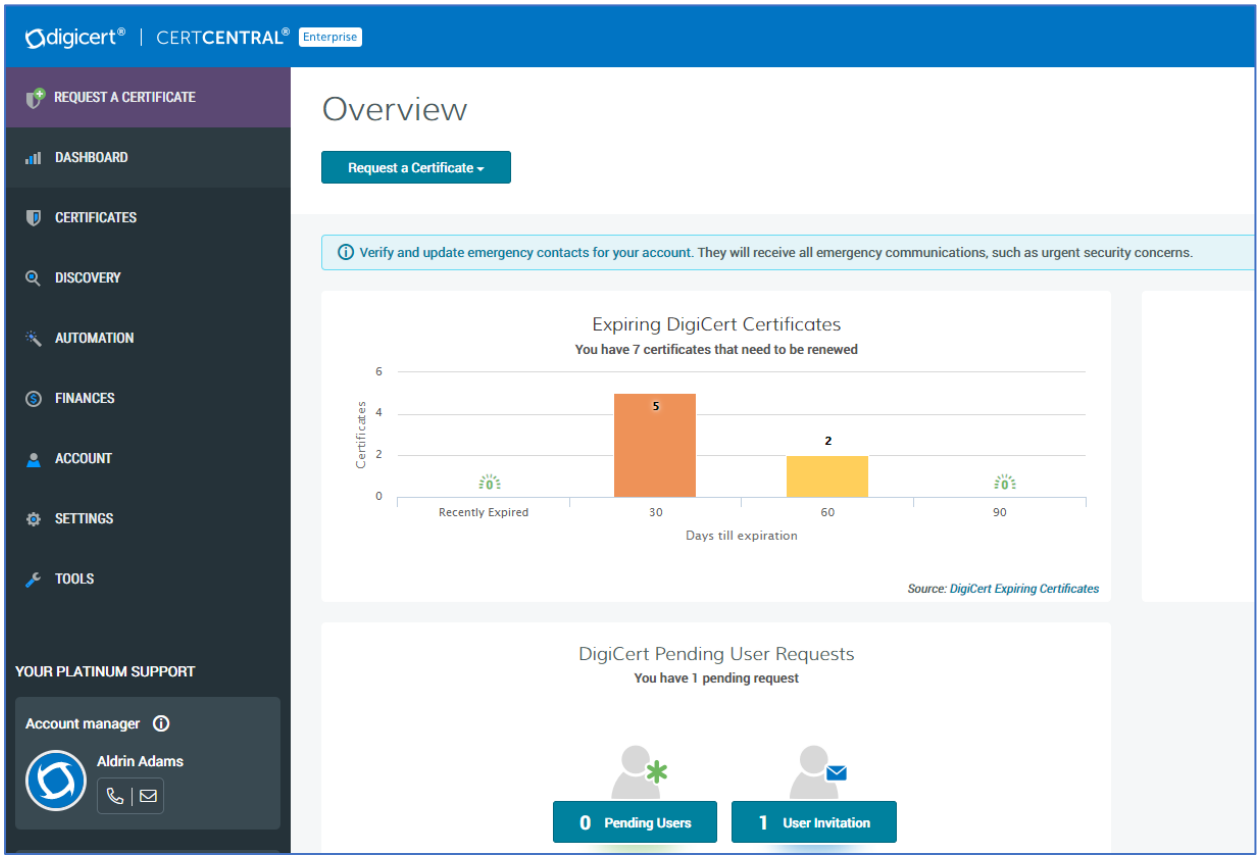
Certificaciones técnicas DigiCert Guía de estudio de CertCentral® Professional

2021 v2



2021 DigiCert, Inc. Todos los derechos reservados. DigiCert es una marca registrada de DigiCert, Inc. en Estados Unidos y en otros países. Todas las demás marcas comerciales y registradas son propiedad de sus respectivos dueños.

Contenido

Introducción 4
Objetivos 5
Productos de certificados SSL/TLS 6
Certificados Flex 6
Ventajas del certificado Secure Site 7
Sello inteligente DigiCert 9
Opciones de perfil de certificado 10
Productos de certificados de firma de código 11
Configuración de productos 12
Validación de dominios y organizaciones 12
Validación de control de dominio (DCV) 12
Validación de la organización 13
Gestión de pedidos y certificados 14
Aprobación del certificado 16
Duplicación de certificados 17
Reemisión del certificado 17
Descargar un certificado 17
Campos de pedido personalizados 18
Notificación de renovación 19
Subcuentas y divisiones 20
Divisiones 20
Subcuentas 21
Funciones de usuarios 21
Métodos de control de acceso/autenticación de usuarios 23
Contraseñas 23
Autenticación de dos factores 23
Restricciones a la IP 24
Inicio de sesión único (Single Sign-On) 24
Opciones de acceso para invitados 25
URL para invitados 25
Acceso para invitados 26
Informes y notificaciones 27
Informes 27

Notificaciones por correo electrónico 27
Registro de auditoría..... 28

Introducción

Esta guía de estudio está diseñada para ayudarle a preparar el examen de evaluación de la Certificación Técnica DigiCert: CertCentral Professional. El examen constará de 50 preguntas tipo test con un tiempo máximo de 1 hora.

El público objetivo de esta evaluación es cualquier persona que trabaje con la plataforma de gestión de certificados CertCentral de DigiCert en un papel técnico (soporte técnico, administrador de SSL/TLS, etc.).

Antes de intentar una evaluación de certificación, debe revisar los objetivos que se indican a continuación. Si cree que ya es capaz de cumplir todos los objetivos enumerados, le invitamos a programar una evaluación. Sin embargo, si hay algún objetivo de la lista en el que pueda necesitar una preparación adicional, debe planificar la investigación de estos temas en detalle antes de programar una evaluación.

Puede encontrar más información en la Guía de Formación Profesional de CertCentral, que puede descargarse de https://www.digicert.com/tls-ssl/tls-certification-program. Tenga en cuenta que estos recursos son sólo un punto de partida. Se recomienda encarecidamente que investigue más para estar totalmente preparado para una evaluación sobre todos los objetivos, incluyendo la experiencia práctica utilizando DigiCert CertCentral.

Además, es posible asistir a un taller de DigiCert impartido por un instructor, que ofrecerá información detallada sobre muchos de los objetivos de la evaluación. Póngase en contacto con su gestor de cuentas de DigiCert si desea obtener más información.

Objetivos

Antes de intentar el examen de evaluación de la Certificación Técnica DigiCert: CertCentral Professional, debe ser capaz de hacer lo siguiente:

- Enumerar y comparar los productos de certificados SSL/TLS y Code Signing disponibles en DigiCert CertCentral Enterprise
- Describir los derechos del certificado SSL para empresas, por ejemplo, el monitoreo de registros de TC (CT Log Monitoring), el escaneo de malware, el DigiCert Smart Seal
- Describir las opciones de perfil de certificado disponibles en DigiCert CertCentral, por ejemplo, intercambio firmado HTTP
- Describir las políticas y los métodos utilizados por DigiCert para la validación de dominios y organizaciones
- Enumerar y comparar los roles de los usuarios en DigiCert CertCentral
- Demostrar la gestión de pedidos, certificados, organizaciones y dominios en DigiCert CertCentral
- Explicar y demostrar los métodos de control de acceso/autenticación de usuarios en DigiCert CertCentral, por ejemplo, SAML, 2FA
- Explicar y demostrar el uso de subcuentas y divisiones en DigiCert CertCentral
- Describir las opciones de informes disponibles en DigiCert CertCentral
- Describir y demostrar las opciones de acceso de invitados en CertCentral: URL de invitados y función de acceso de invitados

Productos de certificados SSL/TLS

La mayoría de las empresas utilizan la gama de certificados SSL para empresas de DigiCert:

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

Estos productos certificados tienen muchas opciones y ventajas. Se describen a continuación.

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

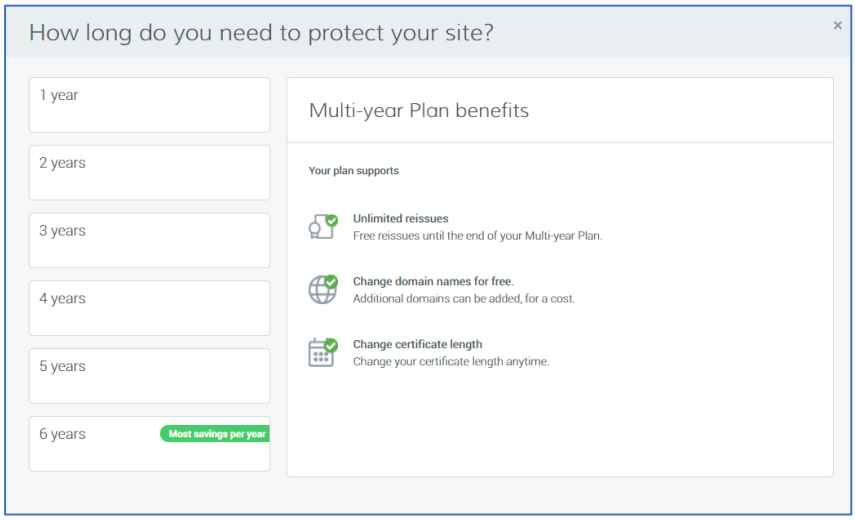
Certificados Flex

Los certificados DigiCert Secure Site y Secure Site Pro admiten cualquier tipo de configuración de dominio y pueden solicitarse como certificados de dominio único o multidominio con cualquier combinación de nombre de dominio completo (FQDN) y SANs comodín.

Esto le da la flexibilidad de pedir exactamente lo que quiere y añadir SANs adicionales durante la vida del certificado sin necesidad de cambiar de producto. Estos certificados no tienen versiones multidominio o comodín dedicadas, sino que se añaden al configurar el certificado base.

Más información: https://docs.digicert.com/es/manage-certificates/flex-certificates/

Planes Plurianuales



Los planes plurianuales de DigiCert le permiten pagar un único precio por hasta seis años de cobertura de certificados SSL/TLS. Con los planes plurianuales, usted elige el certificado SSL/TLS, la duración de la cobertura que desea (hasta seis años) y la validez del certificado. Hasta que el plan expire, usted reedita su certificado sin coste alguno cada vez que llega al final de su periodo de validez. Tenga en cuenta que el periodo máximo de validez de un certificado SSL/TLS de confianza pública es actualmente de 397 días, por lo que es posible que tenga que reemitir dicho certificado varias veces durante un Plan Plurianual.

