



Permeo Security Driver User's Guide for Windows Systems

Version 4.2.2

Revised: 19-Jun-03

Permeo Security Driver 4.2.2 User's Guide for Windows Systems

Copyright © 1999-2003, Permeo Technologies, Inc.

All rights reserved.

This document is for informational purposes only. Permeo Technologies makes no warranties, expressed or implied.

Information in this document is subject to change without notice and does not represent a commitment on the part of Permeo Technologies. The software described in this document is furnished under a license agreement. The software may be used only in accordance with the terms of that agreement. The software may not be copied on any medium except as specifically allowed in the license or nondisclosure agreement. No part of this document may be reproduced or retransmitted in any form or by any means, electronically or mechanically, for any purpose other than the purchaser's personal use, without the express written permission of Permeo Technologies.

Trademarks

UNIX is a registered trademark of UNIX System Laboratories, Inc.

Solaris is a registered trademark of Sun Microsystems, Inc.

SPARC is a trademark or registered trademark of SPARC International, Inc.

Microsoft, Windows, and Windows 95, 98, NT, XP, and 2000 are trademarks or registered trademarks of Microsoft Corporation.

RSA ACE/Server is a registered trademark of RSA Security, Inc.

RSA SecurID is a registered trademark of RSA Security, Inc.

InstallShield is a registered trademark and service mark of InstallShield Corporation.

All other product names, trademarks, registered trademarks, service marks, or registered service marks, mentioned throughout any part of this document belong to their respective owners.

Table of Contents

1	Getting Started.....	1
2	Introduction to Permeo Security Driver	2
3	Security Driver Installation	3
4	Secure Access Plug-ins	9
4.1	Plug-in Setup Requirements.....	10
5	Security Driver Features.....	11
6	Security Driver Components	13
6.1	System Properties Window.....	14
6.1.1	Plug-ins Tab.....	15
6.1.2	Advanced tab	18
6.2	User Properties Window	21
6.2.1	General Tab	22
6.2.2	Credential Tab	27
6.2.2.1	Username/Password Authentication	29
6.2.2.2	LDAP Authentication	29
6.2.2.3	RADIUS Authentication.....	30
6.2.2.4	Secure Token for RSA SecurID® Authentication.....	31
6.2.2.5	TACACS+ Authentication	31
6.2.2.6	Windows Domain authentication	32
6.2.2.7	SSL Certificate.....	32
6.2.3	Logging tab.....	33
6.2.3.1	Log File Directories.....	34
6.2.4	Errors Tab	35
6.2.5	About Tab	36
6.2.5.1	View/Enter License Key	36
6.2.5.2	View Copyright / License Agreement	37

6.3	Configuration Window	38
6.3.1	Proxy tab.....	39
6.3.1.1	Entering Server Settings	40
6.3.1.2	Entering Destination Settings	42
6.3.1.3	Entering Destination Server Host Names and IP Addresses	43
6.3.1.4	Entering Destination Server Ports	44
6.3.1.5	Proxy Rule Order with Multiple Servers	45
6.3.2	Applications tab.....	49
6.3.2.1	Proxy All applications except those in Exclude List.....	50
6.3.2.2	Proxy Only applications specified in Include list.....	51
6.3.2.3	Enable Windows Networking Services	52
6.3.3	DNS tab	53
6.3.3.1	Resolving Domain Names	54
6.3.3.2	DNS Examples.....	54
6.3.4	Update tab.....	55
6.3.4.1	Remote Configuration Download – On-demand.....	56
6.3.4.2	Remote Configuration Download – Automatic	57
6.4	Administrator's Tool.....	58
6.4.1	Configuration Filenames	59
6.4.2	Importing a Configuration File.....	60
6.4.3	Exporting a Configuration File.....	61
6.4.4	Driver Diagnostics.....	62
7	Wireless LAN Solution.....	63
7.1	Security Server Requirements.....	63
7.2	Client Requirements & Options.....	63
7.2.1	Wireless Auto-Detect Server Option.....	63
8	Configuring Remote File and Printer Sharing for Administrators.....	65
8.1	Network Requirements	65
8.2	Client Requirements.....	66
8.3	Changing the Workgroup.....	66
8.4	Setting the client computer to use the network WINS server	67
8.5	Enabling Microsoft Networking Services.....	69
8.6	Changing NetBIOS Settings	70

9	Advanced Configuration Options for Administrators.....	71
9.1	Manually Import a Configuration File.....	71
9.2	Remote Configuration Download	72
9.3	Advanced Installation Options.....	74
9.3.1	Manual Web install program (prompted)	74
9.3.2	Automatic Web install program (pre-configured)	75
9.3.2.1	Pre-configuring the Automatic Web install	75
9.3.2.2	Customizing the auto.htm file.....	75
9.3.2.3	Running the Automatic Web Install program.....	76
9.3.3	Desktop Silent Install program (pre-configured)	76
9.3.3.1	Creating the Silent install response file	77
9.3.3.2	Modifying the setup.ini file	77
9.3.3.3	Running the Desktop Silent install	78

This page was intentionally left blank.

1 Getting Started

Welcome to the **Permeo Security Driver** for Windows systems – the most efficient way to SOCKS-enable and secure applications working with the **Permeo Security Server**. The Security Server and Security Driver are part of the **Permeo Application Security Platform (PASP)**. To learn more about PASP, visit the Permeo Web site at: www.permeo.com.

Conventions

The User's Guide uses these text formats and symbols:

<i>Italic</i>	Indicates that the text is a place holder for information or parameters that you provide. For example, <i>INSTALLDIR</i> refers to the directory into which you install the Security Server software, <i>number</i> is a parameter to an option that refers to a numeric value you must supply.
[]	Indicates an optional value. When you omit an optional value, the Server uses a default value.
<code>monospace</code>	Indicates text you must type exactly as it appears, such as in policy rules.

Note: This document uses *INSTALLDIR* to indicate the directory into which you installed the Security Server software.

Throughout this document, the **Permeo Security Server** and **Permeo Security Driver** are referred to as Security Server and Security Driver, and Server and Driver, respectively.

Before you begin...

We recommend that you read these documents before running the Permeo Security Server:

- This document
- Product copyright and license agreement
- The Driver's readme file
- Release Notes, when included

Note: Use the **readme** option on the Security Driver submenu to open the Driver's readme file.

2 Introduction to Permeo Security Driver

The **Permeo Security Driver** is a core component of the **Permeo Application Security Platform**. The following explains the purpose of PASP, its key components, and how the Security Driver works within the Platform.

The Platform enables an organization to secure all of its applications – both those deployed internally and those extending beyond the enterprise network. By establishing a virtual application circuit between each application and its user, the Platform provides privacy and data integrity, enforces authentication and access policies, protects the application infrastructure from attack, and includes detailed auditing and logging capabilities. The Platform can be deployed within a LAN, across a WAN or the Internet, or over wireless networks.

The **Permeo Security Server** is a proxy server that allows hosts behind a firewall to gain full access to the Internet without requiring direct IP-reachability. As a proxy server, the Security Server authenticates, authorizes, and processes network requests for Security Server clients.

The Security Server communicates with a client-based **Permeo Security Driver**. The Security Driver sends client network requests to the Security Server, and the Security Server establishes network connections for the client. The Security Server executes the request for the client, and returns data resulting from the request to the client.

The Security Driver includes Username/Password authentication, while support for other authentication methods must be obtained through the **Permeo Secure Access** package.

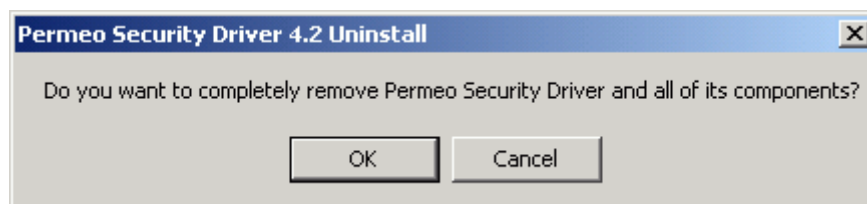
3 Security Driver Installation

This section describes the standard manual desktop installation procedure for the **Permeo Security Driver**. This procedure now automatically installs the **Permeo Secure Access** and **Permeo Encrypt** packages. When prompted, you must enter valid license keys to enable the Security Driver, Secure Access, and Encrypt.

Note: You must have administrator privileges to install the Security Driver on Windows NT®, Windows® 2000, and Windows® XP.



1. Run the Security Driver install executable program.
For example: **permeo-securitydriver-win_4_2.exe**
2. If you have previously installed v4.x, you can click **OK** at the following prompt to remove the existing components. If this is the first time you have installed the Security Driver 4.x on this machine, proceed to step 3.

