Contents
Introduction ......................................................................................................................... 4
Objectives .......................................................................................................................... 5
DigiCert® CertCentral® Training Guide ........................................................................... 6
SSL/TLS certificate products ............................................................................................. 6
  Flex certificates .............................................................................................................. 6
  Multi-year plans ............................................................................................................. 7
  Secure Site certificate benefits ...................................................................................... 7
Certificate profile options ................................................................................................. 8
Product Settings ............................................................................................................... 9
Domain and organisation validation .................................................................................. 9
  Domain Control Validation (DCV) .................................................................................. 9
  Organization validation .................................................................................................. 10
Management of orders and certificates .......................................................................... 11
  Certificate approval ...................................................................................................... 13
  Duplicate certificates .................................................................................................... 13
  Certificate reissue ......................................................................................................... 13
  Downloading a certificate .............................................................................................. 14
  Custom order fields ....................................................................................................... 15
  Renewal notification ..................................................................................................... 16
Subaccounts and divisions ............................................................................................... 17
  Divisions ........................................................................................................................ 17
  Subaccounts .................................................................................................................. 17
User roles ......................................................................................................................... 19
User access/authentication control methods ..................................................................... 21
  Passwords ....................................................................................................................... 21
  Two-Factor Authentication ............................................................................................ 21
  IP restrictions .................................................................................................................. 21
  Single Sign-On ............................................................................................................... 21
Guest access options ....................................................................................................... 22
  Guest URL ....................................................................................................................... 22
DIGICERT® CERTIFICATION PROGRAM

Guest access.................................................................................................................................................. 22
Reporting options .......................................................................................................................................... 23
Audit logging .................................................................................................................................................. 24
Introduction
This study guide is designed to help you prepare for the DigiCert Technical Certification: CertCentral Professional assessment exam. The exam will consist of 50 multiple-choice questions with a maximum time allowed of 1 hour.

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

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

Below you will find information on each of the listed objectives, plus links for further information. Please note – these resources are just a starting point! It is strongly recommended that you do further research in order to be fully prepared for an assessment on all the objectives, including hands-on experience using DigiCert CertCentral.

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

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

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

SSL/TLS certificate products

Most Enterprises use the DigiCert range of Business SSL certificates:

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

These certificate products are “Flex” certificates and come with many options and benefits. These are described below.

<table>
<thead>
<tr>
<th>FEATURES</th>
<th>SECURE SITE</th>
<th>SECURE SITE EV</th>
<th>SECURE SITE PRO</th>
<th>SECURE SITE PRO EV</th>
</tr>
</thead>
<tbody>
<tr>
<td>CT Monitoring</td>
<td>—</td>
<td>—</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>PQC Access</td>
<td>—</td>
<td>—</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Priority validation</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Priority support</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Two premium site seals</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Malware and Blacklist check</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Wildcard Support</td>
<td>●</td>
<td>—</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>SAN Limit</td>
<td>250</td>
<td>250</td>
<td>250</td>
<td>250</td>
</tr>
<tr>
<td>Inc. Base Domain</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Industry-Leading Warranties NW/RP</td>
<td>1.75$/2$ Million</td>
<td>1.75$/2$ Million</td>
<td>2$/2$ Million</td>
<td>2$/2$ Million</td>
</tr>
</tbody>
</table>

Flex certificates

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

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

More information: [https://docs.digicert.com/manage-certificates/flex-certificates/](https://docs.digicert.com/manage-certificates/flex-certificates/)
Multi-year plans

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

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

Secure Site certificate benefits

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

- Priority validation—Secure Site orders are placed at the top of our validation queues so our agents can respond to these orders first.
- Priority support – Secure Site certificates come with access to two priority support queues so our Support team can respond to your needs first: Order and validation status and Installation and configuration.
- Two premium site seals—Secure Site certificates come with the two most recognized trust marks on the web: DigiCert and Norton. Pick the premium site seal you want to use to display proof of trust on your site.
- CT (Certificate Transparency) Log Monitoring - The CT Log monitoring service allows you to monitor the public CT logs for SSL/TLS certificates issued for the domains on your Secure Site Pro or Secure Site Pro EV certificate. After you've enabled CT Log monitoring for a Secure Site Pro certificate order, you'll receive two types of email notifications: Daily CT log digest and if needed, Urgent notifications. Email notifications are sent to account admins allowing them to check the CT logs for their domains without signing in to their CertCentral account every day. The CT log monitoring service pulls the discovered SSL/TLS certificates into your CertCentral account, where you can view details about the certificates to quickly identify any miss-issued certificates for your domains. You can
also download copies of the non-DigiCert certificates right from your CertCentral account. More information: https://docs.digicert.com/certificate-tools/ct-log-monitoring-service/