Cuando se reemiten certificados para un Plan Plurianual, se puede hacer lo siguiente:

- Establecer una nueva fecha de caducidad para el certificado reemitido: El período máximo de validez de un certificado reemitido es la vida útil máxima del certificado definida por los requisitos básicos de CA/B Forum o el final del Plan Plurianual, lo que ocurra antes.
- Cambiar o eliminar dominios: Eliminar y cambiar dominios requiere que DigiCert revoque todos los certificados emitidos anteriormente. DigiCert espera entre 48 y 72 horas antes de revocar el certificado original y los duplicados y reemisiones existentes.
- Añadir dominios: Añadir dominios puede suponer un coste adicional. Los precios de los nuevos dominios se prorratean y se aplican en función del tiempo restante del Plan Plurianual.

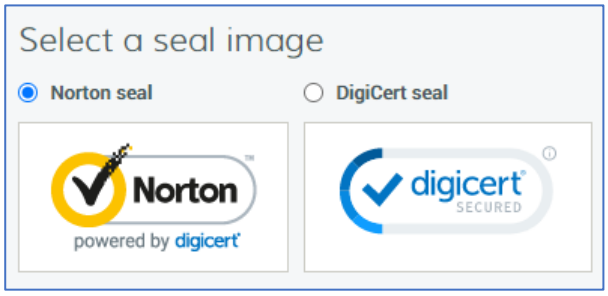
Más información: https://docs.digicert.com/es/manage-certificates/multi-year-plans/

Ventajas del certificado Secure Site

Además de la encriptación industrial de 2048 bits, los certificados DigiCert Secure Site incluyen beneficios adicionales, como el soporte prioritario. Estas ventajas están disponibles durante la vigencia de su pedido de certificado. Cada vez que renueve el pedido del certificado Secure Site, sus beneficios se trasladarán automáticamente al nuevo pedido.

- Validación prioritaria: los pedidos de Secure Site se colocan en la parte superior de nuestras colas de validación para que nuestros agentes puedan responder a estos pedidos primero.

- Asistencia prioritaria: los certificados Secure Site tienen acceso a dos colas de asistencia prioritaria para que nuestro equipo de asistencia pueda responder a sus necesidades en primer lugar: estado del pedido y validación e instalación y configuración.
- Dos sellos de sitio premium - Los certificados Secure Site vienen con las dos marcas de confianza más reconocidas en la web: DigiCert y Norton. Elija el sello de sitio premium que desea utilizar para mostrar una prueba de confianza en su sitio.



- Monitoreo del registro de CT (Certificate Transparency): el servicio de monitoreo del registro de CT le permite monitorear los registros CT públicos de los certificados SSL/TLS emitidos para los dominios de su certificado **Secure Site Pro** o **Secure Site Pro EV**. Una vez que haya habilitado el monitoreo del registro CT para un pedido de certificado Secure Site Pro, recibirá dos tipos de notificaciones por correo electrónico: resumen diario del registro CT y, si es necesario, notificaciones urgentes. Se envían notificaciones por correo electrónico a los administradores de cuentas, lo que les permite comprobar los registros CT de sus dominios sin tener que iniciar sesión en su cuenta de CertCentral todos los días. El servicio de monitorización de registros CT extrae los certificados SSL/TLS descubiertos en su cuenta de CertCentral, donde puede ver los detalles de los certificados para identificar rápidamente cualquier certificado mal emitido para sus dominios. También puede descargar copias de los certificados que no son de DigiCert directamente desde su cuenta de CertCentral. Más información: https://docs.digicert.com/es/certificate-tools/ct-log-monitoring-service/
- Evaluación de la vulnerabilidad - Los certificados **Secure Site EV, Secure Site Pro SSL y Secure Site Pro EV** incluyen el acceso a un servicio de evaluación de la vulnerabilidad. Este servicio le permite identificar y actuar contra los puntos débiles más explotables de su sitio web. Para saber más, consulte https://docs.digicert.com/es/certificate-tools/vulnerability-assessment-service/
- Comprobación de malware: los certificados Secure Site incluyen un cómodo acceso a una comprobación de malware de VirusTotal. Analice rápidamente sus dominios públicos con más de 70 escáneres antivirus y servicios de listas negras de URL/dominios. Utilice los resultados del escaneo para identificar las amenazas de malware, de modo que pueda tomar medidas para mantener su sitio fuera de las listas negras, que pueden perjudicar la disponibilidad del sitio y la facturación online. Más informacion: https://docs.digicert.com/es/manage-certificates/access-your-secure-site-certificate-benefits/access-secure-site-malware-check/
- Criptografía post-cuántica (PQC) - Los clientes que adquieren un certificado **Secure Site Pro o Secure Site Pro EV** tienen acceso al kit de herramientas de criptografía post-cuántica (PQC) de DigiCert. Más información: https://docs.digicert.com/es/certificate-tools/post-quantum-cryptography/
- Garantías líderes en el sector: los certificados Secure Site incluyen garantías para protegerle a usted y a sus clientes: una garantía de protección Netsure de 1,75 millones de dólares o de 2 millones de dólares para su empresa y una garantía agregada de 2 millones de dólares para sus clientes.

Sello inteligente DigiCert

El DigiCert Smart Seal es un nuevo sello de sitio dinámico que ofrece a los visitantes del sitio web la confianza de que su información está segura en la web. Los indicadores de seguridad en tiempo real, habilitados a través de varias microinteracciones, alertan a los visitantes de que el sello está presente de forma activa en la página, que el sitio ha sido validado y que está protegido por un certificado activo de la autoridad certificadora más fiable del mundo.

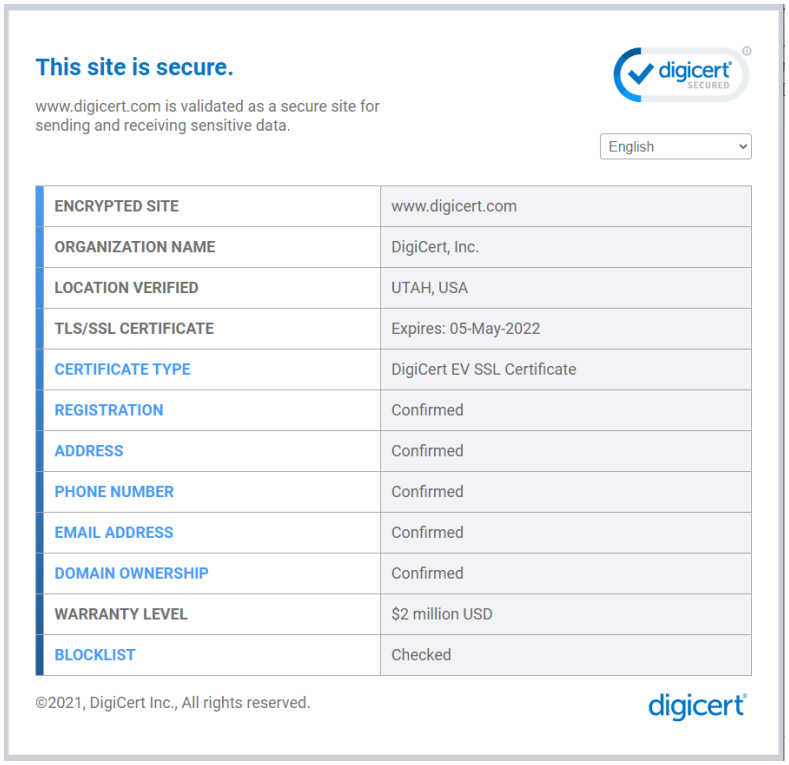
Cuando los visitantes del sitio web pasan el ratón por encima del Sello Inteligente DigiCert, ven el logotipo de la empresa (si está cargado y verificado por DigiCert). También ven información útil sobre la seguridad del sitio entregada directamente al sello, de modo que los usuarios no tienen que abandonar la página para verificar la identidad legítima de un sitio.

El Sello Inteligente puede ser configurado para mostrar las siguientes opciones en la página de información:

Escaneo de malware: Añade la fecha del último escaneo de malware realizado. Los visitantes del sitio pueden ver que usted vigila su sitio web en busca de virus y malware.

Monitorización de registros CT: Añade la fecha en la que activaste la monitorización de registros CT para el dominio de tu sitio web. Los visitantes del sitio pueden ver que usted supervisa los registros de transparencia, lo que le permite actuar rápidamente si un mal actor emite un certificado fraudulento para su dominio. Esta función sólo está disponible para los certificados Secure Site Pro.

Lista de bloqueo: Añade una comprobación de la lista de bloqueo. Los visitantes del sitio pueden ver que su empresa está libre de las listas de bloqueo de gobiernos y países.



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.

Escaneo de cumplimiento PCI: Añada la fecha del último escaneo de cumplimiento PCI realizado. Los visitantes del sitio pueden ver que usted supervisa su sitio web para asegurarse de que cumple con las normas DDS de la PCI. Esta función sólo está disponible para los certificados Secure Site Pro y Secure Site EV y requiere que el servicio de Evaluación de Vulnerabilidad esté habilitado para su pedido de certificados.

Cliente verificado: Muestra el tiempo que lleva siendo cliente de DigiCert. Los visitantes del sitio pueden ver el tiempo que lleva utilizando uno de los nombres más fiables en certificados TLS/SSL para proteger sus sitios.

Opciones de perfil de certificado

Los perfiles de certificado le permiten hacer más cosas con sus certificados. Algunas opciones le permiten incluir un campo adicional en su certificado, mientras que otras le permiten incluir una extensión x.509 adicional.

