ESTABLISH YOUR BLUEPRINT FOR CENTRALIZED CERTIFICATE LIFECYCLE MANAGEMENT

Consolidate processes and SSL providers without interruption using Entrust SSL management and monitoring services

Table of contents

1 **Address business & security challenges**
Page 3

2 **Should I switch or consolidate vendors?**
Page 4

3 **Create a certificate inventory**
Page 5

4 **Perform assessment**
Page 7

5 **Develop a renewal plan**
Page 9

6 **Consolidate using Entrust SSL services**
Page 10

7 **Conclusion**
Page 13

8 **Migration checklist**
Page 14

Address business & security challenges

Whether due to security events, industry changes, compliance requirements, the necessity to improve business processes and reduce costs, the need to identify and manage SSL certificates is critical to goals of your organization.

Managing the purchase, deployment, renewal and expiry of digital certificates for multiple Web servers, purposes and users — sometimes in many different locations — can be time-consuming and costly.

Certificate management is often a dynamic, complicated undertaking. Tracking expiry, vendor compliance and key sizes can be difficult, even for organizations with a small number of certificates in use. But this task is magnified in large organizations with hundreds of certificates deployed across different networks, systems and applications.

Leverage Web-based, self-service certificate management and discovery solutions — core components of Entrust Cloud — to streamline certificate lifecycle management and provide dramatic improvements in efficiency and cost control.

Consolidating all your SSL certificates into a single lifecycle management platform is not a simple process. Nevertheless, it's a process that can be managed, without disruption, via a systematic transition plan. It's critical to prepare for change.

This whitepaper provides a blueprint for migrating to Entrust SSL certificates and related services. It's based on experiences that help many customers, in a wide variety of environments, bring their SSL certificate management under the centralized administration.

Consolidation Scenarios

- CIO-driven management initiatives to eliminate IT operational cost and complexity
- Pro-active or reactive compliance and security improvement initiatives
- Mergers or acquisitions requiring the integration of multiple network systems
- Departmental reorganizations and business process redesign projects: requiring local control with centralized oversight
- Merging data centers, public/private cloud expansion, requiring deployment and/or movement of certificates from one physical or virtual location to another

Should I switch or consolidate vendors?

The general perception is that switching or consolidating vendors can be a poor use of resources and not worth the costs. While the management of SSL certificates can be a costly and time-consuming activity for organizations, this is largely the result of working with multiple vendors, tracking systems, manual processes, and a lack of procedures and centralized oversight.

Eliminating the aforementioned complexity, fragmentation and redundancy through proper consolidation will decrease operational costs significantly. At the same time, by consolidating purchase to a single vendor you'll gain the ability take advantage of greater volume discounts due to an increased quantity of purchased certificates.

Some (self-serving) SSL vendors have helped to promote the notion that it can difficult to change providers for technical reasons. The reasons given? Installing new roots is difficult, time-intensive and prone to error. They also make the same argument as it relates to certificate validation procedures (e.g., CRL and OCSP paths needing to be manually replaced).

Both arguments are easily dismissed since SSL certificates are standards-based and the installation procedures are the same across vendors. This standardization helps to avoid any unforeseen complications and can be taken into account during a planned transition.

So while there may be concern over perceived "vendor lock-in," the reality is that a well-planned migration and consolidation will result in both cost- and time-savings. The following outlines a four-step process for moving to Entrust Certificate Services for platform.

Step 1: Create a certificate inventory

The essential first step to routine and confident certificate management for your organization is to obtain a complete and up-to-the-minute view of all certificates deployed in your environment. Once certificates have been located, their properties can be examined, evaluated against applicable policy and reported to responsible authorities.

Consider all sources

It's likely that there isn't one authoritative source for this information, so it's best to use as many sources as possible to gain a complete picture of certificate use.

Your organization's inventory should aim to take into account a variety of factors that you can view in aggregate, which will inform your assessment and go forward plan

This should include:

- How many certification authorities (CA) you are using to issue certificates across both internal PKIs and external vendors
- How many certificates are in use, as well as the number of servers and applications using SSL certificates
- What is the expiration timeline horizon for these certificates?
- How many administrators are involved in SSL management?

