Reports ................................................................................................................................. 25
Email Notifications ............................................................................................................. 25
Audit logging ....................................................................................................................... 26
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.

More information can be found in the CertCentral Professional Training Guide which can be downloaded from https://www.digicert.com/tls-ssl/tls-certification-program. 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, 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 and Code Signing certificate products available in DigiCert CertCentral Enterprise
- Describe the Business SSL certificate entitlements, e.g. CT log monitoring, malware scanning, DigiCert Smart Seal
- 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
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 come with many options and benefits. These are described below.

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>Secure Site OV</th>
<th>Secure Site EV</th>
<th>Secure Site Pro</th>
<th>Secure Site Pro EV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wildcard Support</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>SAN Limit</td>
<td>250</td>
<td>250</td>
<td>250</td>
<td>250</td>
</tr>
<tr>
<td>PQC Toolkit</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>CT Monitoring</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Assessment</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Malware/Blacklist Check</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Premium Site Seals</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Priority Validation</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Priority Support</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Netsure Protection Warranty</td>
<td>$1.75M</td>
<td>$1.75M</td>
<td>$2M</td>
<td>$2M</td>
</tr>
<tr>
<td>Relying Party Warranty</td>
<td>$2M</td>
<td>$2M</td>
<td>$2M</td>
<td>$2M</td>
</tr>
</tbody>
</table>

Flex certificates

DigiCert Secure Site and Secure Site Pro 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. Note that the maximum validity period for a publicly-trusted SSL/TLS certificate is currently 397 days, so you may need to reissue such as certificate multiple times during a Multi-year Plan.

When you reissue certificates for a Multi-year Plan, you can do the following:

- Set a new expiration date for the reissued certificate: The maximum validity period for a reissued certificate is the maximum certificate lifetime defined by CA/B Forum baseline requirements or the end of the Multi-year Plan, whichever is sooner.
- Change or remove domains: Removing and changing domains requires DigiCert to revoke all previously issued certificates. DigiCert waits 48-72 hours before revoking the original certificate and any existing duplicates and reissues.
- Add domains: Adding domains may result in additional costs. Prices for new domains are pro-rated and applied based on the remaining time in the Multi-year Plan.

More information: [https://docs.digicert.com/manage-certificates/multi-year-plans/](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/](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/](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/](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.
The DigiCert Smart Seal is a new dynamic site seal that gives website visitors confidence that their information is secure on the web. Real-time security indicators enabled through various microinteractions alert visitors that the seal is actively present on the page, the site has been validated, and the site is protected by an active certificate from the world’s most trusted certificate authority.

When site visitors hover over the DigiCert Smart Seal, they see the company’s logo (if uploaded and verified by DigiCert). They also view usable information about the site’s security delivered right to the seal, so users do not have to leave the page to verify a site’s legitimate identity.

The Smart Seal can be configured to show the following options on the information page:

**Malware scan:** Add the date of the most recently completed malware scan. Site visitors can see that you monitor your website for viruses and malware.

**CT log monitoring:** Add the date you enabled CT log monitoring for your website's domain. Site visitors can see you monitor the transparency logs allowing you to act quickly if a bad actor issues a fraudulent certificate for your domain. This feature is only available for Secure Site Pro certificates.

**Blocklist:** Add a blocklist check. Site visitors can see your business is clear from government and country-specific blocklists.

**PCI compliance scan:** Add the date of the most recently completed PCI compliance scan. Site visitors can see that you monitor your website to ensure it is compliant with PCI DDS Standards. This feature is only available for Secure Site Pro and Secure Site EV certificates and requires the Vulnerability Assessment service to be enabled for your certificate order.

**Verified Customer:** Display how long you’ve been a DigiCert customer. Site visitors can see how long you’ve been using one of the most trusted names in
TLS/SSL certificates to protect your sites.

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/](https://docs.digicert.com/manage-certificates/certificate-profile-options/)

Code Signing Certificate Products
A DigiCert Code Signing Certificate increases trust by verifying the source and integrity of your application.

- Digitally signs a program to prove that it has not been altered or compromised
- Supports Microsoft Authenticode, Office VBA, Java, Adobe AIR, Apple's Mac OS, and Mozilla objects
- Avoids unnecessary warning messages and ensure your applications can be trusted

A DigiCert EV Code Signing Certificate increases trust by verifying the source and integrity of the application. It also helps users avoid warning messages when downloading the application.

- Combines the benefits of a standard Code Signing Certificate with a rigorous Extended Validation process
- Provides compatibility and grants immediate reputation with Windows 8 and Internet Explorer, eliminating warning messages
- Supports Microsoft Authenticode, Office VBA, Java, Adobe AIR, Apple's Mac OS, and Mozilla objects
- Extended Validation ensures additional organization vetting to protect your users and your reputation
- Includes two-factor authentication for enhanced security

A DigiCert EV Code Signing Certificate can be provisioned with the following options:
**DIGICERT® CERTIFICATION PROGRAM**

- Preconfigured Hardware Token: DigiCert installs your EV CS certificate on a secure token and ships the token to you with instructions for how to activate it.
- Existing Token: After DigiCert issues your EV CS certificate, you need to install the certificate on your token.
- HSM: After DigiCert issues your EV CS certificate, install it on your HSM device. (Note: You must have a FIPS 140-2 Level 2 or Common Criteria EAL4+ compliant device.)

More information: [https://docs.digicert.com/manage-certificates/code-signing-certificate/](https://docs.digicert.com/manage-certificates/code-signing-certificate/)

**Product Settings**

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.

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.

By default, CertCentral accounts are configured for one-step certificate request approvals. An account admin must approve a certificate request before DigiCert can start processing the order (validating the organization, etc.). However, you can remove the approval step from the OV/EV SSL certificates issuance workflows for your CertCentral administrators, managers, and finance managers. 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-ssltls-certificate/

Certificate reissue
All DigiCert certificates come with unlimited free reissues. 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-ssltls-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/](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 (usually 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.

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>Administrator</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>
<tr>
<td></td>
<td>- Manage account settings (authentication settings, IP access restrictions, product restrictions, and more), audit settings, and audit logs.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Standard User</th>
<th>Account users with these permissions:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Limited User

Account users with these permissions:

- Request certificates.
- Monitor their own certificate requests and orders.
- A manager or administrator must approve changes.

### Finance Manager

Limited account users whose primary role is to manage account finances.

Includes these permissions:

- View balance history, spending reports, and account pricing.
- Manage purchase orders and deposit funds.
- Manage order reports.
- Request certificates.
- Monitor their own certificate requests and orders.

### Manager

Limited account users whose primary role is to help manage the account.

Includes these permissions:

- Access and manage Discovery.
- View divisions and manage account users (edit).
- View organizations and manage domains (add or deactivate).
- View all certificate requests and certificate orders, request certificates, approve certificate requests, and run order reports.
- Manage account finance settings and finances (view balance history, run spending reports, deposit funds, and more).
- Manage audit settings and audit logs.

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.

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/)
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 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.

You can control what order contacts are eligible for Guest access by enabling or disabling the Organization contact, Technical contact, Guest URL requester (subscriber) (the email address that placed the order), and “Additional emails” listed on order checkboxes.

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.

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

Email Notifications
CertCentral sends out emails to users throughout the order/approval process, and when a certificate is expiring or has expired. You can customize these email templates so they suit your account or organization’s needs.

Basic notification settings allows you to specify the email recipients and the email language.

Custom email templates allows you to edit the standard email templates.

More information:
https://docs.digicert.com/manage-account/account-notifications/customize-email-templates/
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.

Clicking on **Audit Log Notifications** to create email notifications for specific events.