- OCSP Must-Staple: Permite incluir la extensión OCSP Must-Staple en los certificados SSL/TLS OV y EV. Los navegadores que soportan el must-staple OCSP pueden mostrar un intersticial de bloqueo a los usuarios que acceden a su sitio. Asegúrese de que su sitio esté configurado para servir adecuadamente y con solidez las respuestas OCSP engrapadas antes de instalar el certificado.
- HTTP Signed Exchange: Permite incluir la extensión CanSignHTTPExchanges en un certificado OV y EV SSL/TLS. La extensión HTTP Signed Exchange está en desarrollo activo. Es posible que se produzcan cambios adicionales en los requisitos a medida que el sector siga desarrollándose.
- Credenciales delegadas: Permite incluir la extensión DelegationUsage en los certificados SSL/TLS OV y EV. La extensión de credenciales delegadas para TLS está en desarrollo activo dentro del Grupo de Trabajo de Ingeniería de Internet (IETF). Es posible que se produzcan cambios adicionales en los requisitos a medida que el sector siga desarrollándose.
- Cifrado de datos: Permite incluir la extensión de uso de claves de cifrado de datos en los certificados SSL/TLS OV y EV. Es útil cuando se quiere utilizar la clave pública del certificado para cifrar los datos del usuario y de la aplicación.

Más información: https://docs.digicert.com/es/manage-certificates/certificate-profile-options/

Productos de certificados de firma de código

Un certificado de firma de código DigiCert aumenta la confianza al verificar el origen y la integridad de su aplicación.

- Firma digitalmente un programa para demostrar que no ha sido alterado o comprometido
- Admite Microsoft Authenticode, Office VBA, Java, Adobe AIR, Mac OS de Apple y objetos de Mozilla
- Evita los mensajes de advertencia innecesarios y garantiza la confianza en sus aplicaciones

Un certificado de firma de código DigiCert EV aumenta la confianza al verificar el origen y la integridad de la aplicación. También ayuda a los usuarios a evitar los mensajes de advertencia al descargar la aplicación.

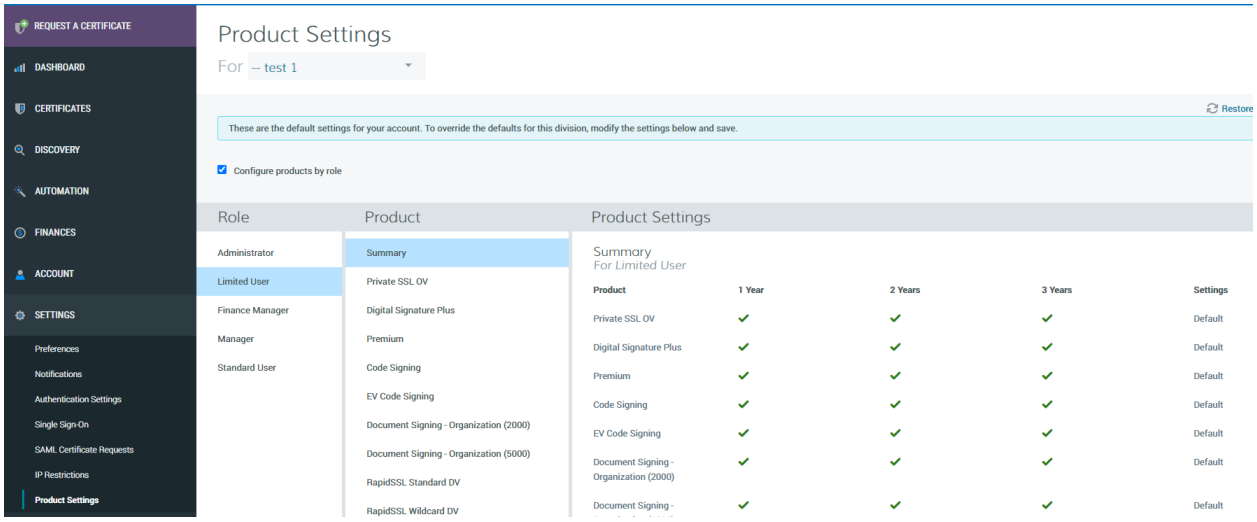
- Combina las ventajas de un certificado de firma de código estándar con un riguroso proceso de validación ampliada
- Proporciona compatibilidad y otorga reputación inmediata con Windows 8 e Internet Explorer, eliminando los mensajes de advertencia
- Admite Microsoft Authenticode, Office VBA, Java, Adobe AIR, Mac OS de Apple y objetos de Mozilla
- La Validación Extendida garantiza una investigación adicional de la organización para proteger a sus usuarios y su reputación
- Incluye la autenticación de dos factores para mejorar la seguridad

Un certificado de firma de código DigiCert EV puede ser aprovisionado con las siguientes opciones:

- Token de hardware preconfigurado: DigiCert instala su certificado EV CS en un token seguro y le envía el token con instrucciones para activarlo.
- Token existente: Después de que DigiCert emita su certificado EV CS, debe instalar el certificado en su token.
- HSM: Después de que DigiCert emita su certificado EV CS, instálelo en su dispositivo HSM. (Nota: Debe tener un dispositivo que cumpla con FIPS 140-2 Nivel 2 o Common Criteria EAL4+).

Más información: https://docs.digicert.com/es/manage-certificates/code-signing-certificate/

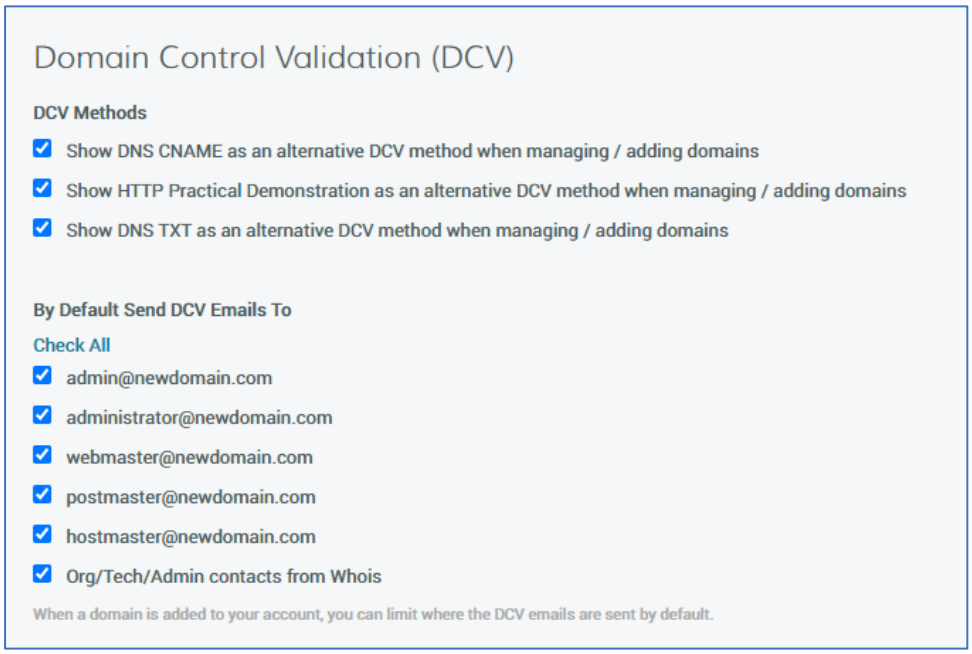
Configuración de productos



La página de configuración de productos le permite configurar qué productos de certificado pueden seleccionarse por cuenta o por división. Además, las opciones de los productos también pueden configurarse por rol de usuario.

Validación de dominios y organizaciones

Validación de control de dominio (DCV)



Antes de que DigiCert pueda emitir un certificado SSL/TLS, debe demostrar el control sobre los dominios y cualquier SAN (Subject Alternative Names) en el pedido. Nos referimos a este proceso como el proceso de Validación de Control de Dominio (DCV).

Actualmente, DigiCert admite estos métodos DCV:

- Validación por correo electrónico: Con este método de validación, DigiCert envía tres conjuntos de correos electrónicos DCV: basados en WHOIS, construidos y basados en DNS TXT. Para demostrar el control sobre el dominio, un destinatario de correo electrónico sigue

las instrucciones de un correo electrónico de confirmación enviado para el dominio. El proceso de confirmación consiste en visitar el enlace proporcionado en el correo electrónico y seguir las instrucciones de la página.

- Validación DNS CNAME: Con este método de validación, usted añade un valor aleatorio generado por DigiCert (proporcionado para el dominio en su cuenta CertCentral) al DNS del dominio como un registro CNAME. Cuando DigiCert hace una búsqueda de registros DNS CNAME asociados al dominio, podemos encontrar un registro donde el valor del registro incluye el valor aleatorio de DigiCert.
- Validación DNS TXT: Con este método de validación, usted añade un valor aleatorio generado por DigiCert (proporcionado para el dominio en su cuenta CertCentral) al DNS del dominio como un registro TXT. Cuando DigiCert hace una búsqueda de los registros TXT del DNS asociados al dominio, podemos encontrar un registro en el que el valor del registro incluye el valor aleatorio de DigiCert.
- Validación de archivos (demostración práctica HTTP, también denominada FileAuth): Con este método de validación, usted aloja un archivo que contiene un valor aleatorio generado por DigiCert (proporcionado para el dominio en su cuenta de CertCentral) en una ubicación predeterminada de su sitio web: [dominio]/.well-known/pki-validation/fileauth.txt. Una vez creado el archivo y colocado en su sitio, DigiCert visita la URL especificada para confirmar la presencia de nuestro valor aleatorio.

Nota: Para los certificados DV en CertCentral, DigiCert admite actualmente los siguientes métodos DCV: correo electrónico basado en WHOIS, correo electrónico construido, contacto de correo electrónico a DNS TXT, DNS TXT y validación de archivos.

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

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

Validación de la organización

Para validar una organización, DigiCert comprueba primero que la organización que solicita un certificado está en regla. Esto puede incluir la confirmación de la buena reputación y la inscripción activa en los registros corporativos. También puede incluir la comprobación de que la organización no figura en ninguna base de datos de fraude, phishing o entidades restringidas por el gobierno y antiterroristas.

Además, verificamos que la organización que solicita un certificado es, de hecho, la organización a la que se emitirá el certificado. También verificamos el contacto de la organización.

Añadir organizaciones a su cuenta de CertCentral y conseguir su validación es un requisito previo para conseguir la validación de sus dominios. Validar a las organizaciones lo antes posible acelera el proceso de emisión de certificados.