Consider the following methods and sources for developing a comprehensive catalog of certificates and managers

Import from certification authorities

Gather what you already know about the certificates from existing CAs. Keep in mind that you shouldn't assume that an import from your known CAs will provide an accurate inventory of all certificates; it's only one source and a starting point that must be augmented by certificate discovery.

Import reports from administrators

Network and system-based discoveries can take time and it may not be possible to perform them in all corporate locations. So it's important to educate and involve all your administrators and make sure they are regularly reporting any certificates they are aware of and adding them to the inventory.

Perform network discovery

Perform a network discovery to find certificates that are present on a listening port such as HTTPS. Start by gathering your network address ranges and then collect a list of ports to check. You can initially check on port 443, but there are many ports on which certificates are commonly present.

Perform system level discovery

Many certificates are not discoverable via network ports, such as client-side certificates used for mutual authentication on SSL. Finding these certificates typically involves performing file system scans on servers and client systems with a locally installed scanner.

Key attributes to capture and identify

In addition to capturing the volume of certificates in use, you will also want to capture other information that will guide your assessment and migration strategy as follows:

- **Certificate properties**
  Significant certificate properties include: the subject domain name or address; the domain to which they are attached; cryptographic key properties (including algorithm, size and strength); issuing authority; certificate quality; revocation status; list of subject alt names (SAN); and expiry date.
- **Applications and servers**
  Locate and identify the types of servers and applications with installed certificates. You will need this information to determine the necessary steps for root replacement and local management responsibilities.
- **Current managers and chain of command**
  Does every certificate have someone responsible for its management? Is that person still with the organization? As you're developing your inventory, establish a correlation of who the contacts and owners are for certificates. Wherever possible, assign groups as the contacts, instead of individuals, to avoid a single point of failure. Some helpful sources include CAs, tracking spreadsheets and even a configuration management database (CMDB).
- **Non-compliant certificates**
  Depending on your organization's policies, certificates may be non-complaint for a variety of reasons, such as: key strength (e.g., 1028-bit), hashing algorithm (e.g., SHA-1), verification type (e.g., OV or DV) or other reasons. If you can catalog and flag non-conformant certificates during the inventory process, it will make your assessment and migration plan faster.

Step 2: Perform assessment

Getting the big picture

Based on the information you've gathered during the inventory process, you will be able to determine the scope of the project. This information should take into account the number and timing of certificates to be replaced, the number of vendors you will be phasing out, and the key administrative contacts.

In addition to current inventory, take into account operations coming offline or online that will impact the certificate count and management plan.

Consolidation options

Once you see the "big picture," choose to either replace all your certificates at once or take a phased approach; the two main considerations are financial and operational.

Financial considerations are based on how you budget for the cost of certificates and the extent of your "sunk costs" in existing certificates. Your operational consideration should take into account the level of effort required for a one-time effort, monitoring old certificates throughout the rest of their lifecycle and the chance that employees will deploy rouge certificates.

One-time find and replace

A one-time effort will eliminate the use on non-Entrust certificates within a short time frame or designated cutover date. This approach maximizes volume discounts and gets all administration into a central view in the quickest manner.

Using this approach, you may choose to migrate all your certificates to Entrust if you want to align certificate purchases with a specific budget cycle, project or departmental charge-back. You may also want to align the expiration dates of your certificates to coincide with maintenance schedules.

In the event you need to revoke a certificate for any reason, you will need to do so via the issuing CA, as no vendor or system has the authority to revoke a certificate purchased from another CA.

Even if you have remaining time on some of your certificates, the amount you can save due to volume discounts may be large enough to merit the purchase all at once.

Should you Ditch the Final Months of your Certificates?

Even if you have remaining time on some of your certificates, the amount you can save due to volume discounts may be large enough to merit the purchase all at once.

Phased transition

Alternately, you may choose to replace certificates on a case-by-case basis, replacing each certificate as it expires. Using this approach, you will spend less time up-front performing replacements, but will still have services running concurrently, which could potentially result in renewals taking place with the CA you are phasing out.

This approach may be more palatable in organizations with many network segments or organizational units operating on different schedules and/or resource or budgetary constraints. Volume-based discounts still apply in this scenario. Entrust can accommodate either method of transition.

Technical details to consider

There are two major technical details to take into account during transition that will ensure the proper installation and performance of certificates.

