

# **Entrust Authority™ Security Manager Proxy 6.0 Administration Guide**

© 2002 Entrust. All rights reserved.

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.

Release 6.0

# Contents

About this guide . . . . .	7
Typographic conventions . . . . .	8
CHAPTER 1	
About Entrust Authority™	
Security Manager Proxy 6.0 . . . . .	9
What is Security Manager Proxy? . . . . .	10
Deployment scenarios . . . . .	12
Tunnelling HTTP and TLS messages over the Internet . . . . .	12
Using Proxy as a Filter . . . . .	13
CHAPTER 2	
Preparing for installation . . . . .	15
Securing your environment and data . . . . .	16
Securing the servers . . . . .	16
Compiling configuration data . . . . .	19
CHAPTER 3	
Installing Security Manager Proxy 6.0 . . . . .	21
Installing Security Manager Proxy 6.0 on Solaris . . . . .	22
Installing Security Manager Proxy 6.0 on Windows . . . . .	24
CHAPTER 4	
Configuring Security Manager Proxy . . . . .	29
Configuring Security Manager Proxy 6.0 on Solaris . . . . .	30
Modifying user Path environment variables . . . . .	35
Viewing syslog messages . . . . .	35
Configuring Security Manager Proxy on Windows . . . . .	37

Configuring your clients .....	47
Entrust.ini file changes .....	47
DNS Host Name Resolution .....	48

## CHAPTER 5

### Security Manager Proxy administration ..... 49

Administering Security Manager Proxy .....	50
Monitoring Security Manager Proxy log activity .....	52

## CHAPTER 6

### Advanced configuration ..... 53

Understanding the config.tcl file .....	54
Config.tcl file location .....	54
Adding and modifying variables .....	54
Configuring for TLS .....	56
Creating Entrust profiles for Security Manager Proxy .....	58
Using Server Login with Security Manager Proxy .....	59
Configuring for Authenticated LDAP .....	62
Configuring for specific firewalls .....	64
Configuring for HTTP Proxies .....	65
HTTP proxies between the Client Proxy and the Internet .....	65
HTTP proxies between the Internet and the	
Server Proxy .....	65
Configuring for multiple CAs/Servers .....	67
Configuring for Entrust Authority Timestamp Server .....	70
Configuring the proxy.log file .....	71

## CHAPTER 7

### Uninstalling Security Manager Proxy. .... 73

Uninstalling Security Manager Proxy on Solaris .....	74
Uninstalling Security Manager Proxy on Windows .....	75

APPENDIX A

Security Manager Proxy variables . . . . .77

APPENDIX B

Security Manager Proxy error messages . . . . .91

Index . . . . .95



# About this guide

The guide describes

- what Entrust Authority™ Security Manager Proxy 6.0 is and why you would use it
- how Security Manager Proxy 6.0 works
- system requirements
- installation information
- configuration details
- variable and error message information

For information on public-key infrastructures concepts and the Entrust cryptographic model, see the Entrust Authority™ documentation.

# Typographic conventions

The following typographic conventions appear in this guide.

- Commands and text that you must enter appear in bold courier type and look like this:

**user\_setattribute**

- Variables appear in italic courier type and look like this:

*name\_of\_person*

- Options (which by definition are things you may or may not choose to specify) appear in Courier type in angle brackets. For example:

<option>



# Chapter 1

## About Entrust Authority™ Security Manager Proxy 6.0

This chapter provides an overview of Entrust Authority™ Security Manager Proxy 6.0. It contains the following sections:

- “What is Security Manager Proxy?” on page 10
- “Deployment scenarios” on page 12

# What is Security Manager Proxy?

Entrust Authority Security Manager Proxy 6.0 is 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. Clients communicate using one of seven supported protocols:

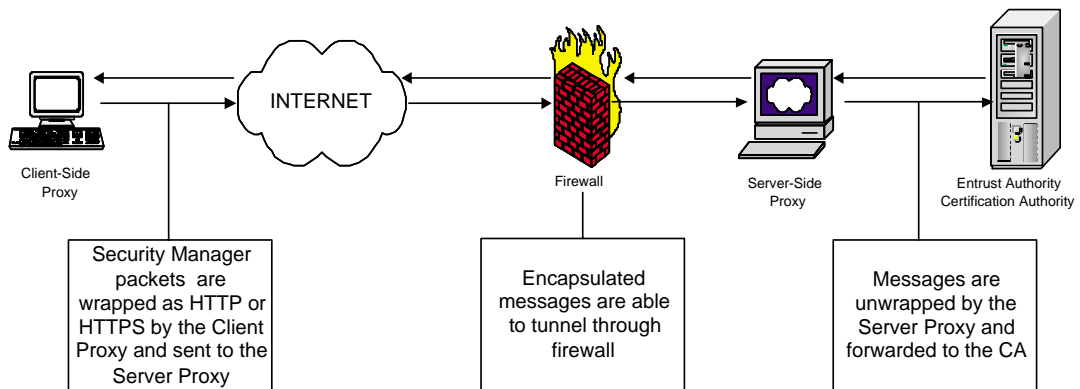
Protocol	Used by...
SEP	CA (For all Entrust/PKI versions up to 6.0)
PKIX-CMP	CA (For all Entrust PKI/Security Manager versions)
ASH	CA
PROTO-PKIX	CA, Entrust Authority Enrollment Server, Entrust Authority Enrollment Server for Web, Entrust Authority Enrollment Server for VPN, and Entrust Authority Enrollment Server for Smart Cards
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 Roaming Server). Firewalls typically restrict incoming traffic to HTTP or TLS packets on specific ports. As a result, data packets sent by regular Authority protocols cannot reach the CA.

## How the Proxy works

- 1 Data packets sent from a client machine are encapsulated by the Client Proxy as HTTP or TLS so that they can tunnel through the firewall.
- 2 Once the packets are through the firewall, the Server 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 Proxy 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 Proxy so the client can understand the CA response.

**Figure 1:** Security Manager Proxy Overview



# Deployment scenarios

This section describes two example scenarios of how Security Manager Proxy 6.0 might be deployed for your enterprise.

## Tunnelling HTTP and TLS messages over the Internet

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, the CA must be accessible by clients—either inside a company's firewall, or over the Internet.

In this scenario, this is accomplished through the following actions:

- Security Manager Proxy is installed on one client workstation at a remote site. Multiple other client machines connect to this Client Proxy instance in order to send packets to the CA.
- The Server Proxy is installed on one server workstation behind the firewall that is visible from the Internet.

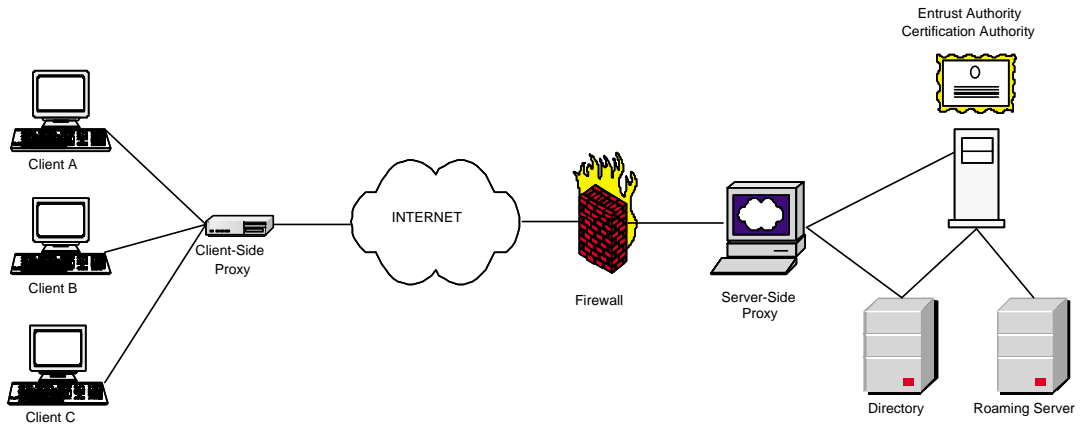
Data packets for the CA are forwarded from Clients A, B, and C to the Client Proxy. The packets are encapsulated as HTTP or TLS and tunnelled through the firewall to the Server Proxy. The Server Proxy forwards the messages to the Entrust CA or back-end servers.

---

**Note:** If you want to perform authenticated LDAP binds to the Directory, use TLS to provide a secure connection over the Internet. For more information, see “Configuring for Authenticated LDAP” on page 62.

---

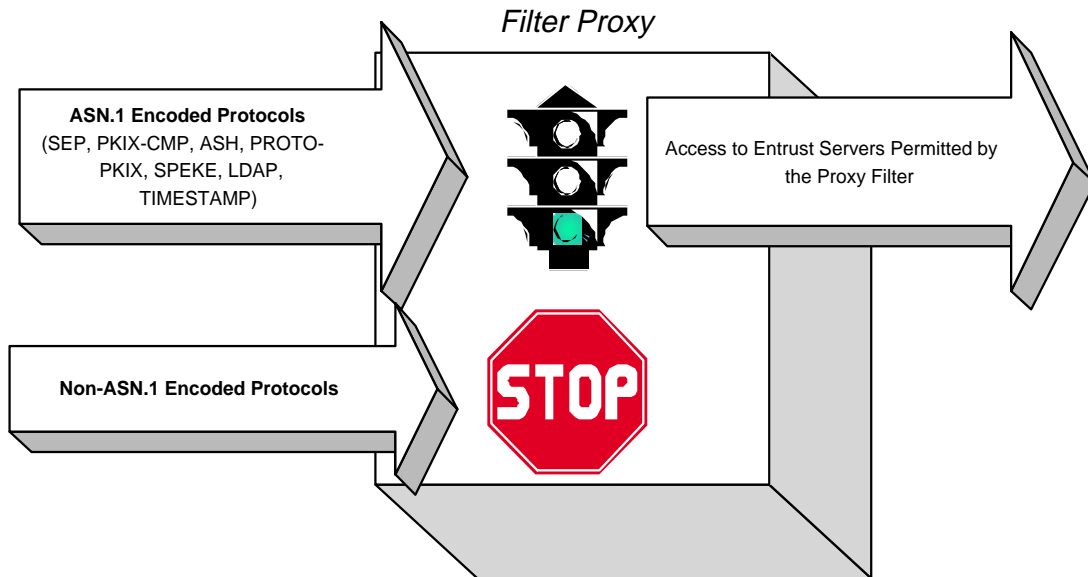
**Figure 2:** HTTP Tunnelling Example



## Using Proxy as a Filter

All of the Entrust-permitted protocols are created according to ASN.1 Basic Encoding Rules (BER). Security Manager Proxy can be configured as a filter to ensure that packets that do not conform to BER are blocked from gaining access to the Entrust CA and back-end servers. When Security Manager Proxy is configured as a filter, all messages not sent using one of the supported protocols are blocked by the Proxy.

**Figure 3:** Filter Proxy Operation Example



---

**Note:** By default, Proxy instances configured for HTTP tunnelling also automatically perform BER filtering. As a result, if you have a Server Proxy installed for HTTP tunnelling but also require BER filtering, do not install an additional Filter Proxy.

---

# Chapter 2

## Preparing for installation

This chapter describes how to organize and plan a Security Manager Proxy 6.0 installation.

Read this chapter if you are the system administrator who will configure the Solaris or Windows machines that will host Security Manager Proxy 6.0. Carefully consider and answer questions in this chapter before you begin installing Security Manager Proxy 6.0.

This chapter includes the following sections:

- “Securing your environment and data” on page 16
- “Compiling configuration data” on page 19

# Securing your environment and data

Before you install the Proxy, you must ensure that the servers that will host it are physically and network-secure. Only the highly trusted administrator who is responsible for installation should have administrative privileges on the servers that will host Security Manager Proxy 6.0.

Entrust strongly recommends you install the Server Proxy on a server separate from the server that hosts your Directory (that is, either a third-party, LDAP-compliant Directory or Microsoft Active Directory), and separate from the server that hosts the Entrust CA.

You must secure all Security Manager Proxy 6.0 servers against unauthorized physical and network access.

## Securing the servers

The following steps describe how you can improve the security of the Solaris and Windows servers that will host Security Manager Proxy 6.0. See “To improve Solaris server security” on page 16 and “To improve Windows server security” on page 17.

### To improve Solaris server security

- 1** Restrict physical access to the servers that will host Security Manager Proxy 6.0. For example, put the servers in a locked room to which only a few of your most highly trusted administrative users have access. Set up an audit log of users who visit this room; for example, a proximity badge reader can provide this information for you. Also, restrict physical access to your backup tapes and the uninterruptible power supply, if you have one.
- 2** Ensure you have a connection to your network using the TCP/IP protocol. You need to be connected to your network using the TCP/IP protocol to allow communication between the Security Manager Proxy 6.0 and the various components of Security Manager (that is, the Directory, Security Manager, Security Manager Administration, the Security Manager database, and client applications such as Desktop Manager). For information about how to ensure you have a connection to your network using the TCP/IP protocol, consult the documentation for your operating system.
- 3** Disable inbound remote logins, such as those which use telnet, rlogin, ftp, and an X Window System. Also disable remote job execution (for example, through “rsh” or “remsh”) and delete all .rhosts and hosts.equiv files.
- 4** Arrange for a formal security audit of physical and system security. Consider setting up a software tool (for example, Internet Security Scanner) to go through your system to look for vulnerabilities.



- 5** Disable all diagnostic services in inetd: for example, chargen, echo, and netdate.
- 6** Disable inetd unless specifically required.
- 7** Examine running processes and disable unnecessary applications such as sendmail.
- 8** Get instructions from the vendor of your operating system on how to properly secure the servers hosting these operating systems.
- 9** Change all passwords. Use password verification software to ensure that passwords are not weak or empty.
- 10** The servers that will host Security Manager Proxy 6.0 should not allow indirect root login.
- 11** After the installation, only a few highly trusted administrators should have accounts to access the server. Require administrators to log in under their own username from the console and use “su” or “sudo” to obtain root access as required.
- 12** Redirect all log messages to a separate and secured server using “syslog” to provide an audit log that cannot be altered. For more information on setting up syslog with Security Manager Proxy 6.0, see “Viewing syslog messages” on page 35.
- 13** Disable the stack by opening the /etc/system file in a text editor, and adding the following line:

```
set noexec_user_stack=1
```

### **To improve Windows server security**

- 1** Ensure you have a connection to your network using the TCP/IP protocol. You need to be connected to your network using the TCP/IP protocol to allow communication between the Security Manager Proxy 6.0 and the various components of Security Manager (that is, the Directory, Security Manager, Security Manager Administration, the Security Manager database, and client applications such as Desktop Manager). For information about how to ensure you have a connection to your network using the TCP/IP protocol, consult the documentation for your operating system.

