



KEY BENEFITS

- Simple, intuitive portal to view and manage certificates across your organization, irrespective of source
- Provides certificate issuance, renewal and revocation for Entrust Authority® Security Manager, Entrust® Certificate Services, and Microsoft Active Directory Certificate Services
- Automated certificate import via Entrust Discovery Agent or Certificate Authority scanner
- Automated expiry notifications for managed and monitored certificates
- Report Designer allows for creation and scheduling of user-defined reports
- On-premises deployment optimized for enterprise private or public cloud hosting
- User administration with MFA authentication through your enterprise IDP or through built-in integration to Entrust Datacard® IntelliTrust™ Cloud Authentication Service
- Agentless certificate deployment via SFTP
- Pluggable architecture for expansion

ENTRUST DATACARD® CERTIFICATE HUB

Find, Control, and Automate the Management of Your Certificates

Certificates continue to proliferate, driven by increased security awareness across industries, new use cases, and the need for organizations to secure and protect the integrity of their data and digital ecosystems. Traditional use cases — like user authentication — have extended to enterprise mobility management, while newer use cases — like software service containerization and IoT — have created an entirely new demand for short-lived certificates and massively distributed infrastructures. Plus, DevOps trends such as CI/CD have made use cases like code signing more prevalent, with enterprises striving to do potentially hundreds of software releases a day.

This large growth in certificate footprint within an organization and the general trend of short validity periods means customers are managing more certificates more frequently, while simultaneously attempting to address legacy deployments as they migrate to newer algorithms or technology providers. Whether it be the use of “unmanaged” certificates or “rogue” CAs within an organization, the ability to find issues and either notify owners or take direct action is a necessity for any IT or security operations team.

The Solution: Entrust Datacard Certificate Hub

Entrust Datacard Certificate Hub was created to provide simple and intuitive certificate oversight across your organization. Its certificate discovery and advanced reporting help you find and manage certificates. Certificate Hub provides active certificate lifecycle management across multiple CAs, giving you a single enforcement point for centralization efforts.

With Certificate Hub, you can view and manage all certificates across your enterprise, regardless of issuer. And with its intuitive “single pane of glass” view, you can **find**, **control**, and **automate** the management of certificates. It helps increase security and reduce outages while lessening the workload on IT security/operations staff. CISO's can sleep easier knowing they have central oversight.

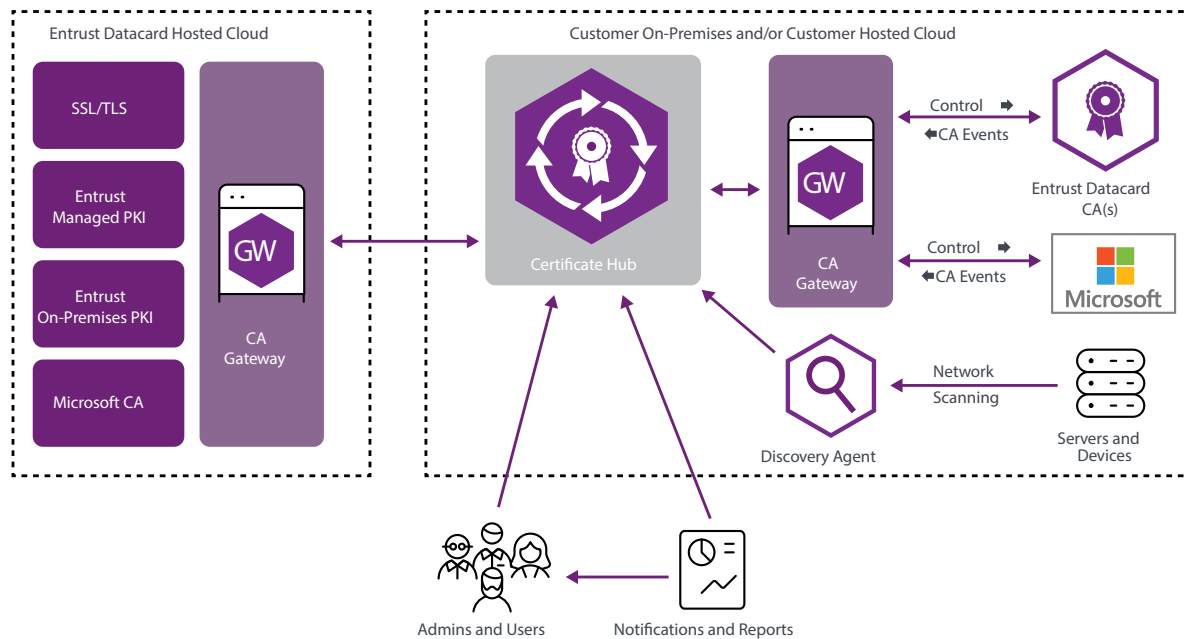
Certificate Hub helps you hold your organization and employees accountable by tracking certificates to owners. You can define your own set of metadata then tag certificates with details, such as owner, organization, or cost center. You can also notify owners of upcoming actions they need to take, monitor activity, and set up automated generation and distribution of reports to provide management visibility.

