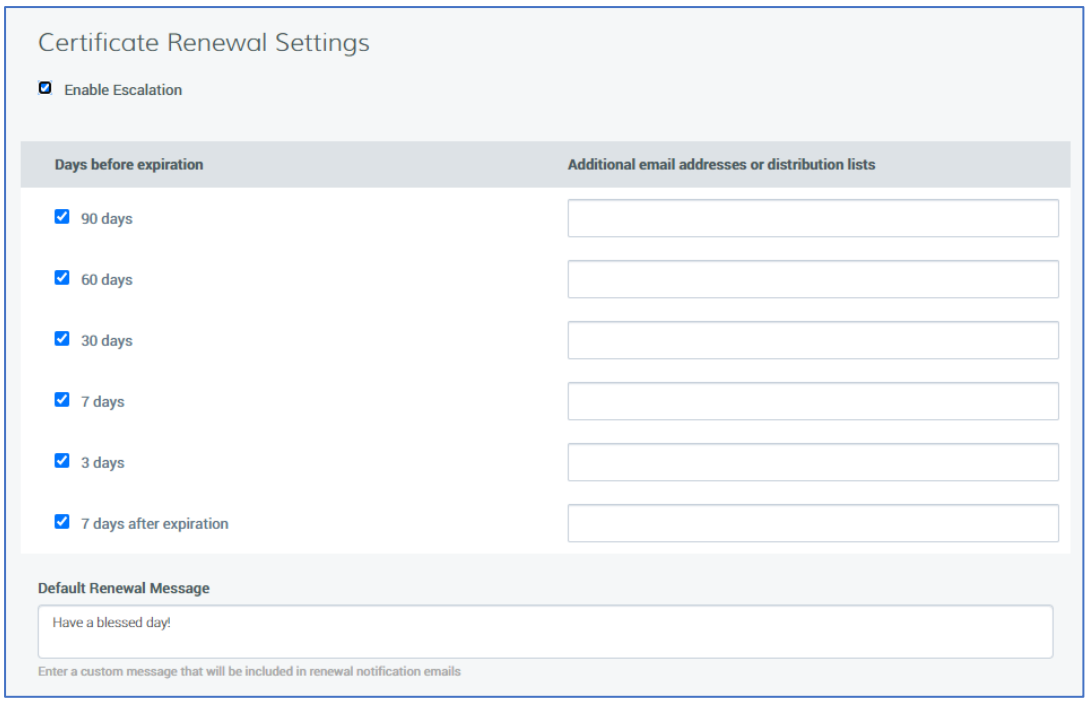


默认情况下，CertCentral 在证书过期前 90、60、30、7 和 3 天以及证书过期后 7 天发送证书更新通知。你可能想配置你的证书更新设置，以确定何时发送更新通知以及哪些电子邮件地址会收到通知。

