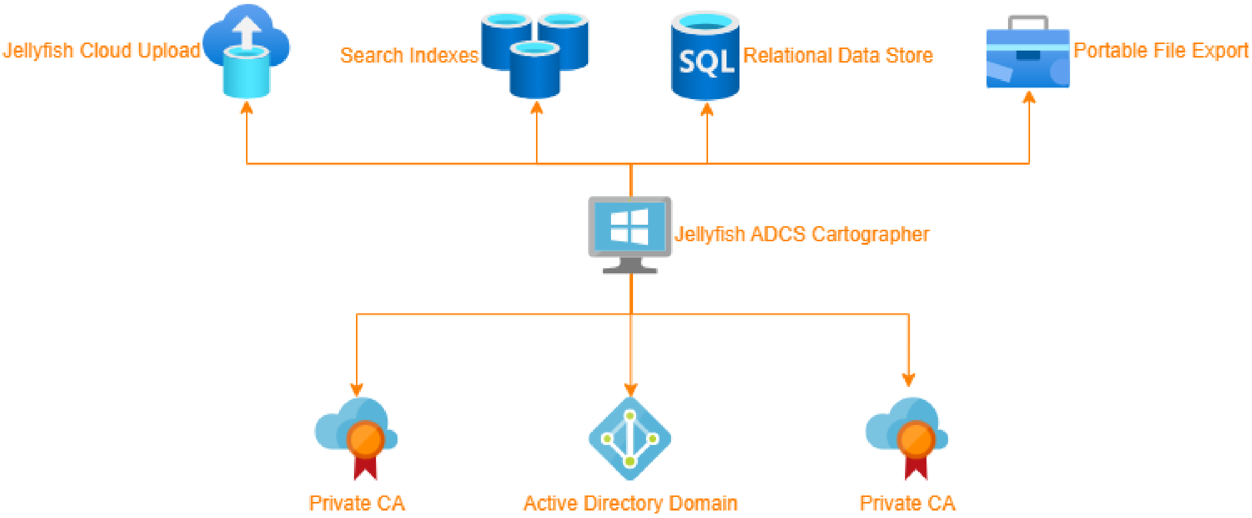
Fact Sheet

Cogito Group

Jellyfish AD CS Cartographer

Jellyfish Cartographer for Active Directory Certificate Services

Cartographer is an advanced tool developed by Cogito Group to support better visibility of certificates and PKI infrastructure. It provides enhanced functionality beyond what is available through standard Windows Certificate Authority software. This accessible software offers technological advantages that set it apart from any other AD CS extension technology.



We’ve worked closely with our consultant to distill our expertise into a powerful tool that automates advanced data aggregation techniques. **Cartographer** consolidates critical PKI insights—previously buried within the complex and outdated Active Directory tooling—into a single, intuitive, and exportable interface.

Gain full oversight of your PKI without the need for expert-level knowledge, costly consultants, or time-consuming manual analysis. Instantly access the essential details you need, presented in a clear and actionable format.

Cartographer makes PKI monitoring faster and more accessible. Find certificates, monitoring system health, and preventing outages has never been simpler.

Feature Summary

- Advanced real time on demand domain certificate scanning
- High speed, multi-modal certificate search
- Report on certificate throughput and throughput trends
- Report on upcoming certificate expirations
- Analyze connections between certificates, reporting on user and device certificate holdings across domains
- Analyze certificate template availability and usage across certificate authorities and domains
- CRL and OCSP monitoring and alerting
- Certificate authority uptime KPIs
- Email alerting
- Automation and scheduling
- RESTful API and API key delegation

Enhanced Functionality Beyond AD CS

Cartographer goes beyond the capabilities of the Windows Certificate Authority by offering an intuitive and user-friendly interface to scan, consolidate, and analyze all aspects of your PKI inventory.