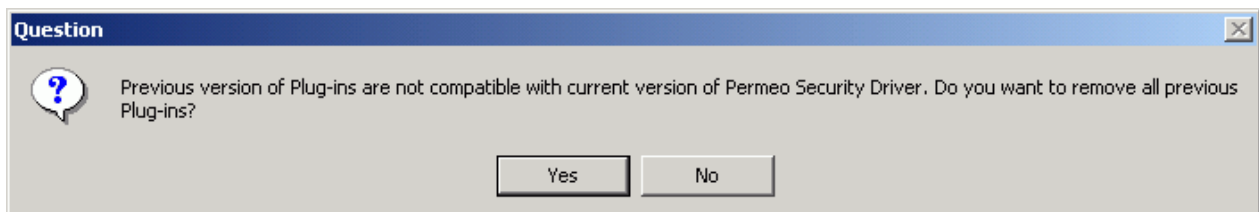


3. When prompted to restart your computer, answer **Yes**, and click **Finish**. Your machine will reboot.

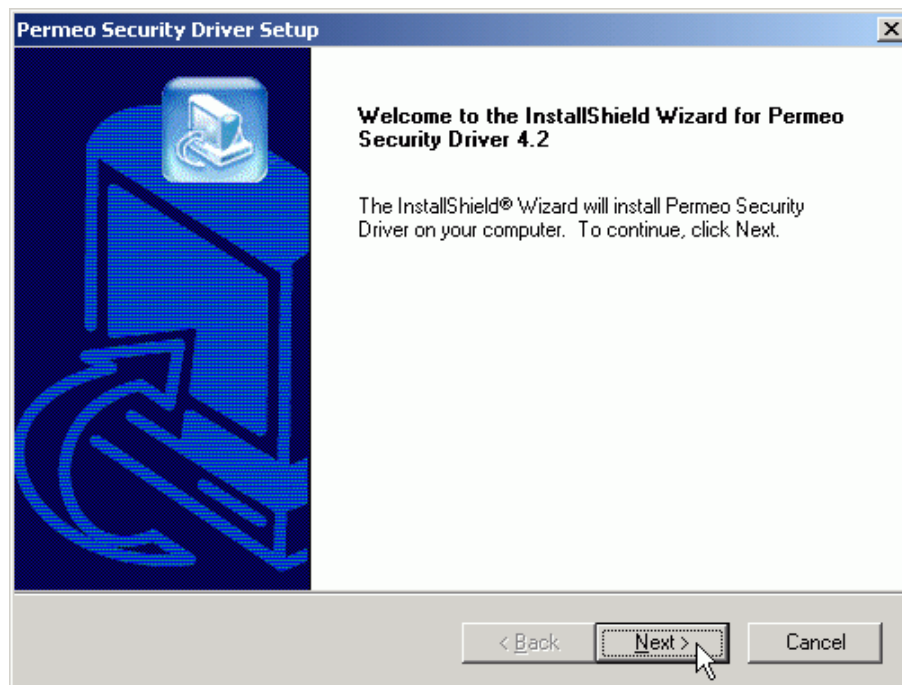
Note: It is highly recommended that you restart your machine at this step to ensure a smooth Security Driver installation.



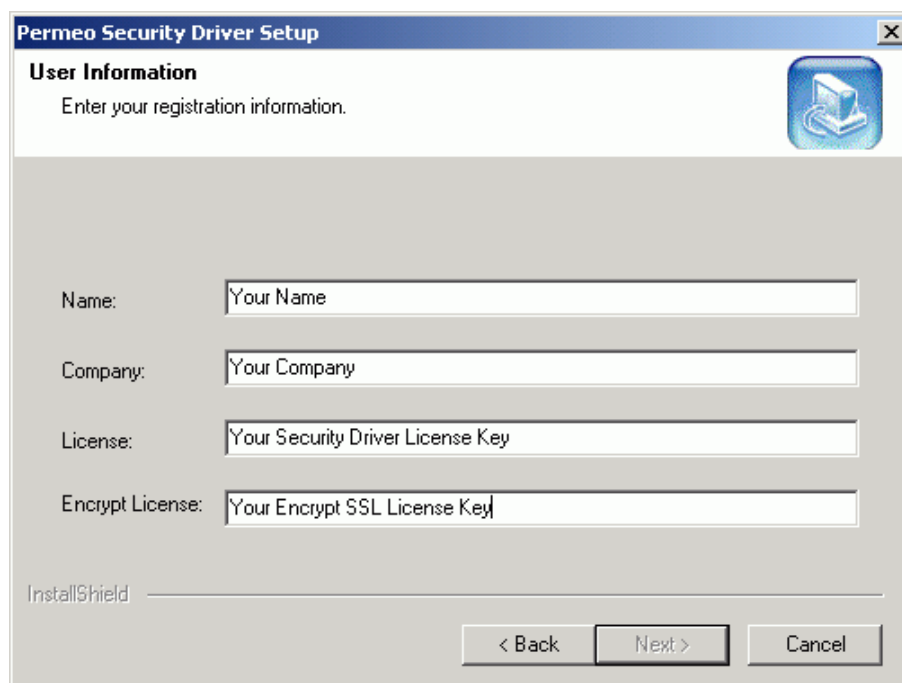
3. Log back into your computer.
4. If you are installing version 4.2 over a previous version of the Driver, you will see an error message that states the previous version of the plug-ins are not compatible with the current version of the Security Driver. Click **Yes** to remove all previous plug-ins and continue, or **No** to exit the Setup program.



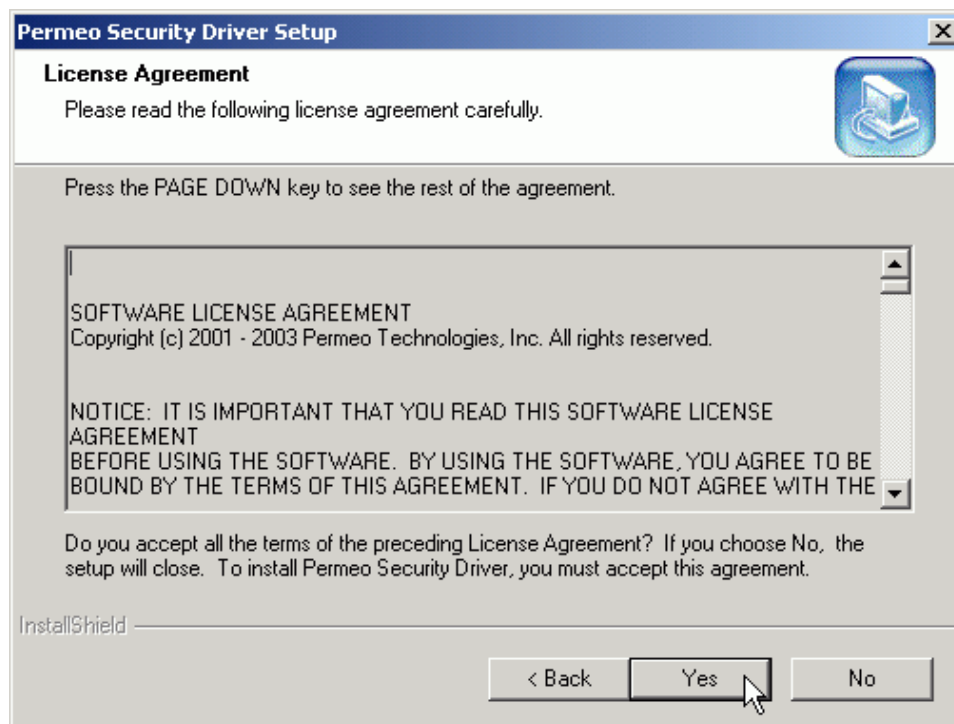
5. Upon successful login, the **Permeo Security Driver 4.2 Setup** screen appears. Click **Next**.



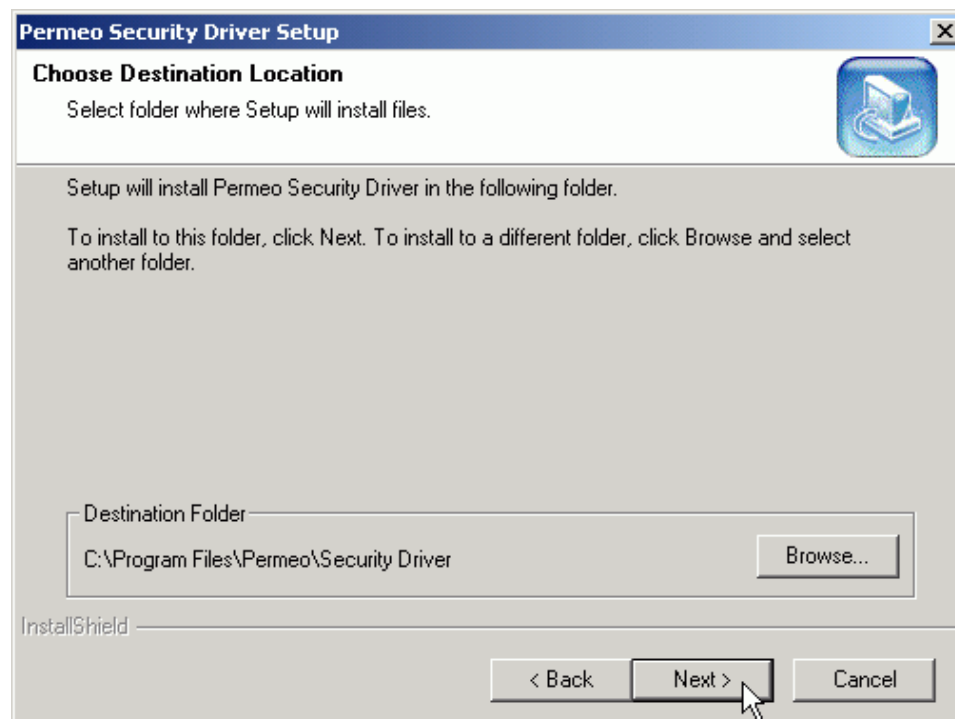
6. Enter your **User Name**, **Company Name**, and product **License** into the **User Information** screen. Upon entry of a valid Security Driver License key, the **Next** button becomes available. Click **Next** to continue. **Note:** the Encrypt License key is optional.

The image shows the 'Permeo Security Driver Setup' window at the 'User Information' step. The title bar reads 'Permeo Security Driver Setup'. The subtitle is 'User Information' with the instruction 'Enter your registration information.' and a small computer icon. There are four text input fields: 'Name:' with 'Your Name', 'Company:' with 'Your Company', 'License:' with 'Your Security Driver License Key', and 'Encrypt License:' with 'Your Encrypt SSL License Key'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a black border, indicating it is active.

