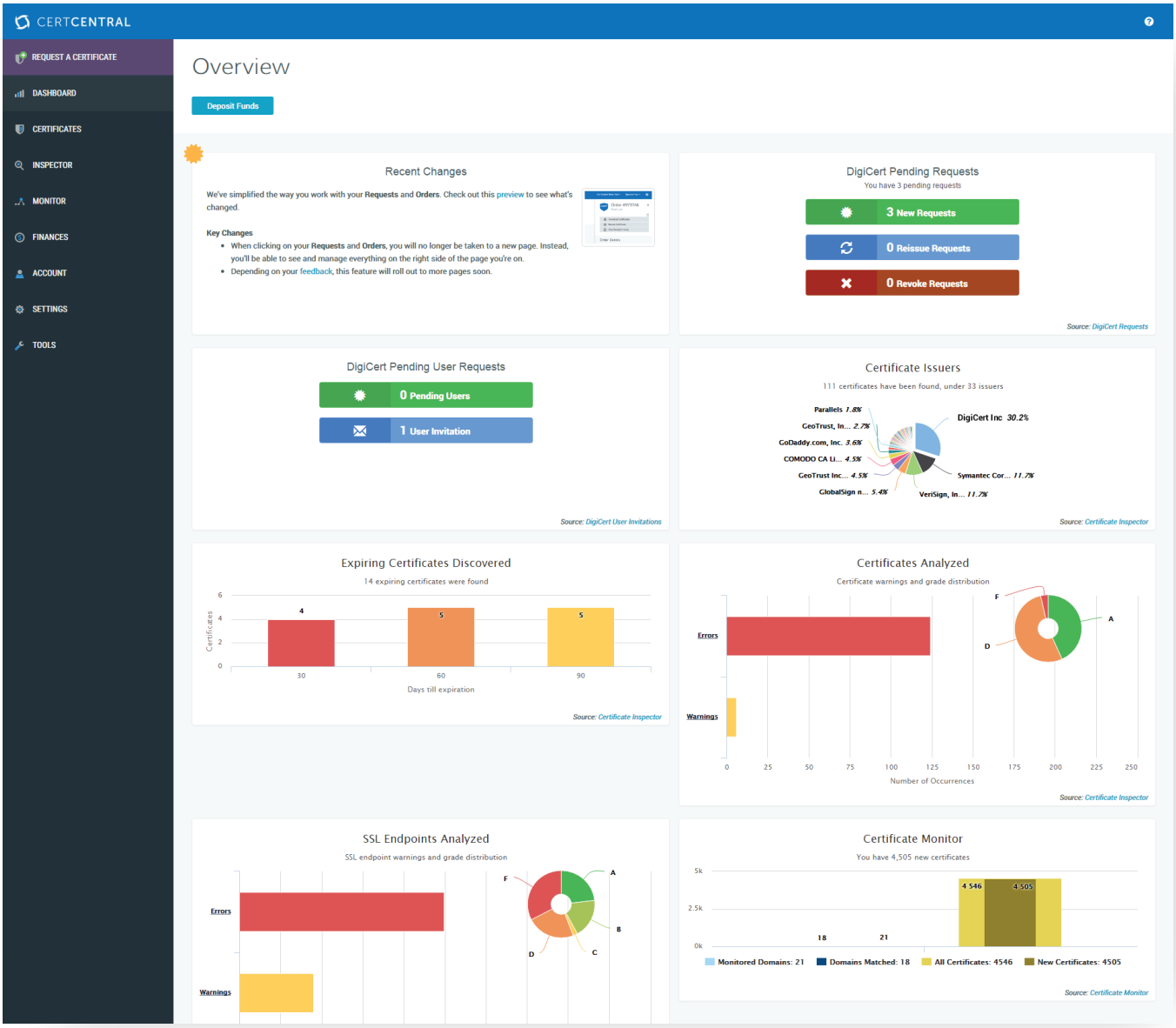
# CertCentral® Certificate Management Made Easy

## Leave the Spreadsheets Behind

CertCentral® is a platform designed for managing all your SSL Certificates throughout the certificate lifecycle. The platform empowers administrators by enabling them to monitor, inspect, reissue, revoke, renew, and order new certificates in one place.

This platform streamlines certificate management and eases the burden of admins by eliminating the need to manually track critical certificate details. CertCentral increases efficiency and lowers an organization's bottom-line IT costs.

