



ENTRUST



Entrust Certificate Hub

Find, control, and automate the management of machine identities.

BUSINESS CHALLENGE

Keeping up with the rapid rise of machine identities

The number of certificates that organizations are issuing and managing continues to grow at a rapid rate. Some of this can be accredited to the continued growth of traditional use cases and the need to secure remote and distributed workforces. But much of it has to do with the continuing rise in machine identities.

From mobile and IoT devices to applications and containers, machine identities now outnumber human identities. Machines are also diversifying in nature, too:

- The Internet of Things introduced new physical devices like sensors that transmit data
- The cloud has given rise to “virtual” machines or software that emulate more traditional physical machines such as desktops and servers
- DevOps has accelerated the cloud with self-contained runtime environments known as containers that consist of individual modules called microservices

While the explosion in the number of machines creates exciting opportunities for organizations, it also introduces risks associated with unmanaged certificates or “rogue” CAs – not to mention the complexities of dealing with issues such as massive-scale, distributed infrastructures and short-life certificates.

Organizations must be able to identify, authenticate, and secure all the machines – as well as their communication with other machines – across the IT environment.

SOLUTION

Centralized machine identity lifecycle management

Entrust Certificate Hub brings together all the machine identities across your organization and provides a simple and intuitive “single pane of glass” view.

Available on-premises or managed, Certificate Hub helps resolve some complexities that can come with machine identities by providing one of the most critical components of machine identity management: automation.

Learn more about Certificate Hub at [entrust.com](https://www.entrust.com)



Entrust Certificate Hub

KEY FEATURES & BENEFITS

Centralized visibility and management through an intuitive interface

- Provides a single enforcement point for centralized policy configuration and certificate lifecycle management
- Simple, intuitive portal lets you view and manage certificates across your entire organization, irrespective of source
- Advanced reporting helps you discover the machine identities deployed across your organization, from multiple CAs, giving you centralized visibility with a single-pane-of-glass view
- Allows you to import all your Entrust managed certificates using the Certificate Hub source connection; certificate import methods include:
 - Discovery Scanner
 - Bulk import through import API
 - Manual upload through UI
 - Source sync with CA database
- Convenient browser-based user interface for both administrators and end-certificate owners

Convenient admin controls, reporting, and notifications

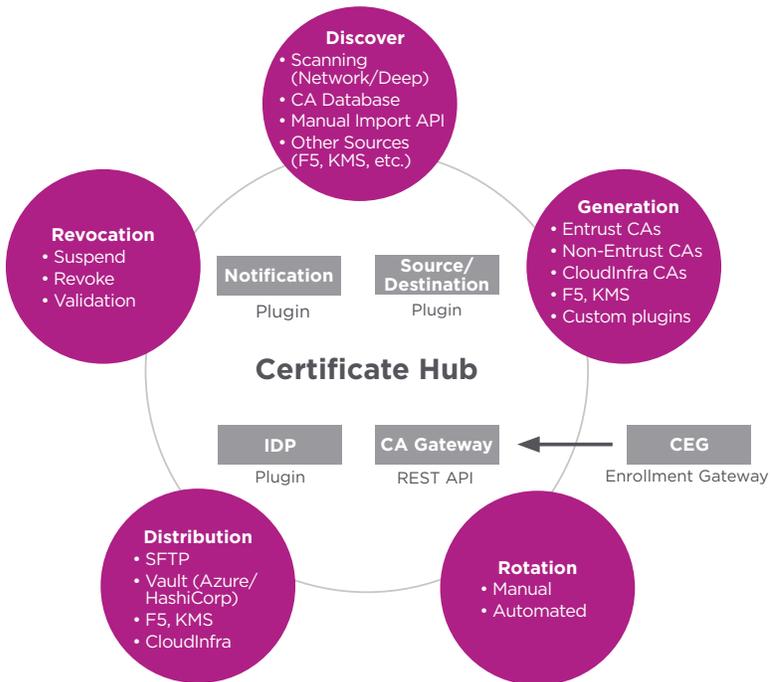
- Administrators can customize settings such as access permissions, system metadata, notifications, and report branding
- Role-based access control with customizable roles helps you with regulatory compliance, separation of duties, and delegation of responsibilities; authorization tags provide even more granular access
- Automated expiry notifications for managed and monitored certificates
- Connects to cloud KMS services and CAs to allow notification and orchestration
- Administrators can configure Discovery to automatically associate custom metadata to augment certificate
- Report Designer allows you to create and schedule user-defined reports
 - Rules and actions supporting notifications (email, SMS, etc.) for certificate and administrative events
 - Certificate archival allows for clean reporting, notifications, and certificate management views
 - Ability to perform bulk operations for easy certificate notification management
- Advanced reporting provides alerts and notifications of any upcoming certificate events or action that needs to take place
- Deep scanning support – beyond network scanning and discovery – is available for finding and auditing digital certificates stored in Java key stores, binary files, compressed files, etc.