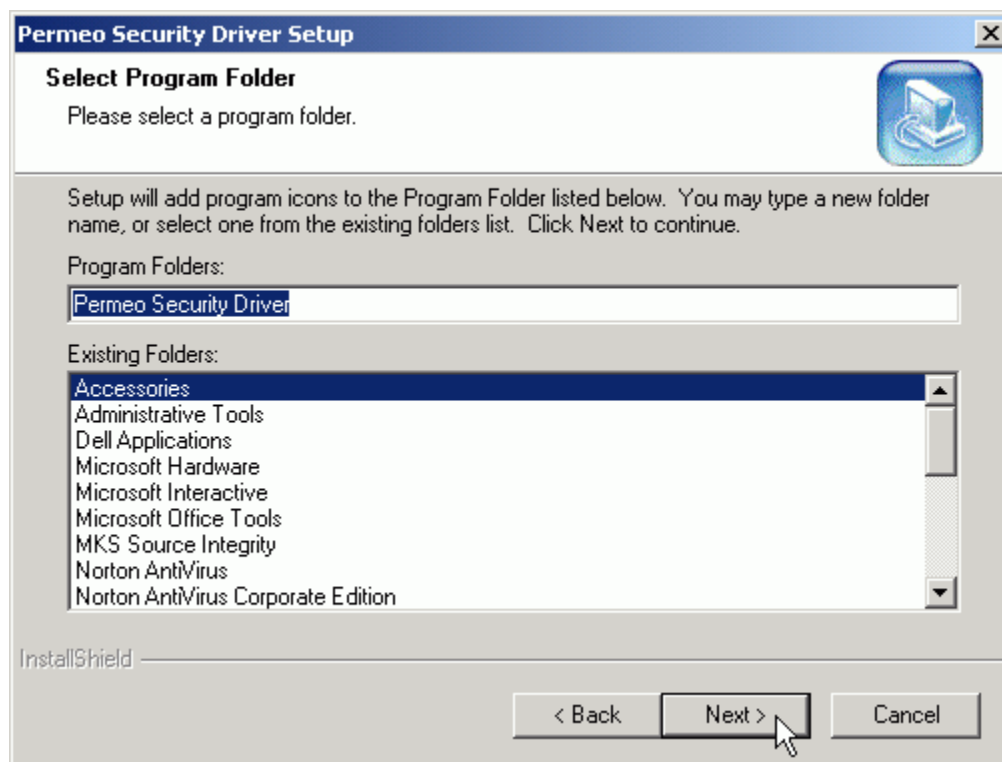
7. The **License Agreement** screen appears. Upon accepting the terms of the license agreement, click **Yes** to continue.



8. At the **Choose Destination Location** screen, browse to a different **Destination Folder**, or accept the default path. Click **Next** to continue.



9. At the **Select Program Folder** screen, browse to a different **Program Folder**, or accept the default folder. Click **Next** to continue.



10. If this is the first time you have installed version 4.x of the Security Driver, or you are reinstalling version 4.x and there are no previous configuration files found, the following dialog box appears:

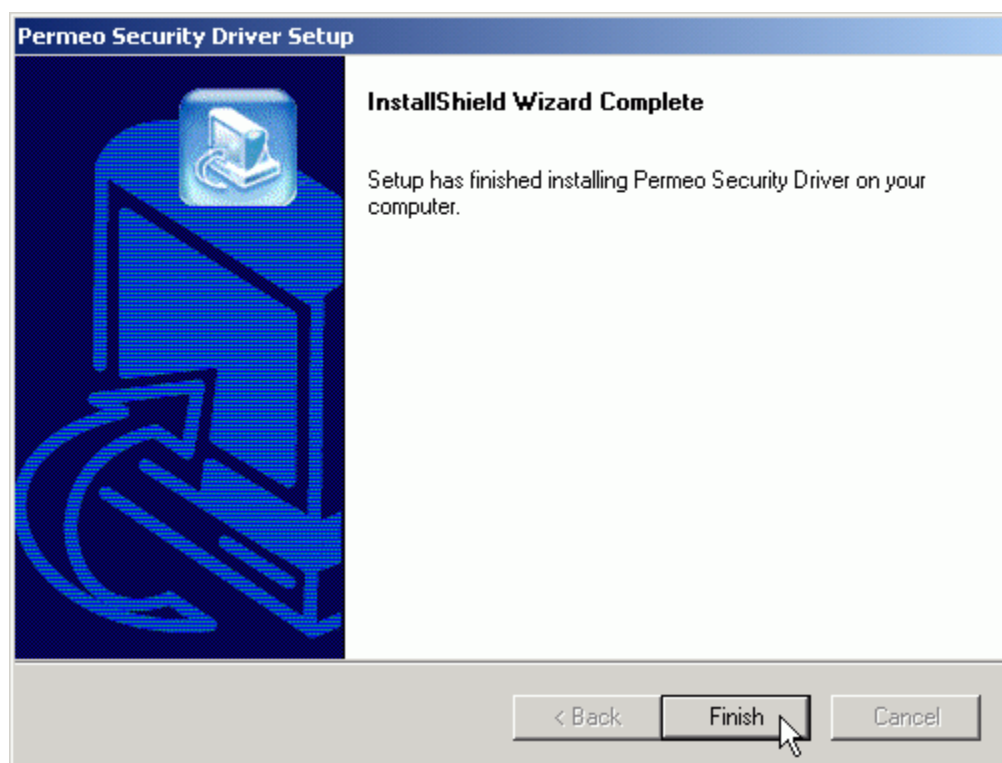
To simplify initial setup, the Install Wizard allows you to specify the name or IP address of the Permeo Security Server you will be using, or a URL of a Security Driver configuration file that contains settings pre-configured by your network administrator. Your network administrator will supply this information.

Note to Administrators:

For information on deploying the **Remote Configuration Download** feature, please see section 9.2 - **Remote Configuration Download** later in this document.



11. When the Driver Setup is complete, the following screen appears. Click **Finish**.



4 Secure Access Plug-ins

The **Permeo Security Driver** supports multiple authentication methods through the use of plug-ins. The Security Driver includes the Username/Password authentication plug-in.

The following plug-ins are available in the **Permeo Secure Access** package for Windows systems:

- **LDAP** (Lightweight Directory Authentication Protocol): The LDAP plug-in enables the Server to authenticate a user with an LDAP Server.
- **RADIUS** (Remote Access Dial-In User Services): The RADIUS plug-in enables the Server to authenticate a user with a RADIUS Server.
- **Secure Token for RSA SecurID®**: The Secure Token for RSA SecurID® authentication plug-in enables the **Permeo Security Server** to authenticate users with an RSA ACE/Server®.
- **TACACS+** (Terminal Access Controller Access Control System): The TACACS+ plug-in enables the Server to authenticate a user with a TACACS+ Server.
- **Windows Domain Authentication**: The Windows Domain plug-in allows users to authenticate to the **Permeo Security Server** using the Windows NTLM security service provider.

Microsoft Networking Services support is also provided through the **Permeo Secure Access** package. It enables remote file and printer sharing capabilities when a valid WINS server is properly configured. For information on enabling and configuring this feature, please see section 8 - [Configuring Remote File and Printer Sharing for Administrators](#).


The **SSL Plug-in** is available in the **Permeo Encrypt** package. The **SSL Plug-in** enables the **Permeo Security Server** and **Security Driver** to establish an encrypted channel and authenticate Server hosts and users using public key technology.

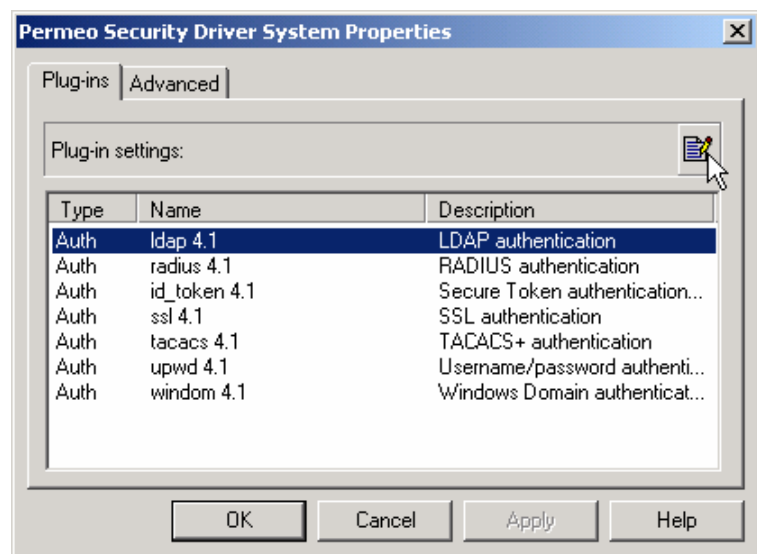
4.1 Plug-in Setup Requirements

1. **Server Secure Access** plug-ins must be installed on your **Permeo Security Server** by a network administrator.
2. **Driver Secure Access** plug-ins must be installed on the client, and enabled in the **System Properties** window.

➤ Access the Security Driver **System Properties** window through the Windows® Control Panel: Click **Start > Settings > Control Panel > Permeo Security Driver**

➤ Use the **Plug-ins** tab to enable, disable, or change plug-in settings.

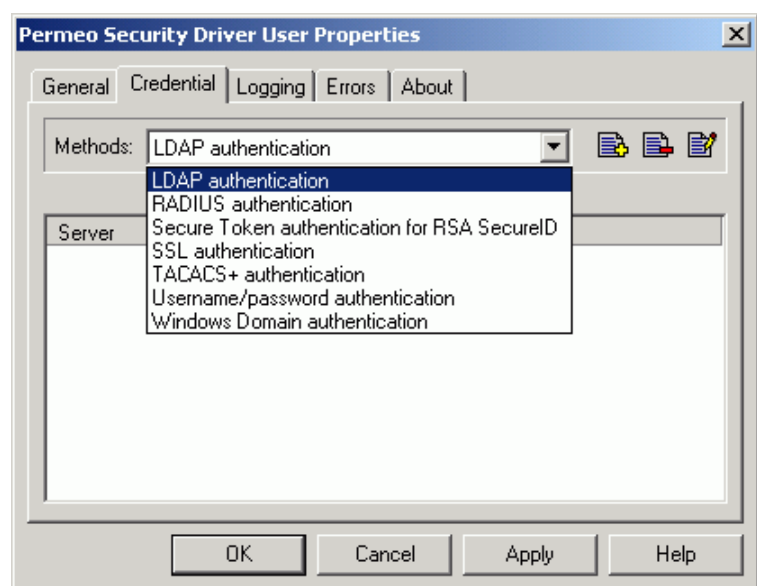
- Double-click on a selected plug-in row
-or-
- Select a plug-in and click the **Edit**  button.



3. **Credentials** and other options must be entered by the user in the **User Properties** window.

➤ Access the Security Driver **User Properties** window: Click **Start > Permeo Security Driver > User Properties**

➤ Instruct users to access the **Credential** tab to allow them to view, add, delete, and update their credential information. For more information, see section 6.2.2 - **Credential Tab**.