- **Vulnerability assessment** – Secure Site EV, Secure Site Pro SSL, and Secure Site Pro EV certificates include access to a vulnerability assessment service. This service allows you to identify and act against the most exploitable weaknesses on your website. To learn more, see https://docs.digicert.com/certificate-tools/vulnerability-assessment-service/

- **Malware check** – Secure Site certificates come with convenient access to a VirusTotal malware check. Quickly analyze your public domains with 70 plus antivirus scanners and URL/domain blacklist services. Use scan results to identify malware threats so you can take actions to keep your site off blacklists that can cripple site availability and online revenue.

- **Post-quantum Cryptography (PQC)** – Customers purchasing a Secure Site Pro SSL or Secure Site Pro EV SSL have access to DigiCert’s post-quantum cryptographic (PQC) toolkit. More information: https://docs.digicert.com/certificate-tools/post-quantum-cryptography/

- **Industry-leading warranties** – Secure Site certificates include warranties to protect you and your customers: a $1.75M or $2M Netsure Protection Warranty for your business and an industry-best $2M aggregate Relying Party Warranty for your customers.

**Certificate profile options**

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

- **OCSP Must-Staple**: Allows you to include the OCSP Must-Staple extension in OV and EV SSL/TLS certificates. Browsers with support for OCSP must-staple may display a blocking interstitial to users accessing your site. Ensure that your site is configured to properly and robustly serve stapled OCSP Responses before installing the certificate.

- **HTTP Signed Exchange**: Allows you to include the CanSignHTTPExchanges extension in an OV and EV SSL/TLS certificate. The HTTP Signed Exchange extension is under active development. There may be additional changes to the requirements as industry development continues.

- **Delegated Credentials**: Allows you to include the DelegationUsage extension in OV and EV SSL/TLS certificates. The Delegated Credentials for TLS extension is under active development within the Internet Engineering Task Force (IETF). There may be additional changes to the requirements as industry development continues.

- **Data Encipherment**: Allows you to include the Data Encipherment key usage extension in OV and EV SSL/TLS certificates. Useful when you want to use the public key in the certificate to encrypt user data and application data.

More information: https://docs.digicert.com/manage-certificates/certificate-profile-options/
The Product Settings page allows you to configure which certificate products can be selected per account or per division. In addition, product options can also be configured by user role.

Domain and organisation validation

Domain Control Validation (DCV)

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

DigiCert currently supports these DCV Methods:

- Email Validation: With this validation method, DigiCert sends three sets of DCV emails: WHOIS-based, constructed, and DNS TXT-based. To demonstrate control over the domain, an email recipient follows the instructions in a confirmation email sent for the domain. The confirmation process consists of visiting the link provided in the email and following the instructions on the page.
• DNS CNAME Validation: With this validation method, you add a DigiCert generated random value (provided for the domain in your CertCentral account) to the domain’s DNS as a CNAME record. When DigiCert does a search for DNS CNAME records associated with the domain, we can find a record where the record’s value includes the DigiCert random value.

• DNS TXT Validation: With this validation method, you add a DigiCert generated random value (provided for the domain in your CertCentral account) to the domain’s DNS as a TXT record. When DigiCert does a search for DNS TXT records associated with the domain, we can find a record where the record’s value includes the DigiCert random value.

• File Validation (HTTP Practical Demonstration, also referred to as FileAuth): With this validation method, you host a file containing a DigiCert generated random value (provided for the domain in your CertCentral account) at a predetermined location on your website: [domain]/.well-known/pki-validation/fileauth.txt. Once the file is created and placed on your site, DigiCert visits the specified URL to confirm the presence of our random value.

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


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

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

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

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

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

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

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

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

Management of orders and certificates

Orders and certificates can be managed directly from the CertCentral platform.
An order relates to the chosen multi-year plan. A certificate belongs to an order and may be reissued many times during the lifetime of the order. Important options for an order include:

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

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

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

Certificate management includes the following actions:

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

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

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

Approval requirements can be configured in the Settings/Preferences page of CertCentral.

