DIGICERT CERTCENTRAL®
DISCOVERY & AUTOMATION

digicert®

digicert®

DigiCert CertCentral Discovery & Automation

Comprehensive oversight of your TLS certificates

At-a-glance

DigiCert CertCentral® manager gives businesses complete visibility and lifecycle control over any certificate in their environment, helping them reduce risk, quickly respond to threats, and control operational costs.

The Discovery and Automation features are customizable solutions to make certificate management simple and efficient for your business. We give you multiple options to best fit your organization's infrastructure to help you monitor and renew your digital certificates.

Technical specifications

- Cloud-based and on premises discovery
- Scan both private and public certificates
- Install sensors for secure analytics and control
- Automation enabled with: ACME, proprietary enterprise automation or APIs
- ACME controller agent allows management of ACME clients within CertCentral UI (Beta)
- Integrates easily with most web servers including: Apache, IBM, NGINX; load balancers: F5 Networks, Citrix NetScaler, A10 Networks; and DevOps tools: Azure, AWS, SaltStack and more.
- Customized auto-renewal and notifications delivered to separate users at specific times
- Get real-time certificate statuses for: approval, issuance, revocation, and renewal of all certificates
- Auto CSR generation and installation
- Automation currently supports high-assurance TLS/SSL certificates (OV & EV)

Complete visibility of certificate management

DigiCert CertCentral management console can scan your entire network—regardless of size or complexity—for expired and rogue certificates that could lead to unexpected certificate related outages or vulnerabilities. It's easy to manage, track and run reports on your entire certificate portfolio from a single pane of glass so you can be confident that nothing slips through the cracks.

We provide multiple scanning options to uncover and monitor all certificates, private and public, regardless of the Certificate Authority (CA). When a certificate is discovered, users will see details such as the issuing CA, certificate expiration date, signature algorithm, and ciphers.

Two methods of Discovery:

1. Cloud-based: This fast and easy option requires no installation and can be turned on in an instant to identify untracked certificates before they expire and become a potential problem to your business.
2. On-premises: Mitigate risks and increase control through the use of proprietary enterprise sensor technology to scan, catalog and report across your entire certificate inventory.

Automate certificate workflows

CertCentral automation gives IT administrators the ability to streamline every step of the certificate lifecycle—from issuance and renewal to updates and revocation—while quickly provisioning and issuing certificates to users or devices anywhere.

- ACME: Certificate-level automation for Extended Validation (EV) and Organization Validated (OV) certificates.
  - Manage multiple ACME clients, running on Windows or Linux, giving you an efficient way to automate certificate delivery—regardless of the quantity.
  - Improve the security of using ACME in your network through CertCentral's discovery sensors. The sensor can act as a secured relay ensuring the ACME client doesn't directly speak to an unsecure third party.
- APIs: CertCentral allows for direct integration between DigiCert tools and your system or platform of choice, providing you with the ideal solution for your environment.
  - The DigiCert REST API provides a secure and simple path for administrators to manage the certificate lifecycle and automate the process of purchasing and deploying SSL certificates across their network.
- Automation Tools: Get proprietary discovery and automation features that seamlessly integrate with other OEM solutions, such as F5, Citrix, and more.
  - Deploy sensors across your network to allow scans of all your certificates regardless of network complexity.
  - Customize the automation to fit your unique needs.

As custom as your business demands

The Discovery and Automation features within CertCentral are the best solution for enterprises looking to scale with flexibility and customization. Both of these features seamlessly integrate with other platforms to allow the best option for your enterprise.

5 key benefits of Automation and Discovery

1. Visibility: Locate and monitor all public and private TLS/SSL certificates in your network from a single pane of glass, regardless of the issuing Certificate Authority (CA).
2. Efficiency: Reduce the time, money and resources your IT team spends managing SSL certificates and network access.
3. Flexibility: Avoid unexpected cert expirations by using the automation method that best fits your organization's needs. Leverage a full suite of integration options such as ACME, REST API and GraphQL.
4. Consistency: Maintain organizational security policies and best practices by running reports to ensure that all certificates are using the approved key lengths, hashing algorithms and validation. Reduce errors in certificate deployments by implementing both Discovery and Automation features together.
5. Scalability: Issue, track, and automate workflows for an unlimited number of certificates or user identities from one platform. Locate and control any certificate, regardless of certificate type, or if it's integrated into a device on your network.

Reach out to your account manager for more information:

1.877.438.8776 (Americas)
+61.3.9674.5500 (Asia Pacific, Japan)
+44.203.788.7741 (Europe, Middle East, Africa)

digicert®