5 Security Driver Features

The **Permeo Security Driver** maintains policy configuration information that enables the Driver to control and manage connection requests based on application, service, and network settings. The Security Driver provides the ability to specify:

- **Multiple Security Servers to proxy requests.** The Security Driver can help to achieve load-balancing automatically, or based on policy. The Driver can direct proxy requests to a specific Server based on destination address, destination port, or it can randomly choose a Server from a list of Permeo Security Servers.
- **Local or remote DNS management through multiple domain lists.** You can specify a domain list the Driver resolves, a domain list the Server resolves, and specify when the Driver or Server should resolve domains not included in the lists.
- **A list of destination addresses that do not require a proxy server.** This allows the Driver to connect directly to those addresses specified.
- **Specific Servers for different applications.** With many applications, specifying the port is the same as specifying the application, because those applications use well-known ports. For example, Web applications, HTTP, use port 80. Some applications, including FTP, use multiple ports. Many applications, for example streaming and UDP applications, use multiple ports that get allocated dynamically. When you define the Server and set the port, you define the applications that use that Server.
- **The priority for choosing each Server when using multiple Servers.** When you define proxy rules for multiple Servers, you can prioritize the order in which the Driver attempts to connect to the Servers.
- **Authentication requirements to use the Server.** Some Servers require the Security Driver to use Username/Password, LDAP, RADIUS, RSA SecurID®, TACACS+, or SSL sub-authentication to authenticate with the Server to gain access. The Driver also includes a setting that allows users to save their credentials to disk for automatic retrieval.
- **A list of applications to proxy, a list of applications not to proxy, or choose to proxy all network applications.** The Security Driver provides an easy way to include or exclude selected Internet applications to proxy.
- **Multiple configuration settings.** The Security Driver allows users and/or administrators to create and select between three different configurations for three different types of access, e.g. “in office”, “out of office,” and “wireless.”
- **Centralized configuration files.** The Security Driver allows users to import a pre-configured Driver configuration file, or download a remote configuration file from a Web server or Security Server. In addition, the remote configuration file can be set to automatically download upon every user logon. The **Remote Configuration Download** feature ensures uniformity of settings amongst groups of distributed users.

- **Shared system configuration.** The Security Driver provides a System Properties interface that allows administrators to create a shared system configuration that ensures uniformity of settings for multiple users on one machine.
- **Temporarily disable proxy services.** A user can easily disable, then re-enable the Security Driver when necessary.
- **Enable Microsoft Networking Services.** This feature, available through the **Permeo Secure Access** package, enables remote file and printer sharing capabilities on Windows® 2000 and XP systems, when a valid WINS server is properly configured.
- **Wireless LAN solution.** In addition to the “in office” and “out of office” configurations, users can choose to create a “wireless” configuration on the client to ensure secure wireless connections between the Security Driver and Security Server.
- **User enabled logging and error tracking.** Users can enable and set error logging for trouble-shooting purposes, as well as quickly diagnose connection problems with on-screen error tracking.

6 Security Driver Components

The Security Driver consists of four components that provide an easy interface for configuring Driver settings.

- **System Properties window:** Use to edit plug-in properties and create a shared system configuration file for use by multiple users on one machine. This window also contains a feature that allows or disallows users to save their credentials to disk. System Properties is primarily used by network administrators or users who have permissions to configure the Security Driver for other users. For more information, see section 6.1 - [System Properties Window](#).
- **User Properties window:** Use to set credential and license key information, disable/enable the proxy, enable logging for trouble-shooting purposes, view an error list, and access configuration files for intranet and extranet access. For more information, see section 6.2 - [User Properties Window](#).
- **Configuration window:** Use to specify all proxy server and destination settings, applications to be proxied, DNS settings, and to specify the URL or Security Server where an optional remote configuration file is located. Configuration window settings can be set manually by an experienced user or network administrator, or imported or downloaded from a pre-configured settings file. For more information, see section 6.3 – [Configuration Window](#).
- **Administrator's Tool:** After defining Security Driver settings, the administrator's tool can be used to export the current settings to a configuration file that can subsequently be imported or downloaded by other users. This program also provides Ping and Traceroute diagnostics. For more information, see section 6.4 - [Administrator's Tool](#).

6.1 System Properties Window

The Security Driver **System Properties** window allows administrators to configure plug-ins and enable and edit system configuration settings.

Access the Security Driver **System Properties** through the Windows® Control Panel:

Click **Start > Settings > Control Panel > Permeo Security Driver**



The following tabs are accessible through the **System Properties** window:


Tab	Description
Plug-ins	View installed plug-ins, edit plug-in settings, and enable/disable plug-ins
Advanced	Control whether users can save their credentials to disk, enable and set system configuration settings

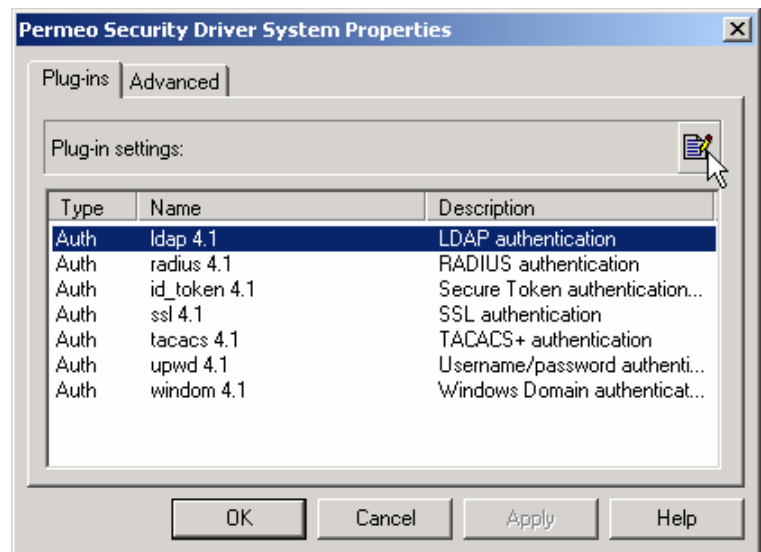
6.1.1 Plug-ins Tab

Use the **Plug-ins** tab in the **System Properties** window to view installed plug-ins, edit plug-in settings, and enable/disable plug-ins.

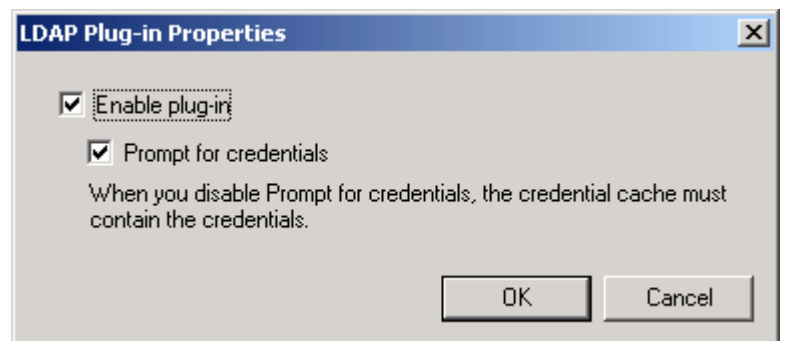
Note: The Security Driver includes the Username/Password authentication plug-in. Additional authentication plug-ins are available in the **Permeo Secure Access** package. The SSL authentication plug-in is available in the **Permeo Encrypt** package. For information on available Secure Access plug-ins, see section 4 - [Secure Access Plug-ins](#).

To change settings for a plug-in:

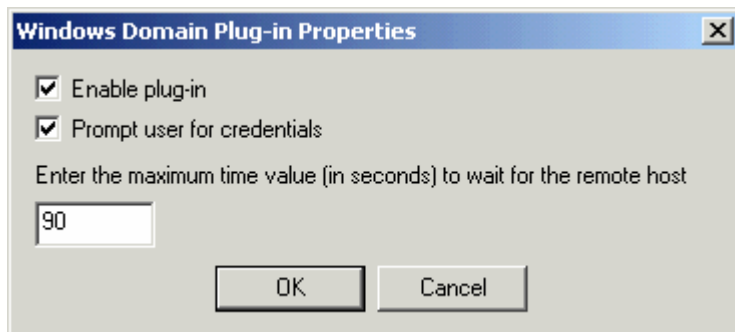
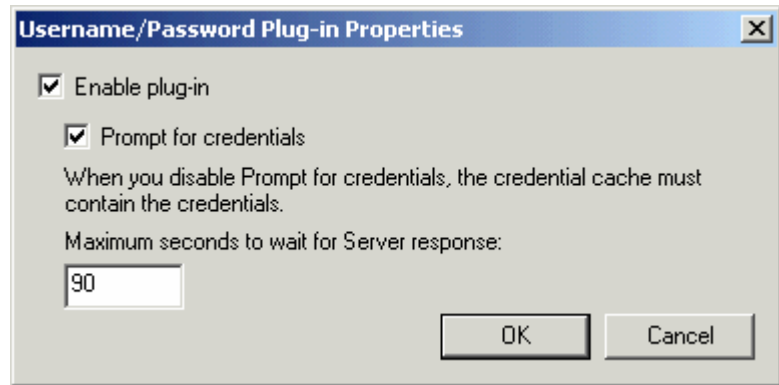
1. Select the plug-in you want to change, then click the **Edit**  icon.
– or –
Double-click on the plug-in row.



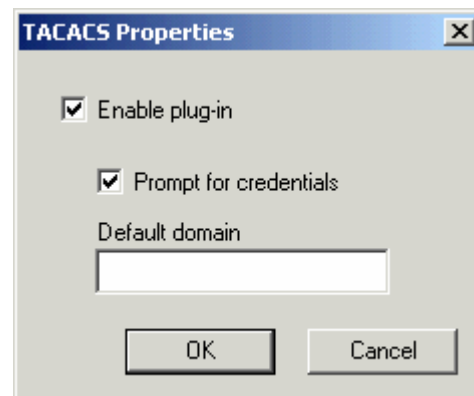
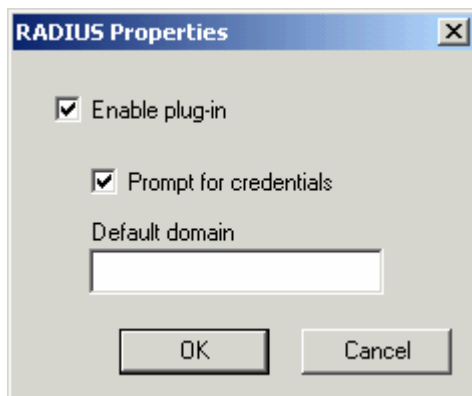
2. The Driver opens a **Properties** box for the selected plug-in. Most plug-ins include a check box to **Enable** the plug-in and a check box to **Prompt for credentials**.



