Active Directory Certificate Services Overview

By Archiveddocs

Archived: 2026-04-06 00:07:42 UTC

Applies To: Windows Server 2012 R2, Windows Server 2012

This document provides an overview of Active Directory Certificate Services (AD CS) in Windows Server® 2012. AD CS is the Server Role that allows you to build a public key infrastructure (PKI) and provide public key cryptography, digital certificates, and digital signature capabilities for your organization.

Did you mean…

- Active Directory Domain Services Overview
- Active Directory Rights Management Services Overview
- Active Directory Federation Services Overview
- Active Directory Lightweight Directory Services Overview

Note

To comment on this content or ask questions about the information presented here, please use our Feedback guidance.

AD CS provides customizable services for issuing and managing digital certificates used in software security systems that employ public key technologies.

The digital certificates that AD CS provides can be used to encrypt and digitally sign electronic documents and messages. These digital certificates can be used for authentication of computer, user, or device accounts on a network. Digital certificates are used to provide:

1. Confidentiality through encryption
2. Integrity through digital signatures
3. Authentication by associating certificate keys with computer, user, or device accounts on a computer network

You can use AD CS to enhance security by binding the identity of a person, device, or service to a corresponding private key. AD CS gives you a cost-effective, efficient, and secure way to manage the distribution and use of certificates.

Applications supported by AD CS include Secure/Multipurpose Internet Mail Extensions (S/MIME), secure wireless networks, virtual private network (VPN), Internet Protocol security (IPsec), Encrypting File System (EFS), smart card logon, Secure Socket Layer/Transport Layer Security (SSL/TLS), and digital signatures.

There are multiple changes to AD CS in Windows Server 2012 and the What's New in AD CS article (https://go.microsoft.com/fwlink/?LinkID=224385) describes these changes.

The installation of AD CS role services can be performed through the Server Manager. The following role services can be installed:

Role service	Description
Certification Authority (CA)	Root and subordinate CAs are used to issue certificates to users, computers, and services, and to manage certificate validity.
Web Enrollment	CA Web enrollment allows users to connect to a CA by means of a Web browser in order to request certificates and retrieve certificate revocation lists (CRLs).
Online Responder	The Online Responder service decodes revocation status requests for specific certificates, evaluates the status of these certificates, and sends back a signed response containing the requested certificate status information.
Network Device Enrollment Service	The Network Device Enrollment Service (NDES) allows routers and other network devices that do not have domain accounts to obtain certificates.
Certificate Enrollment Policy Web Service	The Certificate Enrollment Policy Web Service enables users and computers to obtain certificate enrollment policy information.
Certificate Enrollment Web Service	The Certificate Enrollment Web Service is an Active Directory Certificate Services (AD CS) role service that enables users and computers to perform certificate enrollment by using the HTTPS protocol. When used together, the Certificate Enrollment Web Service and the Certificate Enrollment Policy Web Service enable policy-based certificate enrollment for - domain member computers not connected to the domain - computers that are not domain members

The following table provides additional resources for evaluating AD CS.

Content type	References
Product evaluation	- Test Lab Guide: Deploying an AD CS Two Tier PKI Hierarchy - Test Lab Guide: Demonstrating Key-Based Renewal

Content type	References
	- Test Lab Guide Mini-Module: Cross-Forest Certificate Enrollment using Certificate Enrollment Web Services
Community resources	- Community directory for documentation and information: Windows PKI Documentation Reference and Library - Frequently asked questions (FAQs) list Active Directory Certificate Services (AD CS) Public Key Infrastructure (PKI) Frequently Asked Questions (FAQ) - Support forum: Windows Server Security Forum - Product team blog: Windows PKI Blog - Support Team Blog: Ask the Directory Services team - Script repository: TechNet Script Center Repository search for Certification, Certificate, or PKI. - Community technology overview: Active Directory Certificate Services (AD CS) Overview
Related technologies	Active Directory Domain Services Active Directory Rights Management Services Active Directory Federation Services Active Directory Lightweight Directory Services

Note

To comment on this content or ask questions about the information presented here, please use our Feedback guidance.