La gestión de las organizaciones suele consistir en añadir una organización y enviarla para su validación. También puede desactivar una organización que ya no sea necesaria.

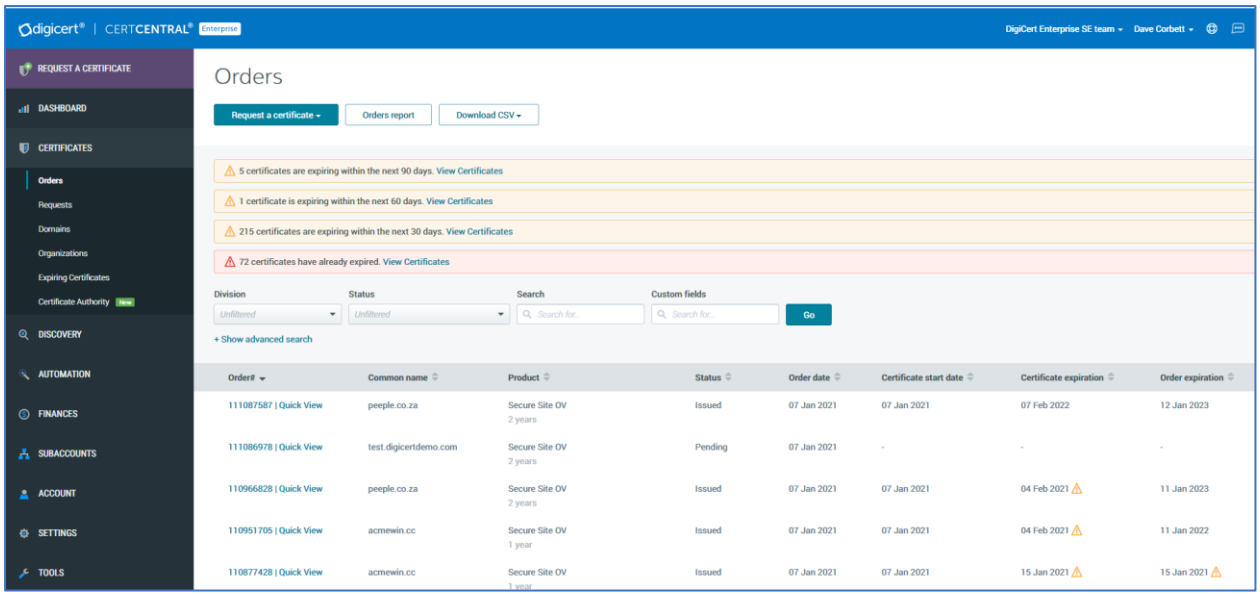
Más información: https://docs.digicert.com/es/manage-certificates/organization-domain-management/manage-organizations/

Una vez que haya enviado sus organizaciones para su validación, puede empezar a enviar dominios para su validación y el tipo de autorización para la cual el dominio debe ser validado.

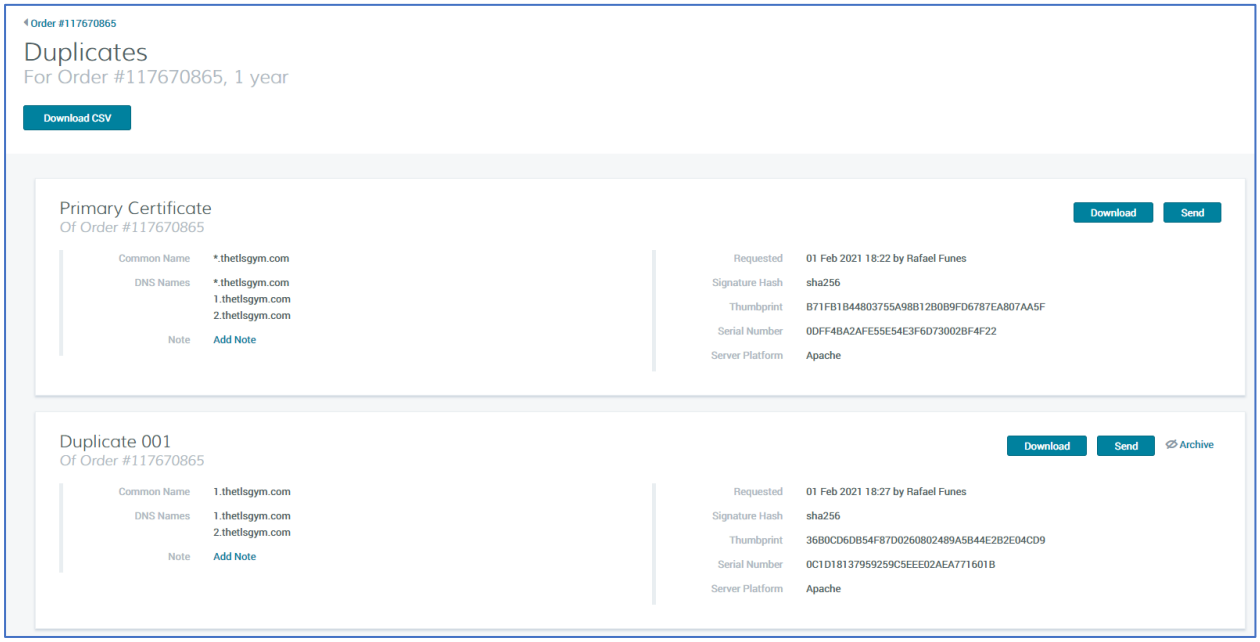
Más información: https://docs.digicert.com/es/manage-certificates/organization-domain-management/managing-domains-cc-guide/

Por lo general, es preferible validar los dominios y las organizaciones antes de solicitar los certificados, aunque también es posible añadir nuevos dominios y organizaciones al solicitar un certificado.

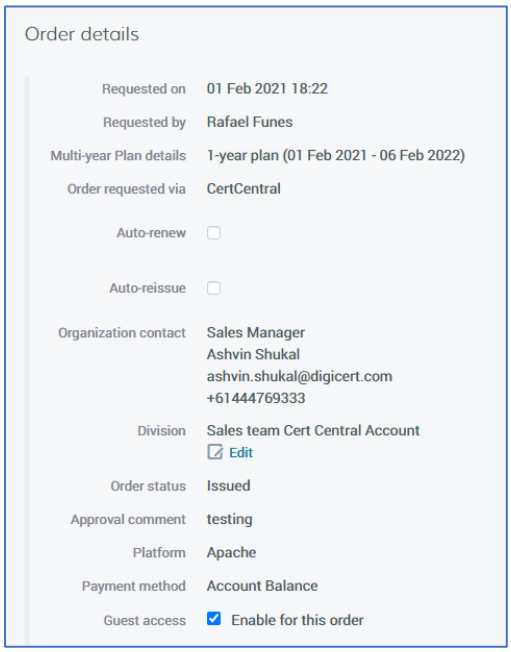
Gestión de pedidos y certificados



Los pedidos y los certificados se pueden gestionar directamente desde la plataforma CertCentral.



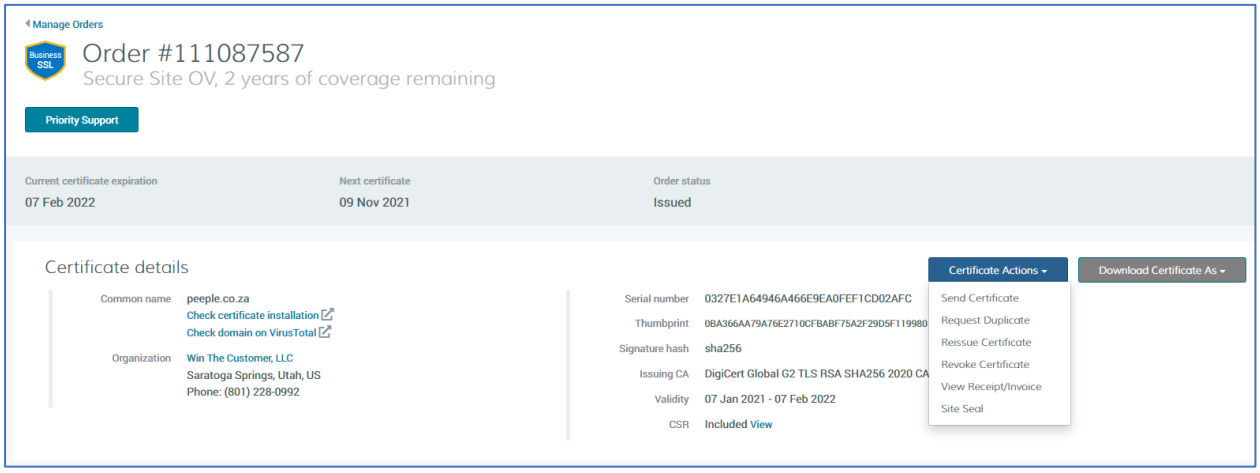
Una orden se refiere al plan plurianual elegido. Un certificado pertenece a una orden y puede ser reemitido muchas veces durante la vida de la orden. Las opciones importantes para un pedido son:



Renovación automática: Renueva automáticamente el plan plurianual 30 días antes de la fecha de vencimiento del plan actual.

Reemisión automática: emite automáticamente un nuevo certificado 30 días antes de la fecha de caducidad del certificado actual.

Tenga en cuenta que no se puede emitir un certificado con una fecha de finalización posterior a la fecha de finalización de la orden correspondiente.



La gestión de certificados incluye las siguientes acciones:

- Solicitar certificado
- Aprobar la solicitud de certificado
- Solicitar un duplicado del certificado
- Reemitir el certificado
- Revocar el certificado
- Obtener el código de sello del sitio

Aprobación del certificado

Por defecto, las solicitudes de certificados requieren aprobación antes de ser enviadas a DigiCert para su emisión. Después de que un usuario solicite un certificado, un administrador, un gestor, un usuario verificado por EV, un usuario verificado por CS o un usuario verificado por EV CS debe aprobar la solicitud de certificado. A continuación, la solicitud se envía a DigiCert para verificar que se han cumplido todos los requisitos de validación previa.