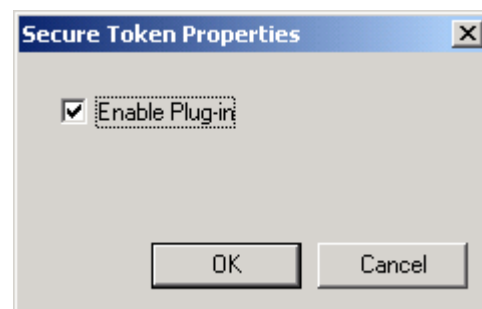
- **Username/Password** and **Windows Domain** plug-ins also include an option to specify a **timeout value**, the time the Driver waits for a response from the Server regarding authentication success.



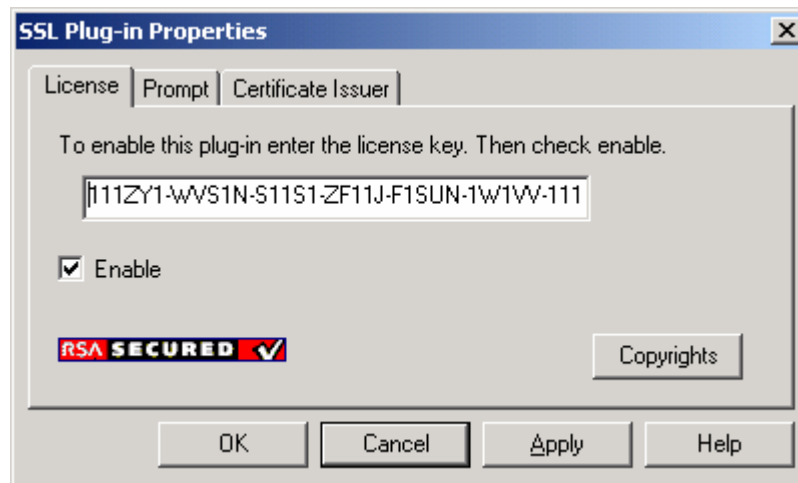
- The **RADIUS** and **TACACS+** plug-ins also include a **Default domain** box. Enter the identifier for the collection of RADIUS or TACACS+ users to which you belong.



- The **Secure Token for RSA SecurID® (id_token)** plug-in only contains an **Enable** checkbox.

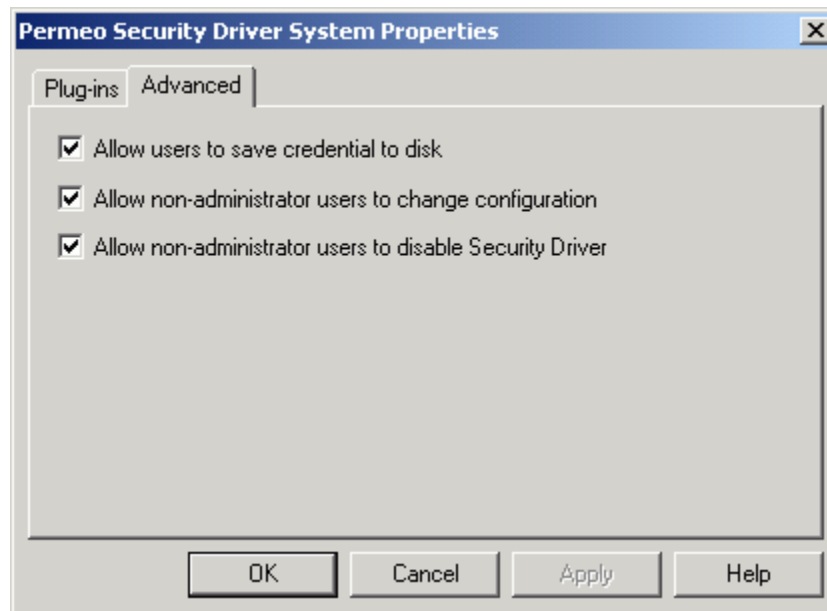


- The SSL plug-in requires a **license key**, **certificate issuer**, and includes **prompt** options.



6.1.2 Advanced tab

The **Advanced** tab in the **System Properties** window allows network administrators to control whether users can save their credentials to disk, edit their own Driver configurations, and disable the Security Driver. These features are designed for use by individuals managing and configuring the Security Driver for use by other users.



- **Allow users to save credential to disk:**

Check this option to allow users to save their credential to disk in supported authentication plug-ins. A **Save password on disk** option will appear on credential windows.

Uncheck this option to remove the user option of saving a password. For increased security, do not allow users to save their credential to disk – requiring them to type their credential/password each time they log on.

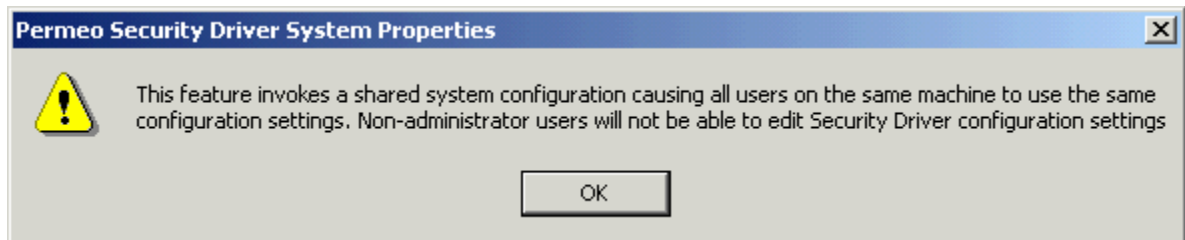


- **Allow non-administrator users to change configuration:**

Check this option to allow users to change and customize their own Driver configurations. Uncheck this option to prevent users from changing Driver configuration settings.

When this option is unchecked, a shared system configuration is invoked – ensuring that all Security Driver users on a particular machine will share the same configuration file. Shared system configuration settings will override any user configuration files previously created on the same machine.

The following prompt appears upon un-checking this feature:



When the shared system configuration is invoked, users can see the system configuration settings in a view-only mode, but not make changes to the configuration.

Notes to Administrators:

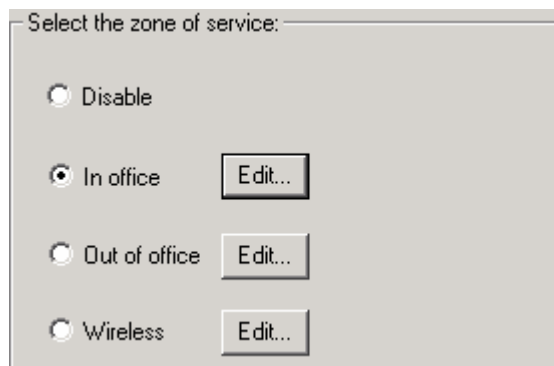
- The **shared system configuration** feature stores the system settings in a shared configuration file named **ebshared.conf**, located in the Windows application data directory. The shared file contains all Driver configurations (In office, Out of office, and Wireless).
- For simplified management of wide-spread users, administrators can configure the Remote Configuration Download feature, allowing users to specify a URL or a Security Server name that downloads a pre-configured remote configuration file.
- For more information, see section 6.3.4 - **Update tab**, and section 9.2 - **Remote Configuration Download**.

To create a shared system configuration:

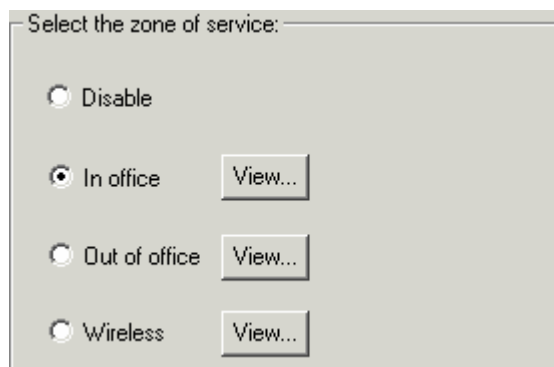
1. From the **Advanced** tab, uncheck **Allow non-administrator users to change configuration**. The default setting is checked.
2. Click **OK** after reading shared system configuration message.
3. Click **Apply** then **OK** to save setting. The following screen shots show the onscreen results:

Users with administrator privileges:

When users with administrator privileges run the Driver's User Properties program, they can select a zone of service, and click an **Edit** button to open the **Configuration** window to customize settings for the selected zone of service.

**Users without administrator privileges:**

When users without administrator privileges run the Driver's User Properties program, they can select a zone of service, and click a **View** button to open the **Configuration** window to view settings for the selected zone of service. They will be unable to make any changes to the configurations.



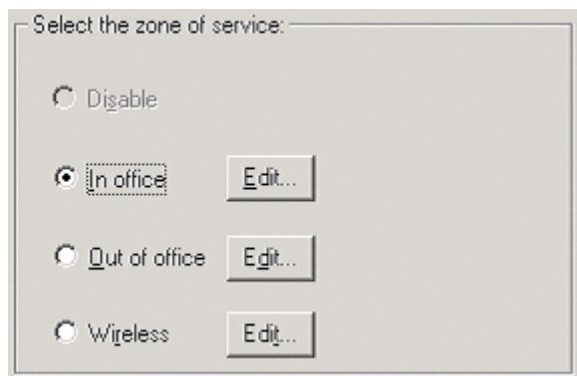
- **Allow non-administrator users to disable Security Driver:**

Check this option to allow non-administrator users to disable the Security Driver.

Uncheck this option to prevent non-administrator users from disabling the Security Driver.

As the screen to the right shows, the Disable option on the General tab of the User Properties window will no longer be available for those users.