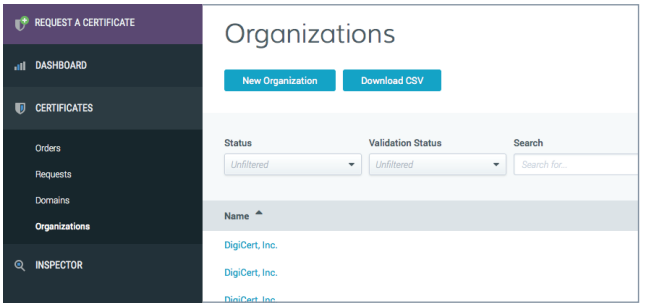
CertCentral also has proprietary DigiCert tools built in, so an admin never has to leave the platform, as well as features that can be customized to meet specific organization needs.

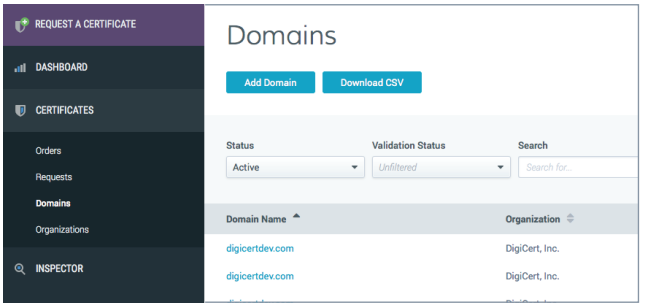



digicert®

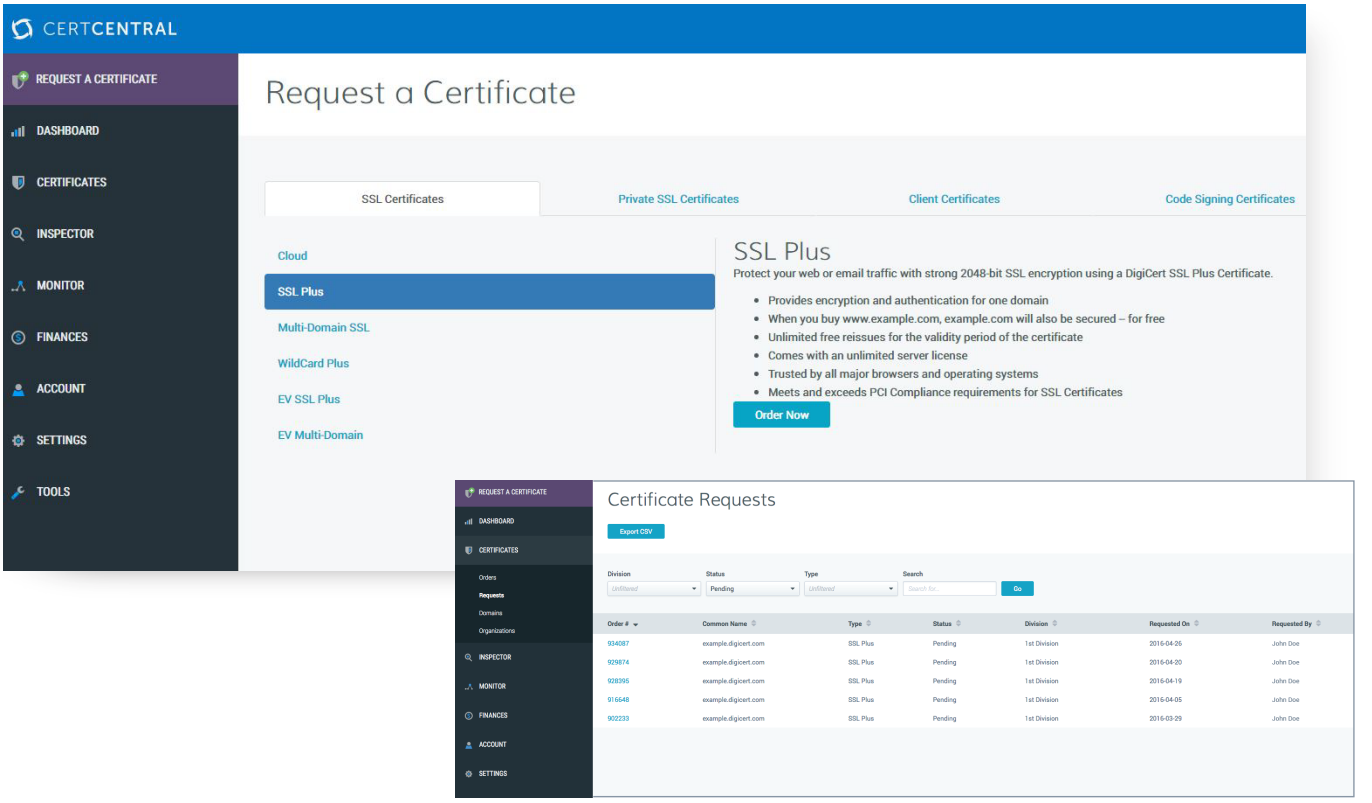
# Easy Certificate Ordering

The ordering process through CertCentral is very easy. First go to the **Certificates tab** and select the "Organizations" option. Click "Add Organization" to enter the organization that you will want listed on the certificates you issue. Then go to the **Domains sub-tab** and click "New Domain" to submit the domain(s) for which you plan to request certificates. New organizations and domains can be added at any time. Once you have submitted those, the DigiCert validation team completes the required verification process; validation is often completed the same day or even the same hour for most certificate types. Use the pre-validation to request certificates at your leisure and receive certificates in under a minute.