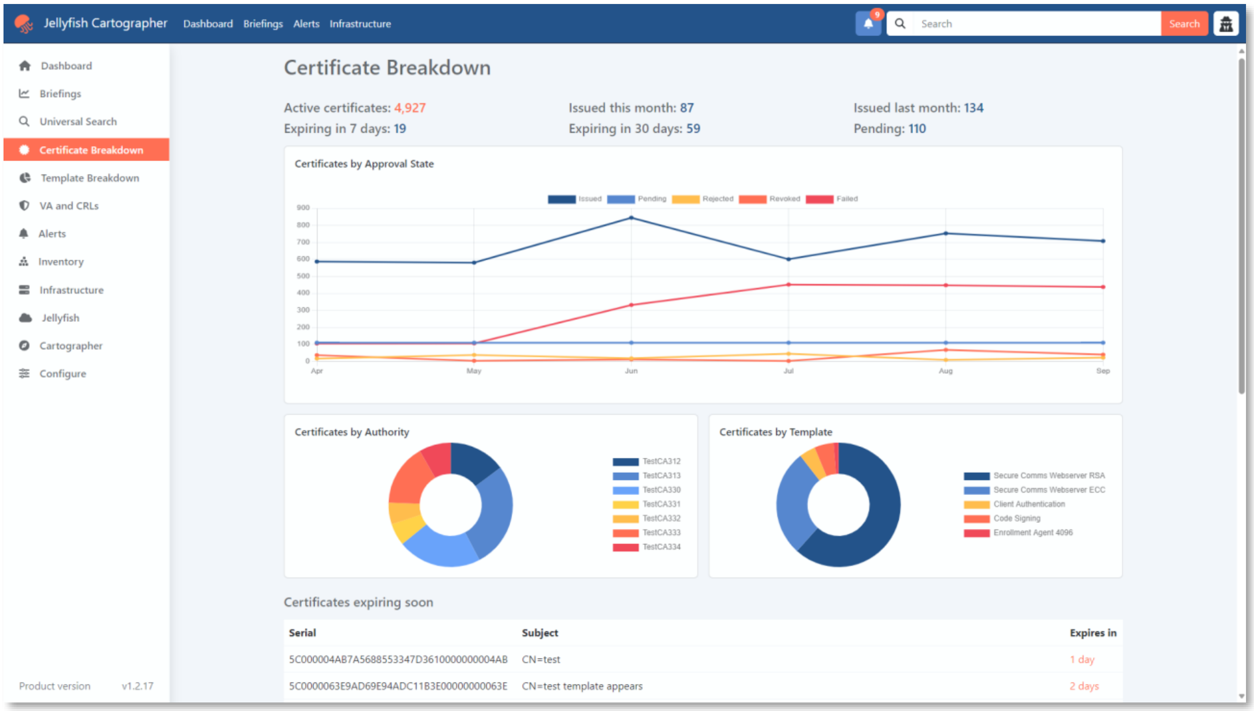
Cartographer offers a single, remotely available web portal to replace the many fragmented certificate authority administration tools otherwise required to monitor an AD CS PKI.

With its ability to access all data from any Certificate Authority within its operating domain, **Cartographer** can analyze all issued, pending, rejected, failed, and revoked certificates throughout the entire lifespan of the Certificate Authority. The tool's robust data analysis capabilities delve deeper into raw certificate PEM data, extracting powerful analytical information that remains unavailable through the standard AD CS database alone.

Jellyfish AD CS Cartographer

Fact Sheet

Collect, search, and action certificates faster and easier with your PKI analytical companion Cogito Jellyfish **Cartographer**.



Certificate Breakdown

Active certificates: 4,927
Issued this month: 87
Issued last month: 134
Expiring in 7 days: 19
Expiring in 30 days: 59
Pending: 110

Certificates expiring soon

Serial	Subject	Expires in
5C000004AB7A5688553347D3610000000004AB	CN=test	1 day
5C0000063E9AD69E94ADC11B3E00000000063E	CN=test template appears	2 days

Advanced Technological Advantages

Powered by the versatile **Cogito AD CS Shadow Catalogue** (an ESENT—JET Blue—database interface), **Cartographer** leverages cutting-edge technology to enable rapid iteration through the contents of an ESENT database without impacting the performance of other tools accessing the database. The **Shadow Catalogue** accesses the CA database through an AD CS access facilitation protocol pass-through, allowing seamless access to the database without requiring the CA services to stop.

Cartographer reads your domain, targets certificate authorities, and aggregates certificate and PKI information from across otherwise segmented active directory data storages.

Cartographer connects to stores for:

- Domains
- Domain Controllers
- Domain Services published Trusted Certificate Authorities
- Certificate Authorities connected to your Domain

- Certificate Templates and their relationships with Certificate Authorities
- Certificates, in any state (pending, issued, revoked) from a connected Certificate Authority

A deep and intimate understanding of Active Directory Directory Services (AD DS) and its integration with AD CS is no longer required to access the information you need to keep your organization running securely and with confidence.

The strong relationships built between certificates, templates, and requesting users and devices provide a comprehensive overview of technology access, utilizing data from the AD CS database. This advanced approach enables organizations to gain deeper insights and a higher level of understanding of their certificate landscape. Improving visibility and reducing risk.

Versatility and Wide-Ranging Applications

Cartographer's versatility makes it applicable to a broad spectrum of data analysis and Certificate Authority migration scenarios. Its powerful analytics, export, backup and recovery capabilities make it an essential tool for organizations looking to enhance their CA operations. Enabling faster, more detailed analyses and providing insights that drive better decision-making and operational efficiency.

Cartographer's integrated web portal provides a wide variety of analytical tools and report templates, flexible enough for even the most sophisticated of data slicing.