你可以配置证书更新通知或紧急更新通知。

- 证书更新设置：允许你在证书临近到期或过期后的每个阶段向相同的电邮地址发

送更新通知。



- 紧急更新设置：在证书接近到期或过期后的每个阶段，设置附加电子邮件地址的更新通知。

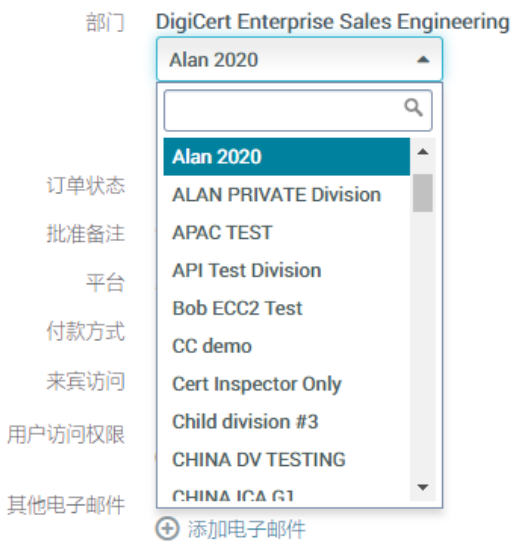
子账户和部门

部门划分

部门是 CertCentral 中用于限制用户和组织的一个特征。您可以将您组织中的用户添加到您的 CertCentral 帐户中并通过用户设置控制他们的权限。

你可以为一个部门提供尽可能多的自由，控制他们创建和管理用户、权限、域名和组织。与子账户不同，您对您账户中的用户、订单、设置和部门的活动有完全的可见性和控制。

此外，各部门可以共享账户资金，或者每个部门可以有自己的资金，只为自己的证书付费。



请注意，证书订单可以在任何时候被重新分配到不同的部门。

更多信息：https://docs.digicert.com/zh-cn/manage-account/division-management/

子账户

子账户是与顶级 "父 "CertCentral 账户相连并由其管理的 CertCentral 账户。子账户让经销商或其他组织让用户单独控制 CertCentral 账户和他们的证书管理过程，同时仍然让您这个 "父 "账户控制产品定价和计费。

子账户是专门为客户-企业关系或其他关系而设计的，在这种关系中，您需要控制子账户的产品定价或订单的计费。CertCentral 有四种类型的子账户。

- 零售业
- 企业
- 合作伙伴
- 管理的（通常只有 API 访问）。

每种账户类型都有一套不同的 CertCentral 功能供其使用。管理型子账户是仅适用于 API 的账户，旨在整合到现有的用户门户，并为父方提供一些额外的控制，如下载证书的能力。

子账户可以深入 3 层，即父级、子级和孙级.

更多信息：https://docs.digicert.com/zh-cn/manage-account/subaccounts-management/

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

用户角色

帐户管理员不给用户分配个人权限。相反，他们给每个用户分配一个角色。

- 管理员
- 标准用户
- 有限用户
- 财务经理
- 经理

分配给用户的角色决定了他们可以访问哪些账户功能。

可用的角色是:

- 标准用户：有权限下达和管理订单，更改须由经理或管理员批准。
- 经理：管理财务、创建和批准请求、管理订单和域名，以及查看和编辑用户的权限。
- 财务经理：管理财务的权限，以及下达和管理订单。
- 管理员：完全的管理权限，包括创建部门和用户的权限，以及管理用户的权限

要创建一个有限用户的角色，请选择标准用户并勾选 "限制下达和管理自己的订单"。

更多细节见下文:

管理员	具有这些权限的完整 CertCentral 账户访问。 • 访问和管理发现。 • 管理部门（创建和编辑）和账户用户（创建、删除和编辑）。 • 管理组织（添加新组织）、域名（添加或停用）、来宾请求和 API 访问。 • 查看所有证书申请和证书订单，申请证书，批准证书申请，并运行订单报告。 • 管理账户财务设置和财务（查看余额历史，运行支出报告，存入资金，以及更多）。 • 管理账户设置（认证设置、IP 访问限制、产品限制等）、审计设置和审计日志。
标准用户	具有这些权限的账户用户。

	• 申请证书。 • 监测证书请求和订单（他们自己的和其他的）。 • 经理或管理员必须批准更改。
有限用户	具有这些权限的账户用户。 • 申请证书。 • 监控他们自己的证书请求和订单。 • 经理或管理员必须批准更改。
财务经理	有限账户用户，其主要作用是管理账户财务。包括这些权限; • 查看余额历史、支出报告和账户定价。 • 管理采购订单和存入资金。 • 管理订单报告。 • 申请证书。 • 监控他们自己的证书请求和订单。
经理	有限账户用户，其主要作用是帮助管理账户。包括这些权限; • 访问和管理发现。 • 查看部门和管理账户用户（编辑）。 • 查看组织和管理域名（添加或停用）。 • 查看所有证书申请和证书订单，申请证书，批准证书申请，并运行订单报告。 • 管理账户财务设置和财务（查看余额历史，运行支出报告，存入资金，以及更多）。 • 管理审计设置和审计日志。