One aspect of installation is related to the type and number of root CA and intermediate root chains you will need to update.

The other is related to the function of verifying that certificate validity is performed by the browser or application, which relies on the maintenance of either certificate revocation lists (CRL) or Online Certificate Status Protocols (OCSP) servers.

Some vendors may try to make this part of the process sound difficult or onerous, however, because SSL/TLS certificates are based on a common standard (x.509), the process for requesting and installing certificate chain components, and establishing certificate validation, is exactly the same for each vendor's certificates.

Moreover, it can be managed with minimal effort using standard tools in the Entrust cloud platform. Consequently, neither of these factors should be a deterrent to changing vendors as long as you verify that new certificates are installed properly.

Since these changes impact your IT infrastructure — and some organizations have change management policies that affect the ability or timing of the installation of new root CAs and ICAs — it's important that you coordinate with CMDB operations, as necessary

Workflows and integrations to consider

Some companies have developed their own request processes, access controls or billing processes that make use of APIs and integrations with existing systems. These should be identified as points where updates may be required, but are generally not impediments since Entrust SSL services support the use of standards-based integrations (e.g., HTTPS Post), as well APIs for most common ERP and CMBD systems.

Step 3: Develop a renewal plan

Assign owners and roles

Once you've determined your migration approach, assign ownership and communicate procedures and responsibilities. Define clear responsibilities for maintenance of certificate contact information.

In addition to policy oversight (which individuals are authorized to manage certificates for the organization), there should be enterprise-wide policy covering all certificate properties. Define super-administrators, administrator requestors, approvers and any other roles required in your organization.

This will make it easy to put in place a management process that operates with checks and balances, and delegates system access according to the required level of control and responsibility.

Once reliable reports can be compiled and distributed, it is a simple matter to identify and resolve policy violations. Alerts of imminent outage can be sent for resolution to those responsible for maintaining system availability.

Map existing certificates to renewals

Map your certificate replacement path. Do you replace with equivalent certificate (e.g., validity period, encryption level, validation type, etc.) or change the certificate type upon upgrade?

Address non-complaint certificates

For non-compliant certificates, the private key can be deleted and the issuing authority asked to revoke them. If certificates are discovered that have been issued by an unapproved authority, then timely corrective action can be taken.

Similarly, if weak keys are discovered, keys of acceptable strength can be rapidly issued to replace these.

Document and communicate consolidation plan

The No. 1 priority is to clearly identify who is responsible, accountable and authorized to act regarding certificate management. With a primary managed account in place, you'll need to establish who can act as authorized administrators to oversee the lifecycle process — from issuance to retirement — and implement those controls within the management system.

Documentation of a defined organization-wide administrative process for oversight and control policies should be developed and maintained in a repository available to everyone who requires access. Also include a mechanism to notify, as necessary, when changes are made.

Establish standard practices for enrollment and provisioning that: maximize reliability and repeatability; ensure security and compliance to policy; and minimize load on your administrators. There are typically 20 or more steps involved in issuing or renewing a certificate. These steps must be standardized and implemented in compliance with policy — every time.

20 Steps?

There are typically 20 or more steps involved in issuing or renewing a certificate. These steps must be standardized and implemented in compliance with policy — every time.

Step 4: Consolidate using Entrust SSL services

Using proven Entrust SSL services, you will be able to perform all the key functions necessary to consolidate your certificate operations, including:

- Seamless integration from current certificate vendor to Entrust
- Import all non-Entrust certificate information into management portal and flag for alerts
- Assign expiration routing with an escalation path that ensures action is taken
- Assign to management groups and/or locations
- Establish the desired workflow for certificate management and monitoring

Create inventory using discovery services

Entrust Cloud Discovery may be deployed immediately in a secure environment without having to secure project resources, purchase hardware or perform installations.

Entrust's Discovery scanner can be installed on any Microsoft® Windows® or Linux-based machine and will be able to find any certificates, regardless of issuer (e.g., commercial CA or internal PKI) on the identified range of IP addresses on the defined network segment.

Using Entrust Discovery, tag non-Entrust certificates that you want to bring under management and renew as Entrust certificates. You may choose not to bring certificates under management if they will not be replaced using an Entrust-issued certificate or may choose to bring them under management to maintain a centralized view of all your certificates.