---

**Note:** The Windows server on which you want to install Security Manager Proxy 6.0 must not host the Domain Name System (DNS) service; it must be a DNS service client only.

---

- 2** Disable inbound remote logins (for example, through telnet or rlogin) and delete unused program files such as ftp.exe, rasdial.exe, and telnet.exe.

- 3** Arrange for a formal security audit of physical and system security. Consider setting up a software tool (for example, Internet Security Scanner) to go through your system and look for vulnerabilities.
- 4** Disable NetBIOS-over-TCP/IP (NBT).
- 5** Disable the Guest account and delete all other user accounts. Only the Windows administrator account should remain. The administrator who will install Security Manager Proxy 6.0 should own this account.
- 6** Change the Windows administrator username from “administrator” to something less obvious, such as “lou\$1Db0Nso0%” (“I owe you money one day but nothing now so no interest”), and choose an equally cryptic but memorable password. Then, attackers must guess the administrator username also, as well as administrator password. Don’t use the example administrator username provided above.

---

**Note:** You can change the administrator username in the Active Directory Users and Computers window. Click Users in the tree view and right-click the “Administrator” username.

---

- 7** Set Windows password security options to specify minimum and maximum password age, password uniqueness, and password length.
- 8** Enable the event-auditing system, and audit all failed operations and low-frequency successes.

# Compiling configuration data

Before you install and configure Security Manager Proxy 6.0, you must obtain or decide on certain details of your Security Manager Proxy 6.0 deployment. You will be asked to provide this data during the installation and configuration of Security Manager Proxy 6.0. Compiling this data before you install and configure the software simplifies these processes by giving you convenient reference sheets with your configuration data.

Depending on the Proxy type you install, you will be prompted to supply the following different configuration information:

Proxy Type	Configuration Data Required
Client	Security Manager Proxy 6.0 data file location Server Proxy IP address or DNS host name
Server or Filter	Security Manager Proxy 6.0 data file location LDAP Directory IP address or DNS host name Security Manager IP address or DNS host name Roaming Server IP address or DNS host name Timestamp Server IP address or DNS host name



## Chapter 3

# Installing Security Manager Proxy 6.0

This chapter describes how to install Security Manager Proxy 6.0. It includes the following sections:

- “Installing Security Manager Proxy 6.0 on Solaris” on page 22.
- “Installing Security Manager Proxy 6.0 on Windows” on page 24.

---

**Note:** Perform all the relevant procedures in “Preparing for installation” on page 15 before beginning the installation process.

---

# Installing Security Manager Proxy 6.0 on Solaris

This section describes how to install the Proxy on Solaris systems.

## To install Proxy on Solaris

- 1 Ensure you are logged in as root.
- 2 Navigate to the root directory of the Security Manager Proxy 6.0 Solaris CD.
- 3 Start the Security Manager Proxy 6.0 Installation and Configuration Utility by entering the following in a terminal window:

```
./install.sh
```

The license agreement appears.

- 4 Read the license agreement.

The license agreement is several screens long. Press the Space bar to advance to the next screen until you have read the entire agreement.

- 5 If you agree with the licensing terms, enter "yes".

The following appears:

```
Please enter the user that will own this installation:
```

- 6 The person who owns this installation has the Solaris userid. Enter the userid, for example:

```
entproxy
```

The following message appears:

```
Please enter the group that will own this installation:
```

- 7 The user who owns your installation belongs to the primary group. Enter the name of that group, for example:

```
entproxy
```

- 8 Accept the default directory for Security Manager Proxy 6.0 (that is, /opt/entrust/proxy6.0), or enter a new directory. If you are entering a new directory, ensure that the parent of this directory already exists and use an absolute path name.

The following message appears:

```
Now extracting files, please wait... Done.
```

```
Would you like to configure an instance of Security Manager  
Proxy now (y/n)? [y]
```

- 9 If you would like to configure an instance of Security Manager Proxy 6.0 now, enter "y". Then proceed to "Configuring Security Manager Proxy 6.0 on Solaris" on page 30.

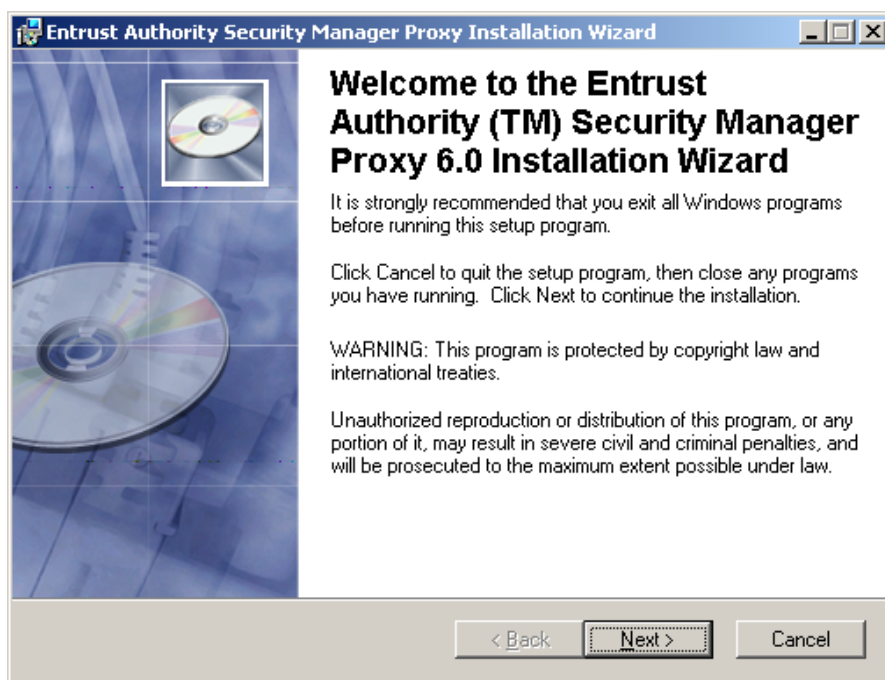
If you want to configure an instance of Security Manager Proxy 6.0 at a later point, enter "n".

# Installing Security Manager Proxy 6.0 on Windows

To install Security Manager Proxy 6.0 on Windows, ensure the domain account you use to log in is a member of the local Administrator's group for the machine that will host Security Manager Proxy 6.0.

## To install Security Manager Proxy 6.0 on Windows

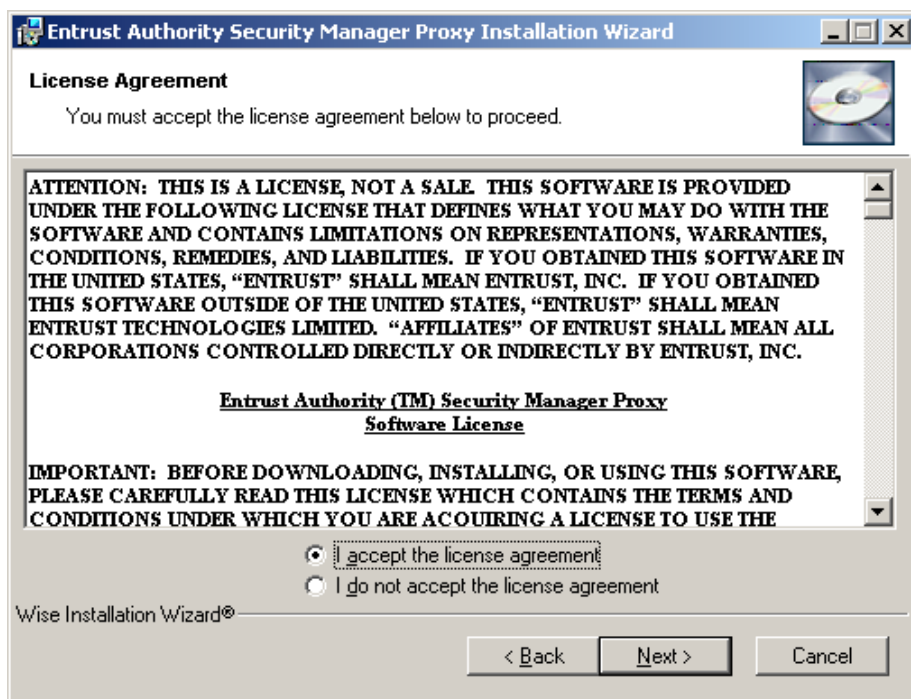
- 1 Insert the Security Manager Proxy 6.0 CD into the CD-ROM drive of the Windows server.  
If Windows does not auto-detect the CD, run setup.exe in the root folder of the CD.
- 2 The Entrust Authority Security Manager Proxy 6.0 Installation Wizard appears.



Ensure all applications are closed, then click *Next*.

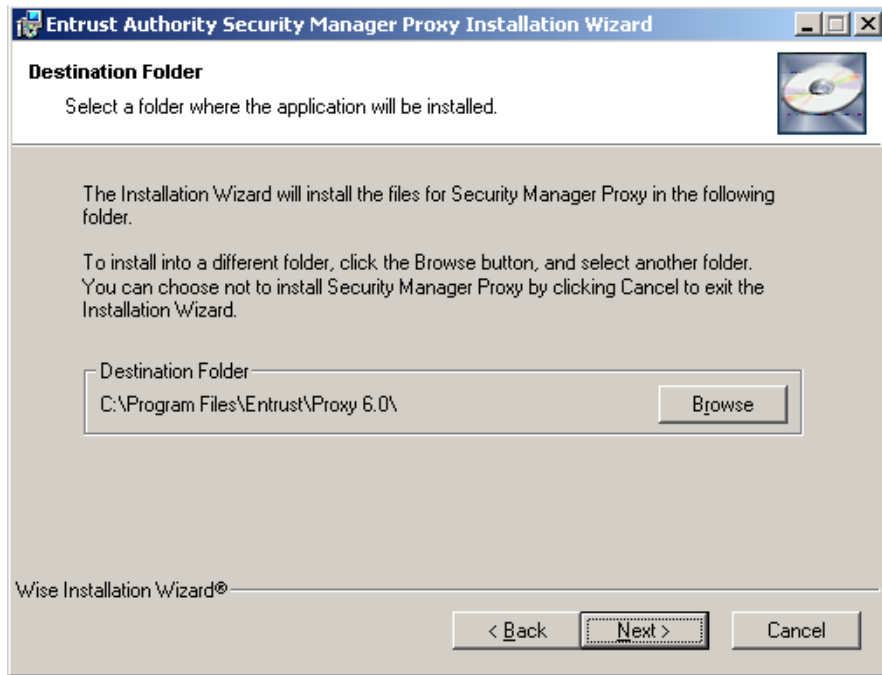


- 3 A software license agreement dialog box appears.



Read the license agreement carefully. If you accept all its terms and conditions, click *I accept the license agreement*, and click *Next* to continue the installation procedure. Otherwise, click *Cancel* to exit the setup wizard.

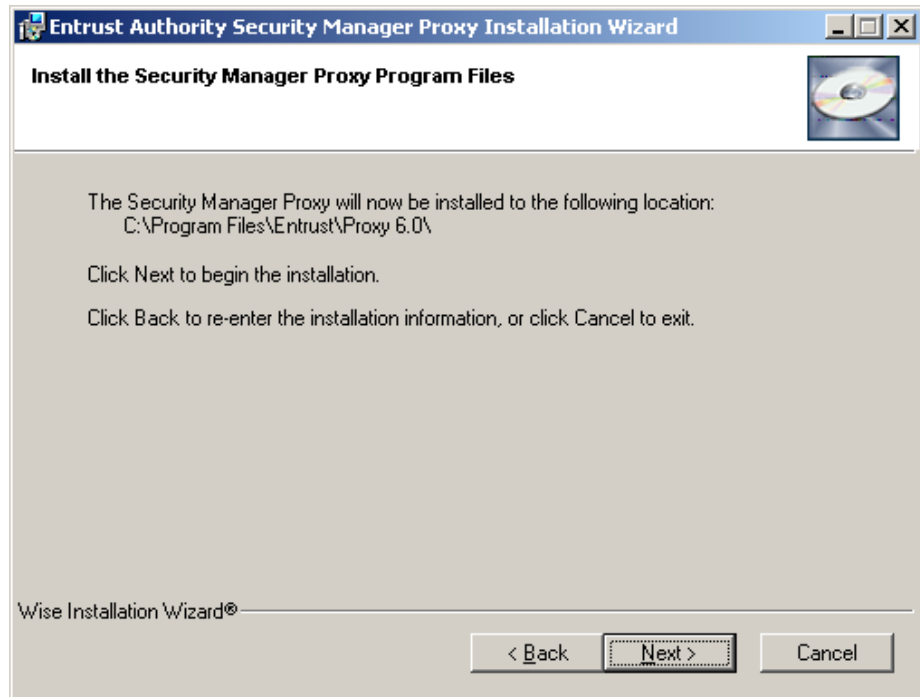
- 4 If you accept the license agreement, the following dialog box appears.



Either accept the default folder location for where Security Manager Proxy 6.0 will be installed, or click *Browse* to specify a different folder location.

When you have finished specifying the folder location, click *Next*.

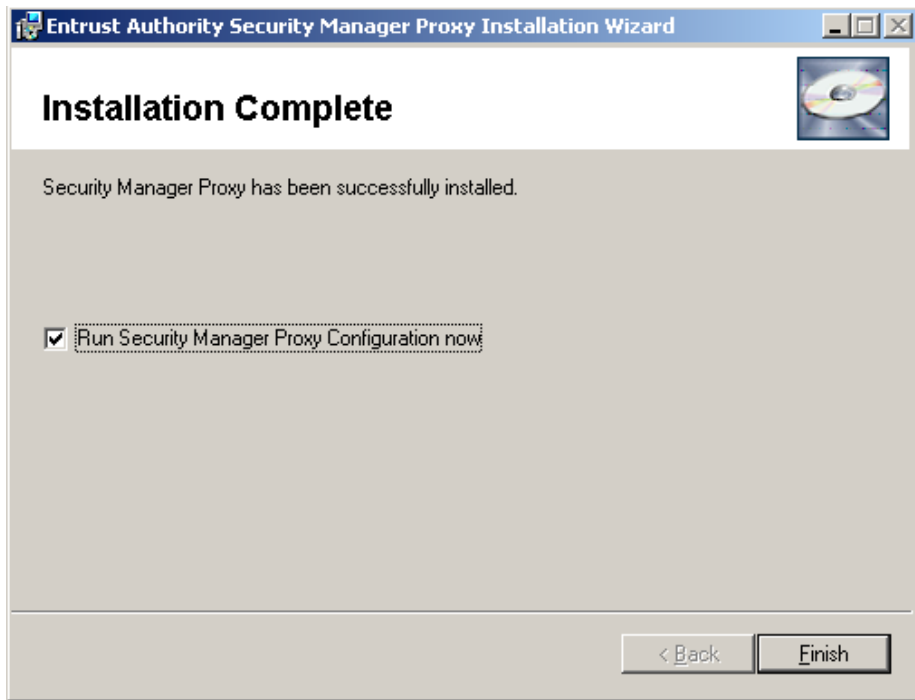
- 5 The following dialog box appears.