Note: This option only affects non-administrator users' ability to disable the Security Driver. They will be able to select between other zones of service and View or Edit configuration settings, based on the status of the **Allow non-administrator users to change configuration** feature.

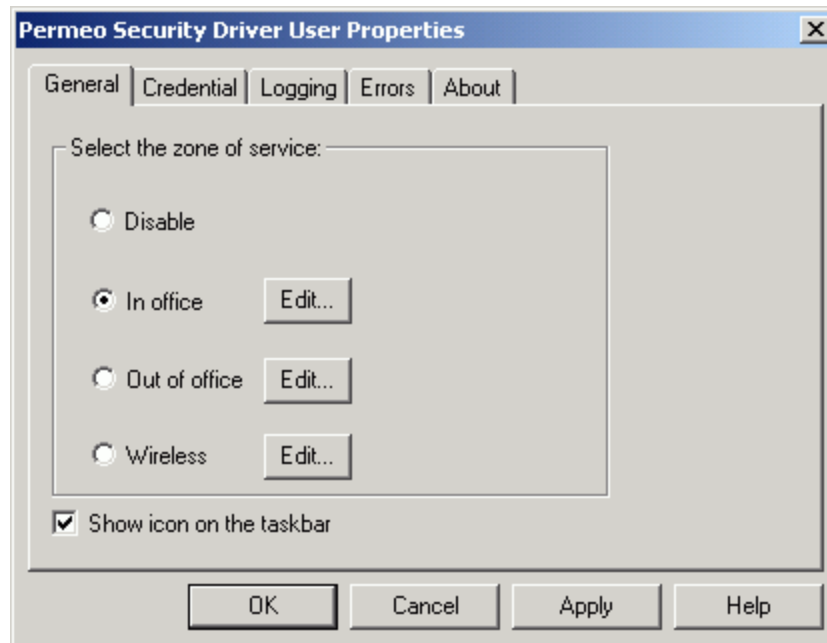


6.2 User Properties Window

The **User Properties** window is used to set credential and license key information, disable and enable the proxy, and to create and edit configuration files for intranet and extranet access.

To access the Security Driver **User Properties** window:

Click **Start > Programs > Permeo Security Driver > User Properties**

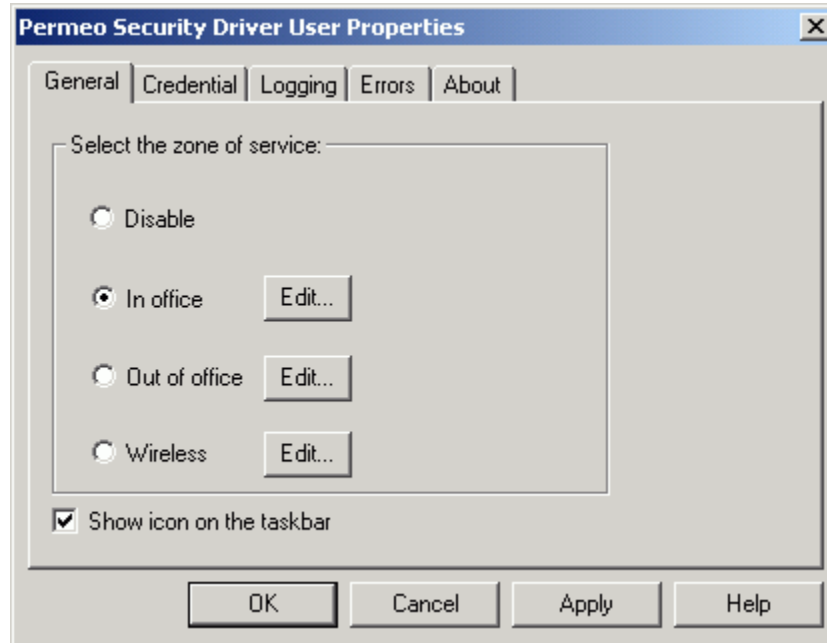


The following tabs are accessible through the **User Properties** window:

Tab	Description
General	Disable the proxy, select a zone of service, create/edit a dual set of configuration settings, and display the Security Driver icon on the taskbar
Credential	View, add, delete, and update credential information
Logging	Enable and set the logging level for trouble-shooting purposes
Errors	View error list to quickly diagnose connection problems
About	View product version information, view/edit the license key, and read the Permeo Security Driver software license

6.2.1 General Tab


The **General** tab of the Security Driver **User Properties** window allows the user to disable the proxy, select a zone of service, create/edit/view multiple configurations, and display/hide the **Permeo Security Driver** icon on the taskbar.



Zone of service: Users can choose the zone of service they want to activate. There are four zones to choose from: **Disable**, **In office**, **Out of office**, and **Wireless**.

Disable:

Choose this zone to turn off all functionality provided by the Security Driver. The Disable option is available to non-administrator users only when the **Allow non-administrator users to disable Security Driver** is checked in the System Properties **Advanced** tab. Otherwise, the Disable option is not available to non-administrator users.

The disabled Driver icon  is displayed on the taskbar when the Driver is disabled and **Show icon on the taskbar** is enabled.

In office/Out of office:

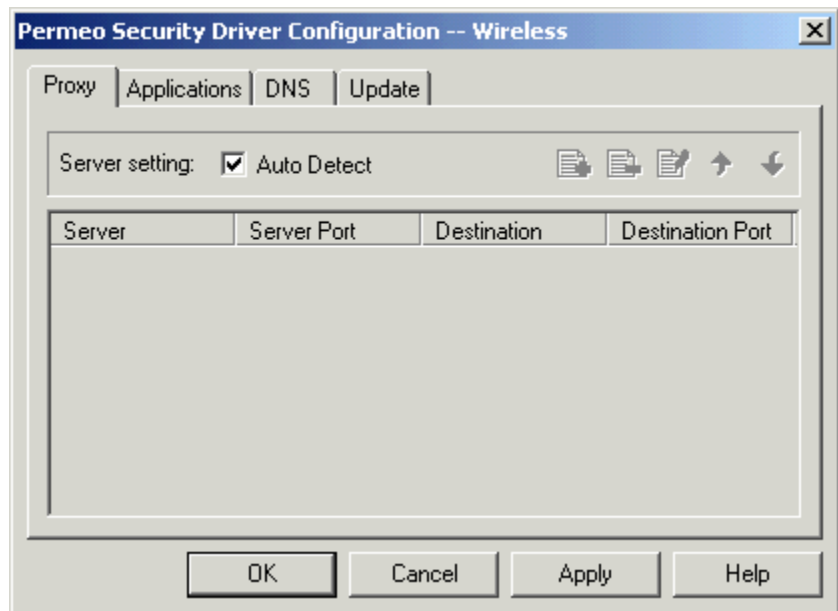
The Security Driver supports multiple configurations, allowing users and/or administrators to create different configurations to choose from. Selecting a desired zone of service simply points the Security Driver to the selected configuration. It is up to the user or administrator to configure the settings correctly for each zone.

For example, the **In office** zone can be configured to allow external access from within the intranet, while the **Out of office** zone can be configured to allow access to an internal network from a remote machine on the Internet.

Wireless:

Users can create a **Wireless** configuration to ensure secure wireless connections between the Driver and the Security Server.

When the configuration window appears, an **Auto-Detect** checkbox appears on the **Proxy** tab. Check the **Auto-Detect** checkbox to enable the Driver to automatically locate a Security Server instead of using Proxy rules.



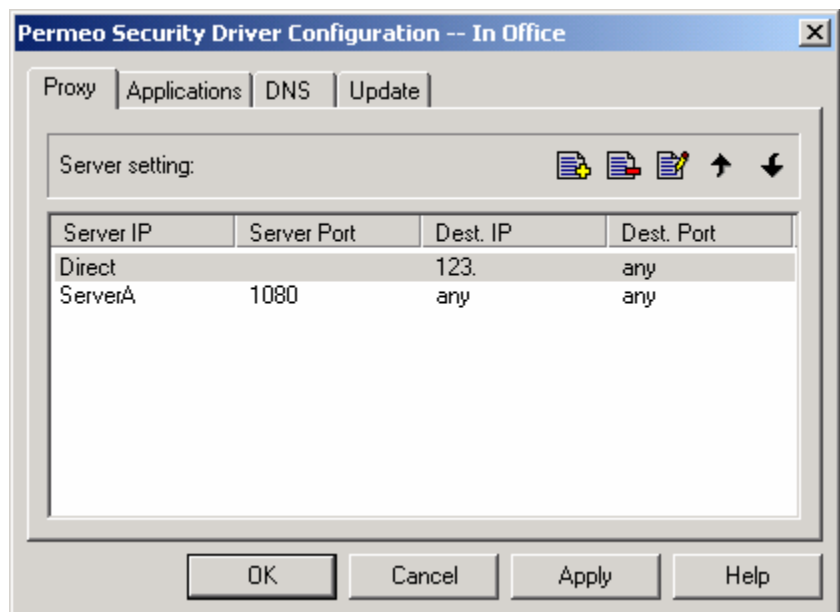
If the Auto-Detect checkbox is not selected, standard Proxy rules must be created for the Wireless configuration.

Note: This zone of service requires the **Permeo Encrypt SSL** plug-in to be installed on the Server and Driver. For more information, please see section 7 - [Wireless LAN Solution](#).

Edit mode: The **Edit** buttons next to **In office**, **Out of office**, and **Wireless** configurations indicate that either a User with administrator privileges is using the Driver, or that the **Allow non-administrator users to change configuration** has been activated by an Administrator.

Click any **Edit** button to open the Security Driver **Configuration** window to modify settings in the selected configuration. The **Edit** mode allows each user to create their own customized configurations.