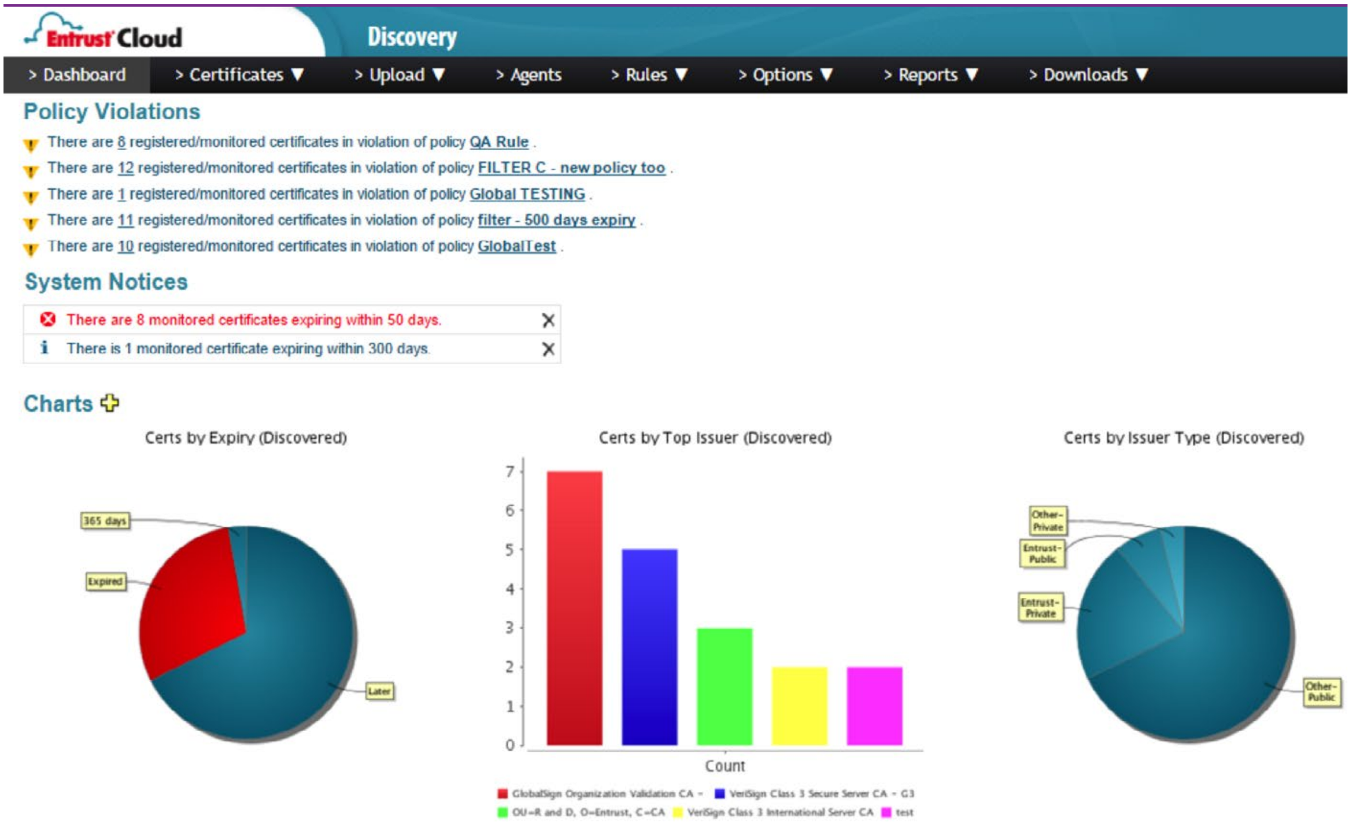
All certificates you assign to be managed will be put into a workflow and assigned owners inline with established policies.

The Cloud Simplifies Certificate Management

Secure cloud tools help reduce costs and simplify management. Explore the many components of cloud-based certificate management solutions — all part of Entrust IdentityGuard Cloud Services.

Explore Cloud Certificate Management ⊕

Figure 1: Entrust Cloud Discovery Report



Policy Violations

- There are 8 registered/monitored certificates in violation of policy QA Rule .
- There are 12 registered/monitored certificates in violation of policy FILTER C - new policy too .
- There are 1 registered/monitored certificates in violation of policy Global TESTING .
- There are 11 registered/monitored certificates in violation of policy filter - 500 days expiry .
- There are 10 registered/monitored certificates in violation of policy GlobalTest .