Review the information presented in the summary dialog box. If the summary information is incorrect, click *Back* until you arrive at the appropriate dialog box and correct the information as required.

When you have finished reviewing the summary information, click *Next* to install Security Manager Proxy 6.0 to the specified folder location.

- 6 After a few moments, the following dialog box appears.



If you do not want to configure Security Manager Proxy 6.0 at this time, deselect *Run Security Manager Proxy Configuration now*. You can run the configuration utility from the Windows Start menu at any time by click *Start > Programs > Entrust > Entrust Authority Security Manager Proxy > Proxy Configuration*. Click *Finish*.

If you are configuring Security Manager Proxy 6.0 now, see “Configuring Security Manager Proxy on Windows” on page 37.

# Chapter 4

## Configuring Security Manager Proxy

This chapter describes how to configure Security Manager Proxy 6.0 and the clients that will point to the Proxy. It includes the following sections:

- “Configuring Security Manager Proxy 6.0 on Solaris” on page 30
- “Configuring Security Manager Proxy on Windows” on page 37
- “Configuring your clients” on page 47

# Configuring Security Manager Proxy 6.0 on Solaris

This section describes how to run the configuration script on Solaris. If you are configuring

- a Client Proxy, see “To configure Security Manager Proxy 6.0 on the client side” on page 30
- a Server Proxy, see “To configure Security Manager Proxy on the server side” on page 31
- a Filter Proxy, see “To configure Security Manager Proxy as a filter” on page 33

## To configure Security Manager Proxy 6.0 on the client side

- 1 Do one of the following:
  - If you are still running the Security Manager Proxy 6.0 Installation and Configuration Utility, go to Step 4.
  - If you are starting the Security Manager Proxy 6.0 Configuration Utility now, go to Step 2.
- 2 Log in as the user specified as the Proxy owner during the installation process.
- 3 From the .../etc directory where Security Manager Proxy was installed (for example, /opt/entrust/proxy6.0/etc), run the following command:

```
./config.sh
```

- 4 The following message appears:

```
Entrust Authority Security Manager Proxy Configuration Utility

A directory will be created to store the server data.
Enter the full path of this directory:
[/opt/entrust/proxy_data/proxy1]
```

This step creates a new directory where all the data related to Security Manager Proxy will be placed. Do not use the name of a directory that already exists.

---

**Note:** If a message appears to indicate the directory could not be created, check that the user who will own this instance of Security Manager Proxy has permission to write to the parent directory, for example, /opt.

---

- 5 Either accept the default path suggested, or enter another path.  
The following message appears:

```
Choose the type of Proxy that you want to configure.
Select one of the following:
1. client
2. server
3. filter
```

- 6 Enter "1" to configure a client-side Proxy.

The following message appears:

```
Server Proxy Address
```

- 7 Enter the IP address or DNS name of the server that will host the Server Security Manager Proxy.



**Attention:** For security reasons, the use of IP addresses is recommended over the use of DNS domain names.

---

The following message appears:

```
Do you want to start the server now (y/n)? [y]
```

- 8 Either accept the default "y" and start the server now, or choose to start the server later by entering "n".

For more information on starting the server, see "Administering Security Manager Proxy" on page 50.

If you accepted the default "y", the following message appears:

```
The server was started successfully.
```

### To configure Security Manager Proxy on the server side

- 1 Do one of the following:
  - If you are still running the Security Manager Proxy 6.0 Installation and Configuration Utility, go to Step 4.
  - If you are starting the Security Manager Proxy 6.0 Configuration Utility now, go to Step 2.
- 2 Log in as the user specified as the Proxy owner during the installation process.
- 3 From the .../etc directory where Security Manager Proxy was installed (for example, /opt/entrust/proxy6.0/etc), run the following command:

```
./config.sh
```

- 4 The following message appears:

```
Entrust Authority Security Manager Proxy Configuration Utility
```

```
A directory will be created to store the server data.  
Enter the full path of this directory:  
[/opt/entrust/proxy_data/proxy1]
```

This step creates a new directory where all the data related to Security Manager Proxy will be placed. Do not use the name of a directory that already exists.

---

**Note:** If a message appears to indicate the directory could not be created, check that the user who will own this instance of Security Manager Proxy has permission to write to the parent directory, for example, /opt.

---

- 5** Either accept the default path suggested, or enter another path.

The following message appears:

```
Choose the type of Proxy that you want to configure.  
Select one of the following:  
1. client  
2. server  
3. filter
```

- 6** Enter "2" to configure a Server Proxy.

The following message appears:

```
Entrust Authority Security Manager Address
```

- 7** Enter the IP address or DNS name of the server that hosts Entrust Authority Security Manager.



**Attention:** For security reasons, the use of IP addresses is recommended over the use of DNS domain names.

---

If you are not setting up a Proxy for Entrust Authority Security Manager, press the Enter key to continue.

The following message appears:

```
LDAP Server Address
```

- 8** Enter the IP address or DNS name of the machine that hosts the LDAP server used by Security Manager.

If you are not setting up a Proxy for an LDAP server, press the Enter key to continue.

The following message appears:

```
Roaming Server Address
```



- 9** Enter the IP address or DNS name of the machine that hosts Entrust Authority Roaming Server.

If you are not using Entrust Authority Roaming Server, press the Enter key to continue.

The following message appears:

```
Entrust Timestamp Server Address
```

- 10** Enter the IP address or DNS name of the machine that hosts Entrust Timestamp Server.

If you are not using Entrust Timestamp Server, press the Enter key to continue.

The following message appears:

```
Do you want to start the server now (y/n)? [y]
```

- 11** Either accept the default (y) and start the server now, or choose to start the server later by entering “n”.

For more information on starting the server, see “Administering Security Manager Proxy” on page 50.

If you accepted the default (y), the following message appears:

```
The server was started successfully.
```

### **To configure Security Manager Proxy as a filter**

- 1** Do one of the following:
- If you are still running the Security Manager Proxy 6.0 Installation and Configuration Utility, go to Step 4.
  - If you are starting the Security Manager Proxy 6.0 Configuration Utility now, go to Step 2.
- 2** Log in as the user specified as the Proxy owner during the installation process.
- 3** From the .../etc directory where Security Manager Proxy was installed (for example, /opt/entrust/proxy6.0/etc), run the following command:

```
./config.sh
```

- 4** The following message appears:

```
Entrust Authority Security Manager Proxy Configuration Utility
```

```
A directory will be created to store the server data.
```

```
Enter the full path of this directory:
```

```
[/opt/entrust/proxy_data/proxyl]
```

This step creates a new Solaris directory where all the data related to Security Manager Proxy will be placed. Do not use the name of a directory that already exists.

---

**Note:** If a message appears to indicate the directory could not be created, check that the user who will own this instance of Security Manager Proxy has permission to write to the parent directory, for example, /opt.

---

- 5** Either accept the default path suggested, or enter another path.

The following message appears:

```
Choose the type of Proxy that you want to configure.  
Select one of the following:  
1. client  
2. server  
3. filter
```

- 6** Enter “3” to configure a Filter Proxy.

The following message appears:

```
Entrust Authority Security Manager Address
```

- 7** Enter the IP address or DNS name of the server that hosts Entrust Authority Security Manager.



**Attention:** For security reasons, the use of IP addresses is recommended over the use of DNS domain names.

---

If you are not setting up a Proxy for Entrust Authority Security Manager, press the Enter key to continue.

The following message appears:

```
LDAP Server Address
```

- 8** Enter the IP address or DNS name of the machine that hosts the LDAP server used by Security Manager.

If you are not setting up a Proxy for an LDAP server, press the Enter key to continue.

The following message appears:

```
Roaming Server Address
```

- 9** Enter the IP address or DNS name of the machine that hosts Entrust Authority Roaming Server.

If you are not using Entrust Authority Roaming Server, press the Enter key to continue.

The following message appears:

```
Entrust Timestamp Server Address
```

- 10** Enter the IP address or DNS name of the machine that hosts Entrust Timestamp Server.

If you are not using Entrust Timestamp Server, press the Enter key to continue.

The following message appears:

```
Do you want to start the server now (y/n)? [y]
```

- 11** Either accept the default (y) and start the server now, or choose to start the server later by entering “n”.

For more information on starting the server, see “Administering Security Manager Proxy” on page 50.

If you accepted the default (y), the following message appears:

```
The server was started successfully.
```

## Modifying user Path environment variables

The user must add the following to their PATH environment variable:

```
install_directory/bin
```

where “install\_directory” is the directory where Security Manager Proxy was installed—for example, “/opt/entrust/proxy 6.0” (see Step 8 on page 22).

The user who owns the installation of Security Manager Proxy must add the following to their LD\_LIBRARY\_PATH environment variable:

```
install_directory/lib
```

where “install\_directory” is the directory where Security Manager Proxy was installed—for example, “/opt/entrust/proxy 6.0” (see Step 8 on page 22).

## Viewing syslog messages

Syslog messages generated by Security Manager Proxy are controlled by settings in two files: *syslog.conf* and *config.tcl*.

Syslog.conf controls what happens to syslog messages based on priority and facility variables. Your syslog.conf file might look something like this:

```
*.err;kern.notice;auth.notice /dev/console
*.warn /dev/console
*.alert root
*.emerg *
```

```
*.debug /var/adm/messages
```

#### The line

```
*.warn /dev/console
```

sends all `*.warn` messages to `/dev/console`. Add this line to your `syslog.conf` file in order to specify where your warn-level syslog messages will appear.

You can set variables in `config.tcl` to modify how syslog messages are logged. By default, level 0 logs are sent to syslog as priority 4 messages (warning). To change this behavior so that Level 0 logs are sent to Syslog as priority 5 messages (notice), you would enter the following line in `config.tcl`:

```
set sf.syslog.prio 5
```

You would then need to modify the `syslog.conf` file to indicate where the notice messages would be sent to (as was done for the warning messages above).

For more information on the Security Manager Proxy variables that you can set and modify in `config.tcl`, see “Security Manager Proxy variables” on page 77.

For more information on priority levels, and on syslog in general, see the “man” pages for “syslog”, “syslogd”, and “syslog.conf”.

# Configuring Security Manager Proxy on Windows

This section describes how to configure Security Manager Proxy on Windows. If you are configuring

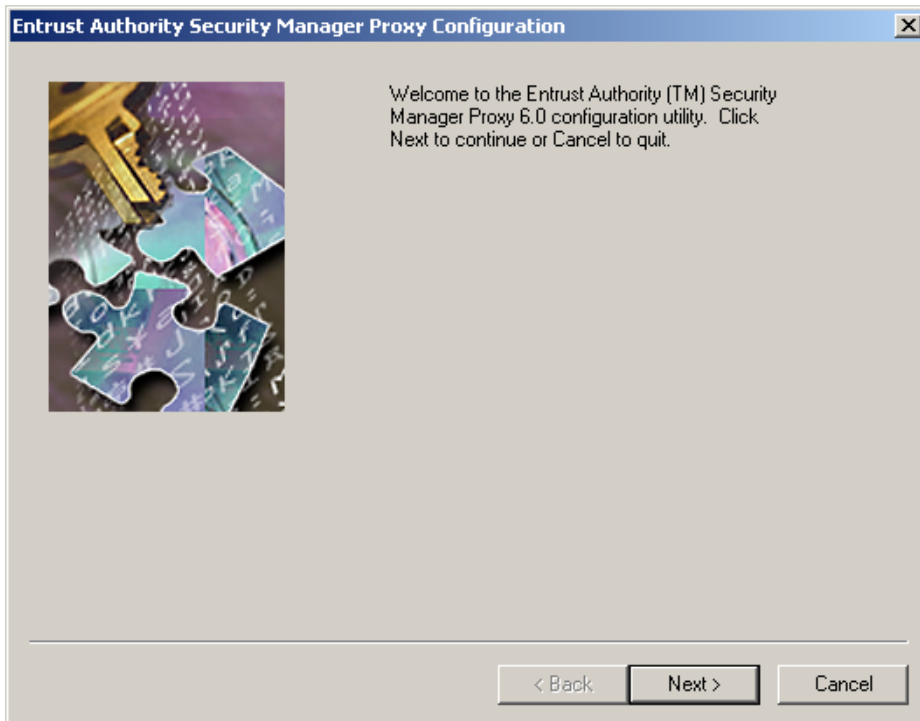
- a Client Proxy, see “To configure Security Manager Proxy on the client side” on page 37
- a Server Proxy, see “To configure Security Manager Proxy on the server side” on page 40
- a Filter Proxy, see “To configure Security Manager Proxy as a filter” on page 43

## To configure Security Manager Proxy on the client side

**1** Do one of the following:

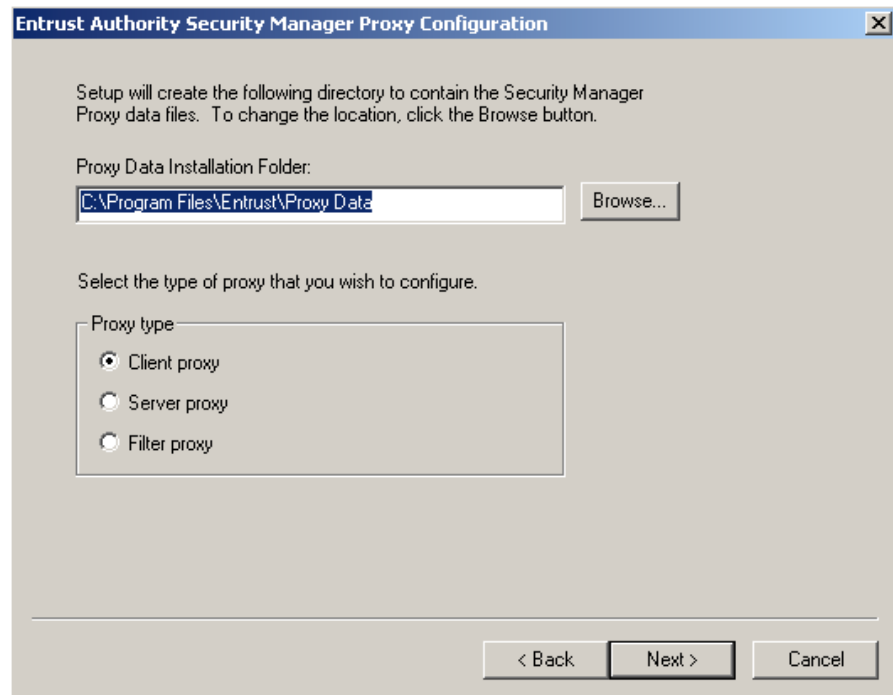
- If you selected *Run Security Manager Proxy Configuration now* when you finished installing Security Manager Proxy, go to Step 2 on page 38.
- If you are starting the Security Manager Proxy 6.0 Configuration Utility now, click *Start > Programs > Entrust > Entrust Authority Security Manager Proxy > Proxy Configuration*.