Entrust Certificate Hub

Flexible integration and scalability

- Manages machine identities for both greenfield and brownfield deployments
- Operates through a Kubernetes cluster or Entrust’s software appliance
- Agent or agentless certificate deployment and management
- Integrates with deep scanning tools through external APIs to locate and inventory all forms of digital certificates (PEM, DER, P12, etc.)
- On-premises deployment optimized for enterprise private or public cloud hosting in either AWS or Azure
- Enterprise IDPs/Active Directory integration used for role-based access controls for performing key operations
- Deployment and version upgrade is through off-the-shelf tools and automation
- Pluggable architecture for expansion



SUPPORTED INTEGRATIONS

Entrust Certificate Hub provides certificate issuance, renewal, and revocation through a single-pane-of-glass interface to support a wide range of applications.

CAs	<ul style="list-style-type: none"> • ECA (Entrust CA) • ECS CA (Entrust Certificate Solutions CA) • DigiCert CA • Microsoft CA • Standalone Microsoft CA • PrimeKey EJBCA
Cloud and DevOps	<ul style="list-style-type: none"> • Ansible • AWS • AZURE • Kubernetes • OpenShift • Rancher
KMS and Vaults	<ul style="list-style-type: none"> • Entrust Vault (Key Control) • Azure Key Vault • HashiCorp Vault
Incident and Workflow	<ul style="list-style-type: none"> • ServiceNow
HSM	<ul style="list-style-type: none"> • Entrust nShield (previously nCipher) • Thales
Enrollment Standards	<ul style="list-style-type: none"> • ACME • EST • INTUNE • MDMWS • SCEP • WSTEP
Abstraction Layer/Extensibility	<ul style="list-style-type: none"> • CA/Enrollment Gateway • IoT Agent • IT Agent (Windows/Mac) • REST API
Servers/Load Balancers, etc.	<ul style="list-style-type: none"> • Apache • F5 • Java • NGINX



Entrust Certificate Hub

HOW IT WORKS

Centralize visibility, oversight, and reporting

Certificate Hub helps you hold your organization and employees accountable by tracking certificates to owners. You can define your own set of custom metadata fields, 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:

- Finds deployed certificates and records the location, type, algorithms, and expiry of each certificate and ties them to an issuer so you can spot policy violations. You can also add notifications and alerts to certificates from external issuers.
- 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.
- 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.
- Ties certificates back to known issuers and, through Entrust 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 been deployed.

- 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.

VERSIONS

Available in two tiers

Whether deployed on-premises or as a service, Certificate Hub is available in two 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 and Automate

- Centrally manage certificate policy, issuance, and access to public and private certificate authorities regardless of vendor
- Monitor CA activity through automated certificate imports from CA databases and cloud services
- Perform operations to issue, renew, and revoke certificates from all connected CAs
- Use API, SSH, and cloud keystore publishing to push keys and certificates directly to endpoints with fully managed rotation and certificate profile management
- Support source plugins for destinations such as AWS ACM CA, Azure Key Vault, and F5 networks



Entrust Certificate Hub

- Manage keys that are generated/stored at a KMIP supported by a key management server and not at a CA
- Leverage SDK to create custom plugins for:
 - Any external **source** automation, which enables the automated import of certificates from the external source points
 - Any external **destination** automation, which enables the manual and automated certificate issuance to these custom destination points



Learn more at
[entrust.com](https://www.entrust.com)



Entrust and the hexagon logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Entrust Corporation reserves the right to change specifications without prior notice. Entrust is an equal opportunity employer. ©2022 Entrust Corporation. All rights reserved. PK23Q1-certificate-hub-sb



ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com [entrust.com/contact](https://www.entrust.com/contact)