Service Name

AWS Certificate Manager

Service Overview

AWS Certificate Manager (ACM) is a service that simplifies the process of creating, managing, and renewing SSL/TLS X.509 certificates and their corresponding private keys. ACM manages public, private, and imported certificates for secure communications across the internet or within internal networks. The service supports both IPv4 and IPv6 on public endpoints and can secure singular domain names, multiple specific domain names, wildcard domains, or combinations of these. ACM automates certificate deployment with integrated AWS services, handles automatic renewals, and uses strong encryption and key management practices to protect private keys. Public certificates are trusted by browsers, operating systems, and mobile devices, while private certificates are used for internal applications and services.

Key Use Cases

- Securing websites and web applications: Deploy SSL/TLS certificates on Elastic Load Balancers, CloudFront distributions, and API Gateway to enable HTTPS communications
- Internal PKI for enterprise applications: Use private certificates signed by AWS Private CA for securing internal applications and services within corporate networks
- Container and Kubernetes workloads: Secure Amazon EKS pods and terminate TLS at Kubernetes Ingress or AWS load balancers using ACM certificates
- Nitro Enclaves security: Install certificates on EC2 instances with Nitro Enclaves for enhanced security applications requiring isolated certificate management

Features

- **Automatic Certificate Renewal**: ACM automatically renews certificates after 11 months of their 13-month validity period to ensure continuous security
- **Domain Validation**: Supports DNS, email, and HTTP validation methods to verify domain ownership before certificate issuance
- **Exportable Public Certificates**: Allows exporting public certificates for use on any workload including EC2 instances, containers, or on-premises hosts
- **AWS Service Integration**: Native integration with ELB, CloudFront, API Gateway, Elastic Beanstalk, App Runner, and other AWS services
- **Multiple Certificate Types**: Supports single domain, multi-domain, and wildcard certificates with various encryption algorithms (RSA 2048-bit, ECDSA 256/384-bit)
- **Private Certificate Authority Support**: Integration with AWS Private CA for issuing private certificates for internal applications

Value Proposition

AWS Certificate Manager eliminates the complexity and cost of purchasing, uploading, and renewing SSL/TLS certificates. Public certificates are provided at no additional cost for use with integrated AWS services, significantly reducing operational expenses compared to third-party certificate authorities:

- The service automates the entire certificate lifecycle including provisioning, deployment, and renewal, reducing manual errors and administrative overhead
- ACM's tight integration with AWS services ensures seamless certificate deployment and management
- The service provides enterprise-grade security with encrypted private key storage using AWS KMS, and supports both public and private PKI use cases
- Automatic renewal prevents service disruptions from expired certificates, while centralized management through the AWS console, CLI, and APIs simplifies operations across multiple certificates and domains

Service Integration

ACM integrates natively with multiple core AWS services for certificate deployment and management. Primary integrations include Elastic Load Balancer (ELB) for load balancer SSL termination, Amazon CloudFront for secure content delivery, and Amazon API Gateway for secure API endpoints:

- Additional integrations encompass AWS Elastic Beanstalk for application environments, AWS App Runner for containerized applications, Amazon EKS for Kubernetes workloads, and AWS Nitro Enclaves for enhanced security applications
- The service also works with Amazon Cognito for user pool configurations, AWS Amplify for custom domains, Amazon OpenSearch Service for Application Load Balancer provisioning, and AWS Network Firewall for TLS inspection
- AWS CloudFormation supports ACM certificates as template resources, enabling infrastructure-as-code deployments across all integrated services

Onboarding and Offboarding

Getting started with ACM requires signing into the AWS Management Console and navigating to the ACM console. Customers can request public certificates by specifying domain names and choosing validation methods (DNS, email, or HTTP):

- For DNS validation with Route 53, ACM can automatically create required CNAME records
- Domain ownership must be validated before certificate issuance
- Once validated, certificates can be deployed to integrated AWS services like load balancers or CloudFront distributions

- For exportable certificates, customers can retrieve the certificate and private key for use on any workload
- Private certificates require setting up AWS Private CA first
- The service provides AWS CLI and API access for programmatic management, and supports Infrastructure-as-Code through CloudFormation templates

Getting Started Guide: https://docs.aws.amazon.com/acm/latest/userguide/gs.html

Data Removal

Certificate removal from ACM involves deleting certificates through the console, CLI, or API. When certificates are deleted, they are immediately removed from ACM and can no longer be used with AWS services. For certificates deployed to integrated services, customers must first remove them from those services before deletion. Private keys stored in ACM are securely deleted using AWS KMS key management. Imported certificates can be deleted without affecting the original certificate authority. Certificate transparency logs may retain public certificate information as they are append-only systems managed by third parties.

