

Entrust Discovery

Certificate Discovery & Management Solution

Organizations are adding more types of digital certificates — for communication, Web security, hardware authentication and more — to properly secure and protect enterprise environments.

But 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.

Entrust Discovery streamlines this process with a solution that finds, inventories and manages digital certificates across diverse systems to prevent outages, data breach and non-compliance.

Avoid Costly Application Outages

Expiring certificates can be expensive. Entrust Discovery helps organizations avoid costly application outages by inventorying your digital certificates, and providing a redundant system of email notifications to responsible parties.

Notifications made easy. Entrust Discovery provides expiry notification emails to certificate owners to ensure they are aware of expiring certificates and where they are installed. And with built-in backup emails to owners, as well as system administrators as you get closer to expiry, you can ensure certificates are not expiring unexpectedly.

Protecting Your Organization

Even if you're an expert at compliance requirements and industry regulations, you may not have the tools or information to ensure your organization is complying properly.

Proving compliance. Your organization most likely has stringent security policies that adhere to internal, industry or federal regulation. But if an organization doesn't have the tools or information to prove policy is being followed, non-compliance risks will arise.

Entrust Discovery provides an inventory of encryption assets, and a policy engine with alerts, to help ensure your organization is following a given policy.

Data breach defense. Is your organization confident that communication channels are secure? What if your security policy requires a change to increase security (e.g., ensuring all 1024-bit rooted keys are properly upgraded to 2048-bit rooted keys)? Entrust Discovery quickly identifies potential problems and helps the user easily correct any issues.

The solution helps identify and replace those vulnerable certificates, ensuring you are being properly defended from malicious attacks. And by inventorying your encryption assets, you can ensure that transmission data is not left unencrypted. This helps prevent the exchange of information from being illegally intercepted without your knowledge.

Discovery Benefits

- Find, inventory and manage digital certificates across your organization
- Perform scans for certificates residing within Microsoft's Cryptographic APIs (CAPI)
- Ensure certificates adhere to corporate compliance policy
- Identify unknown certificates for replacement purposes
- Locate certificates that may allow vulnerabilities to data breach
- Save money and resources with automatic certificate cataloging
- Scales to meet the needs of large organizations and enterprises
- Benefit from flexible subscription options designed for use in any organization
- Partner with the No. 2 provider of SSL digital certificates and services based on Frost & Sullivan evaluation

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 complex spreadsheets or tables.

Avoid unexpected outages. No matter their type or origin, digital certificates expire. 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 certificate copies. Entrust Discovery identifies these risks and makes it easy to rectify any issues — all from within an easy-to-use interface.

Making the Discovery

Entrust Discovery quickly finds and inventories certificates that are exposed to a network service — even those residing within Microsoft's Cryptographic APIs (CAPI).

Entrust Discovery Agent and Entrust Discovery Manager collaborate to help organizations discover any risks caused by rogue or expiring certificates, and then subsequently provide the resolutions to fix any issues. Organizations are able to view detailed data to manage certificates, and the solution includes more than 25 basic or custom policy alert fields.

About Entrust Discovery

Flexible Options. Choose to deploy Entrust Discovery within your own environment (premises model) or take advantage of our Software-as-a-Service (SaaS) option (cloud model). Entrust's subscription models provide the flexibility and security that's right for any organization.

Enterprise-Ready. Entrust 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. When powered by our cloud model, Entrust Discovery can be deployed immediately in a secure environment without having to secure project resources, purchase hardware or perform installations.

Single Sign On with CMS. Entrust Discovery's cloud model is designed for single sign on (SSO) with the Entrust Certificate Management Service (CMS), eliminating the inefficiencies of adding another user management process.

More Information

For more information about Entrust Discovery, contact the Entrust Certificate Services representative in your area at **888-690-2424** or visit **entrust.net/discovery**.

Discovery Agent — Customer-premises software that schedules customized network scans in search of certificates on both internal and external hosts. The Discovery Agent reports summary-level findings, exposing potential problems on your network. The Discovery Agent also allows you to find certificates in Microsoft Windows CAPI certificate stores. This detailed data can then be exported — either manually or automatically — to Discovery Manager for the decision process.

Discovery Manager — Purchase Discovery Manager to consolidate data from multiple Discovery Agents and place certificates under management. This provides access to certificate details, inventory functions, email notifications and reporting. Discovery Manager presents a comprehensive view of the certificate environment, including pending expirations, copies and compliance risks.

About Entrust

A trusted provider of identity-based security solutions, Entrust empowers enterprises, governments, financial institutions, citizens and websites in more than 4,000 organizations spanning 60 countries. Entrust's customer-centric focus is the foundation of delivering organizations an unmatched level of security, trust and value. For strong authentication, credentialing, physical and logical access, mobile security, digital certificates, SSL and PKI, call 888-690-2424, email entrust@entrust.com or visit www.entrust.com. Let's talk.

Entrust[®] Securing Digital Identities & Information