Cartographer reduces the workload of your security team by automating complex PKI data collection and analysis tasks, allowing your experts to focus on strategic decision-making.

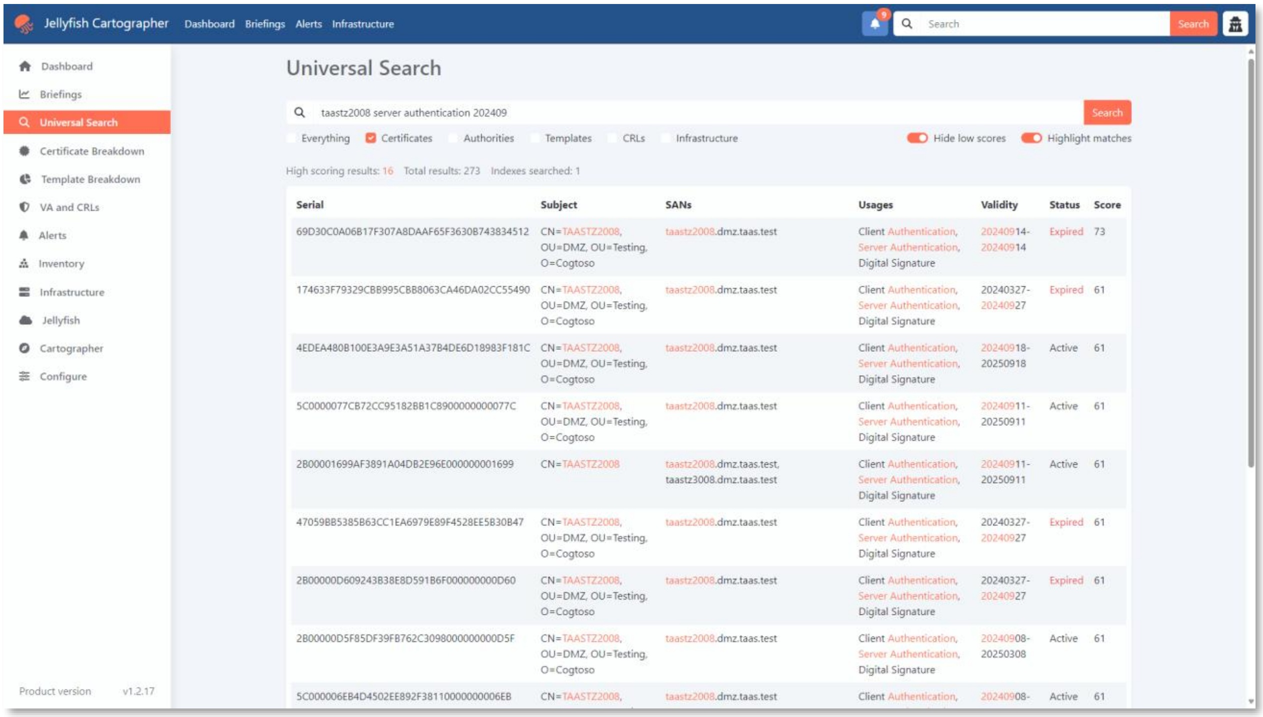
Modern Comprehensive Web User Interface

Cartographer's API server bundles a web portal for a superior and flexible access to the detail you need. The **Cartographer** web portal runs locally, alongside the scanning and analytical services. But may be made accessible to your wider network, enabling access to the reporting and cataloging formation from any device without having to access the AD CS, or AD DS domains or services directly.

User accounts may be delegated to operators without having to grant the otherwise required Administrator privileges that would grant them access to the PKI itself. Separate your concerns and responsibility by allowing analysts and consults only access to the data, not the PKI assets.

Jellyfish AD CS Cartographer

Fact Sheet



Universal Search

taastz2008 server authentication 202409 Search

□ Everything ☑ Certificates □ Authorities □ Templates □ CRLs □ Infrastructure ● Hide low scores ● Highlight matches