Duplicate certificates

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

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

More information: https://docs.digicert.com/manage-certificates/duplicate-ssl-tls-certificate/

Certificate reissue

All DigiCert certificates come with unlimited free reissues. The list below includes some reasons for reissuing a certificate.

- Current certificate about to expire.
- Lost the private key and want to re-key the certificate.
- Need to change the common name on the certificate (for example, you want to remove example.com and add yourdomain.com).
- Need to add, remove, or change some of the SANs listed in the certificate.

The certificate reissue process allows you to modify an issued certificate. Some modifications allow you to build upon the original certificate, resulting in two or more versions of that certificate. For example,
when reissuing a certificate, you can add domains to the original certificate. Adding domains to a certificate doesn’t revoke the original certificate.

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

More information: [https://docs.digicert.com/manage-certificates/reissue-ssl/tls-certificate/](https://docs.digicert.com/manage-certificates/reissue-ssl/tls-certificate/)

**Downloading a certificate**

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

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

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

Custom order forms fields features:

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

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

More information: [https://docs.digicert.com/manage-account/customize-your-certificate-request-forms/managing-custom-order-form-fields/](https://docs.digicert.com/manage-account/customize-your-certificate-request-forms/managing-custom-order-form-fields/)
Renewal notification

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

You can configure certificate renewal notifications or escalation renewal notifications:

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

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

Divisions

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

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

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

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

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

Subaccounts

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

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

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

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

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

Creating a subaccount

On the Create subaccount page, enter the account information for the subaccount:
• Select a subaccount type. Note: Once a subaccount has been created you need to contact your account manager to change its type. Only the following three subaccount types can be created in CertCentral. See this page to create Managed subaccounts.
  o Retail: Gives the user a CertCentral Retail account. Intended for users that only have a few certificates and don’t need complex certificate management or account management features. Not all CertCentral features are available in a Retail account.
  o Enterprise: Gives the user a CertCentral Enterprise account. All features available to the parent account are available to this subaccount.
  o Reseller: Gives the user a CertCentral Partner account. Select this type if your user is a certificate reseller. All features available to the parent account are available to this subaccount.

• Account manager (optional). Select a CertCentral user to manage this subaccount. By default, all administrators in your account can manage all subaccounts. To allow any other user role to manage this subaccount, set them as the account manager. An administrator can change this at any time.

• Allow this subaccount to create the following types of subaccounts. The subaccount you are creating can create subaccounts of their own, which they can manage.

• Subaccount contact. Enter the contact information for the user that this subaccount is registered to.

• Organization details. Enter the information about the organization that this subaccount is registered to. Subaccounts do not inherit organizations from a parent account.

• Product billing. Note: You can change a subaccount’s billing settings after it has been created, unless the subaccount has an assigned contract.
  o Bill subaccount: Orders placed by the subaccount are invoiced and paid by the subaccount.
  o Bill your account name. Orders placed by the subaccount are invoiced to and paid for by your account.
    ▪ Force subaccount children to bill the subaccount. Subaccounts created by this subaccount to be billed to your account.
    ▪ Currency. Display the subaccount’s pricing in their preferred currency. Note that this only affects the price displayed in the subaccount. The Parent account is still billed in its set currency.
    ▪ Product pricing. Use default pricing: The subaccount receives standard pricing for all products in CertCentral. Customize pricing: Allows you to offer the subaccount unique pricing per product
  o Products. Choose which products are available to this subaccount and if you selected Customize pricing, set the unique pricing for each product. This can be changed later.

More information: [https://docs.digicert.com/manage-account/subaccounts-management/](https://docs.digicert.com/manage-account/subaccounts-management/)
User roles

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

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

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

The main roles are:

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

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

More details are given below.