- 2 The Entrust Authority Security Manager Proxy Configuration utility appears.



Click *Next*.

- 3 The following dialog box appears.



Either accept the default folder location for where Security Manager Proxy data files will be installed, or click *Browse* to specify a different folder location.

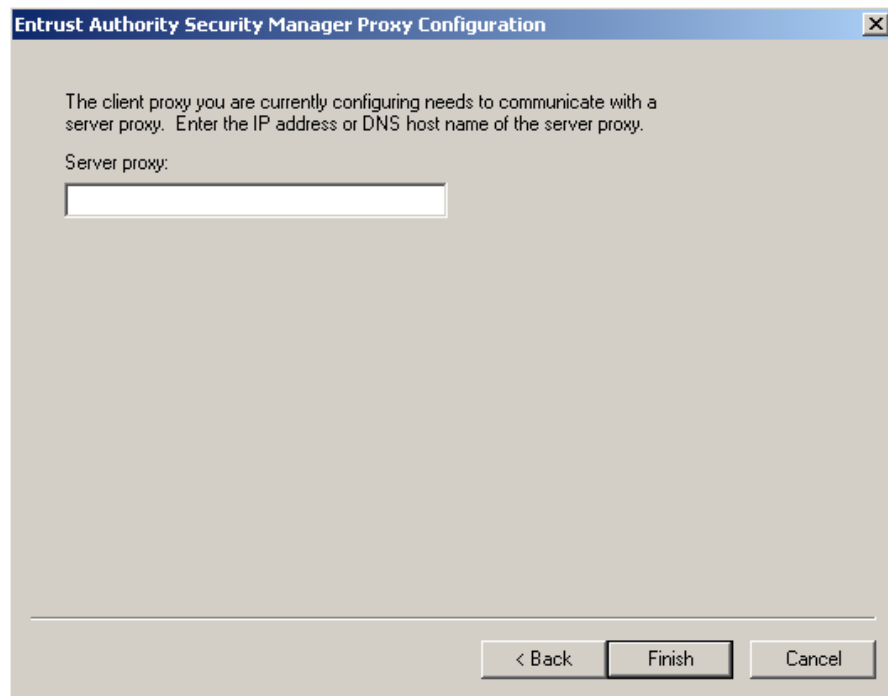
---

**Note:** Retain the \Entrust\Proxy Data part of the pathname if you change the folder location from the default.

---

Select *Client proxy* as the Proxy type, and click *Next*.

- 4 The following dialog box appears.



Enter the IP address or DNS host name of the Server Security Manager Proxy that the client-side Security Manager Proxy will be communicating with, then click *Next*.



**Attention:** For security reasons, the use of IP addresses is recommended over the use of DNS domain names.

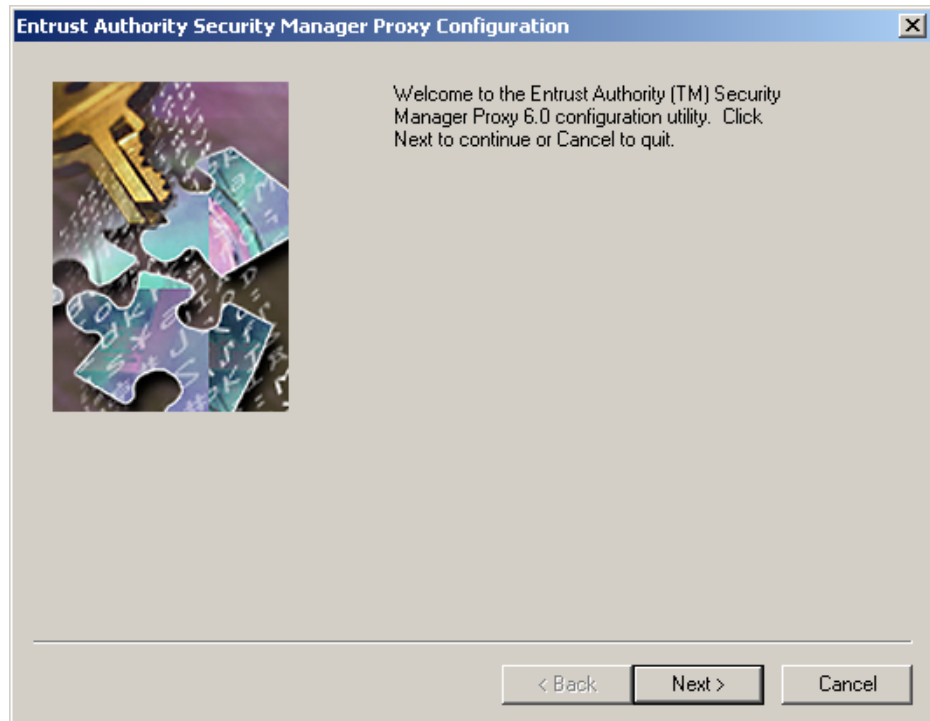
- 5 A success message appears. Click *OK* to complete the Proxy configuration.

### To configure Security Manager Proxy on the server side

- 1 Do one of the following:
  - If you selected *Run Security Manager Proxy Configuration now* when you finished installing Security Manager Proxy, go to Step 2 on page 41.
  - If you are starting the Security Manager Proxy 6.0 Configuration Utility now, click *Start > Programs > Entrust > Entrust Authority Security Manager Proxy > Proxy Configuration*.

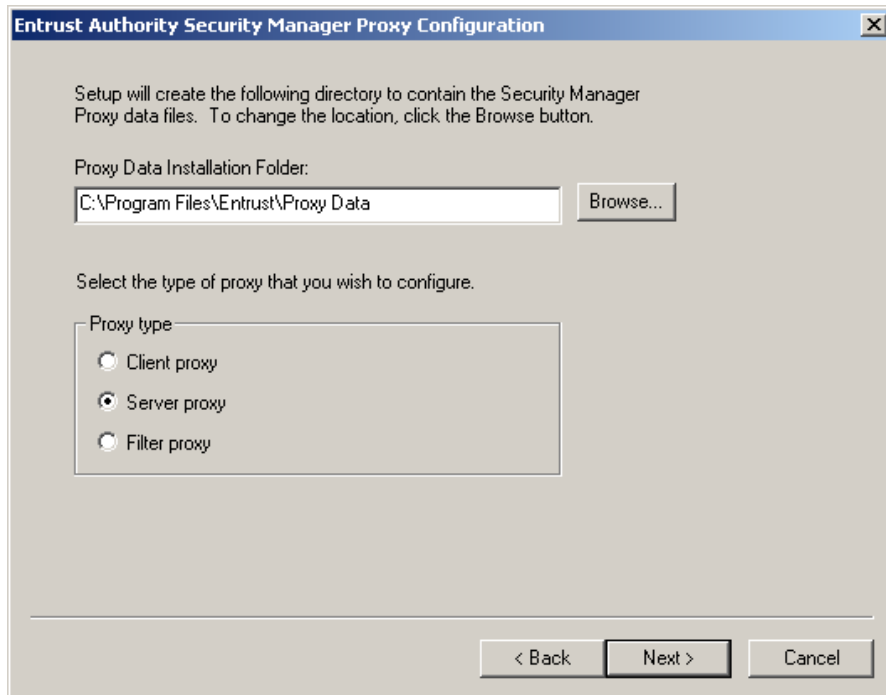


- 2 The Entrust Authority Security Manager Proxy Configuration utility appears.



Click *Next*.

**3** The following dialog box appears.



Either accept the default folder location for where Security Manager Proxy data files will be installed, or click *Browse* to specify a different folder location.

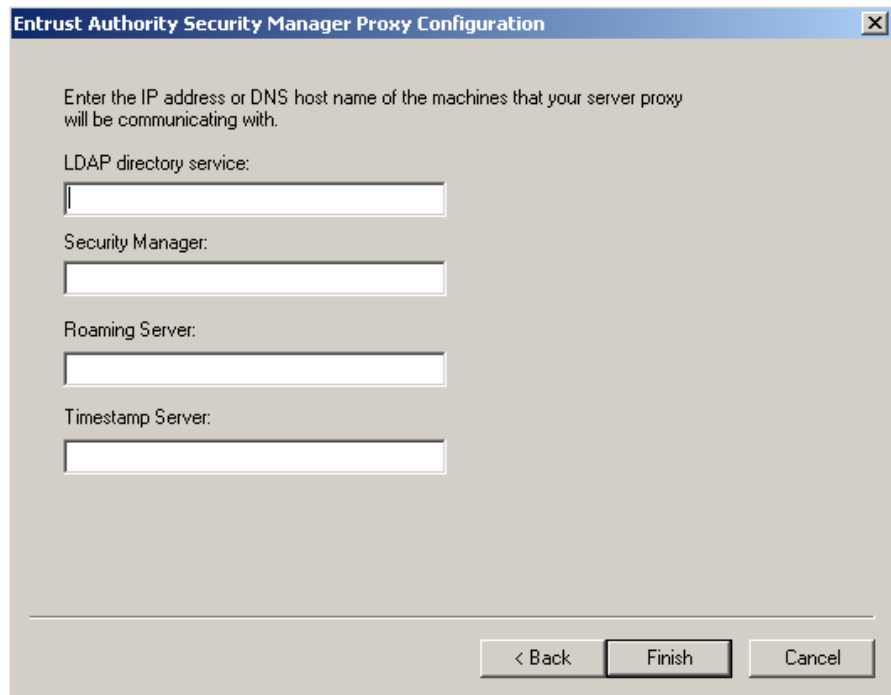
Select *Server proxy* as the Proxy type, and click *Next*.

---

**Note:** Retain the \Entrust\Proxy Data part of the pathname if you change the folder location from the default.

---

- 4 The following dialog box appears.



Enter the IP addresses or DNS host names of the servers that host, respectively, the LDAP Directory service, Entrust Authority Security Manager, Entrust Authority Roaming Server, and Entrust Authority Timestamp Server.



**Attention:** For security reasons, the use of IP addresses is recommended over the use of DNS domain names.

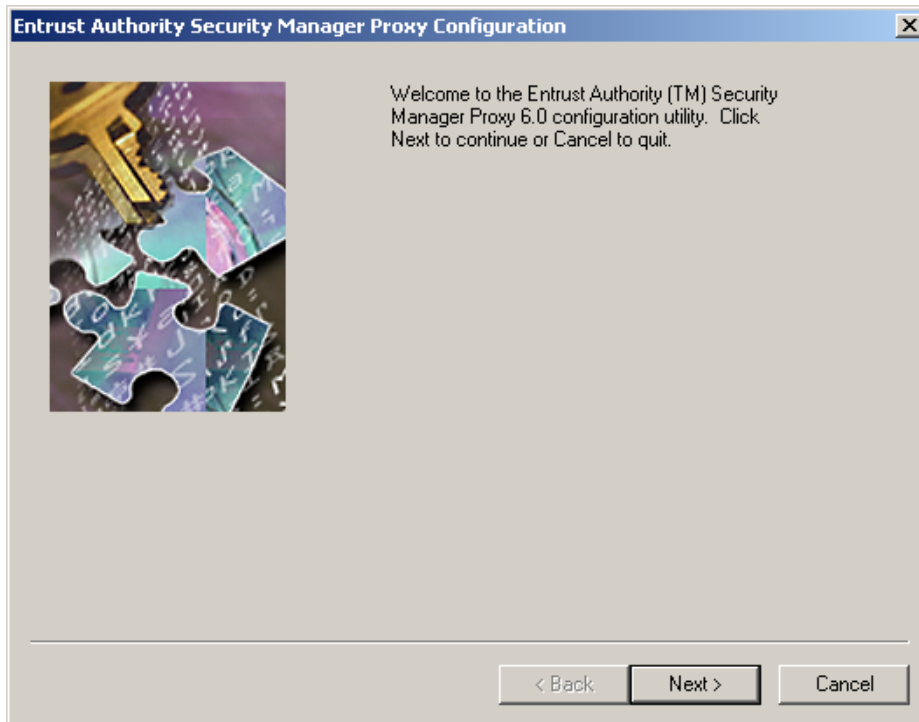
If you are not configuring the Proxy for one or some of these servers, leave the field blank for those servers.

- 5 When you have filled in all the fields, click *Finish*. A success message appears. Click OK to complete the Proxy configuration.

### To configure Security Manager Proxy as a filter

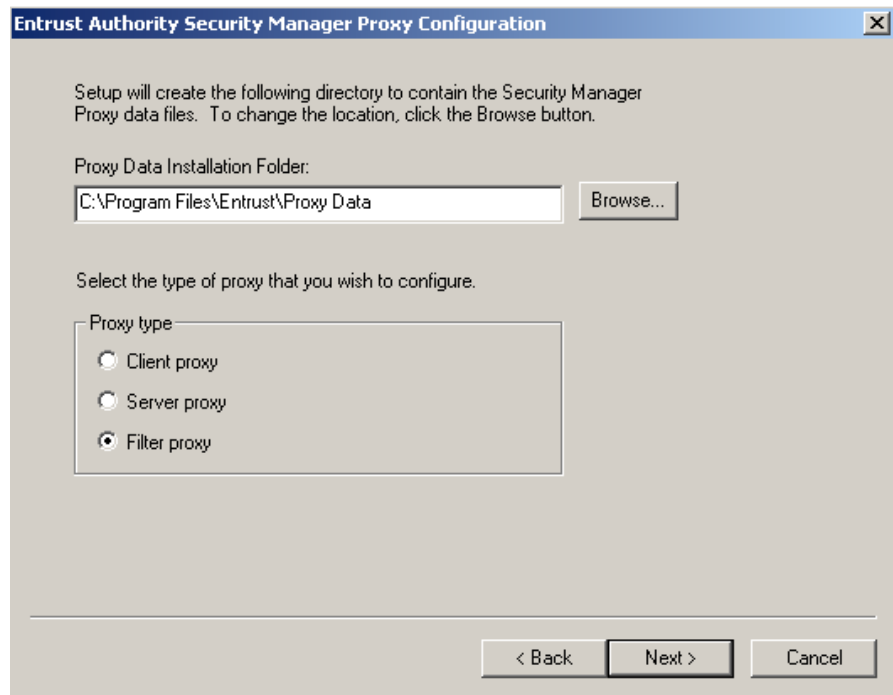
- 1 Do one of the following:
  - If you selected *Run Security Manager Proxy Configuration now* when you finished installing Security Manager Proxy, go to Step 2 on page 44.