Después de que un usuario solicite un certificado, cualquier administrador, gestor, usuario verificado por EV, usuario verificado por CS o usuario verificado por EV puede también rechazar la solicitud de certificado, si es necesario. Por ejemplo, si el usuario pidió el tipo de certificado equivocado.

Por defecto, las cuentas de CertCentral están configuradas para la aprobación de solicitudes de certificados en un solo paso. Un administrador de la cuenta debe aprobar una solicitud de certificado antes de que DigiCert pueda empezar a procesar el pedido (validando la organización, etc.). Sin embargo, puede eliminar el paso de aprobación de los flujos de trabajo de emisión de certificados SSL OV/EV para sus administradores, gestores y responsables financieros de CertCentral. Los requisitos de aprobación pueden configurarse en la página Configuración/Preferencias de CertCentral.

Duplicación de certificados

Todos los certificados DigiCert vienen con un número ilimitado de duplicados gratuitos. Para aumentar la seguridad y facilitar la instalación del certificado en varios servidores, genere una nueva CSR y cree un certificado duplicado para cada servidor.

Los datos del duplicado del certificado serán exactamente los mismos que los del certificado original. Los certificados duplicados nunca requieren que DigiCert revoque las copias anteriores de su certificado.

Más información: https://docs.digicert.com/es/manage-certificates/duplicate-ssltls-certificate/

Reemisión del certificado

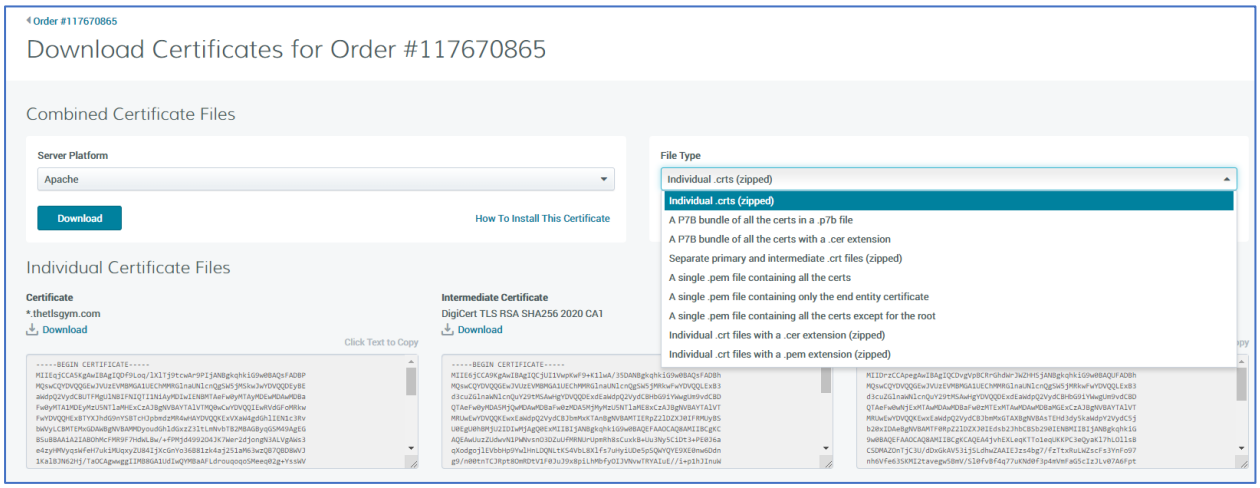
Todos los certificados DigiCert tienen reemisiones gratuitas ilimitadas. El proceso de reemisión de certificados le permite modificar un certificado emitido. Algunas modificaciones le permiten basarse en el certificado original, dando lugar a dos o más versiones de ese certificado. Por ejemplo, al reemitir un certificado, puede añadir dominios al certificado original. Añadir dominios a un certificado no revoca el certificado original.

Otras modificaciones le permiten crear una nueva versión del certificado y requieren que DigiCert revoque el certificado original y cualquier reemisión y duplicado del mismo. Por ejemplo, si se eliminan los SAN o se cambian los SAN en un certificado multidominio, se crea una nueva versión del certificado y se revoca el certificado original y cualquier reemisión anterior y las copias duplicadas.

Más información: https://docs.digicert.com/es/manage-certificates/reissue-ssltls-certificate/

Descargar un certificado

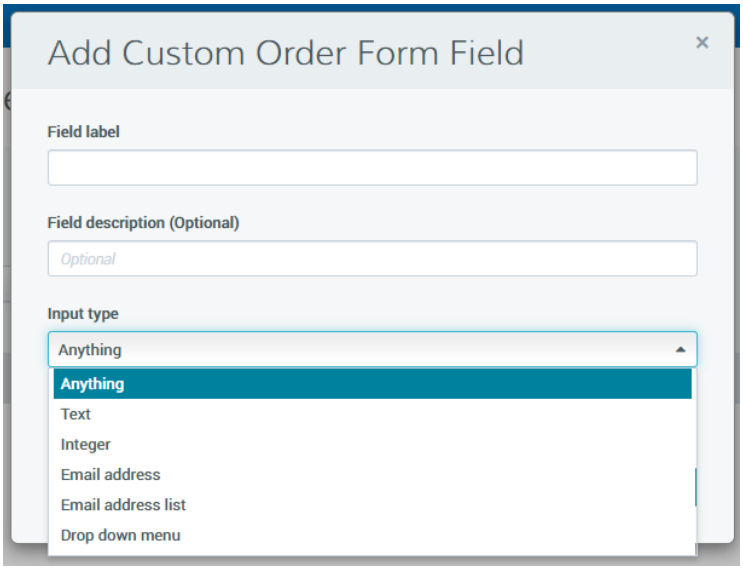
Después de que DigiCert emita su certificado, es posible que desee descargar el certificado directamente a su servidor donde se creó la solicitud de firma de certificado (en otras palabras, el servidor con la clave pública correspondiente al certificado).



CertCentral ofrece una selección de formatos de archivo. Una vez seleccionada la plataforma de servidor adecuada, se ofrecerá una selección de tipos de archivo. También puede descargar el certificado, el certificado intermedio y el certificado raíz directamente como archivos .pem.

Campos de pedido personalizados

CertCentral le permite añadir campos personalizados a sus formularios de solicitud de certificados. Los metadatos del campo personalizado pueden utilizarse para buscar u ordenar un conjunto de pedidos de certificados que coincidan con los criterios de búsqueda de los metadatos.



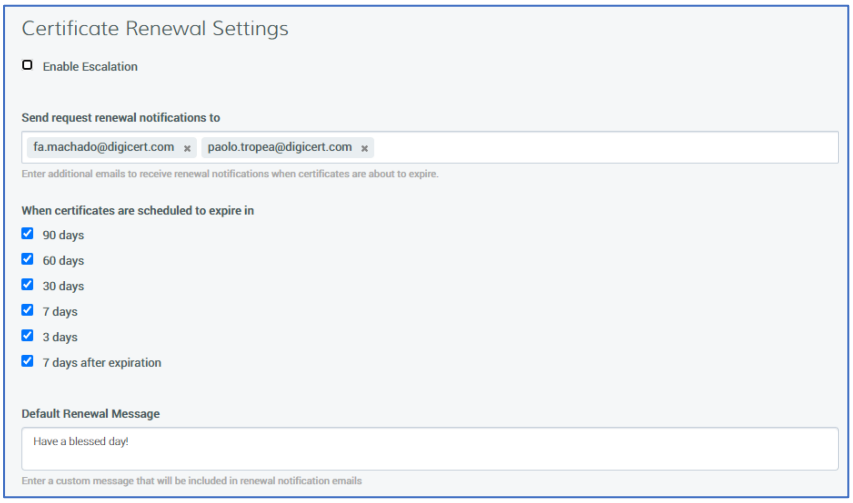
Características de los campos de los formularios de pedido personalizados:

- Aplicar a solicitudes futuras y actuales: Cuando se añaden campos de formulario de pedido personalizados, el campo también se añade a las solicitudes pendientes. Si el campo es obligatorio, las solicitudes pendientes no pueden ser aprobadas hasta que el campo sea completado.
- Aplicar a toda la cuenta: Al añadir campos de formulario de pedido personalizados, los campos se aplican a los formularios de pedido de toda la cuenta. Los campos del formulario de pedido personalizados no se pueden establecer por División.
- Aplicar a todos los tipos de certificado: cuando se crean campos de formulario de pedido personalizados, los campos se añaden a los formularios de pedido para todos los tipos de certificado (SSL, Cliente, Firma de código, etc.). No se puede añadir un campo de formulario de pedido personalizado a los formularios de pedido sólo para los tipos de certificados SSL, etc.
- Aplicar a URLs de invitados: Cuando añada campos de formulario de pedido personalizados, estos campos se añadirán a los certificados solicitados directamente desde su cuenta de CertCentral, así como desde cualquier URL de invitado que haya enviado.
- Diferentes tipos para elegir: Cuando se crean campos de formulario de pedido personalizados, se pueden añadir diferentes tipos de campos, como cuadros de texto de una o varias líneas, cuadros de dirección de correo electrónico y de lista de direcciones de correo electrónico, etc.
- Requerido u Opcional : Cuando añada campos de formulario de pedido personalizados, puede hacerlos obligatorios u opcionales. Los campos obligatorios deben ser completados antes de que el pedido pueda ser aprobado. Los campos opcionales pueden dejarse en blanco.
- Desactivado o activado: Después de añadir un campo de formulario de pedido personalizado, puede desactivar (eliminar) y activar (volver a añadir) el campo según sea necesario. Los campos que se desactivan se eliminan de las solicitudes pendientes pero no de las órdenes emitidas. Los campos que se activan se añaden a las solicitudes pendientes. Si el campo es obligatorio, debe ser completado antes de que la solicitud pueda ser aprobada.

Los datos de los campos personalizados pueden editarse en cualquier momento antes o después de la emisión de un certificado.

