

## Release notes for

# Entrust Authority<sup>™</sup> Security Manager Proxy 6.0

### Server Proxy and Filter:

**For Microsoft<sup>®</sup> Windows<sup>®</sup> 2000 Server (SP1, SP2, SRP1) and  
Sun<sup>®</sup> Solaris<sup>™</sup> 8**

### Client Proxy:

**For Windows 2000 Server (SP1, SP2, SRP1), Windows 2000 Professional  
(SP2), Windows XP Professional, and Solaris 8**

**Date:** August 22, 2002  
**Release:** 6.0

---

If you are reading these release notes on the Entrust Authority<sup>™</sup> Security Manager Proxy 6.0 CD, these may not be the most recent set. For the most recent notes, check the Customer Support Extranet. The Customer Support Extranet contains online versions of product documentation, an information knowledge base, and problem resolutions. It also provides the ability to submit and track service requests via the Web in a secure manner. You must have an account to access this portal. You can sign up for an account at

[www.entrust.com/xtrinet/support/](http://www.entrust.com/xtrinet/support/)

## How to contact Entrust Technical Support

Entrust offers telephone, e-mail, and online support through the Entrust/Reliance customer care program.

### Telephone support

For telephone support, simply call the appropriate number listed in your Customer Resource Kit. The Customer Resource Kit is a package made available to customers after the Entrust/Reliance customer care program has been purchased. You must provide your Unique ID (listed on your Customer Support Extranet account) whenever you call.

### E-mail support

E-mail support is offered to provide assistance for non-critical issues. Questions can be sent to

[support@entrust.com](mailto:support@entrust.com)

### Online support

Online support is provided through the Customer Support Extranet. This portal contains online versions of product documentation, an information knowledge base, and problem resolutions. It also provides the ability to submit and track service requests via the Web in a

secure manner. You must have an account to access this portal. You can sign up for an account at

[www.entrust.com/xtranet/support/](http://www.entrust.com/xtranet/support/)

## System requirements

Following are the *minimum* system requirements you *must* meet when installing Security Manager Proxy 6.0. If you do not meet these system requirements, upgrade your system before you continue.

### Windows

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

- Windows 2000 Server (SP1, SP2, SRP1), Windows 2000 Professional (SP2) or 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're installing over a network)

The Windows server that hosts Security Manager Proxy must meet the following system requirements:

- Windows 2000 Server operating system (SP1, SP2, SRP1)
- 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're installing over a network)

You must have Windows 2000 Server configured according to Microsoft's recommended minimum system requirements. For more information, consult the documentation belonging to your operating system and go to Microsoft's Website at <http://www.microsoft.com>.

## UNIX

The UNIX server that hosts Security Manager Proxy must meet the following system requirements:

- Solaris 8
- Sun Ultra 5 or better
- 128 Mbytes of RAM
- CD-ROM drive
- 50 Mbytes of free disk space for installation

## Issues affecting Security Manager Proxy 6.0

- When using Security Manager Proxy on Windows XP Professional, some periodic data loss may occur across the network. This issue is related to a known issue with Windows XP (see Microsoft KB article Q317949). To prevent these problems, perform the workaround described below.

Note that this workaround will introduce warnings in the log files describing problems binding to ports. These log messages should be followed by a successful bind message on the same port. These logs can safely be ignored. After applying this workaround the Proxy must not be configured to run with more than one process.

Note that only client-side Security Manager Proxies are supported for Windows XP, and that this fix only works if it is configured for only one process (the default configuration).

Open up the file "mon\_cli.tcl", found in the "etc" directory under the Proxy installation directory.

Comment out all the "bind" commands by typing the "#" character at the beginning of each line. The file should then look similar to this:

```
#if { ${proxy.cli.speke.bind} == 1 } { bind "" [ set proxy.cli.speke.port ] }
#if { ${proxy.cli.sep.bind} == 1 } { bind "" [ set proxy.cli.sep.port ] }
#if { ${proxy.cli.ash.bind} == 1 } { bind "" [ set proxy.cli.ash.port ] }
#if { ${proxy.cli.cmp.bind} == 1 } { bind "" [ set proxy.cli.cmp.port ] }
#if { ${proxy.cli.ldap.bind} == 1 } { bind "" [ set proxy.cli.ldap.port ] }
#if { ${proxy.cli.ldapauth.bind} == 1 } { bind "" [ set proxy.cli.ldapauth.
port] }
#if { ${proxy.cli.timestamp.bind} == 1 } { bind "" [ set
proxy.cli.timestamp.port ] }
source [set sf.rootdir]/etc/mon.tcl
```