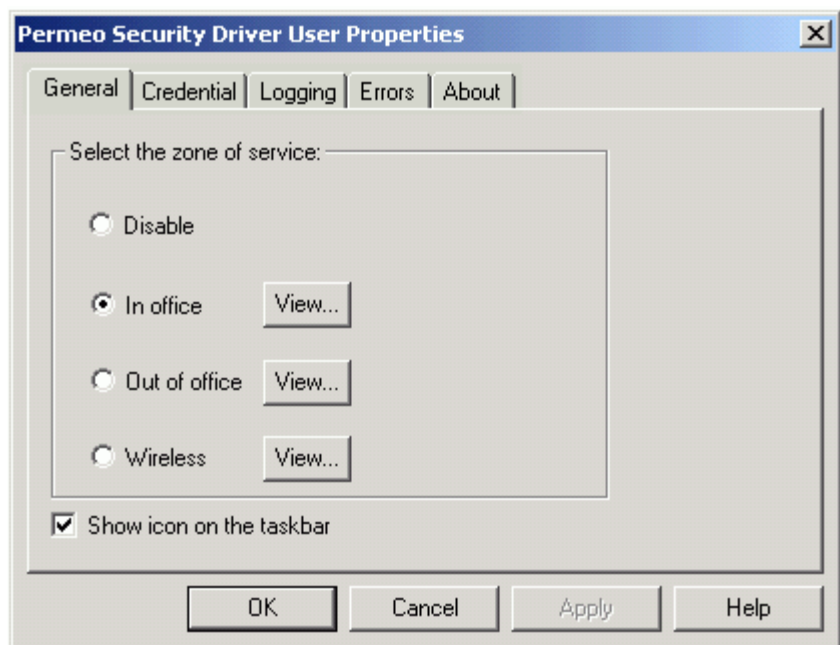
When the configuration window appears, all editing functions are operational, as shown below.



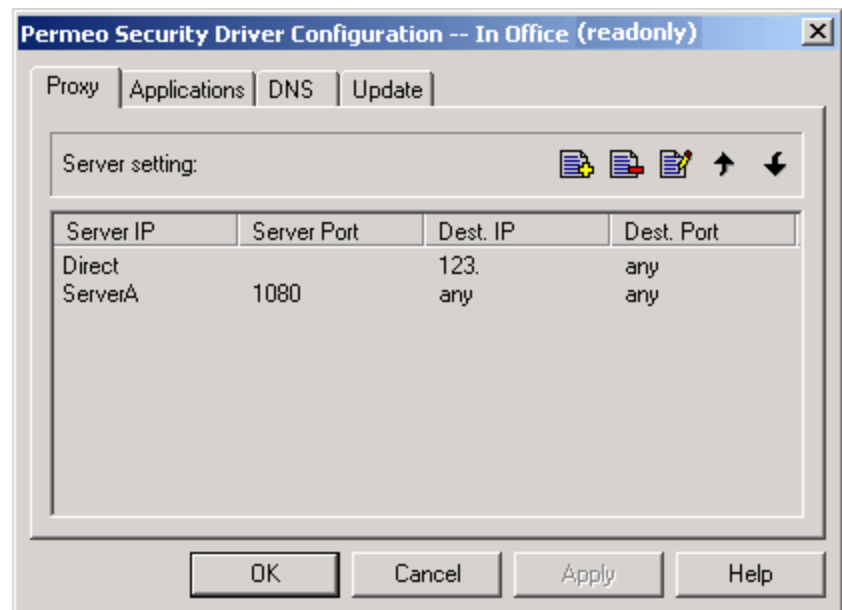
View mode: The **View** buttons next to **In office**, **Out of office**, and **Wireless** configurations indicate that non-administrator users cannot edit configurations, only view configuration settings and select a zone of service to enable.

The **View** buttons also indicate that a **shared system configuration** is active, such that all users on the same machine are using a shared Security Driver configuration.

Click a **View** button to open the **Configuration** window in a read-only mode to display settings for the selected zone of service.



When the configuration window appears in a read-only mode, all data is displayed, but no editing functions are available, as shown below.




For information on creating a shared system configuration, see section 6.1.2 - [Advanced tab](#).

Show icon on the taskbar:

A toggle feature that displays/hides the Security Driver icon on your system tray taskbar.


To Display the Security Driver icon on the taskbar:

1. Click **Show icon on the taskbar** to check box.
2. Click **Apply**.
3. When the SecurityDriver is enabled, the “enabled” Security Driver icon  appears on your system tray.

When the Security Driver is disabled, the “disabled” Security Driver icon  appears on your system tray.

To Hide the Security Driver icon on the taskbar:

1. Click **Show icon on the taskbar** to uncheck box.
2. Click **Apply**.
3. The **Security Driver** icon no longer appears on your system tray.

Note: When **Show icon on the taskbar** is selected and an error occurs, the system tray icon will show a red exclamation mark  when new errors occur. The user must open the Security Driver User Properties window to view the error descriptions. The tooltip over the taskbar icon will say "Permeo Security Driver encountered errors!". The exclamation point will change back to the normal icon after the user interacts with the taskbar icon or the User Properties GUI.

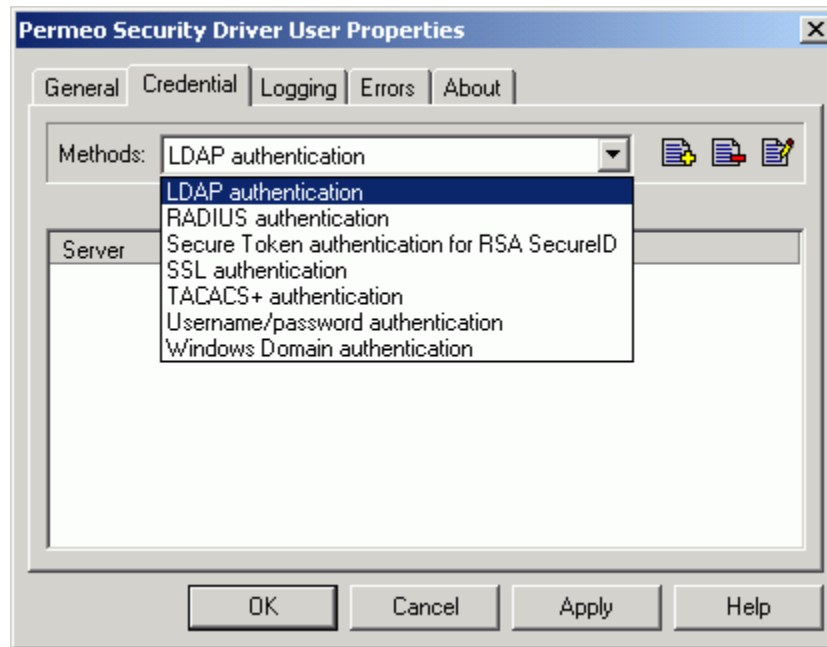
6.2.2 Credential Tab

Use the **Credential** tab to:

- Identify Servers that require authentication
- Specify credentials for required authentication methods
- View, add, delete, and edit credential information
- Indicate whether or not to save your user name and password on disk (if allowed by administrator.)

Note: Using the **System Properties** window **Advanced** tab, a network administrator can control whether or not this feature is enabled.

When the **Permeo Security Server** requires credentials, and **Prompt user for credentials** is checked in the System Properties plug-in's properties box, the Driver prompts the user for credentials once during each session and stores the user's credentials in the credential cache. When the Server requires authentication, the Driver only prompts if the credential is unavailable in the cache.



Specifying Credentials

Select the corresponding authentication plug-in method from the drop-down list. Each plug-in uses a separate credential cache.



To **add** a credential for a particular server, click the **New** icon to open the property box for the selected authentication method.



To **delete** a credential for a particular server, select the server, then click the **Remove** icon. Click **OK** when the Driver asks if you want to remove the Server. The Driver deletes the Server credential entry.



To **change** credential properties for a particular server, select the Server entry, then click the **Edit** icon.

Credential Notes:

- It is not necessary to enter credential information for all authentication methods.
- The Username/Password authentication plug-in is included with the **Permeo Security Driver** package.
- The LDAP, RADIUS, Secure Token for RSA SecurID®, TACACS+, and Windows Domain plug-ins are available in the Driver **Secure Access** package.
- The SSL plug-in is available in the **Permeo Encrypt** package.

Following are credential dialog boxes for each type of authentication method.

Note: If an administrator enables **Allow users to save credential to disk** (see section 6.1.2 - **Advanced tab**), the corresponding authentication box includes a **Save password on disk** option.

6.2.2.1 Username/Password Authentication



The dialog box is titled "Username/Password Authentication". It contains the instruction "Enter your username and password:". Below this are three text input fields: "Server name:", "User name:", and "Password:". At the bottom left is a checkbox labeled "Save password on disk". At the bottom right are "OK" and "Cancel" buttons.

1. Type the IP address for the Server for which you are adding the credential in the **Server name** box.
2. Type the **User name** and **Password** in the appropriate boxes.
3. Click **OK**.

When you check **Save password on disk**, the Driver stores the credentials for subsequent sessions.

When you uncheck **Save password on disk**, the Server prompts for credentials once during each Driver session.

6.2.2.2 LDAP Authentication



The dialog box is titled "Security Server LDAP Authentication". It contains the instruction "Enter your Security Server and LDAP credentials:". Below this is a text input field for "Security Server:". Under "LDAP credential:", there is a table with two columns: "Name" and "Value". To the right of the table are three buttons: "Add", "Edit", and "Remove". At the bottom left is a checkbox labeled "Save password on disk". At the bottom right are "OK" and "Cancel" buttons.

1. Type the IP address for the Server for which you are adding the credential in the **Security Server** box.
2. The Driver builds the credential from one or more **distinguished names**. To add a distinguished name, click **Add**.
3. Type the distinguished name in the **Name** box, and the value for that name in the **Value** box. Click **Add** to continue adding distinguished names, or **Close** to return to the LDAP Authentication box.
4. Click **OK**.

Please see the **LDAP Example** below for an example of adding a credential with a distinguished name.