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

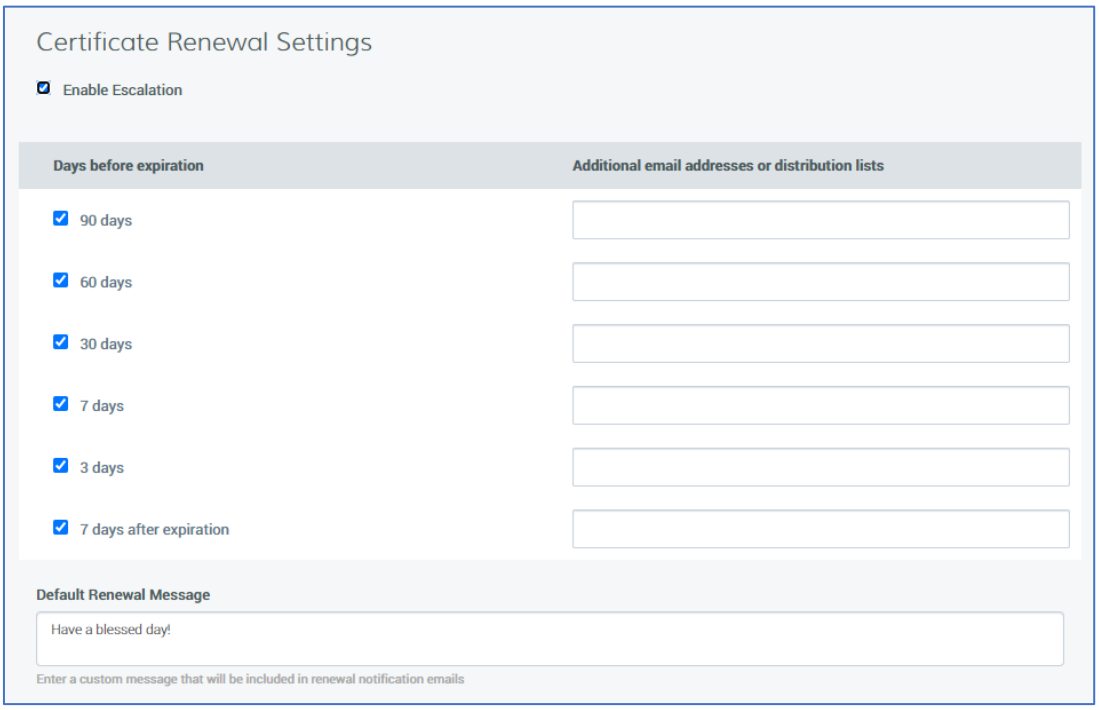
Notificación de renovación



Por defecto, CertCentral envía notificaciones de renovación de certificados 90, 60, 30, 7 y 3 días antes de que caduque un certificado y 7 días después de que caduque. Es posible que desee configurar sus ajustes de renovación de certificados para determinar cuándo se envían las notificaciones de renovación y qué direcciones de correo electrónico reciben las notificaciones.

Puede configurar notificaciones de renovación de certificados o notificaciones de renovación de escalada:

- Configuración de la renovación de certificados: le permite enviar notificaciones de renovación a las mismas direcciones de correo electrónico en cada etapa a medida que los certificados se acercan a la caducidad o después de que hayan caducado.

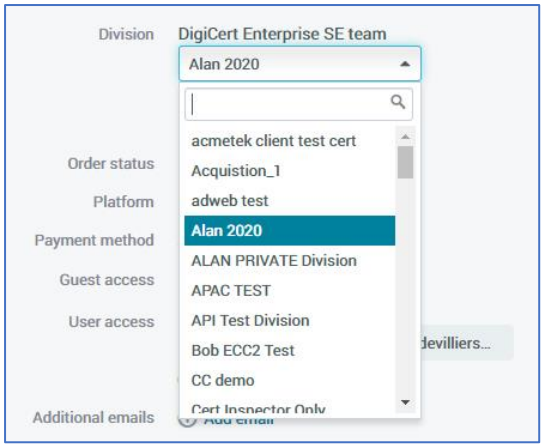


- Configuración de las renovaciones de escalada: le permite determinar qué direcciones de correo electrónico recibirán qué notificaciones de renovación en cada etapa a medida que los certificados se acerquen a su vencimiento o después de que hayan expirado.

Subcuentas y divisiones

Divisiones

Las divisiones son una función de CertCentral para restringir usuarios y organizaciones. Puede añadir usuarios de su organización a su cuenta de CertCentral y controlar su acceso a la cuenta mediante los permisos de usuario.



Puedes proporcionar a una división tanta libertad como quieras, controlando su capacidad para crear y gestionar usuarios, permisos, dominios y organizaciones. A diferencia de las subcuentas, usted tiene total visibilidad y control sobre los usuarios, los pedidos, la configuración y la actividad de las divisiones de su cuenta.

Además, las divisiones pueden compartir los fondos de la cuenta, o cada división puede tener sus propios fondos y pagar sólo sus certificados.

Tenga en cuenta que los pedidos de certificados pueden ser reasignados a una división diferente en cualquier momento.

Más información: https://docs.digicert.com/es/manage-account/division-management/

Subcuentas

Las subcuentas son cuentas de CertCentral vinculadas y gestionadas por una cuenta de CertCentral de nivel superior. Las subcuentas permiten a los distribuidores u otras organizaciones dar a los usuarios un control individual sobre una cuenta de CertCentral y su proceso de gestión de certificados, al tiempo que le permiten a usted, la cuenta "madre", controlar el precio y la facturación del producto.

Las subcuentas están diseñadas específicamente para las relaciones cliente-empresa u otras relaciones en las que se necesita controlar el precio del producto o la facturación de los pedidos realizados por las subcuentas. Hay cuatro tipos de subcuentas:

- Venta al por menor (Retail)
- Empresa (Enterprise)
- Socio (Partner)
- Gestionado (normalmente sólo acceso a la API).

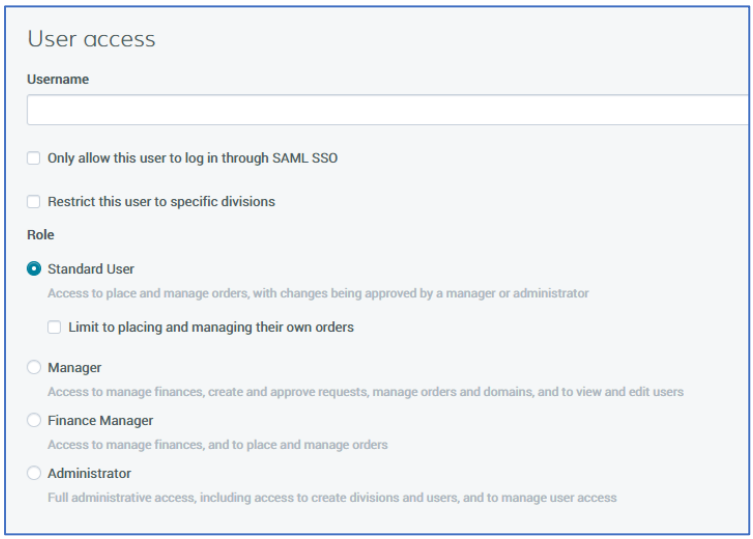
Cada tipo de cuenta dispone de un conjunto diferente de funciones de CertCentral. Las subcuentas gestionadas son cuentas sólo para la API destinadas a la integración en un portal de usuario existente y proporcionan a la cuenta parent (padre) algunos controles adicionales, como la posibilidad de descargar certificados.

Las subcuentas pueden tener 3 niveles de profundidad, es decir, padre, hijo y nieto (parent, child, grandchild).

Más información: https://docs.digicert.com/es/manage-account/subaccounts-management/

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

Funciones de usuarios



Los administradores de cuentas no asignan permisos individuales a un usuario. En cambio, asignan a cada usuario una función:

- Administrador
- Usuario estándar
- Usuario limitado
- Director de Finanzas
- Gerente

La función asignada al usuario determina las características de la cuenta a las que puede acceder.

Los roles principales son:

- Usuario estándar: Acceso a realizar y gestionar pedidos, con los cambios aprobados por un gestor o administrador
- Gerente: Acceso para gestionar las finanzas, crear y aprobar solicitudes, gestionar pedidos y dominios, ver y editar usuarios
- Gerente financiero: Acceso a la gestión de las finanzas y a la realización y gestión de pedidos
- Administrador: acceso administrativo completo, incluido el acceso para crear divisiones y usuarios, y para gestionar el acceso de los usuarios

Para crear un rol de Usuario Limitado, seleccione Usuario Estándar y marque la casilla "Limitar a colocar y gestionar sus propias órdenes".

A continuación se ofrecen más detalles.

Administrador	Acceso completo a la cuenta de CertCentral con estos permisos: • Acceder y gestionar el Discovery. • Gestionar divisiones (crear y editar) y usuarios de cuentas (crear, eliminar y editar). • Gestionar las organizaciones (añadir nuevas organizaciones), los dominios (añadir o desactivar), las solicitudes de invitados y el acceso a la API. • Ver todas las solicitudes y pedidos de certificados, solicitar certificados, aprobar solicitudes de certificados y ejecutar informes de pedidos. • Gestionar los ajustes financieros de la cuenta y las finanzas (ver el historial de saldos, ejecutar informes de gastos, depositar fondos, etc.). • Gestionar la configuración de la cuenta (configuración de la autenticación, restricciones de acceso a la IP, restricciones de productos, etc.), la configuración de la auditoría y los registros de auditoría.
Usuario estándar	Usuarios de la cuenta con estos permisos: • Solicitar certificados. • Controlar las solicitudes y pedidos de certificados (propios y ajenos). • Un gerente o administrador debe aprobar los cambios.
Usuario limitado	Usuarios de la cuenta con estos permisos: • Solicitar certificados. • Controlar sus propias solicitudes y pedidos de certificados. • Un gerente o administrador debe aprobar los cambios.
Gerente financiero	Usuarios de cuentas limitadas cuya función principal es gestionar las finanzas de la cuenta. Incluye estos permisos: • Consulte el historial de saldos, los informes de gastos y los precios de las cuentas. • Gestionar los pedidos de compra y depositar los fondos.