- If you are starting the Security Manager Proxy 6.0 Configuration Utility now, click *Start > Programs > Entrust > Entrust Authority Security Manager Proxy > Proxy Configuration*.
- 2** The Entrust Authority Security Manager Proxy Configuration utility appears.



Click *Next*.

- 3 The following dialog box appears.



Either accept the default folder location for where Security Manager Proxy data files will be installed, or click *Browse* to specify a different folder location.

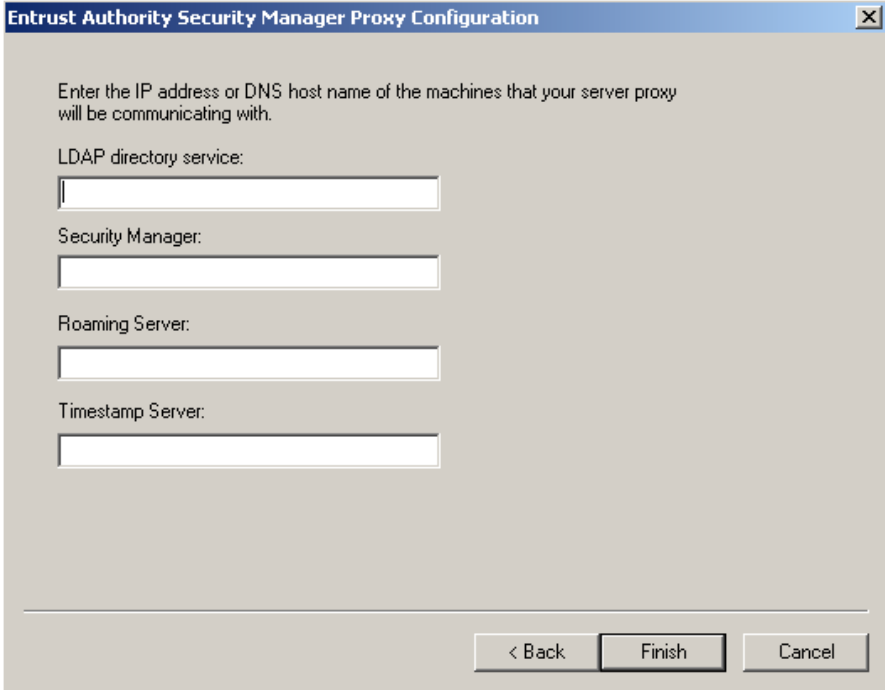
Select *Filter proxy* as the Proxy type, and click *Next*.

---

**Note:** Retain the \Entrust\Proxy Data part of the pathname if you change the folder location from the default.

---

- 4 The following dialog box appears.



Entrust Authority Security Manager Proxy Configuration

Enter the IP address or DNS host name of the machines that your server proxy will be communicating with.

LDAP directory service:

Security Manager:

Roaming Server:

Timestamp Server:

< Back Finish Cancel

Enter the IP addresses or DNS host names of the servers that host, respectively, the LDAP Directory service, Entrust Authority Security Manager, Entrust Authority Roaming Server, and Entrust Authority Timestamp Server.



**Attention:** For security reasons, the use of IP addresses is recommended over the use of DNS domain names.

If you are not configuring the Proxy for one or some of these servers, leave the field blank for those servers.

When you have filled in all the fields, click *Finish*.

- 5 A success message appears. Click OK to complete the Proxy configuration.

# Configuring your clients

Use the information in this section to make the final configuration changes for your Proxy implementation.

Instead of pointing directly at an Entrust CA or an LDAP Directory, clients must point to the Client Proxy. There are two ways of having your clients communicate through the Client Proxy: by modifying each client's `entrust.ini` file, or through DNS host name resolution.

## Entrust.ini file changes

To point clients to the Client Proxy using the `entrust.ini` file, modify the following entries in the `entrust.ini` file:

[Entrust Settings]

```
Authority=IP_address_or_DNS_name_of_client-side_Security_Manager_Proxy +  
port_number  
Manager=IP_address_or_DNS_name_of_client-side_Security_Manager_Proxy +  
port_number  
Server=IP_address_or_DNS_name_of_client-side_Security_Manager_Proxy +  
port_number  
ProfileServer=IP_address_or_DNS_name_of_client-side_Security_Manager_Proxy +  
port_number
```

[ASH Information Section]

```
ASHServer=IP_address_or_DNS_name_of_client-side_Security_Manager_Proxy  
ASHPort=ASH_port_number
```

The default port numbers for the above servers are as follows:

- Authority default port is 829
- Manager default port is 709
- Server (as in, the LDAP server) default port is 389
- ASH server default port is 710
- Roaming server default port is 640

---

**Note:** Roaming Server was formerly referred to as the Profile Server.

---

If you change any of the default listen ports for the client-side Proxy, you must change the port numbers in the `entrust.ini` file to reflect this change.

---

**Note:** If you are using Timestamp Server, see “Configuring for Entrust Authority Timestamp Server” on page 70.

---

## DNS Host Name Resolution

You can also use DNS host name resolution to point clients to the Client Proxy. This is useful if you already have a large number of installed clients that would require the above-mentioned modifications to their `entrust.ini` file. Procedures for setting up, using, and modifying DNS host names are beyond the scope of this document.



**Attention:** For security reasons, the use of IP addresses is recommended over the use of DNS domain names.

---



# Chapter 5

## Security Manager Proxy administration

This chapter describes several common administrative tasks for Security Manager Proxy 6.0. It includes the following sections:

- “Administering Security Manager Proxy” on page 50
- “Monitoring Security Manager Proxy log activity” on page 52

# Administering Security Manager Proxy

To perform normal administrative tasks for Security Manager Proxy, use SFOAM. SFOAM is a command line application that allows you to start and stop the Proxy, check status, and create and remove Proxy instances.

## To use SFOAM

Operating System	Do the following...
Solaris	Enter the following in terminal window: <b>sfoam</b>
Windows	Navigate to the following folder in a command line window:  C:\Program Files\Entrust\Proxy 6.0\bin  Enter your SFOAM commands while in this directory.

The SFOAM application starts.

**Note:** For Solaris installations, you must indicate to SFOAM the location of the Proxy Data directory. To do this, navigate to the Proxy Data directory for your installation before entering an SFOAM command.

Alternatively, you can indicate the location of the Proxy on the machine when entering your SFOAM command. Use the following syntax:

```
sfoam -datdir data_directory SFOAM command
```

where data\_directory is the absolute path for the Proxy Data directory.

## To administer Proxy using SFOAM

With the SFOAM application running in a terminal window, enter any of the following SFOAM commands to administer the Proxy:

Command	Description
status	Use the status command to return status information about a running server. This option is only available for Solaris systems.
start	Use the start command to start the Proxy.

Command	Description
stop	Use the stop command to stop the Proxy.
create <sup>1</sup>	Use the create command to create an instance of a Proxy. The only parameter is directoryName- the name of the directory where the data files will be stored
remove <sup>2</sup>	Use the remove command to remove an instance of a proxy server from the system. The parameters are: directoryName- The directory where the data files are contained all- Use this flag to remove all servers. removedata- Use this flag to have the server data files removed from the system.

1. The create command should only be used by advanced users.

2. The remove command should only be used by advanced users.

### To use the Services application for Windows

In addition to using the SFOAM application to administer the Proxy, Windows users can also use the Services application. To open Services, go to Start > Administration Tools > Services. Right click on the "Entrust Authority Security Manager Proxy" item. Several options are displayed to start, stop, pause, resume and restart the Proxy.

Click the option to want to perform. The Service application displays the new status in the Status column in the item name row.

# Monitoring Security Manager Proxy log activity

You can check Security Manager Proxy performance by opening the following file in a text editor:

```
data_directory\proxy.log
```

where “*data\_directory*” is the directory where Security Manager Proxy was installed—for example, “*/opt/entrust/proxy data*”.

The *proxy.log* file contains the following information on how the application is functioning:

- Thread ID
- Process ID
- Priority
- Date, Time, microsecond time, time zone
- Source file, line

For advanced configuration information, see “Configuring the *proxy.log* file” on page 71.

# Chapter 6

## Advanced configuration

This chapter describes how to perform advanced configuration for the Security Manager Proxy 6.0. It includes the following sections:

- “Understanding the config.tcl file” on page 54
- “Configuring for TLS” on page 56
- “Creating Entrust profiles for Security Manager Proxy” on page 58
- “Using Server Login with Security Manager Proxy” on page 59
- “Configuring for Authenticated LDAP” on page 62
- “Configuring for specific firewalls” on page 64
- “Configuring for HTTP Proxies” on page 65
- “Configuring for multiple CAs/Servers” on page 67
- “Configuring for Entrust Authority Timestamp Server” on page 70
- “Configuring the proxy.log file” on page 71

# Understanding the config.tcl file

All advanced configuration changes for Client and Server Proxies are performed by editing variables in the config.tcl file. The config.tcl file is a script that is executed each time the proxy is started, and is configured by administrators in a text editor.

## Config.tcl file location

The config.tcl file is located in the Proxy data directory. It is found at the following path for Solaris (by default):

```
/opt/entrust/proxy_data/proxy1
```

The config.tcl file is found at the following path for Windows (by default):

```
c:\program files\Entrust\Proxy Data
```

---

**Attention:** Do not edit the config.tcl file found in the <installation directory>/etc directory.

---

## Adding and modifying variables

To enter a new or modify an existing variable in the config.tcl file, use the following syntax:

```
set variable_name value
```

---

**Note:** All variables are case-sensitive.

---

Variable values are represented by a string or numeric data. Enter numeric data directly, with no manipulations. For example:

```
set sf.log.level 6
```

If the variable requires a string, enter it using quotation marks. For example:

```
set proxy.srv.ldap.host "localhost"
```

If the variable string is a filename path, always use a forward slash (/) to separate directories—even if it is a Windows implementation. For example:

```
set sf.tls.epffile "c:/entrust/proxy data/epf/jimsmith.epf"
```

Enter each variable on its own line in the config.tcl file. The following is a sample config.tcl file:

```
set sf.servicename sfproxyserver7
set proxy.srv.ldap.host "localhost"
```

```
set proxy.srv.ldap.port 391
set proxy.srv.cmp.host "host5"
set proxy.srv.sep.host ""
set proxy.srv.ash.host "host5"
set sf.log.level 6
```

---

**Note:** For detailed information on all config.tcl variables, see “Security Manager Proxy variables” on page 77.

---

# Configuring for TLS

It is sometimes necessary to send confidential information over the Internet to communicate with the CA or other Entrust back-end servers. For example, in order to gain access and search the Directory, you have to send your Entrust credentials using the Authenticated LDAP protocol. Such sensitive information, if encapsulated as HTTP, is vulnerable to outside attacks or network “sniffers”.

To send sensitive information more securely, use TLS instead of HTTP. TLS provides channel-oriented encryption security for packets sent in the clear over the Internet.

Use the following procedure to configure Security Manager Proxy 6.0 to work with TLS.

---

**Note:** By default, most firewall configurations allow TLS traffic through on port 443 only.

---

## To configure Proxy for TLS

- 1 Add the following variables (if not already present) to the Client Proxy config.tcl file:

Variable Name	Description
sf.tls.epfFile	This variable sets the file name for the Entrust profile for the Client Proxy.
sf.tls.epfPassword	This is the password you must supply for your Entrust profile if you are not using Server Login while tunnelling over TLS.  <b>NOTE:</b> This variable is only necessary if you are not using Server Login. For information on Server Login, see “Using Server Login with Security Manager Proxy” on page 59.
sf.tls.epfConfiguration	Use this variable to inform the client of the location of the entrust.ini file if you are using an offline connection to the Directory.
proxy.cli.<protocol>.tunneltls	This variable sets the protocol to be tunnelled over TLS

- 2 Save the file, and restart the Client Proxy.



- 3** Add the following variables (if not already present) to the Server Proxy config.tcl file:

Variable Name	Description
sf.tls.epfFile	This variable sets the file name for the Entrust profile for the Server Proxy.
sf.tls.epfPassword	This is the password you must supply for your Entrust profile if you are not using Server Login while tunnelling over TLS.  <b>NOTE:</b> This variable is only necessary if you are not using Server Login. For information on Server Login, see “Using Server Login with Security Manager Proxy” on page 59.
sf.tls.epfConfiguration	Use this variable to inform the client of the location of the entrust.ini file if you are using an offline connection to the Directory.
proxy.srv.tunneltls	This variable sets all protocols that are to be tunnelled over TLS.  <b>NOTE:</b> Setting to “Idapauth” requires specific configuration. See “Configuring for Authenticated LDAP” on page 62.
proxy.srv.tunnelhttp	Set this to variable to zero (0) if you want the Server Proxy to reject all non-TLS traffic.

- 4** Save the file, and restart the Server Proxy.
- 5** Depending on your configuration, you can also add the following optional variables:
- sf.tls.isOfflineLogin
  - sf.tls.acceptAlgorithms
  - sf.tls.clientAuthenticationRequired
  - sf.tls.updateProfileProgram
  - sf.tls.forceStandardsCompliance

---

**Note:** For detailed information on all config.tcl variables, see “Security Manager Proxy variables” on page 77.

---

# Creating Entrust profiles for Security Manager Proxy

To use TLS, create Entrust End User profiles for both the Client and Server Proxies using Entrust Authority Security Manager Administration (formerly Entrust/RA). Use the following procedure to create End User profiles for the Proxy.

## To create Entrust profiles for the Proxy

- 1 Log in to Security Manager Administration as an administrator.
- 2 Create a copy of the End User Policy. Rename it "Proxy Policy".

---

**Note:** To configure the Proxy policy for Server Login, see "Using Server Login with Security Manager Proxy" on page 59.

---

- 3 Click OK to save the new policy.
- 4 Create a new role, call it "Proxy Role".
- 5 Assign the "Proxy" Policy to the new role.
- 6 Add a new user, call it "Client Proxy".
- 7 Assign the "Proxy Role" to the new user.
- 8 Create a profile for the user in Security Manager Administration.
- 9 Repeat Step 1 to Step 6 for the Server Proxy.

---

**Note:** For full details on creating a user in Security Manager Administration, see "Adding a user" in *Using Entrust/PKI 6.0 on UNIX* or *Using Entrust/PKI 6.0 on Windows*.

---

---

**Note:** For full details on creating user policies and roles in Security Manager Administration, see "Customizing Entrust/PKI" in *Administering Entrust/PKI 6.0 on UNIX* or *Administering Entrust/PKI 6.0 on Windows*.

---

# Using Server Login with Security Manager Proxy

Entrust Server Login addresses the requirement for an application to access Entrust credentials, without the need for manual or biometric authentication. Server Login is designed for computers, usually servers, that run Entrust applications as services or as background applications. These computers, running 24 hours a day, seven days a week, do not have a user continuously present and are often in a physically secure area with restricted access.