<table>
<thead>
<tr>
<th><strong>Administrator</strong></th>
<th>Full CertCentral account access with these permissions:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Access and manage Discovery.</td>
</tr>
<tr>
<td></td>
<td>• Manage divisions (create and edit) and account users (create, delete, and edit).</td>
</tr>
<tr>
<td></td>
<td>• Manage organizations (add new organizations), domains (add or deactivate), guest requests, and API access.</td>
</tr>
<tr>
<td></td>
<td>• View all certificate requests and certificate orders, request certificates, approve certificate requests, and run order reports.</td>
</tr>
<tr>
<td></td>
<td>• Manage account finance settings and finances (view balance history, run spending reports, deposit funds, and more).</td>
</tr>
</tbody>
</table>
### DIGICERT® CERTIFICATION PROGRAM

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage account settings</td>
<td>Manage account settings (authentication settings, IP access restrictions, product restrictions, and more), audit settings, and audit logs.</td>
</tr>
<tr>
<td><strong>Standard User</strong></td>
<td>Account users with these permissions:</td>
</tr>
<tr>
<td></td>
<td>• Request certificates.</td>
</tr>
<tr>
<td></td>
<td>• Monitor certificate requests and orders (their own and others).</td>
</tr>
<tr>
<td></td>
<td>• A manager or administrator must approve changes.</td>
</tr>
<tr>
<td><strong>Limited User</strong></td>
<td>Account users with these permissions:</td>
</tr>
<tr>
<td></td>
<td>• Request certificates.</td>
</tr>
<tr>
<td></td>
<td>• Monitor their own certificate requests and orders.</td>
</tr>
<tr>
<td></td>
<td>• A manager or administrator must approve changes.</td>
</tr>
<tr>
<td><strong>Finance Manager</strong></td>
<td>Limited account users whose primary role is to manage account finances. Includes these permissions:</td>
</tr>
<tr>
<td></td>
<td>• View balance history, spending reports, and account pricing.</td>
</tr>
<tr>
<td></td>
<td>• Manage purchase orders and deposit funds.</td>
</tr>
<tr>
<td></td>
<td>• Manage order reports.</td>
</tr>
<tr>
<td></td>
<td>• Request certificates.</td>
</tr>
<tr>
<td></td>
<td>• Monitor their own certificate requests and orders.</td>
</tr>
<tr>
<td><strong>Manager</strong></td>
<td>Limited account users whose primary role is to help manage the account. Includes these permissions:</td>
</tr>
<tr>
<td></td>
<td>• Access and manage Discovery.</td>
</tr>
<tr>
<td></td>
<td>• View divisions and manage account users (edit).</td>
</tr>
<tr>
<td></td>
<td>• View organizations and manage domains (add or deactivate).</td>
</tr>
<tr>
<td></td>
<td>• View all certificate requests and certificate orders, request certificates, approve certificate requests, and run order reports.</td>
</tr>
<tr>
<td></td>
<td>• Manage account finance settings and finances (view balance history, run spending reports, deposit funds, and more).</td>
</tr>
<tr>
<td></td>
<td>• Manage audit settings and audit logs.</td>
</tr>
</tbody>
</table>

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

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

More information: [https://docs.digicert.com/manage-account/certcentral-user-roles-account-access/roles-account-access/](https://docs.digicert.com/manage-account/certcentral-user-roles-account-access/roles-account-access/)
User access/authentication control methods

**Passwords**

Minimum password requirements can be set from the CertCentral portal.

**Two-Factor Authentication**

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

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

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

More information: [https://docs.digicert.com/manage-account/certcentral-two-factor-authentication/configure-two-factor-authentication-requirements/](https://docs.digicert.com/manage-account/certcentral-two-factor-authentication/configure-two-factor-authentication-requirements/)

**IP restrictions**

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

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

**Single Sign-On**

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

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

Guest URL

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

Guest URLs are configured with the following details:

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

More information: [https://docs.digicert.com/manage-account/managing-guest-urls/](https://docs.digicert.com/manage-account/managing-guest-urls/)

Guest access

Guest access allows a person to manage their order without a CertCentral login. With their email address and order number (or FQDN in the certificate), they can download, reissue, or revoke their certificate. Guest access can be enabled for all orders across your account, or on individual orders.

More information: [https://docs.digicert.com/manage-account/saml-single-sign-on-admin-guide/](https://docs.digicert.com/manage-account/saml-single-sign-on-admin-guide/)
Your CertCentral account has a unique Guest access login page. To confirm your person's identity, an authentication email is sent by CertCentral that provides access for two hours. Guest access is available for the organization and technical contact listed on an order.

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

Reporting options

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

Dashboard: A graphically organized view of your certificates, including expiring certificates and pending requests.
Orders Report: Find all certificates issued and filter by any field.

Audit logging

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