System Notices

- ☒ There are 8 monitored certificates expiring within 50 days. X
- i There is 1 monitored certificate expiring within 300 days. X

Charts ⊕

Certs by Expiry (Discovered)
365 days
Expired
Later
Certs by Top Issuer (Discovered)
7
6
5
4
3
2
1
0
Count
🟥 GlobalSign Organization Validation CA -
🟦 VeriSign Class 3 Secure Server CA - G3
🟩 OU=R and D, O=Entrust, C=CA
🟨 VeriSign Class 3 International Server CA
🟪 test
Certs by Issuer Type (Discovered)
Other-Private
Entrust-Public
Entrust-Private
Other-Public

Perform validation of domains and company names

In order to provide the ability for on-demand availability and issuance, Entrust will validate all organization company names and subsidiaries.

Based on inventory and future needs, you will provide Entrust a listing of domains, along with company names and subsidiaries, to be pre-verified. Entrust will validate the domains and company names to allow for instant certificate creation.

Administrator setup and delegation

Your organization will provide Entrust with a list of users and their roles. Your company's account administrators must be approved by the designated company authorization contact. Companies may choose to assign any of the three different user roles (see figure 2) :

- Super Administrator
- Sub Administrator
- Requestor
- Read-Only

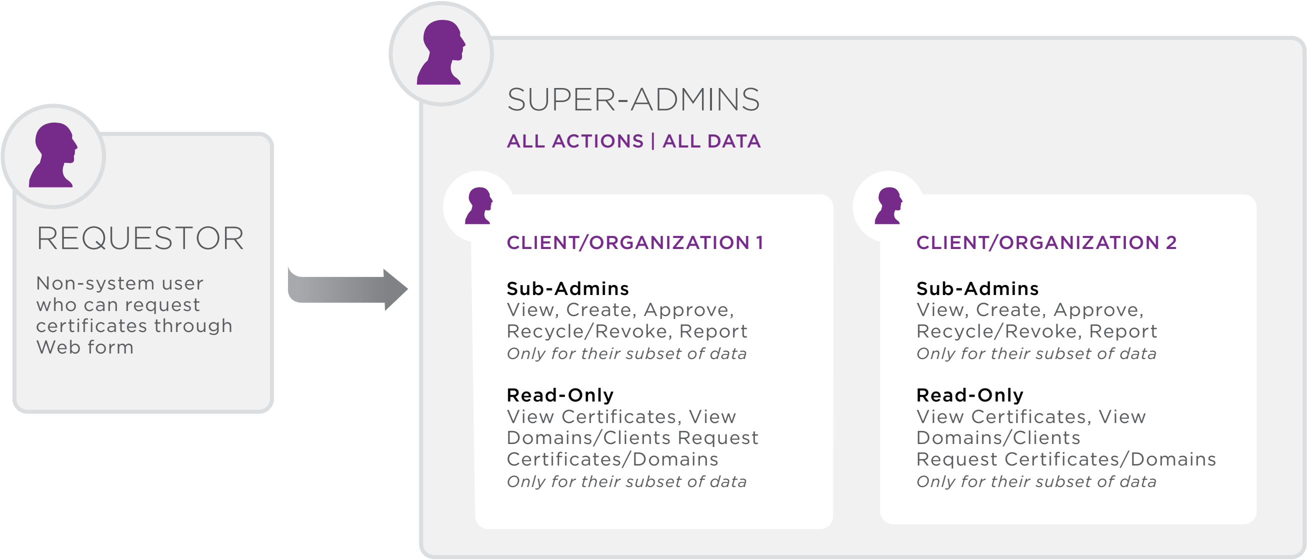

REQUESTOR
Non-system user who can request certificates through Web form
SUPER-ADMINS
ALL ACTIONS | ALL DATA
CLIENT/ORGANIZATION 1
Sub-Admins
View, Create, Approve, Recycle/Revoke, Report
Only for their subset of data
Read-Only
View Certificates, View Domains/Clients Request Certificates/Domains
Only for their subset of data
CLIENT/ORGANIZATION 2
Sub-Admins
View, Create, Approve, Recycle/Revoke, Report
Only for their subset of data
Read-Only
View Certificates, View Domains/Clients Request Certificates/Domains
Only for their subset of data

Figure 2: Sample Configuration

Define certificate management workflow

Depending on what, if any, procedures you have in place, define a workflow for certificate lifecycle management that defines certificate request/approval, as well as revoke/approval processes.