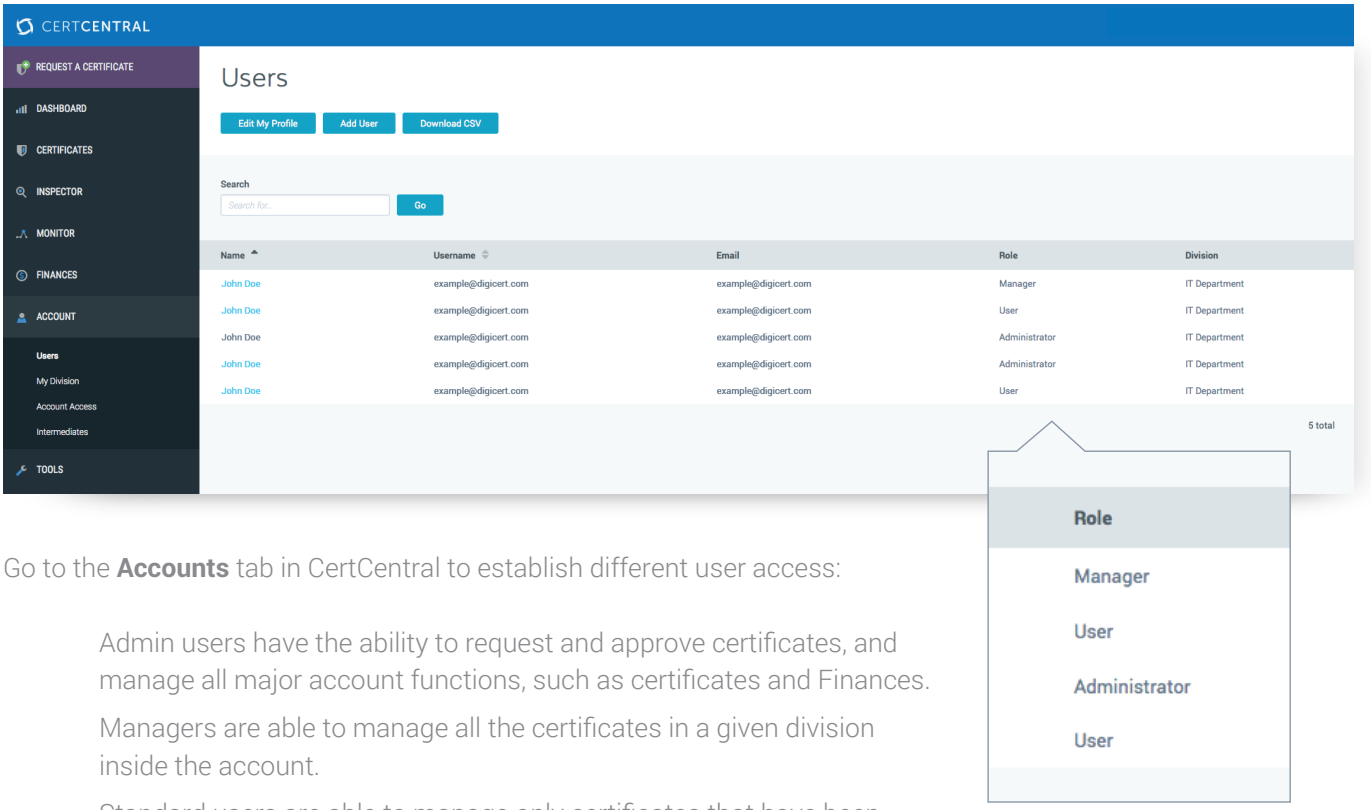




To request certificates go the **Request a Certificate tab** on the left-side navigation. Select the kind of certificate needed from the list then add a CSR if applicable, enter some details (e.g., server type in question), and the certificate will be sent to the **Requests tab**. Any admin in the account can go to "Requests" under **Certificates** and approve them. Once approved, certificates are issued in under a minute. The certificate is available for download inside the account and is also emailed to the certificate requester and to other specified account users.



# Customizable Workflows

CertCentral allows admins to create users and divisions, and assign designated privileges according to the needs of your organization. Admins can also create guest URLs for certificate requests with certain products and validity periods. With a guest URL, a user will be able to request certificates with those specifications, but he will not have the ability to log in to the account to manage certificates or perform any other account functions.