Using Server Login, Security Manager Proxy allows you to create a TLS connection without writing your password in the Entrust.ini file. During login, Server Login verifies that it is operating on an authorized machine to prevent the Entrust profile being used on a computer to which it has not been bound. If a user's policy certificate specifies that Server Login cannot be used, it will display a message stating that the user is not authorized to use Server Login.

---

**Note:** The Server Login feature is not recommended for use on desktop computers.

---

The following is a high-level overview of the steps required to set up Server Login to work with Security Manager Proxy.

- Create a new policy or modify an existing policy in Security Manager Administration in which the “Permit Server Login usage” policy setting is enabled. See “To enable Server Login usage in an Entrust user policy” on page 59.
- Create a new role or choose an existing role and associate that role with the newly created or modified user policy. See “To associate a role with a Server Login-enabled user policy” on page 60.
- Install Server Login. See “To install Server Login for Windows” on page 61.
- Create profiles for use with Security Manager Proxy, specifying the appropriate Server Login-enabled role during the profile creation process. See “Creating Entrust profiles for Security Manager Proxy” on page 58.
- Bind those profiles to the Security Manager Proxy server using the Server Login binder application.

## To enable Server Login usage in an Entrust user policy

- 1 Decide whether you want to create a new policy or modify an existing one.
- 2 Log in to Security Manager Administration as a Security Officer or as an administrative user with the appropriate Security Policy permissions.

- 3 In the tree view, expand Security Policy, and then expand User Policies.  
If you are creating a new policy, you can right-click on the end user policy and click Copy in the pop-up menu, or you can right-click on User Policies and click New in the pop-up menu.  
If you are modifying an existing policy, click the desired policy in the tree view.
- 4 Scroll down to the *Permit Server Login usage* setting and select the check box to enable it.  
If you are creating a new or copied policy, fill in the *Label* and *Common name* fields as well.
- 5 Click *Apply*.  
You have now finished enabling Server Login usage in an Entrust user policy.  
For more information on user policies, refer to *Administering Entrust/PKI 6.0 on UNIX* or *Administering Entrust/PKI 6.0 on Windows*.

### **To associate a role with a Server Login-enabled user policy**

- 1 Decide whether you want to create a new role or use an existing one.

---

**Note:** If you have only modified a user policy (as opposed to creating or copying a new user policy), and if you are using an existing role (rather than creating a new role), then you do not need to carry out the steps in this procedure, because your existing role will have had its user policy enabled for Server Login usage when you carried out the steps in “To enable Server Login usage in an Entrust user policy” on page 59.

---

- 2 Log in as a Security Officer or as an administrative user with the appropriate Roles permissions.
- 3 In the tree view, expand Security Policy, and then expand Roles.  
If you are using an existing role, skip to Step 5.  
If you are creating a new role, right-click on an end user role and click Copy in the pop-up menu.
- 4 Enter a name for the new role in the *Unique name* field. If you want to modify any of the permissions for this role, you can also do so now.
- 5 Associate the role with the appropriate user policy (that is, the policy that was created or modified in “To enable Server Login usage in an Entrust user policy” on page 59) by selecting the appropriate policy in the *User Policy* drop-down list on the Role property page.
- 6 Click *Apply*.  
You have now finished associating a role with Server Login-enabled user policy.

For more information on roles, refer to *Administering Entrust/PKI 6.0 on UNIX* or *Administering Entrust/PKI 6.0 on Windows*.

### **To install Server Login for Solaris**

- 1** Copy the package to your chosen installation directory, for example:  
`/local/entrust/Uncompress`
- 2** Untar the package using the following command  
`zcat packagename | tar xvf -`
- 3** Use the “chown” and “chgrp” commands with flag -R to change the owner and group attributes of the directory (if necessary).
- 4** Check that the permissions of the directory and its contents match your requirements.
- 5** The user must add the following to their PATH environment variable:  
`serverlogin_install_directory/bin`  
where “serverlogin\_install\_directory” is the directory where Security Manager Proxy was installed.
- 6** The user who owns the installation of Security Manager Proxy must add the following to their LD\_LIBRARY\_PATH environment variable:  
`serverlogin_install_directory/lib`  
where “serverlogin\_install\_directory” is the directory where Server Login was installed.

### **To install Server Login for Windows**

- 1** Log into the server that will host the component with which you will use Server Login.
- 2** Insert the Security Manager Proxy 6.0 CD, and from the Server Login directory, run `ettksrverlogin-6_0-win.EXE`.
- 3** Follow the prompts in the installation wizard.  
You have now installed Server Login.
- 4** Be sure to read the Server Login release notes, which contain important information not covered here. To access the release notes, click Start > Programs > Entrust Toolkit > Server Login > Release Notes.  
You are now ready to perform the next step in setting up Server Login. See “Using Server Login with Security Manager Proxy” on page 59 for a list of these steps.

# Configuring for Authenticated LDAP

By default, the following configuration is set for LDAP communications with Entrust back-end servers:

- The Client Proxy accepts anonymous-only LDAP requests on port 389, and encapsulates them in HTTP for transport over the Internet and through the firewall
- The Server Proxy, listening for the packets on port 80, accepts, unwraps and forwards the packets to the destination server

Anonymous LDAP communication with the Directory allows you read-only access to system information. If you require authorized access to the Directory with full read/write privileges, configure both the Client and Server Proxies for authenticated LDAP.

---

**Note:** Authenticated LDAP communicate must take place over TLS connections only. To configure your Proxies for TLS, see “Configuring for TLS” on page 56.

---

## To configure the Proxy for Authenticated LDAP

- 1 On the Client Proxy workstation, open the config.tcl file in a text editor.
- 2 If not present, add the following line:

Variable Name	Description
<code>set proxy.cli.ldapauth.tunneltls 1</code>	This setting instructs the Client Proxy to tunnel the authenticated LDAP packets over TLS instead of HTTP.

---

**Note:** By default, the Client Proxy listens for authenticated LDAP requests on port 1389. To change this port setting, edit the variable “proxy.cli.ldapauth.port” in the config.tcl file. For more information, see “Security Manager Proxy variables” on page 77.

---

- 3 Save the file, and restart the Client Proxy.
- 4 On the Server Proxy workstation, open the config.tcl file in a text editor.

- 5 If not present, add the following lines:

Variable Name	Description
<code>set proxy.srv ldapauth.tunneltls 1</code>	This setting instructs the Server Proxy to allow for authenticated LDAP binds to the Directory and other back-end servers.

- 6 Save the file, and restart the Server Proxy.

---

**Note:** For detailed information on all Security Manager Proxy variables, see “Security Manager Proxy variables” on page 77.

---

# Configuring for specific firewalls

The default configuration for both the Client and Server Proxy encapsulates supported protocols as HTTP or TLS for access through firewall ports 80 or 443. For most firewalls, this configuration provides unimpeded access to the Server Proxy and back-end servers. In these cases, no changes to the HTTP header information is required.

For some firewall configurations, however, it may be necessary to alter the HTTP header information on the Client Proxy. Use the following procedure to make the necessary changes.

## To configure HTTP headers for specific firewalls

- 1** On the client-side workstation, open the config.tcl file in a text editor.
- 2** If not present, add the following variables.
  - set sf.http.requestURL
  - set sf.http.contentType
  - set sf.http.statusResult
  - set sf.http.useragent
  - set sf.http.server
- 3** If an attempted connection gets rejected by the firewall, configure these variables based on the error data in your firewall logs or proxy.log file.

---

**Note:** For detailed information on the proxy.log file, see “Configuring the proxy.log file” on page 71.

---

- 4** Save the file, and restart the Proxy.

---

**Note:** For detailed information on all Security Manager Proxy variables, see “Security Manager Proxy variables” on page 77.

---



# Configuring for HTTP Proxies

If your network architecture contains HTTP proxies on either the client or server-sides, some Client or Server Proxy configuration changes may be required.

## HTTP proxies between the Client Proxy and the Internet

To allow Client Proxy traffic to communicate with the CA or back-end servers through an HTTP proxy on the client side, you may have to make some or all of the following configuration changes.

### To configure for access through a client-side HTTP proxy

Add the following lines to the Client Proxy config.tcl file to allow the Client Proxy packets to proceed through the HTTP proxy:

- `set proxy.cli.host HTTP_proxy_IP_address_or_DNS_host_name`
- `set proxy.cli.port HTTP_proxy_port`
- `set sf.http.requestURL Server_Proxy_IP_address_or_DNS_host_name`

### To configure for authentication on a client-side HTTP proxy

Add the following lines to the Client Proxy config.tcl file if the HTTP proxy requires Basic Authentication:

- `set sf.http.authname(authentication domain) username`
- `set sf.http.authpasswd(authentication domain) password`

If the domain contains a space, encase the variable in braces. For example:

- `set {sf.http.authpasswd(new business.com)} password`

---

**Note:** If the HTTP proxy uses NTLM authentication, no config.tcl changes are required. NTLM uses the Windows user credentials for the current Proxy user.

---

## HTTP proxies between the Internet and the Server Proxy

To allow traffic from the Server Proxy to reach destination clients through an HTTP proxy on the server side, you may have to make some or all of the following configuration changes.

### To configure for access through a server-side HTTP proxy

If the HTTP proxy is on the Server Proxy side, no config.tcl changes are required as the HTTP proxy should automatically forward all packets to the specified destination.

### To configure for authentication on a server-side HTTP proxy

On the server side, use only Basic Authentication. To configure for Basic Authentication on the HTTP proxy, add the following changes to the Client Proxy config.tcl:

- `set sf.http.authname(web domain) <username>`
- `set sf.http.authpasswd(web domain) <password>`

If the domain contains a space, encase the variable in braces. For example:

- `set {sf.http.authpasswd(new business.com)} <password>`

Add these two settings for each domain. To use the same passwords for each web domain, enter (\*) for the web domain for each of the config.tcl variables above.

---

**Note:** For detailed information on all Security Manager Proxy variables, see “Security Manager Proxy variables” on page 77.

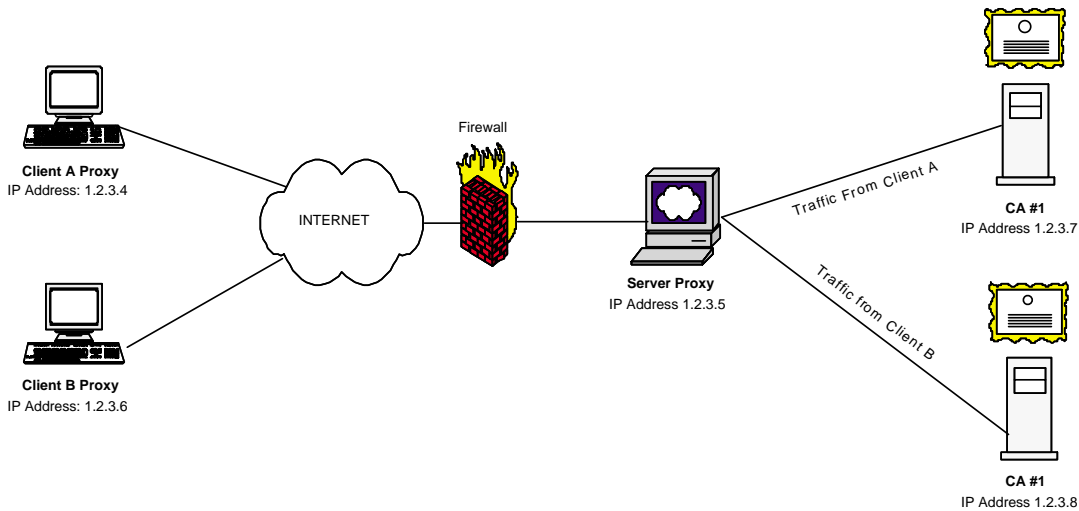
---

# Configuring for multiple CAs/Servers

Depending on your implementation of Entrust Authority Security Manager, you may have one Server Proxy that needs to distribute packets from different client machines to several different CAs or back-end servers. To allow one or more clients to communicate with multiple CAs or back-end servers, specific variables must be configured for both the Client and Server Proxy config.tcl files.

As an example, consider that Clients A and B need to communicate over the Internet with different CAs through the same Server Proxy. Both clients are tunnelling the CMP protocol over HTTP through the firewall.

**Figure 4:** Communicating with multiple CAs through one Server Proxy



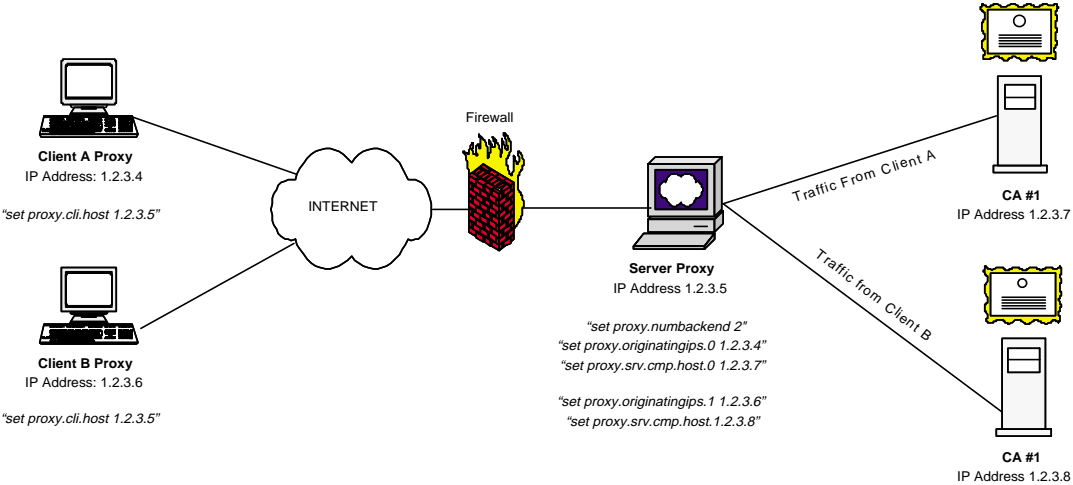
To ensure the Server Proxy forwards CMP packets to the intended CA destination, make the following changes to the config.tcl file for each Proxy:

Proxy	Config.tcl file change required
Client A Proxy	Add the following line: set proxy.cli.host 1.2.3.5

Proxy	Config.tcl file change required
Client B Proxy	Add the following line:  <pre>set proxy.cli.host 1.2.3.5</pre>
Server Proxy	Add the following lines:  <pre>set proxy.numbackend 2 set proxy.originatingips.0 1.2.3.4 set proxy.srv.cmp.host.0 1.2.3.7 set proxy.originatingips.1 1.2.3.6 set proxy.srv.cmp.host.1 1.2.3.8</pre>

These settings instruct the Client Proxies to send the CMP packets to the Server Proxy, and the Server Proxy to take all CMP messages from Client A to CA #1, and from Client B to CA #2.