所有的用户角色都可以被限制在指定的部门中处理证书。

默认情况下，管理员和经理没有权限批准 EV 证书、EV 代码签名证书或代码签名证书请求。为了批准这些类型的请求，经理必须被分配适当的子权限。

更多信息：https://docs.digicert.com/zh-cn/manage-account/certcentral-user-roles-account-access/roles-account-access/

用户访问/认证控制方法

密码

最低密码要求可从 CertCentral 设置。

双因素认证

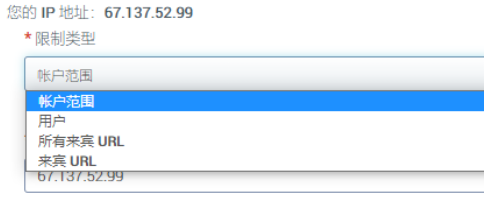
要在你的登录过程中增加第二种身份验证形式，你需要为你的账户配置双因素认证要求。你可以根据需要为所有用户和个别用户配置一个要求。

除了用户 ID/密码要求外，还可以要求用户使用以下因素之一。

- 一次性密码（OTP）：应用此规则将要求用户在下一次登录时初始化其 OTP 应用程序或设备，并生成一次性密码。OTP 身份验证要求使用任何支持基于时间的一次性密码 (TOTP) 协议的移动应用程序。
- 客户端证书：应用此规则将要求用户在下一次登录时在浏览器中生成客户端证书。Internet Explorer（Windows）和 Safari（Mac）是唯一支持客户端证书生成的浏览器。

更多信息：https://docs.digicert.com/zh-cn/manage-account/certcentral-two-factor-authentication/configure-two-factor-authentication-requirements/

IP 限制



为了提高安全性，DigiCert 提供了限制你帐户的能力，以便只能从某些 IP 地址访问你的帐户。这些都是可以设定的。

- 帐户范围
- 每个用户
- 每个来宾的 URL
- 所有来宾的 URL

单点登录

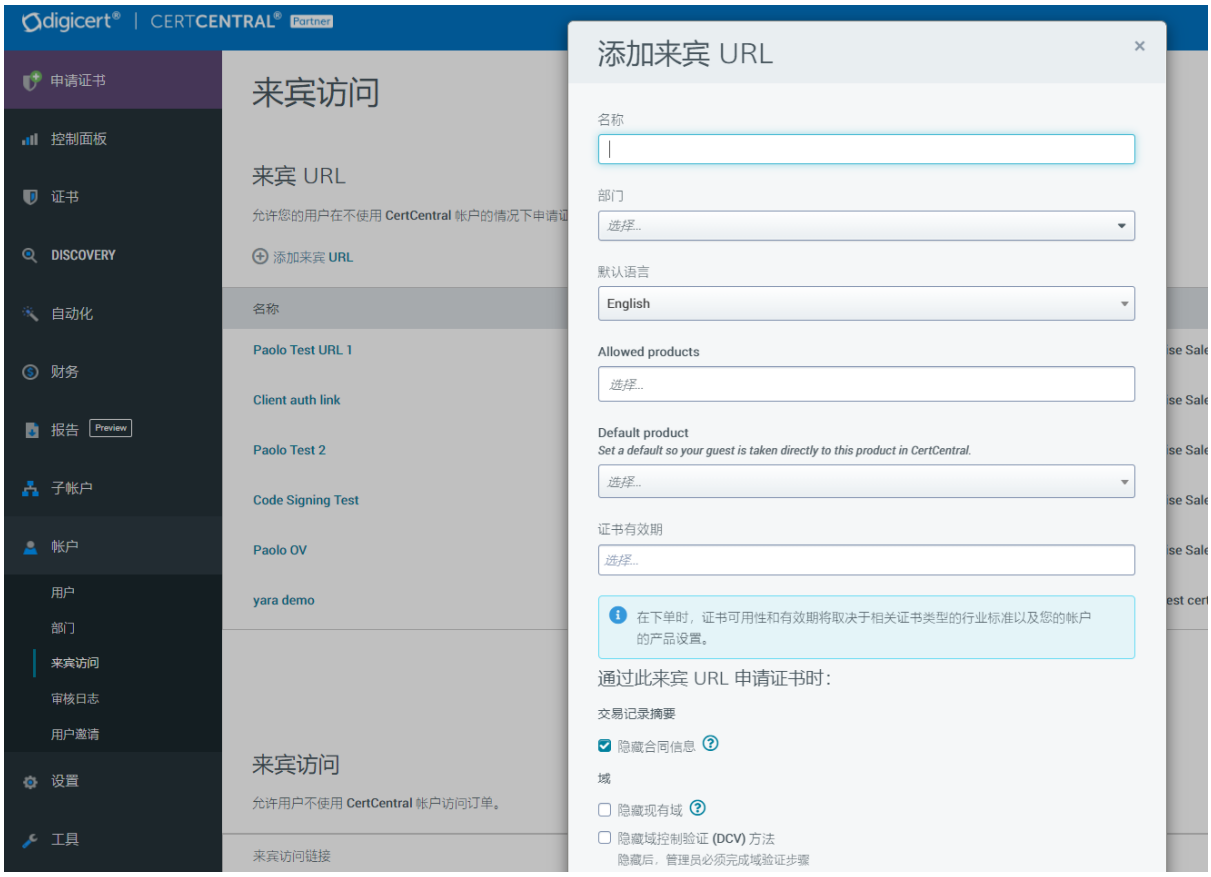
消除对多个密码的需求并使用 SAML 单点登录（SSO）将您的身份提供者（IdP）与 CertCentral 连接起来。