Certificate Hub Discovery finds deployed certificates and ties them to an issuer so you can spot policy violations, identify rogue certificates, and verify deployment of managed certificates. You can also add notifications and alerts to certificates from external issuers.

Certificate Hub can control all your Entrust and Microsoft CAs. Working in conjunction with Discovery, all issued certificates are catalogued and tied to the known destinations where they are deployed in order to spot unused and orphaned certificates.

Certificate Hub provides you with the rapid-response reporting and management tools needed to spot issues and take timely actions — without the need to impact existing user workflows.

Entrust Datacard Certificate Hub:



Certificate Hub:

- Is a container-based set of services that is amenable for on-premises or commercial cloud hosting. Deployment and version upgrade is through off-the-shelf tools and automation. It provides a browser-based user interface for administrators and end-certificate owners.
- Scans your enterprise’s networks or portions of networks for the most recent information about deployed certificates, then records the location, type, algorithms, and expiry of each certificate. Administrators can configure Discovery to automatically associate custom metadata to augment certificate management. Agent setup and management is simple with the central Certificate Hub interface and headless agent design.
- Ties certificates back to known issuers and, through Entrust Datacard CA Gateway, obtains a direct feed of issued certificates from supported CAs. It correlates issuance with discovery, providing end-to-end verification of which certificates have actually been deployed.
- Supports Entrust Authority Security Manager (on-premises and Entrust-managed), Entrust Public Certificate Services, and Microsoft CAs, providing active management through a single-pane-of-glass interface.
- Provides an end-certificate owner self-service interface for certificate issuance, renewal, and revocation. Certificate owners receive automatic notifications when they need to take action and can create reports summarizing activity.
- Allows administrators to customize settings such as access permissions, system metadata, notifications, and report branding.

Certificate Hub Versions

Certificate Hub is available in three tiers:

Find

- Inventory certificates across your organization through network discovery and automated certificate import.
- Provide organizational visibility with an easy-to-use report designer and scheduler.
- Issue notifications and reports via email to remind certificate owners of actions they need to take.

Control

- Centrally manage certificate policy, issuance, and access to public and private certificate authorities regardless of vendor.
- Monitor CA activity through automated certificate import from CA databases and cloud services.
- Perform operations to issue, renew, and revoke certificates from all connected CAs.

Automate

- Use API, SSH, and cloud keystore publishing to push keys and certificates directly to endpoints with fully managed rotation and certificate profile management.
- Leverage pluggable capabilities to allow custom automation.



About Entrust Datacard Corporation

Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide.

Corporate Headquarters

U.S. Toll-Free Phone: 888-690-2424
International Phone: +1-952-933-1223
info@entrustdatacard.com
entrustdatacard.com