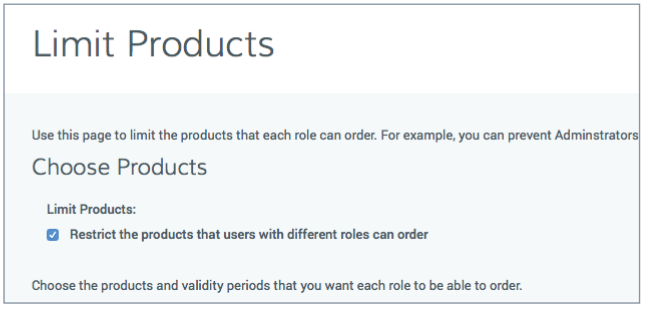

Go to the **Accounts** tab in CertCentral to establish different user access:

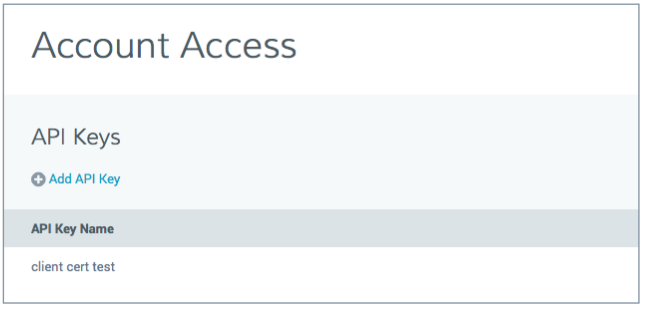
Admin users have the ability to request and approve certificates, and manage all major account functions, such as certificates and Finances.

Managers are able to manage all the certificates in a given division inside the account.

Standard users are able to manage only certificates that have been requested by that specific user.

Finance users have the same permissions as a standard user, but also have the ability to make payments, place PO's, view account balances, etc.



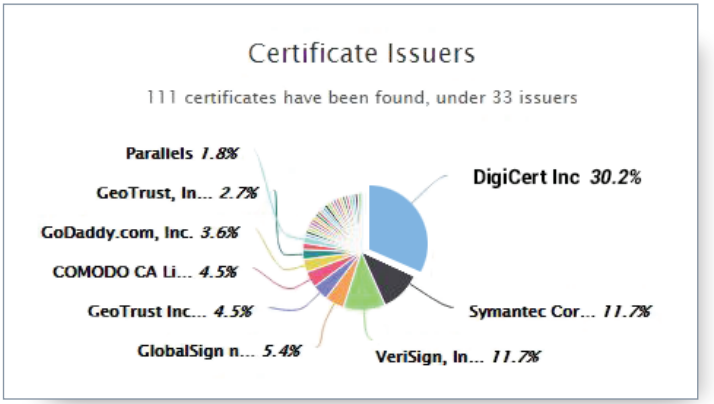

You also have the ability, under the **Settings tab**, to restrict user access by IP range, OTP, or Client Certificate.

DigiCert has a REST API. Under the **Account tab**, users can request one or more API keys. API documentation can be provided upon request, which will allow you full access.

digicert

## Certificate and Endpoint Inspection

Certificate Inspector™ allows admins to quickly discover all of the certificates in a network and analyzes every certificate, so security problems with certificates or endpoints are easy to spot. Certificate Inspector scans for vulnerabilities, provides an overview of a certificate landscape, and reports details in BI-style reports.




## Some FAQs

### Will there be a problem if I have certificates with DigiCert and also have certificates with my old provider on the same domain?

No. If you have active certificates on a given domain and request certificates through DigiCert on the same domain there will be no conflict. The old certificates are not invalidated by the issuance of new certificates and will continue to be active until they expire or until you manually replace them on the servers where they are currently installed. This allows you to slowly transition your certificates on a certificate-by-certificate basis from your past provider to DigiCert.

### What effect will moving to DigiCert have on the root certificate of my certificates, and how will that affect ubiquity?

All Certificate Authorities have unique root certificates. When you switch to DigiCert, your newly issued certificates will be issued off a DigiCert root certificate. Our root certificates have 99.9% ubiquity across different browsers and devices. This makes for a worry-free switch.

### What if I need help replacing my old certificates?

We have a tool to help. Certificate Inspector is an agent you can run on any Windows or Linux machine. The tool scans your environment, including the different certificate stores and keystores, and reports back to show you all of your certificates (internal and external), regardless of provider. The results are displayed inside your CertCentral® account. Next to every listed certificate there is a “Replace Certificate” button. When clicked it will place a request for you in your DigiCert account for a certificate with the same Common Name and SANs as your other certificate. Once the certificate issues, you can install it in place of the old certificate.

## Schedule a demo and see for yourself.

To learn more call 1.855.800.3444, visit digicert.com or email sales@digicert.com



digicert®