

# Entrust Authority™ Security Manager Proxy



The Entrust Authority™ Security Manager Proxy is a new component of the Entrust Authority product portfolio.

Using standard Internet protocols, the Entrust Authority Security Manager Proxy allows customers to operate a Certification Authority (CA) over the Internet without making changes to existing firewall settings. This promotes greater flexibility, facilitates communication and reduces the impact on existing infrastructures.

The Entrust Authority Security Manager Proxy works with Entrust products allowing customers to deploy Entrust solutions from a central location without modifying existing security policies. The Security Manager Proxy uses standard Internet protocols to communicate with Entrust Authority products.

A CA is a trusted entity whose central responsibility is certifying the authenticity of users for a secure organization. As the holder of updated public-key information for an enterprise, software clients must have access to the CA-either inside a company's firewall, or over the Internet. The functionality of the Security Manager Proxy is very applicable to business-to-business applications, Trusted Service Providers and companies whose employees communicate with the CA, Directory and back-end servers via the Internet

## Features and Benefits

**Entrust Authority Security Manager Proxy** working with Entrust products, facilitates communication and deployment of a certification authority (CA). Specifically, the Security Manager Proxy makes it possible for all communication with the Entrust Authority products to be conducted over standard firewall friendly protocols, i.e. HTTP and TLS.

The product consists of a client-server architecture where requests to communicate to various back-end infrastructure servers are sent to the client component and wrapped in



HTTP and/or TLS and sent to the server component. The server component unwraps the requests and sends them to the specific back-end infrastructure server.

The Security Manager Proxy software:

- **Facilitates Communication with the CA** - The Security Manager Proxy facilitates the communication between the client and various back-end corporate infrastructure servers in standard Internet protocols. Many customers operate a Certificate Authority from a central location and have several applications communicating with that CA over the Internet. The Security Manager Proxy eliminates the need to open extra ports in a firewall by communicating with the Certificate Authority using standard Internet protocols.
- **Provides Support for Standard Internet Protocols (HTTP and TLS)** - The Security Manager Proxy provides a generic mechanism to allow Entrust products to travel over well-known and supported protocols (HTTP and TLS) on any port in order to pass through firewalls. This generic mechanism increases flexibility so that customers can use Entrust products without adding to existing firewall configuration concerns.

- **Enables Trusted Service Providers** - Trusted Service Providers can operate a Certificate Authority over the Internet with minimal changes to their firewall policies or that of their customers. This accelerates a Service Providers time to market with more services.
- **Enables Customers to Deploy** - Entrust from a central location without requiring that they circumvent their existing security policy including changes to firewall ports or authentication.
- **Provides Filtering** - The Security Manager Proxy software can be configured as a filter so that packets that are not recognized are blocked from gaining access to the CA.
- **Enables Secure LDAP communication** - Secure LDAP communications between Entrust products and LDAP Directories. Communications between the client side proxy and server side proxy can be protected with Transport Layer Security (TLS). This enables customers to locate Entrust Administrative clients remotely and have them communicate with back end servers via the Internet without sending username and password in the clear.
- **Provides Additional protection of the Certificate Authority** - By preventing Denial of Service and overload by controlling the number of concurrent sessions by validating packets before they are transmitted from the client side proxy and after they are received at the server side proxy. Both the original communication message and the message after transit through http firewalls and proxies are validated.

## Get Technical

Entrust Authority Security Manager Proxy software runs a service that allows clients to communicate with an Entrust Certification Authority (CA) and back-end servers over the Internet, without making major changes to existing firewall settings.

When using Entrust Authority™ Security Manager (formerly Entrust/PKI) within a company network, clients can communicate easily with the CA, without having to pass through any security measures such as a firewall. Software clients can communicate easily with the CA using one of seven acceptable protocols:

Protocol	Used by...
SEP	CA (For all Entrust Authority™ Security Manager formerly called Entrust/PKI versions up to 6.0)
PKIX-CMP	CA (For all Entrust Authority™ Security Manager formerly called Entrust/PKI versions)
ASH	CA
PROTO-PKIX	CA, Entrust Authority Enrollment Server, Entrust Authority Enrollment Server for Web, Entrust Authority Enrollment Server for VPN, and Entrust Authority Enrollment Server for Smart Cards
PROTO-PKIX	CA, Entrust Authority Enrollment Server, Entrust Authority Enrollment Server for Web, Entrust Authority Enrollment Server for VPN, and Entrust Authority Enrollment Server for Smart Cards
SPEKE	Entrust Authority Roaming Server
LDAP	The Directory
TIMESTAMP	Entrust Authority Timestamp Server

In contrast, data packets sent by clients over the Internet usually have to pass through one or more firewalls before they can be forwarded to the CA or other back-end servers (such as the Directory or the Entrust Authority™ Roaming Server). Firewalls typically restrict incoming traffic to HTTP or TLS packets on specific ports. As a result, data packets sent by regular Entrust Authority protocols cannot reach the CA.

## How the Entrust Authority Security Manager Proxy Works

1. Data packets sent from a client machine are encapsulated by the Client component of the Security Manager Proxy as HTTP or TLS so that they can tunnel through the firewall.
2. Once the packets are through the firewall, the Server component of the Security Manager Proxy receives and unwraps the packets, and forwards them to the CA.

3. The response information from the CA or other back-end servers is then re-wrapped by the Server component in HTTP or TLS so that it can proceed back through the firewall to the Internet.
4. The response information is received by the client machine and unwrapped by the Client component of the Security Manager Proxy so the client machine can understand the CA response.

## System Requirements

Entrust Authority™ Security Manager Proxy product consists of a client-server architecture.

### Client

The Microsoft® Windows® client machine that hosts the Security Manager Proxy must meet the following system requirements:

- Microsoft® Windows® 2000 Server (SP1, SP2, SRP1), Microsoft® Windows® 2000 Professional (SP2) or Microsoft® Windows® XP Professional operating system
- 256 Mbytes of RAM
- 128 Mbytes of swap space
- Pentium 300 MHz or better
- One 2X or faster CD-ROM drive
- TCP/IP protocol stack installed
- 50 Mbytes hard disk with a minimum of 1 Gbyte of free space (more if you are installing over a network)

### Server

The Microsoft® Windows® Server that hosts Security Manager Proxy must meet the following system requirements:

- Microsoft® Windows® 2000 Server operating system (SP1, SP2, SRP1)
- 256 Mbytes of RAM
- 128 Mbytes of swap space
- one 2X or faster CD-ROM drive
- TCP/IP protocol stack installed
- 50 Mbytes hard disk with a minimum of 1 Gbyte of free space (more if you are installing over a network)

The Microsoft® Windows® 2000 Server must be configured according to Microsoft's recommended minimum system requirements.

### About Entrust

Entrust, Inc. [Nasdaq: ENTU] is a world-leading provider of Identity and Access Management solutions. Entrust solutions for secure identity management, secure messaging and secure data enable enterprises and governments to extend their business reach to customers, partners and employees by transforming the way transactions are done online.

### For More Information

Please call us at 888-690-2424, or send an e-mail to: [entrust@entrust.com](mailto:entrust@entrust.com)  
Visit us on the Web at: [www.entrust.com](http://www.entrust.com)