Backup/Restore and Disaster Recovery

ACM certificates are regional resources that must be requested or imported separately in each region. The service provides built-in resilience through multiple Availability Zones within each region. For disaster recovery, customers should provision certificates in multiple regions and implement cross-region failover strategies. ACM does not provide traditional backup functionality as certificates can be re-issued or imported as needed. Private CA certificates can be backed up through AWS Private CA's disaster recovery capabilities including cross-region subordinate CA deployment strategies.

Backup Capabilities

ACM does not offer traditional backup capabilities as certificates are managed resources that can be re-provisioned. The service maintains certificate metadata and can re-issue certificates upon request:

- For exportable certificates, customers can export and securely store certificates externally
- ACM does not integrate with AWS Backup service as certificates are not considered data requiring backup
- Certificate renewal maintains continuity without requiring backup restoration processes

Disaster Recovery

ACM supports disaster recovery through regional redundancy and certificate re-provisioning capabilities. Certificates are regional resources requiring separate provisioning in each region for multi-region DR strategies:

- The service does not integrate with AWS Elastic Disaster Recovery as certificates can be quickly re-issued or imported during recovery scenarios
- For comprehensive DR, customers should provision certificates in multiple regions and implement automated failover mechanisms using services like Route 53 health checks

Recovery Objectives

ACM supports rapid certificate provisioning to meet Recovery Time Objectives (RTO), with public certificates issued within seconds after domain validation. Recovery Point Objectives (RPO) are minimal as certificate metadata is maintained by AWS. For disaster recovery scenarios, certificates can be quickly re-issued or imported in alternate regions. Automated renewal ensures certificates remain valid during extended outages. Integration with AWS services enables rapid restoration of secure communications during recovery operations.

Service Constraints

Service Quotas: https://docs.aws.amazon.com/acm/latest/userguide/acm-limits.html

FAQ: https://aws.amazon.com/certificate-manager/faqs/

Technical Requirements

Service Documentation: https://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html

User Guide: https://docs.aws.amazon.com/acm/latest/userguide/gs.html

API Reference: https://docs.aws.amazon.com/acm/latest/APIReference/Welcome.html

Pricing Overview

Please see the AWS UK G Cloud 15 Pricing Document accompanying this service in the Digital Marketplace.

Public Pricing: https://aws.amazon.com/certificate-manager/pricing/

Cost Optimization

ACM provides significant cost optimization through free public certificates for integrated AWS services, eliminating annual certificate authority fees that can cost hundreds of

dollars per certificate. Exportable public certificates cost only $15 per FQDN and $149 per wildcard, significantly below market rates:

- The service includes 10,000 free certificate export API calls monthly
- Automatic renewal eliminates manual certificate management costs and prevents expensive service outages from expired certificates
- Wildcard certificates can secure multiple subdomains under a single certificate, reducing the total number of certificates needed
- Import capabilities allow using existing certificates without additional ACM charges
- The service's integration with AWS services eliminates third-party SSL proxy costs and reduces infrastructure complexity

Savings Considerations

Primary cost savings come from eliminating traditional certificate authority fees, which typically range from $50-500+ annually per certificate. Organizations can save thousands of dollars annually by replacing third-party certificates with free ACM public certificates:

- Automatic renewal prevents costly service disruptions and eliminates manual certificate management labor costs
- Wildcard certificates provide economies of scale for organizations with many subdomains
- The service reduces operational costs through centralized certificate management and automated deployment
- Integration with AWS services eliminates need for dedicated certificate management infrastructure
- For exportable certificates, ACM's pricing is substantially lower than traditional enterprise certificate authorities while providing the same security and trust levels
- Organizations moving from on-premises certificate management can realize significant cost reductions in both licensing and operational expenses