	• Gestionar los informes de los pedidos. • Solicitar certificados. • Controlar sus propias solicitudes y pedidos de certificados.
Gerente	Usuarios de cuentas limitadas cuya función principal es ayudar a gestionar la cuenta. Incluye estos permisos: • Acceder y gestionar el Discovery. • Ver las divisiones y gestionar los usuarios de la cuenta (editar). • Ver las organizaciones y gestionar los dominios (añadir o desactivar). • Ver todas las solicitudes y pedidos de certificados, solicitar certificados, aprobar solicitudes de certificados y ejecutar informes de pedidos. • Gestionar los ajustes financieros de la cuenta y las finanzas (ver el historial de saldos, ejecutar informes de gastos, depositar fondos, etc.). • Gestionar la configuración de la auditoría y los registros de auditoría.

Todos los roles de usuario pueden ser restringidos a trabajar con certificados en divisiones específicas.

Por defecto, los administradores y gestores no tienen permiso para aprobar solicitudes de certificados EV, certificados EV de firma de código o certificados de firma de código. Para aprobar este tipo de solicitudes, el gestor debe tener asignados los subroles correspondientes.

Más información: https://docs.digicert.com/es/manage-account/certcentral-user-roles-account-access/roles-account-access/

Métodos de control de acceso/autenticación de usuarios

Contraseñas

Los requisitos mínimos de contraseña pueden establecerse desde el portal CertCentral.

Autenticación de dos factores

Para añadir una segunda forma de verificación de identidad a su proceso de inicio de sesión, debe configurar los requisitos de autenticación de dos factores para su cuenta. Puede configurar un requisito para todos los usuarios y para usuarios individuales según sea necesario.

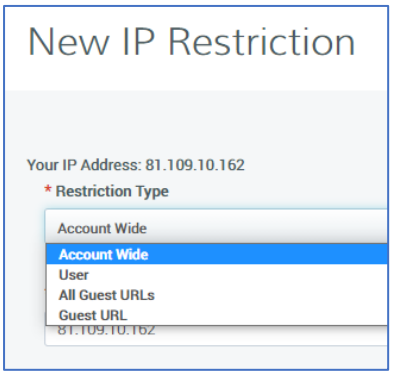
Además del requisito de ID de usuario/contraseña, se puede exigir a los usuarios que utilicen uno de los siguientes factores:

- Contraseña de un solo uso (OTP): La aplicación de esta regla requerirá que los usuarios inicialicen su aplicación o dispositivo OTP y generen una contraseña de un solo uso la próxima vez que inicien sesión. La autenticación OTP requiere el uso de cualquier aplicación móvil que admita el protocolo Time-Based One-Time Password (TOTP).

- Certificado de cliente: La aplicación de esta regla requerirá que los usuarios generen un certificado de cliente en su navegador la próxima vez que inicien sesión. Internet Explorer (Windows) y Safari (Mac) son los únicos navegadores que admiten la generación de certificados de cliente.

Más información: https://docs.digicert.com/es/manage-account/certcentral-two-factor-authentication/configure-two-factor-authentication-requirements/

Restricciones a la IP



Para aumentar la seguridad, DigiCert ofrece la posibilidad de restringir su cuenta para que sólo se pueda acceder a ella desde determinadas direcciones IP. Estos pueden ser fijados:

- En toda la cuenta
- Por usuario
- Por URL de invitado
- Para todas las URLs de invitados

Inicio de sesión único (Single Sign-On)

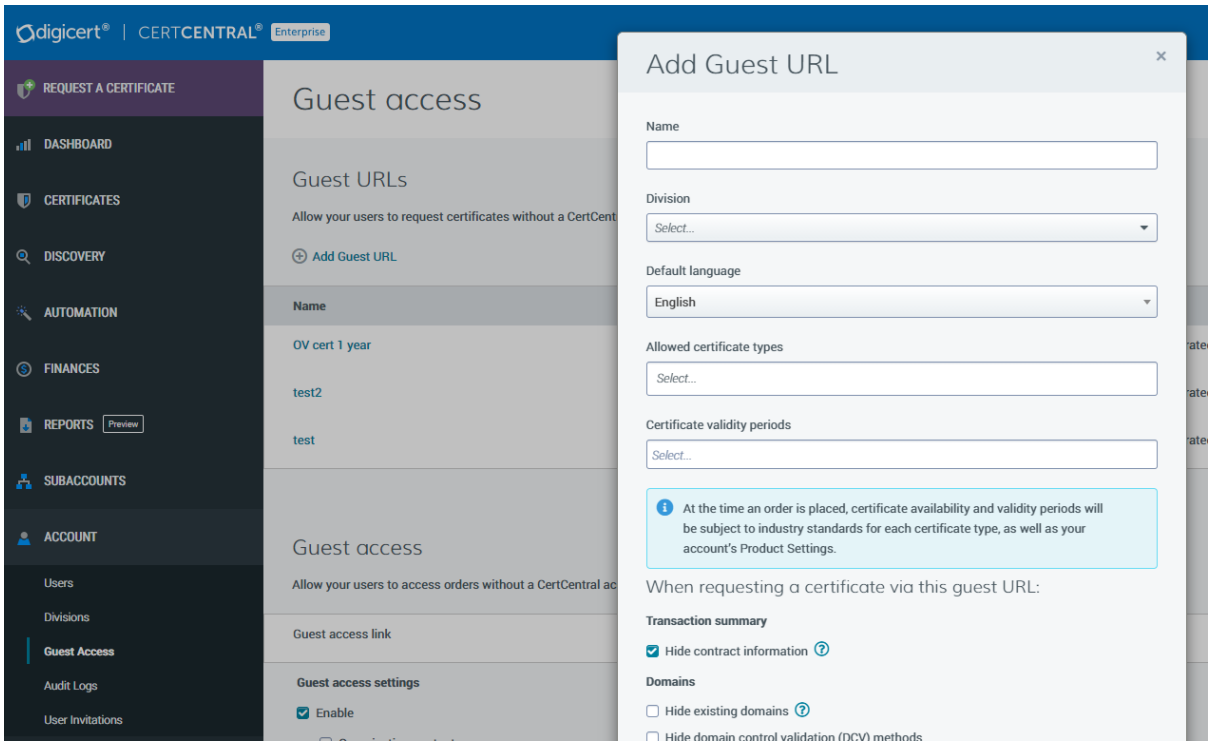
Elimine la necesidad de múltiples contraseñas y utilice el inicio de sesión único (SSO) de SAML para conectar su proveedor de identidad (IdP) con CertCentral.

Una vez que haya configurado la conexión de SAML a CertCentral, sus usuarios de CertCentral podrán utilizar sus credenciales de SSO para iniciar sesión. Accederán a la página de inicio de sesión de la cuenta SSO a través de una URL SSO personalizada iniciada por el proveedor de servicios que DigiCert proporciona o una URL SSO iniciada por el IDP que usted proporciona.

Más información: https://docs.digicert.com/es/manage-account/saml-single-sign-on-admin-guide/

Opciones de acceso para invitados

URL para invitados



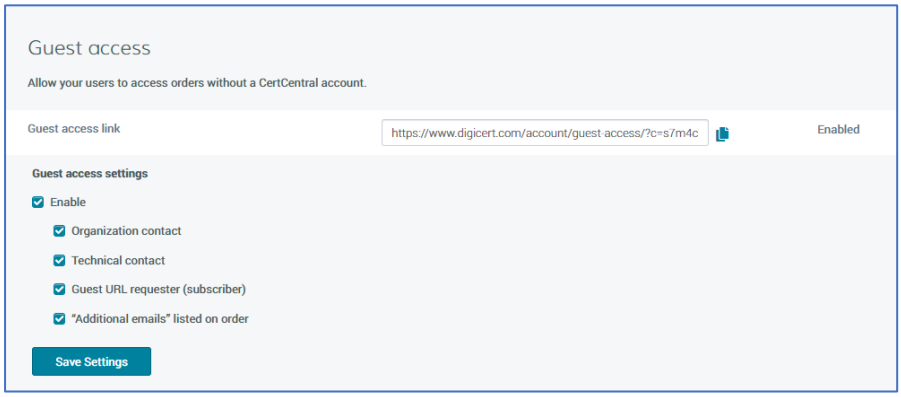
Una URL de invitado le permite ofrecer a un usuario invitado la posibilidad de solicitar un certificado sin añadirlo a su cuenta. Las URLs de invitados sólo dan acceso a los usuarios a una página específica de solicitud de certificados dentro de la cuenta. El usuario no puede acceder a nada más dentro de la cuenta.

Las URLs de invitados se configuran con los siguientes datos:

- Nombre
- División
- Tipos de certificados permitidos
- Períodos de validez de los certificados

Más información: https://docs.digicert.com/es/manage-account/managing-guest-urls/

Acceso para invitados

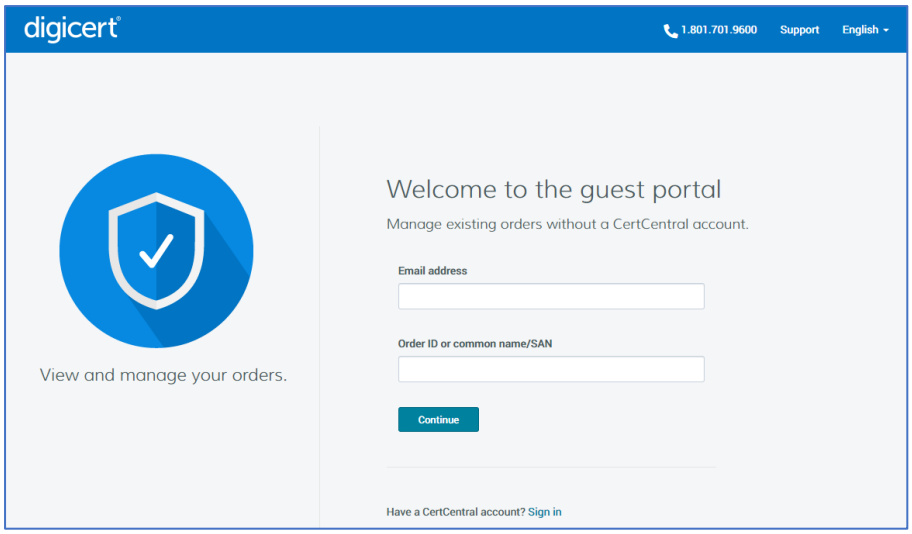


El acceso de invitados permite a una persona gestionar su pedido sin tener credenciales de CertCentral. Con su dirección de correo electrónico y número de pedido (o FQDN en el certificado), pueden descargar, reemitir o revocar su certificado.