High scoring results: 16 Total results: 273 Indexes searched: 1

Serial	Subject	SANs	Usages	Validity	Status	Score
69D30C0A06B17F307A8DAAF65F3630B743834512	CN=TAASTZ2008, OU=DMZ, OU=Testing, O=Cogtoso	taastz2008.dmz.taas.test	Client Authentication, Server Authentication, Digital Signature	20240914-20240914	Expired	73
174633F79329CBB995CBB8063CA46DA02CC55490	CN=TAASTZ2008, OU=DMZ, OU=Testing, O=Cogtoso	taastz2008.dmz.taas.test	Client Authentication, Server Authentication, Digital Signature	20240327-20240927	Expired	61
4EDEA480B100E3A9E3A51A37B4DE6D18983F181C	CN=TAASTZ2008, OU=DMZ, OU=Testing, O=Cogtoso	taastz2008.dmz.taas.test	Client Authentication, Server Authentication, Digital Signature	20240918-20250918	Active	61
5C0000077CB72CC95182BB1C8900000000077C	CN=TAASTZ2008, OU=DMZ, OU=Testing, O=Cogtoso	taastz2008.dmz.taas.test	Client Authentication, Server Authentication, Digital Signature	20240911-20250911	Active	61
2B00001699AF3891A04DB2E96E000000001699	CN=TAASTZ2008	taastz2008.dmz.taas.test, taastz3008.dmz.taas.test	Client Authentication, Server Authentication, Digital Signature	20240911-20250911	Active	61
47059BB5385B63CC1EA6979E89F4528EE5B30B47	CN=TAASTZ2008, OU=DMZ, OU=Testing, O=Cogtoso	taastz2008.dmz.taas.test	Client Authentication, Server Authentication, Digital Signature	20240327-20240927	Expired	61
2B00000D609243B38E8D591B6F000000000D60	CN=TAASTZ2008, OU=DMZ, OU=Testing, O=Cogtoso	taastz2008.dmz.taas.test	Client Authentication, Server Authentication, Digital Signature	20240327-20240927	Expired	61
2B00000D5F85DF39FB762C3098000000000D5F	CN=TAASTZ2008, OU=DMZ, OU=Testing, O=Cogtoso	taastz2008.dmz.taas.test	Client Authentication, Server Authentication, Digital Signature	20240908-20250308	Active	61
5C000006EB4D4502EE892F3811000000006EB	CN=TAASTZ2008,	taastz2008.dmz.taas.test	Client Authentication,	20240908-	Active	61

Key Features

- **Comprehensive Overview:** See all Certificate Authorities across your Active Directory Forest.
- **Briefings and Insights:** Regular, detailed briefings keep your security team updated on the status and health of your PKI.
- **Template Tracking:** Monitor certificate templates across all authorities, including detailed metrics on requested, issued, rejected, and failed certificates.
- **Performance Metrics:** Get detailed metrics on certificates, including issuance throughput, helping you quickly identify and address performance anomalies.
- **Revocation Management:** Track Certificate Revocation Lists (CRL), online CRL responders, and OCSP responders.
- **Throughput Warnings:** Be alerted to high volumes of failed or rejected certificate requests, ensuring prompt attention to potential issues.

- **Service Status Monitoring:** Stay informed when critical AD CS services, online responders, or enrollment agent services are offline.

Connect - Backup - Replace - Recover

Cartographer makes it easy to capture a copy of your certificate authority. Make a snapshot of your CA at a point in time, export it, and recovery when necessary. Take a detailed snapshot of all **Cartographer** inventory, or a subset of the inventory categories, and take it with you for further data analysis.

Export your data in a variety of formats, including a SQLite portable database file, CSV file, or **Jellyfish Command and Control** Import file.

Connect your **Cartographer** server to your **Jellyfish Cloud** or **Jellyfish on-prem Command and Control** portal. Improve the efficiency at which you manage your PKI through the advanced and extensive tools provided by the **Jellyfish** family of products.

Recover your data in the event of a loss of service or integrate cartographer into your backup and disaster recovery plan.

Offline or Online Modes

Cartographer can operate in an offline or disconnected mode or an online mode. This allows you to gain insights while maintaining all data locally with the PKI. Alternatively when used in the online mode, you can get additional functionality and insights, such as the aggregated results of more than one **Cartographer** instance. This is achieved by connecting with online instances of Jellyfish, either in your own environment or through our as a Service (aaS) offering, SecureSME.

Simple RESTFUL API for Integration with Your Workflows

Every organization implements a bespoke and sophisticated reporting or early warning system. **Cartographer's** API makes improving your reporting with AD CS details simpler than previously thought possible.

The **Cartographer** API exposes endpoints tailor made to support a wide variety of Reporting or Alerting use cases. Generate API keys and integrate your reporting tools with access to the **Cartographer** API to integrate our insights with your reporting and monitoring technology solution.

Postman, Curl, Power Shell, Custom Application, all of these can now access your PKI as easily as your operators can, through access to the **Cartographer's** streamlined API backend.

For example:

- Assess all certificate authoritie's health and list any problems with the Health API:

`https://Cartographer.PKI.Cogtoso/API/Health/CertificateAuthority`

- Assess a single certificate authority for any certificate throughput traffic anomalies with the throughput query parameter:

`https://Cartographer.PKI.Cogtoso/API/Health/CertificateAuthority/CogCA360?category=throughput`

- Return the quantity and identifying information of certificate expiring soon with the Certificate API:

`https://Cartographer.PKI.Cogtoso/API/Health/Certificate?category=expiringsoon`

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated ICT company, specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.