Entrust Certificate Services Discovery⁺

Centralize certificate management to one dashboard regardless of issuing CA

Market Challenge

As various types of digital certificates are introduced to an organization, it becomes more difficult to track and manage certificates – particularly if they're issued from different certification authorities (CAs).

Solution

Entrust Certificate Services (ECS) now consolidates all Entrust and non-Entrust certificates into a single, centralized dashboard, making it easier to find, inventory, audit, and manage all of your digital certificates across variant systems regardless of issuing CA. Centralized management helps to prevent outages, data breaches, and non-compliance.

BENEFITS

- One dashboard to locate, track, audit, and manage all digital certificates

- Locate and automatically import TLS/SSL certificates from any source, mitigating vulnerabilities

- Scan for certificates within Microsoft's Cryptographic APIs (CAPI)

- Ensure certificates adhere to corporate compliance policy

- Identify unknown certificates

- Save money and resources with automatic certificate cataloging

- Scale to meet your needs

- Flexible subscription options

Entrust Certificate Services Discovery⁺

Discovery+ at a glance

Experience the power our suite of tools provide! Find, import, and audit all digital certificates regardless of issuing CA, with the option to consolidate management of foreign certificates to our centralized dashboard.

Discovery Agent – scans your network across disparate systems enterprise-wide to locate all digital certificates

CT Log Import – query and import certificates from the CT Logs for certificates issued to your configured list of domains. This method helps you to find certificates you may not be aware of, which may or may not be installed in your known environments

Manual – known, accessible certificates that cannot be scanned and have not been added to the CT logs can be imported for centralized management

CAPI Scanner – Windows network users can continually run our script to find certificates in Microsoft's Windows Crypto certificate stores and automatically import them to ECS for centralized management

Features

Customized notifications and alerts. Stay updated on expiring certificates to avoid unexpected outages. Centralizing visibility of all certificates into your ECS certificate inventory helps you to avoid costly system outages due to non-compliant certificates.
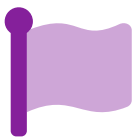
Expiry notifications for Entrust and non-Entrust certificates. Alert certificate owners of expiring certificates and installation location with automated emails and escalations to avoid unexpected security gaps.

Visibility into your certificate inventory. Gain clear insight into your organization's publicly trusted certificates to mitigate risk and maintain uptime. Avoid costly losses due to security gaps, system downtime and even brand erosion.

Entrust Certificate Services Discovery⁺

Simple certificate inventory

Efficient Inventory

By simplifying the certificate discovery and inventory process, you save the management effort of manually inventorying machines and tracking certificate expiries in confusing spreadsheets or across various platforms.

Avoid unexpected outages

From a missed email notification to a previously undiscovered certificate, it's not difficult to lose track of certificate expiry dates. And it's even more challenging to track the use of unknown certificates. ECS identifies these risks and makes it easy to rectify any issues – all from within a single easy-to-use interface.

Identify & replace

Identify and replace vulnerable certificates to ensure you are properly protected from malicious attacks. And by inventorying your encryption assets, you can avoid security gaps.

ECS offers seamless integration for inventorying, managing, and purchasing TLS/SSL and specialty certificates, alongside your discovered certificates – all from the same interface.

Entrust Certificate Services Discovery[+]

Flexible certificate discovery

Discover risks caused by rogue or expiring certificates, and the tools to resolve them. Organizations are able to view detailed data to manage certificates.

Enterprise-ready

ECS Discovery[+] is easily scalable to meet the needs of large enterprises, and even supports enterprise-level operating systems (e.g., Linux, Microsoft, Windows).

Immediate protection

The ECS Discovery Agent may be deployed immediately in a secure environment without any additional project resources or hardware purchases.

Make the discovery

Quickly find and inventory certificates within your environment that are exposed to a network service – even those residing within Microsoft's Cryptographic API store (CAPI).

Management licensing fees

ECS supports discovery and manual certificate importing, and includes up to 100 management licenses (depending on annual Platinum support). A management license is required to manage foreign (non-Entrust) certificates in ECS.

Use management licenses to consolidate data from multiple sources and put them under centralized management. This provides access to certificate details, inventory functions, email notifications and reporting. Users get a comprehensive view of the certificate environment, including pending expirations, copies, and compliance risks.

Start centralizing certificate management to one dashboard with Discovery+. Contact us today at info@entrust.com.

Learn more at
entrust.com

ENTRUST

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