一旦您配置了 SAML 到 CertCentral 的连接，您的 CertCentral 用户就可以使用他们的 SSO 凭证来登录。他们将通过 DigiCert 提供的服务提供商发起的自定义 SSO URL 或你提供的 IDP 发起的 SSO URL 访问 SSO 账户登录页面。

更多信息：https://docs.digicert.com/zh-cn/manage-account/saml-single-sign-on-admin-guide/

来宾访问选项

来宾 URL



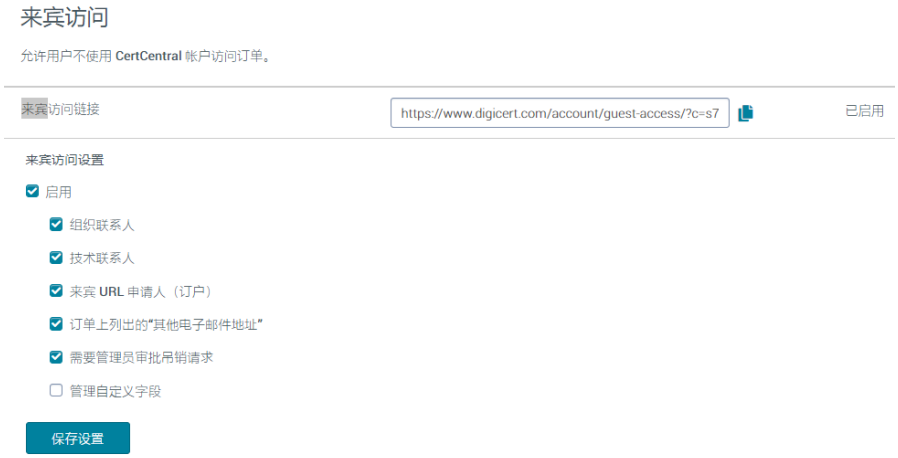
来宾 URL 让你为用户提供申请证书的能力，而无需将他们加入你的账户。来宾 URL 只允许用户访问账户内的特定证书请求页面。该用户不能访问账户内的任何其他东西。