El acceso de invitados puede activarse para todos los pedidos de su cuenta o para pedidos individuales.

Puede controlar qué contactos del pedido pueden acceder como invitados activando o desactivando las casillas de contacto de la organización, contacto técnico, solicitante de la URL de invitado (suscriptor) (la dirección de correo electrónico que realizó el pedido) y "Correos electrónicos adicionales" que aparecen en los pedidos.

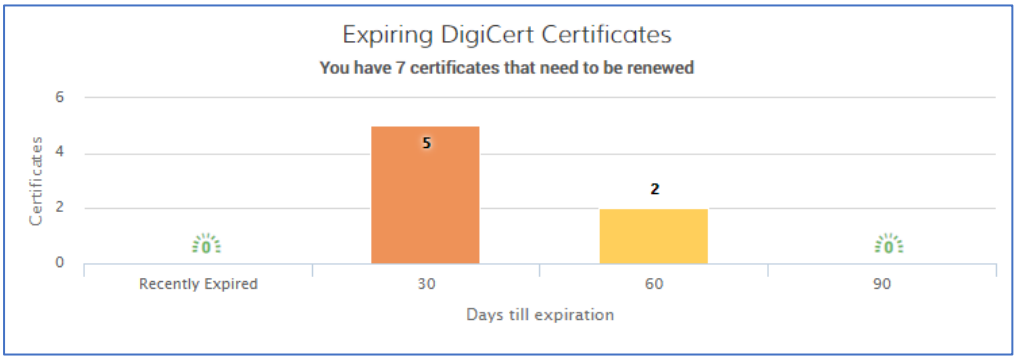
Su cuenta de CertCentral tiene una página de acceso única para invitados. Para confirmar la identidad de la persona, CertCentral envía un correo electrónico de autenticación que permite el acceso durante dos horas.



Más información: https://docs.digicert.com/es/manage-account/guest-access/

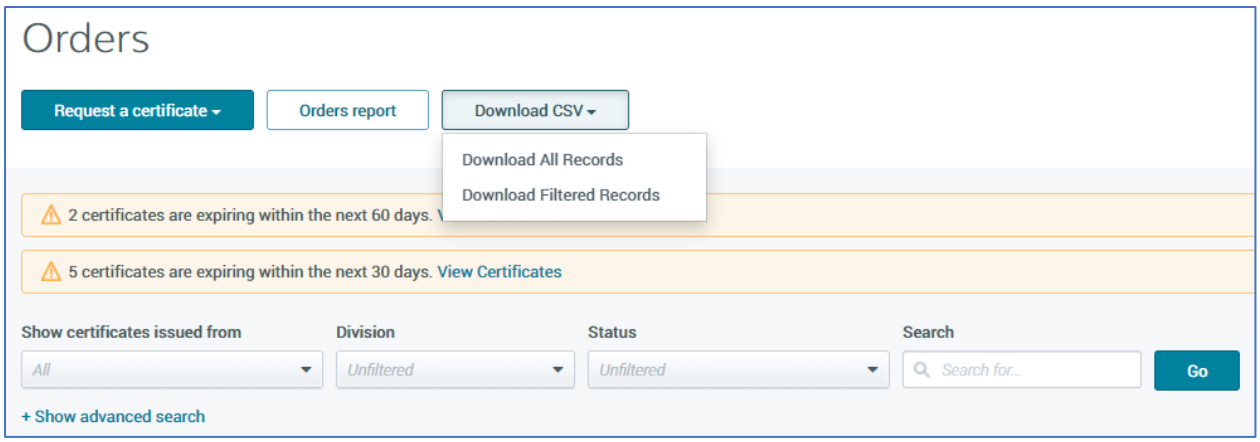
Informes y notificaciones

Informes



CertCentral ofrece cuadros de mando e informes dentro de la consola o a través de las API.

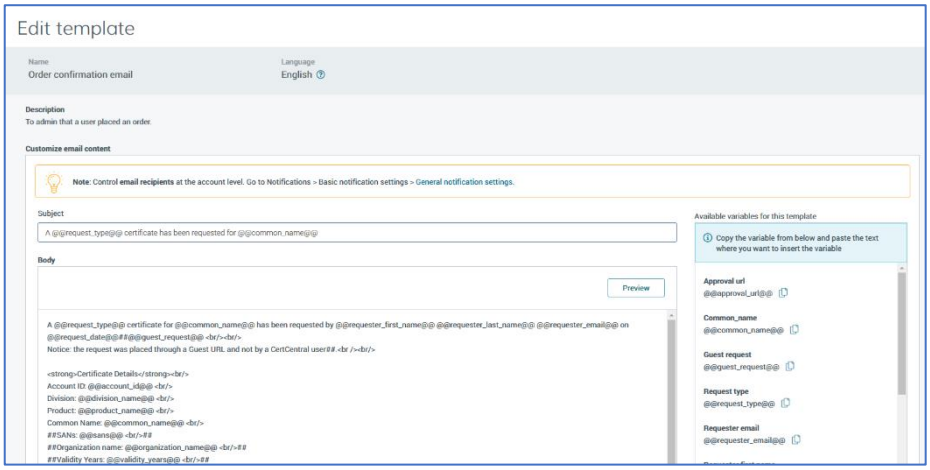
Tablero: una vista organizada gráficamente de sus certificados, incluidos los que caducan y las solicitudes pendientes.



Informe de pedidos: Encuentre todos los certificados emitidos y filtre por cualquier campo.

Notificaciones por correo electrónico

CertCentral envía correos electrónicos a los usuarios durante todo el proceso de pedido/aprobación, y cuando un certificado caduca o ha caducado. Puede personalizar estas plantillas de correo electrónico para que se adapten a las necesidades de su cuenta u organización.



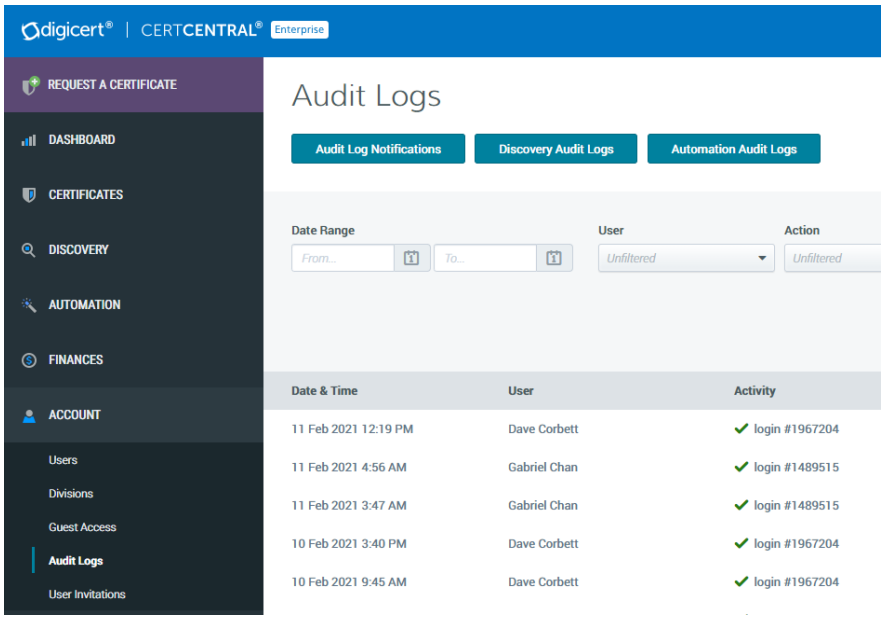
La configuración básica de las notificaciones permite especificar los destinatarios del correo electrónico y el idioma del mismo.

Las plantillas de correo electrónico personalizadas le permiten editar las

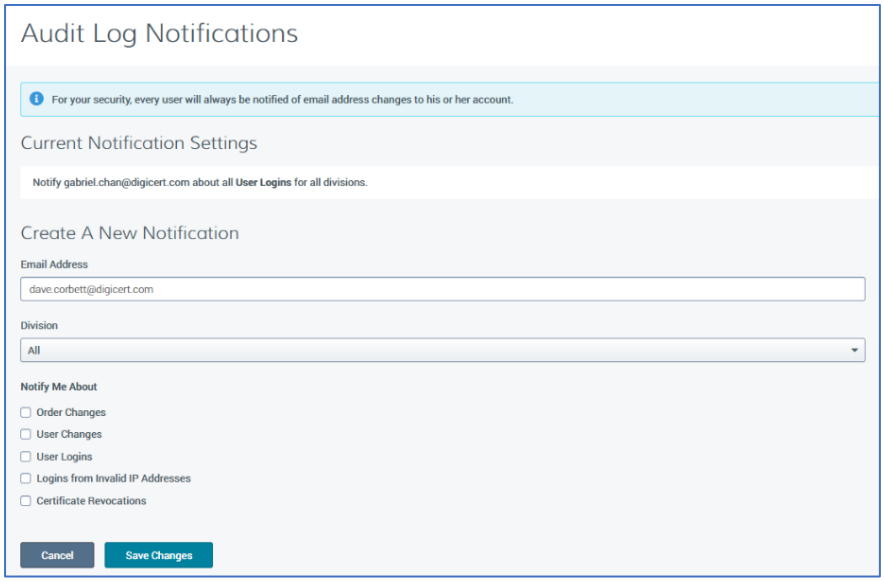
plantillas de correo electrónico estándar.

Más información: https://docs.digicert.com/es/manage-account/account-notifications/customize-email-templates/

Registro de auditoría



Los registros de auditoría son un historial de las acciones que ocurren en su cuenta. CertCentral mantiene automáticamente registros de auditoría que registran más de 50 acciones diferentes en su cuenta (incluyendo inscripciones, solicitudes de certificados y revocaciones), junto con la marca de tiempo y el usuario que realizó la acción. Para ver los registros de auditoría de su cuenta, visite la página Registros de auditoría.



Haciendo clic en ***Notificaciones del Registro de Auditoría*** para crear notificaciones por correo electrónico para eventos específicos.