If you have a workflow already in place, mimic the current workflow or add more granularity and flexibility as needed. Conversely, you can build this from the ground up.

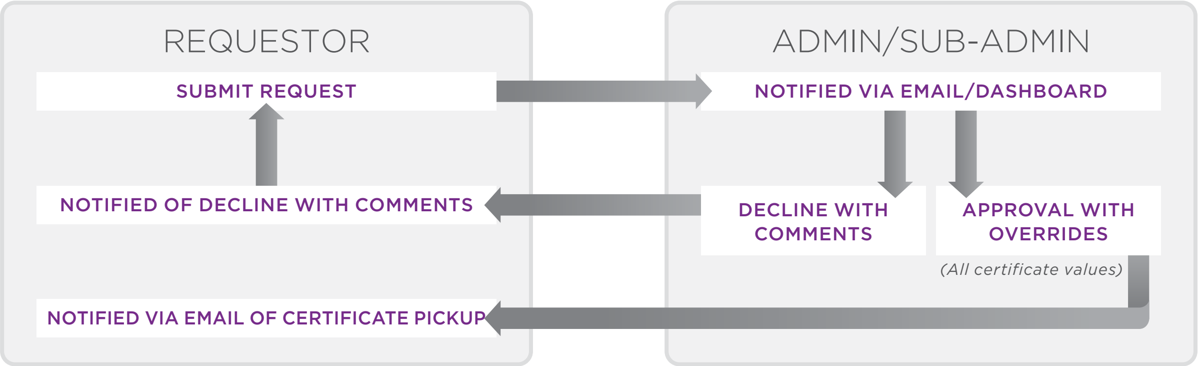


Figure 3: Sample Certificate Management Workflow

Renew certificates with Entrust as they expire

Whether you're performing a one-time update or phased approach, you'll use the centralized portal to manage the renewal of expiring certificates from other vendors.

When using Entrust Cloud, you'll be notified when these certificates are about to expire. When expiry notification is received, renew that certificate with Entrust and retire the previous certificate in line with your policy.

As mentioned, because SSL/TLS certificates are based on a common standard (x. 509), the process of requesting and installing certificate chain components is exactly the same for each vendor's certificates.

The Entrust Cloud service provides installation-checking tools to ensure the proper configuration of certificates and ensures you go live without any complications.

Enable continuous discovery and monitoring

There is the continuous threat that rouge certificates will get deployed because someone legitimately procures a certificate in test or development environments on their own, an outside vendor deploys one, or a bad actor installs one for their benefit.

Continually monitor and scan the environment to ensure the integrity of the process and prevent against outages and security risks. Review current practices against regulatory and other policies.

Conclusion

Following the above recommendations and procedures has been shown to provide a seamless migration for many Entrust customers. This approach offers a dramatic reduction in the cost and complexity of managing SSL certificates.

In addition to the many tutorials and self-help modules included within the SSL services platform, Entrust world-class customer support is available to assist with your transition.

Contact Me ⊕

+1-866-267-9297 | entrust@entrust.com

Start Your Transition

Need help getting started? Contact an Entrust SSL certificate expert and we'll guide you through the entire process. Let's get started.

Migration checklist

Migration Checklist

Action	Complete?	Date	Entrust	Customer
Provide Domain List				✓
Provide Company Name List				✓
Validate Domains			✓	
Validate Company Names			✓	
Provide List of Admins & Roles				✓
Validate Admins			✓	
Deligation Setup			✓	✓
Establish Desired Workflow for Certificate Request & Approval			✓	✓

About Entrust Datacard

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.

For more information about Entrust products and services, call **888-690-2424**, email **entrust@entrust.com** or visit **www.entrust.com**.

Headquarters
Entrust Datacard
1187 Park Place
Shakopee, MN 55379
USA

Twitter Facebook Youtube LinkedIn Google+ RSS

Entrust Datacard™