来宾 URL 的配置有以下细节。

- 命名
- 部门
- 允许的证书类型
- 证书的有效期限

更多信息：https://docs.digicert.com/zh-cn/manage-account/managing-guest-urls/

来宾访问



来宾访问允许用户在没有 CertCentral 帐户的情况下管理其订单。通过他们的电邮地址和订单号（或证书中的 FQDN），他们可以下载、重新补发或吊销证书。来宾访问可以为账户中的所有订单启用，也可以为单个订单启用。

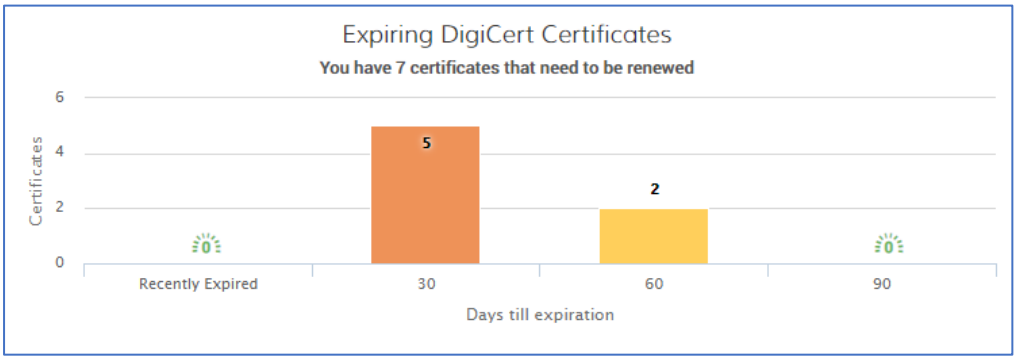
您可以通过启用或禁用组织联系人、技术联系人、来宾 URL 请求者（订户）（下订单的电邮地址）以及订单复选框中列出的 "其他电子邮件 "来控制哪些订单联系人有资格获得来宾访问。