- The following issues may affect ASH communications.
  1. The maximum number of concurrent sessions supported by the default configuration is three. If you attempt to establish more concurrent sessions (using Security Manager Administration, Self Administration Server or Administration Toolkit for C applications), these sessions will hang until one of the other sessions times out. To establish more sessions, configure the number of ASH threads to be one higher than the number of sessions required. For example, to permit four simultaneous sessions, add or edit the following line in the config.tcl file:

```
set proxy.*.ash.numthreads 5
```

2. When you disconnect an active session, for example by exiting Security Manager

Administration, the session remains in use until its idle timeout (default 50 seconds) elapses. If you try to establish another session by starting and logging into Security Manager Administration, you may encounter the issue described above.

- You may experience problems running the Security Manager Proxy configuration utility on Windows. This may be due to insufficient permissions or using a path name that is too long. Check to ensure the user running the configuration tool has administrative privileges, and that the path to the data directory is under 200 characters.
- If the proxy is installed on Windows by a user other than the default "Administrator" account, the "Proxy Configuration" icon may not appear in the Windows Programs menu. If this is the case, the tool can be run from the "bin" directory under the install location.
- If running a version of Entrust Authority Security Manager (formerly Entrust/PKI) and Security Manager Proxy on the same machine, you may experience problems initializing or starting your CA. To solve this problem, stop all instances of the Proxy before initializing or starting your CA.
- There may be problems if the Proxy's data or log files change while the Proxy is running, or if the permissions associated with the data or log files change. To avoid these problems, ensure the data directory and its subdirectories are always writable by the proxy service, and do not delete any data or log files while the Proxy is running.
- During install and configuration on Windows, you may see a dialog stating "You must restart your system for the configuration changes made to Entrust Authority (TM) Security Manager Proxy to take effect. Click Yes to restart now or No if you plan to restart manually later". If this happens, Click Yes to reboot and continue the installation.
- Errors may result with sfoam communication on Solaris if the sf.http.statusResult variable is changed. The server will not function correctly if this variable is set to a non-standard HTTP result code. If this variable is set to a standard HTTP result code (other than 200), the sfoam "status" command will not work correctly, but the errors reported by sfoam when trying to start or stop a server can be ignored.
- If you are using your Security Manager Proxy in a multiple CA or back-end server environment, be aware of the following:
  1. If you are using TLS tunnelling, the Entrust profile (EPF) file on the client-side and the server-side must either be issued from the same CA, or have a trust relationship. For information on setting up trust relationships, see "Cross-certifying with other CAs" on page 203 of *Administering Entrust/PKI 6.0 on Windows*, or "Cross-certifying with other CAs" on page 213 of *Administering Entrust/PKI 6.0 on UNIX*.
  2. If you have one or more authenticated LDAP connections tunnelling over TLS, you must indicate for each originating IP address which host to use for authenticated LDAP connections, and whether or not to use TLS for authenticated LDAP connections. The following example illustrates the proper syntax when one originating IP address uses authenticated LDAP (with TLS turned on), and one originating IP address that does not (with TLS turned off).

```

set proxy.numbackend 2
set proxy.srv.tunneltls 1

set proxy.originatingips.0 "123.1.2.3"
set proxy.srv.cmp.host.0 "134.3.7.3"
set proxy.srv.ash.host.0 "132.65.2.67"
set proxy.srv.ldapauth.tunneltls.0 0

set proxy.originatingips.1 "123.2.4.6"
set proxy.srv.cmp.host.1 "134.3.7.3"
set proxy.srv.ash.host.1 "132.65.2.67"
set proxy.srv.ldapauth.tunneltls.1 1
set proxy.srv.ldapauth.host.1 "123.4.5.6"

```

## Trademark information

Entrust is a trademark or a registered trademark of Entrust, Inc. in certain countries. All Entrust product names and logos are trademarks or registered trademarks of Entrust, Inc. in certain countries. All other company and product names and logos are trademarks or registered trademarks of their respective owners in certain countries.

Entrust's partnerships with vendors that have key expertise, products and services are helping us secure the enterprises and operations of our customers in a way that meets their needs and compliments their business processes. For a complete list of all Entrust partners, see [www.entrust.com/partners](http://www.entrust.com/partners).