**Figure 5:** Variable assignments for multiple CA communication



### To configure the Proxy for multiple CAs or Servers

- 1 Add the following variable to the Client Proxy config.tcl file:  

```
set proxy.cli.host host_IP_address
```

This variable sets the intended destination server IP address for packets sent from this client machine.
- 2 Save the file.

**3** Add the following variables to the Server Proxy config.tcl file:

Variable Name	Description
<code>proxy.numbackend #</code>	This variable sets the number of possible back-end server destinations.
<code>proxy.originatingips.X IP address</code>	This variable sets the originating IP address for the data packet. "X" represents the number (starting at zero) indicating the originating IP address with which it is linked.
<code>proxy.srv.&lt;protocol&gt;.host.X host IP address</code>	This variable sets the server IP address where data packets of a specific protocol from that originating IP address are to be forwarded. "X" represents the number (starting at zero) indicating the originating IP address with which it is linked.

**4** Save the file.

**5** Restart both the Client and Server Proxies.

---

**Note:** For detailed information on all Security Manager Proxy variables, see "Security Manager Proxy variables" on page 77.

---

# Configuring for Entrust Authority Timestamp Server

Unlike the other protocols used to communicate with Entrust products, the Timestamp protocol requires no modifications to the client `entrust.ini` file. However, in order for the client to communicate with the Timestamp Server, the CA must have access to the `enttimestamp.ini` file in its local directories.

The `enttimestamp.ini` file contains the IP address (or DNS name) of the server hosting the Timestamp Server, with an optional port specification (the default is 309). To grant timestamp access to a client-side Proxy, the Proxy IP address must be added to the `enttimestamp.ini` file. Add the following section and line:

```
[Timestamp Servers]
default=clientproxyIPaddress
```

where `clientproxyIPaddress` is the IP address for the Client-side Proxy workstation.

For more information on Timestamp Server, see the *Entrust/Timestamp 4.0 User Guide*.

# Configuring the proxy.log file

## Configuring the number and size of log files

To change the number and size of proxy.log files, configure specific variables in the config.tcl file.

If not already present, add the following variables in the config.tcl file:

Variable Name	Description
sf.log.filemax	The value for sf.log.filemax controls the maximum size (in kilobytes) for the proxy.log file before a new one is started automatically by the system.  The default value is 50.
sf.log.numfiles	The value for sf.log.numfiles controls the maximum number of extra log files the system automatically creates when required. When a current log file size is reached, a new log file is started.  The default value is 2.  When the last allowable file has been created, the Proxy deletes the oldest file and a new one is started in its place.

## Configuring the log file detail

To modify the level of detail delivered in your proxy.log file, add a specific variable to your config.tcl file. If not already present, add the following variable in the config.tcl file:

```
sf.log.level
```

This variable defines the level of detail displayed in the log. The value is from 1 to 10, where 1 displays the least detail and 10 the most detail.





# Chapter 7

## Uninstalling Security Manager Proxy

This chapter describes how to uninstall Security Manager Proxy 6.0 and its associated files from your system. It includes the following sections:

- “Uninstalling Security Manager Proxy on Solaris” on page 74
- “Uninstalling Security Manager Proxy on Windows” on page 75

# Uninstalling Security Manager Proxy on Solaris

Use the following procedure to uninstall Security Manager Proxy 6.0 on Solaris.

## To uninstall Proxy on Solaris

- 1 Ensure you are logged in as root, and that all Proxy services are stopped.
- 2 From the .../etc directory where Security Manager Proxy was installed (for example, /opt/entrust/proxy6.0/etc), run the following command:

```
./uninstall.sh
```

The following message appears:

```
/opt/Entrust/proxy6.0 will be removed. Are you sure you want to  
continue (yes/no)?
```

- 3 Type "yes", and press Enter.

The following message appears:

```
The Entrust Proxy uninstallation is complete.
```

---

**Note:** Uninstalling the Proxy removes the Proxy Server application, but does not delete any Proxy log information that already exists. To remove all existing Proxy log data from your machine, delete the following folder:

```
installation_directory/Proxy Data
```

---

# Uninstalling Security Manager Proxy on Windows

Use the following procedure to uninstall Security Manager Proxy 6.0 on Windows.

## To uninstall Proxy on Windows

- 1 Close all open windows on the Proxy machine.
- 2 Select Start > Settings > Control Panel > Add/Remove Programs.
- 3 Select Entrust Authority Security Manager Proxy, and click *Change/Remove*.
- 4 Click *Next*. The following screen asks if you would like to keep your Proxy server data.  
Click Yes. The uninstallation process starts.
- 5 When the process is finished, the following screen displays:



Click *Finish*.



# Appendix A

## Security Manager Proxy variables

This section contains a reference table that lists all of the variables that can be modified in the config.tcl file to configure the Security Manager Proxy. This table includes the variable names, the value type (Integer, String or Boolean), and a description of each variable.

---

**Note:** For information on modifying the config.tcl file, see “Understanding the config.tcl file” on page 54.

---

Variable Name	Value Type	Description
sf.reader.readtimeout	Integer	<p>This variable specifies the maximum time (in seconds) that the Proxy waits on a read operation from a connected client without receiving data.</p> <p>If the Proxy receives data after the maximum time has elapsed, the connection is disconnected.</p> <p>Default Value = 5</p>
sf.readtimeout	Integer	<p>This variable specifies the maximum time (in seconds) that the Proxy waits on a read operation from a connected client to a secondary server without receiving data.</p> <p>If the Proxy receives data after the maximum time has elapsed, the connection is disconnected.</p> <p>Default Value = 60</p>
sf.idletimeout	Integer	<p>This variable specifies the maximum amount of time (in seconds) that an application may remain connected to a server port without transmitting a request. If this time period elapses with no requests, the connected client is disconnected.</p> <p>Default Value = 0</p>
sf.maxbuf	Integer	<p>This variable specifies the maximum internal buffer size (in bytes) that is allocated for message processing. Incoming requests that require buffers larger than this are rejected.</p> <p>Default Value = 8 * 1024 * 1024</p>
sf.qsize	Integer	<p>This variable specifies the maximum number of messages which can be internally queued processing. Requests received when the service queue is full will be rejected. Larger queues may improve the ability to handle longer bursts of incoming request at rates in excess of the service rate. Too large a setting may result in the response time being too long and cause clients to timeout.</p> <p>Default Value = 100</p>

Variable Name	Value Type	Description
sf.watchdog	Integer	<p>This variable specifies the maximum amount of time that a service operation may take to complete after processing begins. This setting protects against internal failures or hangs which could otherwise result in service outage.</p> <p>Default Value = 300</p>
sf.autoRestart	Integer	<p>This variable specifies the time period between automatic restarts of processes. The automatic restart feature provides protection against memory fragmentation or leak issues. Value of 0 disables this feature.</p> <p>Default Value = 86400</p>
sf.maxMemory	Integer	<p>[Solaris only] This variable specifies the maximum amount of memory that a process can allocate after starting up. If more than this amount of memory is allocated then the process will shut down (and be restarted). This feature provides protection against memory leaks.</p> <p>Default Value = 8388608</p>
sf.mon.restartsMax	Integer	<p>This variable specifies the time period between automatic restarts of processes. The automatic restart feature provides protection against memory fragmentation or resource leak issues. Value of 0 disables this feature.</p> <p>Default Value = 10</p>
sf.mon.restartOk	Integer	<p>This variable specifies the amount of time a process must be up for before it is assumed to have started successfully. If it fails within this period it is counted as a failed restart attempt.</p> <p>Default Value = 30</p>
sf.mon.restartMinDelay	Integer	<p>This variable specifies the delay between attempts to restart a process.</p> <p>Default Value = 10</p>
sf.mon.procStartTimeout	Integer	<p>This variable specifies the maximum amount of time to wait for a process to start up.</p> <p>Default Value = 30</p>

Variable Name	Value Type	Description
sf.tcp.backlog	Integer	This variable controls the maximum tcp backlog size for accepted connections. Larger values may be required to protect against syn-ack flooding attacks.  Default Value = 5
sf.tcp.linger	Integer	This variable specifies whether TCP sockets should remain open for the transmission of responses.  Default Value = 0
sf.ber.maxdepth	Integer	This variable limits the maximum nesting depth to accept when validating BER structures.  Default Value = 1024
proxy.*.maxlength	Integer	This variable specifies the generic maximum length of a packet for all pdus subject to the sf.maxbuf setting. This value is used as the default if it is not configured on a per protocol basis.  Default Value = 65536
proxy.CMP.maxlength	Integer	This variable specifies the maximum length of a PKIX-CMP request packet  Default Value = 65536
proxy.SEP.maxlength	Integer	This variable specifies the maximum length of an Entrust-SEP or proto-PKIX request packet.  Default Value = 65536
proxy.LDAP.maxlength	Integer	This variable specifies the maximum length of an LDAP request.  Default Value = 65536
proxy.Timestamp.maxlength	Integer	This variable specifies the maximum length of an Entrust-Timestamp packet.  Default Value = 65536
proxy.SPEKE.maxlength	Integer	This variable specifies the maximum length of an Entrust-SPEKE (Roaming) packet.  Default Value = 65536
proxy.ASH.maxlength	Integer	This variable specifies the maximum length of an Entrust-ASH (Roaming) packet.  Default Value = 65536



Variable Name	Value Type	Description
sf.http.header.maxlength	Integer	This variable controls the maximum length for HTTP headers. The minimum value is 256. Default Value = 1024
sf.http.body.maxlength	Integer	This variable controls the maximum length that a HTTP message body may be. Default Value = 65536
proxy.*.timeout	Integer	This variable specifies the maximum time (in seconds) for a client exchange to complete. If the exchange does not complete in this time then the back-end server connection will be dropped. This value is used as the default for all protocols if not configured specifically. Default Value = 60
proxy.CMP.timeout	Integer	This variable specifies the protocol exchange timeout for PKIX-CMP requests. Default Value = 60
proxy.SEP.timeout	Integer	This variable specifies the protocol exchange timeout for Entrust-SEP and proto-PKIX requests. Default Value = 60
proxy.SPEKE.timeout	Integer	This variable specifies the protocol exchange timeout for Entrust-SPEKE (Roaming) requests. Default Value = 60
proxy.ASH.timeout	Integer	This variable specifies the timeout for ASH connections. This should be no longer than the value configured at the CA. Default Value = 60
proxy.LDAPauth.timeout	Integer	This variable specifies the LDAP server connection timeout for non multiplexed LDAP connections. Default Value = 60
sf.tls.isOfflineLogin	Boolean	This variable specifies whether or not an offline login is allowed with the TLS profile. If this is 1, no attempts to connect to the directory will be made in order to retrieve revocation information, and TLS connections can be established even if revocation information is not available.

Variable Name	Value Type	Description
sf.tls.acceptAlgorithms	String	<p>This variable defines the accepted algorithms for use in TLS. This value can be any one or a list of any of the following:</p> <ul style="list-style-type: none"> <li>-RSA_WITH_IDEA_CBC_SHA: uses 1024-bit RSA with 128-bit IDEA</li> <li>-RSA_WITH_3DES_EDE_CBC_SHA: uses 1024-bit RSA with 168-bit triple DES</li> <li>-RSA_WITH_RC4_128_MD5: uses 1024-bit RSA with 128-bit RC4</li> <li>-RSA_WITH_RC4_128_SHA: uses 1024-bit RSA with 128-bit RC4</li> <li>-RSA_WITH_DES_CBC_SHA: uses 1024-bit RSA with 56-bit DES</li> <li>-RSA_EXPORT1024_WITH_DES_CBC_SHA: uses 1024-bit RSA with 56-bit DES</li> <li>-RSA_EXPORT1024_WITH_RC4_56_SHA: uses 1024-bit RSA with 56-bit RC4</li> <li>-RSA_EXPORT_WITH_RC4_40_MD5: uses 512-bit RSA with 40-bit RC4</li> <li>-RSA_EXPORT_WITH_DES40_CBC_SHA: uses 512-bit RSA with 40-bit DES</li> <li>-RSA_WITH_NULL_SHA: uses 1024-bit RSA with no encryption (data is sent as plaintext)</li> <li>-RSA_WITH_NULL_MD5: uses 1024-bit RSA with no encryption (data is sent as plaintext)</li> </ul> <p>} "string" {RSA_WITH_3DES_EDE_CBC_SHA} { min } { max }</p>
sf.tls.clientAuthenticationRequired	Boolean	This variable applies only to a server TLS connection. If this is 1, the server will require the client side of the connection to provide a verification certificate during the handshake.
sf.tls.epfFile	String	This variable points to the path of the epf file for use with TLS. This variable is required if TLS is to be used.
sf.tls.epfPassword	String	If you are not using Server Login while tunnelling over TLS, then you must supply the password for your EPF.

