



Entrust Authority Enrollment Server for Web

Entrust Authority™ Enrollment Server for Web works with Entrust Authority™ Security Manager to issue digital certificates to any or all of the following applications and devices:

- Secure Web servers and browsers (SSL/TLS)
- Secure remote access (VPN/IPSec)
- Secure e-mail (S/MIME)
- Secure downloadable software (code/object signing)
- Secure wireless communication (WAP/WTLS)

These digital certificates make it possible to secure communications with customers, partners, suppliers and employees over a variety of devices. Specifically, the Enrollment Server for Web delivers:

Enhanced Security — The Entrust Authority Enrollment Server makes it possible to issue digital certificates to standard Web servers and Web browsers to enable Secure Sockets Layer (SSL) communications. SSL is the standard used by Web sites to secure the information passed between a Web browser and a Web server, and to identify parties in the transaction. The Enrollment Server issues digital certificates to make it possible to communicate securely with anyone using Web browsers (including e-mail) such as Mozilla® Firefox, Microsoft® Internet Explorer or Netscape® Navigator.

The solution can also issue digital certificates for securing VPN communications. Digital certificates from the Entrust Authority Enrollment Server for Web enables privacy, data integrity and strong identification for the IPSec capabilities of Microsoft® Windows® Server 2003, the Nortel Contivity™ VPN device and others.

Versatility — The Entrust Authority Enrollment Server can be leveraged across the most common applications for the issuance of certificates to today's most popular Web browsers, and to Web servers such as Microsoft, IBM, Apache and others. The solution also issues certificates to Nokia, Motorola and Ericsson WAP servers.

Ease of Use — The Entrust Authority Enrollment Server uses a Web-based interface, providing users with a straightforward method to request and retrieve digital certificates. Using any HTML editor, this Web-based interface can be customized for a specific look and feel, or you can use the templates provided right out of the box. A guided step-by-step process makes certificate retrieval easy for users.

Benefits :

- Provides easy, efficient issuance of digital certificates
- Works with today's most popular Web browsers and servers
- Offers straightforward, easy-to-use Web interface to request or retrieve certificates
- Standards-based interoperability supports common security and IP protocols, including SSL (TLS), IPSec, S/MIME, PKCS 10/7, WAP and WTLS
- Proven, scalable platform can manage issuance of up to 500,000 certificates and large number of administrators



Ease of Deployment — The Enrollment Server for Web installs in minutes on standard Web servers and is simple to operate. There is no client-side software to download or install. With no software distribution and modest support requirements, IT departments can deploy their scarce resources elsewhere.

Digital certificates issued through the Enrollment Server can have lifetimes of up to 60 months, with no annual renewal fees. Longer certificate lifetimes mean less administrative overhead, freeing up your staff and customers to focus on doing business, not managing certificates.

Interoperability — The Entrust Authority Enrollment Server is standards-based. It supports and enables a variety of common security and IP protocols including: SSL (TLS), IPSec, S/MIME, PKCS 10/7, WAP and WTLS.

Scalability — Each Entrust Authority Enrollment Server for Web can issue up to 500,000 certificates and can support a large number of Administrators. The Enrollment Server for Web can also be geographically separated from Entrust Authority Security Manager, adding additional flexibility to large deployments. Multiple certification authority (CA) configurations can extend the number of users into the millions.

Product Specifications

Entrust Products

- Entrust Authority™ Security Manager 7.0 or higher
- Entrust Authority™ Self-Administration Server 8.0 or higher (optional)

Supported Platforms

Operating Systems

- Microsoft® Windows® 2000 Server and Advanced Server
- Microsoft® Windows® Server 2003 (Enterprise, Standard)
- Microsoft® Windows® Server 2003 R2 (Enterprise, Standard)
- Hewlett-Packard® HP-UX® 11.0, 11i v1
- Sun® Solaris™ Operating Environment 8, 9, 10 (including Containers)

Web Servers

- Microsoft Internet Information Server 6.0
- Sun® One™ Web Server 6.0 SP5 or higher
- Sun® Java System™ Web Server 6.1 SP4 or higher
- IBM® HTTP Server 1.3.26 or higher
- Apache HTTP Server 2.0 or higher

Browsers

- Microsoft IE 6.x, IE 7
- Netscape Navigator 7.x, 8.x, 9.x
- Mozilla 1.7.x
- Firefox 2.x, 3.x

Client Operating Systems

Client-side Windows, HP-UX and Solaris Operating Systems that support the browsers listed above are supported for certificate enrollment with Entrust Authority Enrollment Server for Web.

About Entrust

Entrust [NASDAQ: ENTU] secures digital identities and information for consumers, enterprises and governments in 1,700 organizations spanning 60 countries. Leveraging a layered security approach to address growing risks, Entrust solutions help secure the most common digital identity and information protection pain points in an organization. These include SSL, authentication, fraud detection, shared data protection and e-mail security. For information, call 888-690-2424, e-mail entrust@entrust.com or visit www.entrust.com.

Entrust® Securing Digital Identities & Information

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. In Canada, Entrust is a registered trademark of Entrust Limited. All other Entrust product names and service names are trademarks or registered trademarks of Entrust, Inc. or Entrust Limited in certain countries. All other company names, product names and logos are trademarks or registered trademarks of their respective owners. © Copyright 2008 Entrust. All rights reserved.