您的 CertCentral 账户有一个独特的来宾访问登录页面。为了确认您个人的身份，CertCentral 会发送认证邮件，提供两小时的访问。

更多信息：https://docs.digicert.com/zh-cn/manage-account/guest-access/

报告和通知

报告



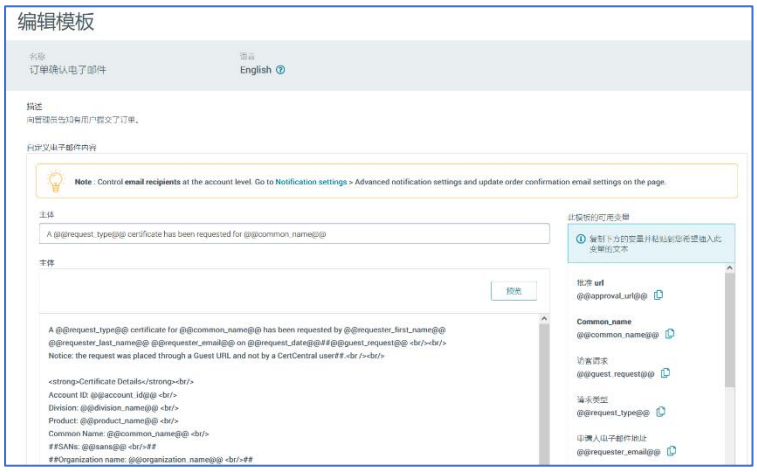
CertCentral 在控制台内或通过 API 提供控制面板和报告。

控制面板：以图形方式组织你的证书，包括即将到期的证书和待处理请求。

订单报告：查找所有签发的证书，并通过任何领域进行筛选。

通知

CertCentral 在整个订单审批过程，以及在证书即将到期或已经到期时，都会向用户发送电邮。你可以定制这些电子邮件模板，使它们适合你的账户或组织的需要。

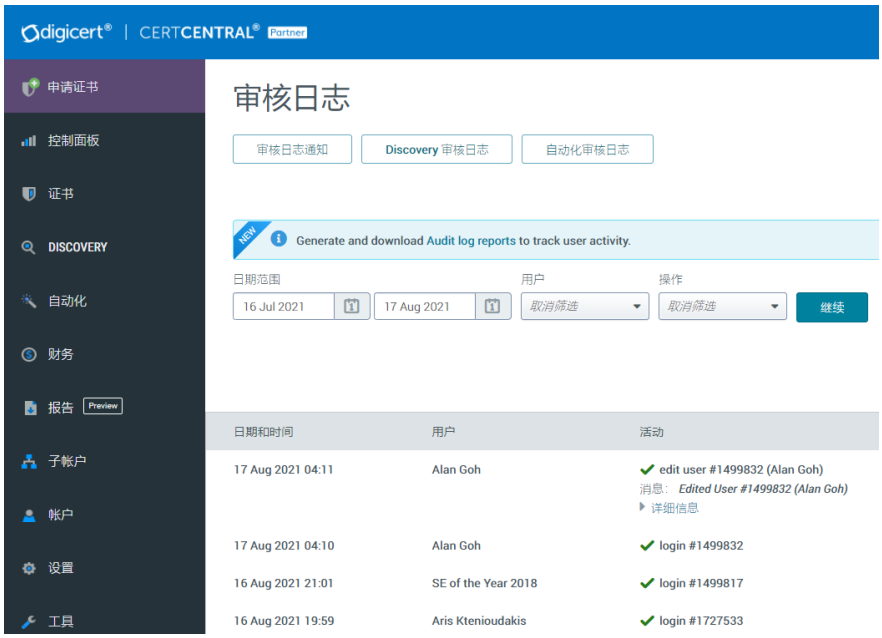


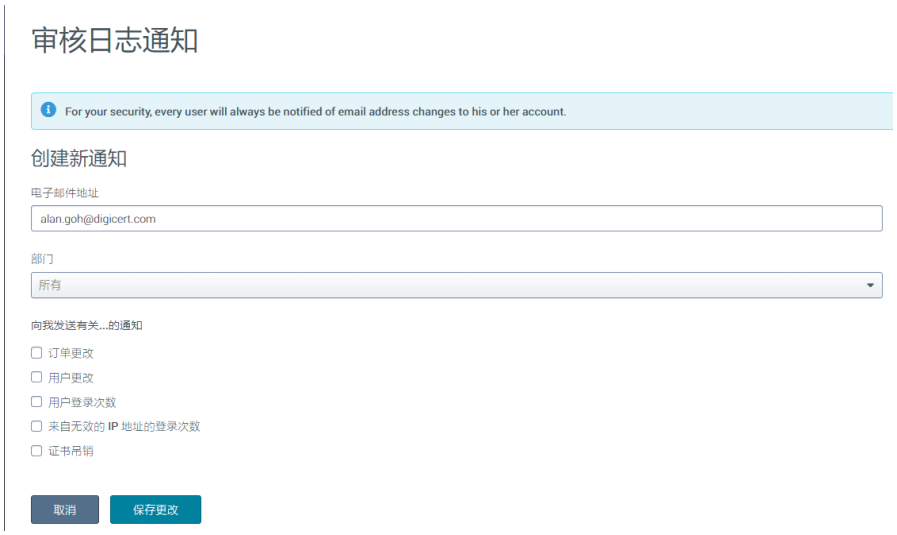
基本通知设置允许你指定电子邮件收件人和电子邮件语言。

自定义电子邮件模板允许你编辑标准的电子邮件模板。

更多信息：https://docs.digicert.com/zh-cn/manage-account/account-notifications/customize-email-templates/

审核日志





审核日志是你账户中发生的活动历史记录。CertCentral 自动保留审计日志，记录您账户中 50 多种不同的操作（包括登录、证书请求和吊销），以及时间戳和执行该操作的用户。要查看你账户中的审计日志，请访问审核日志页面。

单击 "审核日志通知"，为特定事件创建电子邮件通知。