Variable Name	Value Type	Description
sf.tls.epfConfiguration	String	If you are using an offline connection to the Directory, use this variable to inform the client of the location of the entrust.ini file.
sf.tls.updateProfileProgram	String	
sf.tls.forceStandardsCompliance	Boolean	This variables determines whether or not standards compliance is required when using TLS. It could potentially be necessary to set this to 0 if some clients using TLS are not standards compliant and you wish them to interoperate use them with a proxy server.
sf.log.dir	String	This variable sets the directory location to store proxy.log files in.
sf.log.level	Integer	This variable sets the Logging level. Minimal logging is 0, verbose logging is 10. Default Value = 1
sf.log.filemax	Integer	The value for sf.log.filemax controls the maximum size (in kilobytes) for the proxy.log file before a new one is started automatically by the system. Default Value = 50.
sf.log.numfiles	Integer	The value for sf.log.numfiles controls the maximum number of extra log files the system automatically creates in addition to the existing proxy.log file. When a current log file size is reached, a new log file is started. Default Value = 2. When the last allowable file has been created, the Proxy deletes the oldest file and a new one is started in its place.
sf.log.filename	String	This variable specifies the name prefix for log files.
proxy.LDAP.errorcode	Integer	This variable defines the default error code to be used when a error message needs to be returned to a client because the message they sent was rejected by the proxy. Default Value = 50

Variable Name	Value Type	Description
proxy.LDAP.errormessage	String	This variable defines the default error text to be used when a error message needs to be returned to a client because the message they sent was rejected by the proxy.
proxy.LDAP.readonlyLDAPmessages	Boolean	When this variable is 1, all LDAP operations that have the ability to modify data in a directory are denied.
proxy.LDAP.anonymous	Boolean	When this variable is set to 1, only anonymous connections are made to a back end server. This variable overrides any other bind method.
proxy.LDAP.bindfail	Boolean	This variable determines if a client should receive a bind error message if they try to bind using a method that is stronger than the one currently being used by the server.
proxy.LDAP.simpledn	String	Set this variable if a simple bind DN should be used during binds to the back end directory.
proxy.LDAP.simplepassword	String	Set this variable to the password of the DN set with proxy.LDAP.simpledn if a simple bind DN should be used during binds to the back end directory.
sf.http.requestURL	String	This variable will be used as the URL in HTTP requests originating from an HTTP client.
sf.http.contentType	String	This variable will be used as the HTTP header Content-Type in HTTP requests.
sf.http.statusResult	Integer	This variable will be used as the as the status number in HTTP responses originating from an HTTP server.  Default Value = 200
sf.http.statusReason	String	This variable will be used as the as the status reason in HTTP responses originating from an HTTP server.
sf.http.useragent	String	This variable sets the value of User-Agent HTTP request header field.
sf.http.server	String	This variable sets the value of Server HTTP response header field.
sf.datdir	String	This variable sets the location of server instance data files. Note: read-only

Variable Name	Value Type	Description
sf.rootdir	String	This variable sets the value of root directory. Note: read-only
sf.instances	String	This variable defines what server instances have been configured. It is a TCL list of directory locations that contain server configurations. This variable is read only, and it is typically read in from a file called datdirs.tcl found in the etc directory under the install location.
sf.servicename	String	This variable defines the windows service name with which the server is associated.
sf.servicenameident	String	
sf.sfoam.monoamname		
sf.syslog.prio	Integer	(Solaris only) This variable sets the priority value used in syslog messages. Default Value = 4
sf.syslog.facility	Integer	(Solaris only) This variable sets the priority value used in syslog messages. Default Value = expr 19 << 3
sf.syslog.ident	String	(Solaris Only) This variable sets the prefix Identifier used in syslog messages.
sf.syslog.console	Boolean	(Solaris Only) This variable logs syslog messages to the console (if true).
proxy.cli.host	String	This variable is used on the Client Proxy to specify the IP or host name of the Server Proxy.
proxy.srv.ASH.host	String	This variable is used on a Server or Filter Proxy to specify the IP or host name of the ASH server.
proxy.srv.CMP.host	String	This variable is used on a Server or Filter Proxy to specify the IP or host name of the CMP server.
proxy.srv.SEP.host	String	This variable is used on a Server or Filter Proxy to specify the IP or host name of the SEP server.
proxy.srv.Timestamp.host	String	This variable is used on a Server or Filter Proxy to specify the IP or host name of the Timestamp server.
proxy.srv.SPEKE.host	String	This variable is used on a Server or Filter Proxy to specify the IP or host name of the SPEKE server.

Variable Name	Value Type	Description
proxy.srv.LDAP.host	String	This variable is used on a Server or Filter Proxy to specify the IP or host name of the LDAP server.
proxy.srv.LDAPauth.host	String	This variable is used on a Server or Filter Proxy to specify the IP or host name of the LDAP server where authenticated LDAP requests should be sent to.
proxy.cli.port	Integer	This variable is used on a client proxy to specify the port of the server proxy where HTTP requests should be directed. Default Value = 80
proxy.cli.https.port	Integer	This variable is used on a client proxy to specify the port of the server proxy where HTTPS requests should be directed. Default Value = 443
proxy.srv.ASH.port	Integer	This variable is used on a Server or Filter Proxy to specify the port of the ASH server where ASH requests should be directed. Default Value = 710
proxy.srv.CMP.port	Integer	This variable is used on a Server or Filter Proxy to specify the port of the CMP server where CMP requests should be directed. Default Value = 829
proxy.srv.SEP.port	Integer	This variable is used on a Server or Filter Proxy to specify the port of the SEP server where SEP requests should be directed. Default Value = 709
proxy.srv.Timestamp.port	Integer	This variable is used on a Server or Filter Proxy to specify the port of the Timestamp server where Timestamp requests should be directed. Default Value = 309
proxy.srv.SPEKE.port	Integer	This variable is used on a Server or Filter Proxy to specify the port of the roaming/profile server where SPEKE requests should be directed. Default Value = 640

Variable Name	Value Type	Description
proxy.srv.LDAPauth.port	Integer	This variable is used on a Server or Filter Proxy to specify the port of the LDAP server where authenticated LDAP requests should be directed. Default Value = 389
proxy.cli.ASH.port	Integer	This variable is used on a Client or Filter Proxy to specify the port on which to listen for ASH requests. Default Value = 710
proxy.cli.CMP.port	Integer	This variable is used on a Client or Filter Proxy to specify the port on which to listen for CMP requests. Default Value = 829
proxy.cli.SEP.port	Integer	This variable is used on a Client or Filter Proxy to specify the port on which to listen for SEP requests. Default Value = 709
proxy.cli.Timestamp.port	Integer	This variable is used on a Client or Filter Proxy to specify the port on which to listen for Timestamp requests. Default Value = 309
proxy.cli.SPEKE.port	Integer	This variable is used on a Client or Filter Proxy to specify the port on which to listen for SPEKE requests. Default Value = 640
proxy.cli.LDAP.port	Integer	This variable is used on a Client or Filter Proxy to specify the port on which to listen for LDAP requests. Default Value = 389
proxy.cli.LDAPauth.port	Integer	This variable is used on a Client or Filter Proxy to specify the port on which to listen for authenticated LDAP requests. Default Value = 1389
proxy.cli.numworkers	Integer	This variable sets the default number of tunnel threads for a Client Proxy. Default Value = 4

Variable Name	Value Type	Description
proxy.srv.numreaders	Integer	This variable sets the default number of tunnel threads for a Server Proxy. Default Value = 4
proxy.*.ASH.numthreads	Integer	This variable sets the default number of ASH threads. Default Value = 4
proxy.*.CMP.numthreads	Integer	This variable sets the default number of CMP threads. Default Value = 2
proxy.*.SEP.numthreads	Integer	This variable sets the default number of SEP threads. Default Value = 2
proxy.*.Timestamp.numthreads	Integer	This variable sets the default number of Timestamp threads. Default Value = 2
proxy.*.SPEKE.numthreads	Integer	This variable sets the default number of SPEKE threads. Default Value = 2
proxy.*.LDAP.numthreads	Integer	This variable sets the default number of LDAP threads. Default Value = 2
proxy.*.LDAPauth.numthreads	Integer	This variable sets the default number of authenticated LDAP threads. Default Value = 2
proxy.ASH.httpcontent	String	This variable defines what tunnel trailer should be used to identify ASH content.
proxy.CMP.httpcontent	String	This variable defines what tunnel trailer should be used to identify CMP content.
proxy.SEP.httpcontent	String	This variable defines what tunnel trailer should be used to identify SEP content.
proxy.LDAP.httpcontent	String	This variable defines what tunnel trailer should be used to identify LDAP content.
proxy.LDAPauth.httpcontent	String	This variable defines what tunnel trailer should be used to identify authenticated LDAP content.



Variable Name	Value Type	Description
proxy.SPEKE.httpcontent	String	This variable defines what tunnel trailer should be used to identify SPEKE content.
proxy.Timestamp.httpcontent	String	This variable defines what tunnel trailer should be used to identify Timestamp content.
proxy.cli.ASH.tunneltls	Boolean	This variable determines if a client proxy should tunnel ASH requests over HTTPS.
proxy.cli.CMP.tunneltls	Boolean	This variable determines if a client proxy should tunnel CMP requests over HTTPS.
proxy.cli.SEP.tunneltls	Boolean	This variable determines if a client proxy should tunnel SEP requests over HTTPS.
proxy.cli.LDAP.tunneltls	Boolean	This variable determines if a client proxy should tunnel LDAP requests over HTTPS.
proxy.cli.LDAPauth.tunneltls	Boolean	This variable determines if a client proxy should tunnel authenticated LDAP requests over HTTPS.
proxy.cli.SPEKE.tunneltls	Boolean	This variable determines if a client proxy should tunnel SPEKE requests over HTTPS.
proxy.cli.Timestamp.tunneltls	Boolean	This variable determines if a client proxy should tunnel Timestamp requests over HTTPS.
proxy.srv.tunneltls	Boolean	This variable determines if a server proxy should untunnel HTTPS requests.
proxy.srv.LDAPauth.tunneltls	Boolean	This variable determines if a server proxy should untunnel authenticated LDAP HTTPS requests.
proxy.srv.tunnelhttp	Boolean	This variable determines if a server proxy should untunnel HTTP requests.
proxy.cli.ASH.bind	Boolean	This variable determines if a client or filter proxy should bind to the ASH port.
proxy.cli.CMP.bind	Boolean	This variable determines if a client or filter proxy should bind to the CMP port.
proxy.cli.SEP.bind	Boolean	This variable determines if a client or filter proxy should bind to the SEP port.
proxy.cli.LDAP.bind	Boolean	This variable determines if a client or filter proxy should bind to the LDAP port.
proxy.cli.LDAPauth.bind	Boolean	This variable determines if a client or filter proxy should bind to the authenticated LDAP port.

Variable Name	Value Type	Description
proxy.cli.Timestamp.bind	Boolean	This variable determines if a client or filter proxy should bind to the Timestamp port.
proxy.cli.SPEKE.bind	Boolean	This variable determines if a client or filter proxy should bind to the SPEKE port.
proxy.doproxying	Boolean	This variable sends initial null messages (workaround for some authenticating proxies)
sf.http.authname	String	This variable sets the Client Proxy domain username if Basic Authentication is required by an HTTP proxy.
sf.http.authpasswd	String	This variable sets the Client Proxy domain password if Basic Authentication is required by an HTTP proxy.

# Appendix B

## Security Manager Proxy error messages

This section contains a description of all the Security Manager Proxy error messages, and potential solutions to the errors.

Number	Text	Description
01_sf_connect_s	Could not connect to X.	This error is caused by a lack of connectivity to a back end server or Server proxy denoted as X. To solve this error, ensure the machine can be seen via a ping command, and ensure it is listening for commands.
02_sf_bind_s	Could not bind to address X, it may already be in use by another service.	This error is caused by another server or process on the local machine that has already bound to the mentioned port. Inspect the process list and services on the machine to determine what is listening on that port, and shut it down and try again. If this is not an option, the proxy must be configured to listen on a different port via config.tcl.
03_sf_eval_s	Error evaluating tcl command X.	This error is caused by the proxy attempting to evaluate invalid config.tcl variables. This is usually caused by improper tampering of config.tcl files, or proxy installation problems. Check to ensure tcl files in both the data directory and the ETC directory are valid and have not been edited.

Number	Text	Description
<b>04_sf_startup</b>	Error during process startup, check config.tcl	This error is caused when errors in startup scripts prevent a process from starting. Check to ensure all config.tcl variables are valid, and look for errors processing TCL commands. As well, check to ensure a valid config.tcl file exists and is readable by the proxy.
<b>05_sfproc_orphan</b>	Shutting down because monitor exited	This error indicates abnormal shutdown of a child process due to the parent process exiting abnormally. This can normally be fixed by restarting the proxy.
<b>06_sf_watchdog</b>	A service operation exceeded the watchdog timeout which protects against service outage. Check the setting sf.watchdog timeout setting is high enough.	This error occurs when a worker thread that is processing a series of request takes too long. The sf.watchdog variable controls how long to let a busy worker process one message for. Usually this error is due to a very busy back end server. Setting the sf.watchdog variable to a higher value fixes this error.
<b>07_mon_mkproc_s</b>	Error starting process X. Check log files for details.	This error is caused when the monitor process is unable to start a child proc process.
<b>08_sf_openlog_s</b>	Error opening logfile X.	This error is normally caused by not having permissions to write to the log file, or the directory that log file is to belong not existing. Check to ensure the path to the logfile mentioned exists, and that the proxy user who runs the processes has write permissions.

Number	Text	Description
<b>09_sf_readtimeout_s_s_d</b>	Timeout (X seconds) while reading on connection from X to local address X. The remote entity may be an incorrect address, faulty, or the timeout settings sf.readtimeout and sf.reader.readtimeout may be set too low.	This error is caused by an io read or query operation on a socket that took too long. This can be a result of a client improperly communicating to the proxy (wrong protocol on wrong port) or a server or server side proxy taking too long to return data. Increase the timeout values to allow for more time for read operations.
<b>10_sf_idletimeout_s_s</b>	Closing idle connection from X to local address X. Timeout (X seconds) while reading on connection from X to local interface X. The remote entity may be faulty or the setting sf.idletimeout or port -idletimout option may be too low.	This is caused by a lack of activity to the local address. This is either nothing to worry about, or the sf.idletimeout variable should be increased to allow for a greater period of inactivity.



# Index

## A

Authenticated LDAP, configuring 62

## C

clients, configuring 47  
config.tcl file  
    location 54  
    understanding 54  
configuring  
    clients 47  
    Solaris 30  
        client-side 30  
        filter 33  
        server-side 31  
    syslog messages, viewing 35  
    user paths, modifying 35  
Windows 37  
    client-side 37  
    filter 43  
    server-side 40  
conventions  
    typographic 8  
cryptographic model 7

## D

data  
    security of 16  
deployment scenarios  
    Proxy as filter 13  
    tunnelling HTTP messages 12

## E

Entrust profiles  
    creating 58  
Entrust.ini, configuring 47

## H

HTTP proxies, configuring for 65

## I

installing

Solaris 22  
Windows 24  
workstation security 16

## M

Multi-CA environments, configuring for 67

## P

profiles  
    Entrust/AutoRA, creating for 58  
protocols 10  
proxy.log  
    configuring 71  
    overview 52  
public key infrastructure  
    concepts 7

## S

securing the server 16  
securing your environment 16  
security  
    securing NT servers 16  
    securing your Security Manager environment 16  
    workstation 16  
Security Manager Proxy  
    administration 50  
    Authenticated LDAP 62  
    client configuration 47  
    deployment scenarios 12  
    Entrust profiles 58  
    firewalls, configuring for specific 64  
    HTTP proxies configuring for 65  
    log file, configuring 71  
    multiple CA environment, configuring for 67  
    overview 10  
    protocols 10  
    Server Login, configuring 59  
    Solaris, configuring 30  
    Solaris, installing 22  
    Solaris, uninstalling 74  
    status, monitoring 52  
    Timestamp, configuring for 70  
    TLS, configuring 56  
    Windows, configuring 37  
    Windows, installing 24  
    Windows, uninstalling 75  
Server Login, installing 59  
starting  
    read this first 7  
syslog messages, viewing 35

## T

- Timestamp server, configuring 70
- TLS, configuring 56
- typographic conventions 8

## U

- uninstalling
  - Solaris 74
  - Windows 75
- user paths, modifying 35

## V

- variables, configuring 54