LDAP Example

To add a credential for a user with user name **testuser** and password **secret** when the Server requires a distinguished name for **username** and one for **password**, in the **Add Distinguished Name** box:

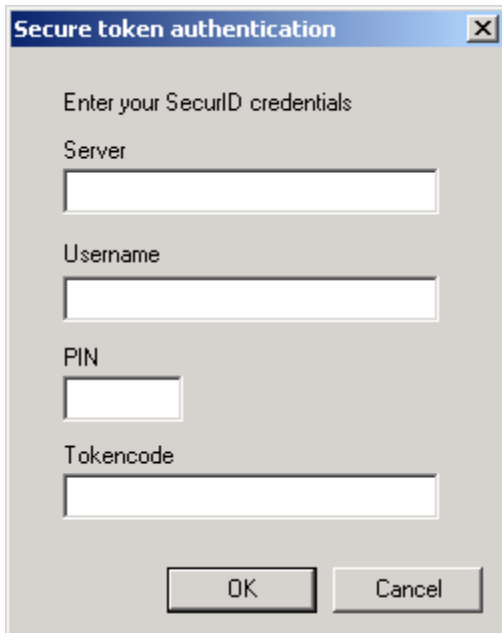
1. Type **username** in the **Name** box, and **testuser** in the **Value** box.
2. Click **Add**.
3. Type **password** in the **Name** box, and **secret** in the **Value** box.
4. Click **Close**. The LDAP Authentication box displays the distinguished name entries.
5. Click **OK**.

6.2.2.3 RADIUS Authentication



1. Type the IP address for the Server for which you are adding the credential in the **Server name** box.
2. Type your **User name** and **Password** in the appropriate boxes.
3. Click **OK**.

6.2.2.4 Secure Token for RSA SecurID® Authentication

A dialog box titled "Secure token authentication" with a close button (X) in the top right corner. The dialog contains the text "Enter your SecurID credentials". Below this text are four input fields: "Server", "Username", "PIN", and "Tokencode". At the bottom of the dialog are two buttons: "OK" and "Cancel".

Use the **Secure Token authentication** box to store the token code issued for use with your RSA ACE/Server®.

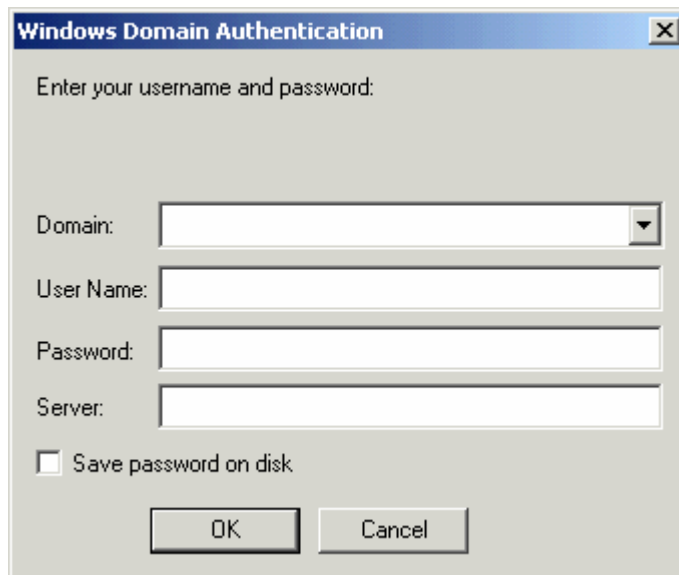
1. Type the IP address for the Server for which you are adding the credential in the **Server** box.
2. Type the **User name** and **Password** in the appropriate boxes.
3. Type your personal identification number in the **PIN** box.
4. Type your token code in the **Tokencode** box. The credential issuer distributes the token code.
5. Click **OK**.

6.2.2.5 TACACS+ Authentication

A dialog box titled "TACACS authentication" with a close button (X) in the top right corner. The dialog contains the text "Enter your username and password:". Below this text are four input fields: "Server:", "Domain:", "User name:", and "Password:". At the bottom of the dialog is a checkbox labeled "Save password on disk" and two buttons: "OK" and "Cancel".

1. Type the IP address for the Server for which you are adding the credential in the **Server name** box.
2. Type your **User name** and **Password** in the appropriate boxes.
3. Click **OK**.

6.2.2.6 Windows Domain authentication



When using Windows Domain authentication, the Driver always uses the user's Windows logon credentials. When the **Security Server** fails to authenticate the user with the Windows credentials, it prompts the user for a domain, and Username and Password for that domain. Use the **Windows Domain Credentials** box to enter additional credentials.

1. Choose a domain from the **Domain** name list, or type a domain name.
2. Type the **User name** and **Password** for the domain in the appropriate boxes.
3. Type the IP address for the Server for which you are adding the credential in the **Server** box.
4. Click **OK**.

6.2.2.7 SSL Certificate



1. Type the SSL certificate file name in the **SSL certificate file** box.
2. Type the SSL private key file in the **SSL private key file** box.
3. Type the SSL private key password in the **SSL private key password** box.
4. Click **OK**.

Note: The SSL authentication plug-in is available in the **Permeo Encrypt** package.

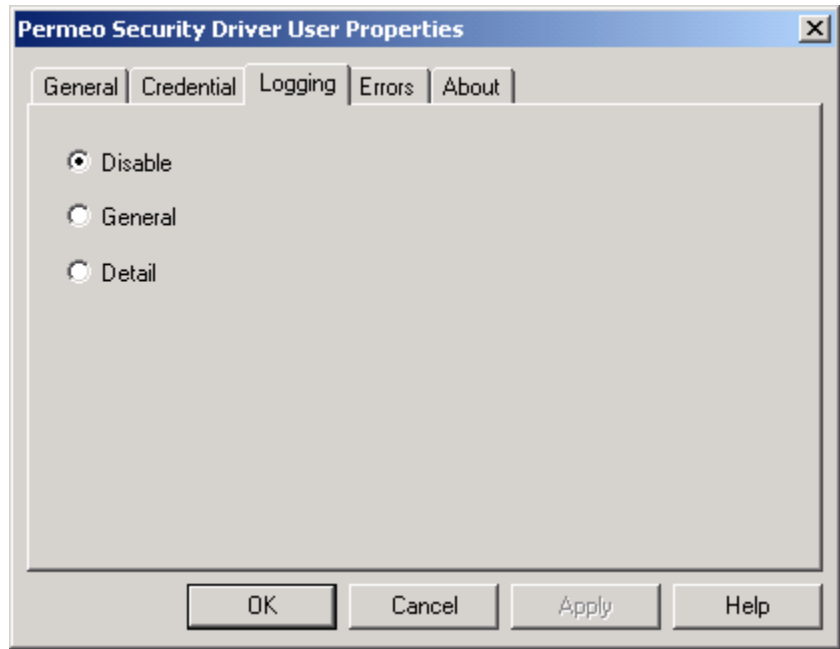
6.2.3 Logging tab

Use the **Logging** tab in the **User Properties** window to enable and set the logging level for trouble-shooting purposes. Do not enable logging for normal operation. Enable logging only when recommended by Permeo Technical Support.

Logging options include:

- **Disable:** Disable logging (default).
- **General:** Enable General level logging.
- **Detail:** Enable Detail level logging.

The Driver creates the log file if it doesn't exist. If the file does exist, the Driver adds to the end of the file until the file exceeds the maximum size.



If you are not experiencing problems with the Driver, do not log. Logging decreases network performance. After resolving problems, we recommend that you remove the log file.

Note: Log files can now be enabled by any user account, not just administrators. The files generated by the logging feature must be interpreted by Permeo Technical Support. **General** level logging generates an **eb_debug.log** file, while **Detail** logging generates both **eb_debug.log** and **eb_ws2.log** files.

6.2.3.1 Log File Directories

Previous versions of the Security Driver stored all Driver log files in the directory where the Security Driver software was installed (*INSTALLDIR*). Driver log files are now generated in the following directories, depending on your operating system:

Platform	Directory
Windows 2000 and XP	<p>Driver log files are generated per user. If multiple users are using the same client machine, their log files will be stored in separate directories, based on Userid.</p> <p><u>Example:</u> If the operating system is installed on the C drive, then log files are generated at:</p> <p>C:\Documents and Settings\Userid\Local_Settings\Temp</p>
Windows NT	<p>Driver log files cannot be generated per user; Driver log files are the same for all users on the same client machine.</p> <p><u>Example:</u> If the operating system is installed on the C drive, then log files are generated at:</p> <p>C:\TEMP</p>
Windows 98	<p><u>Example:</u> If Windows 98 is installed on the C drive, then log files are generated at:</p> <p>C:\WINDOWS\TEMP</p>

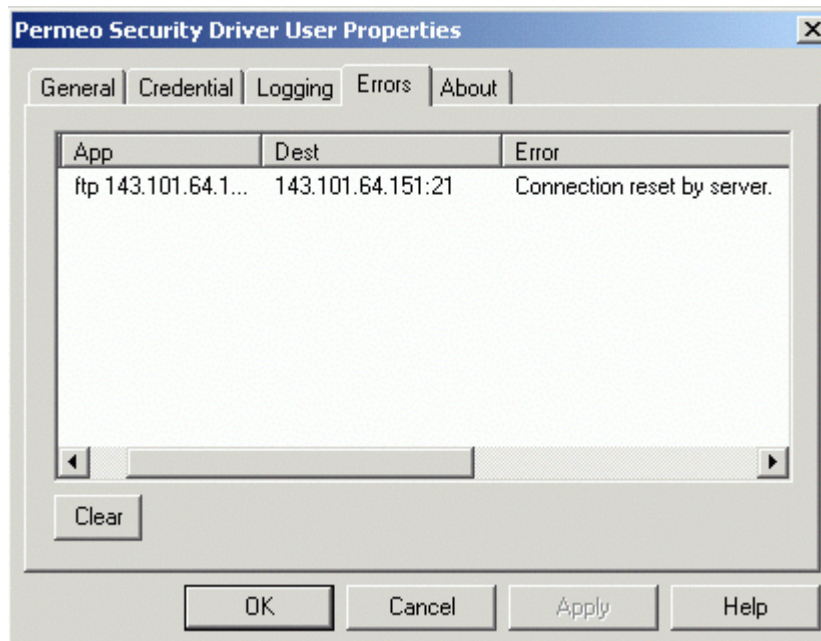
Note: If you have redefined your temporary file path environment variables, or installed your operating system on a different drive, the above directories will change accordingly.

6.2.4 Errors Tab

Use the **Errors** tab in the Security Driver **User Properties** window to quickly diagnose connection problems.


The **Errors** tab is not a replacement for the debug log. It contains a small subset of user-friendly debug messages that can be interpreted by the user. The list of errors will dynamically update, displaying the last 256 errors. When the number of errors exceeds 256, the oldest errors will scroll off the list. Each user login will have its own error list.

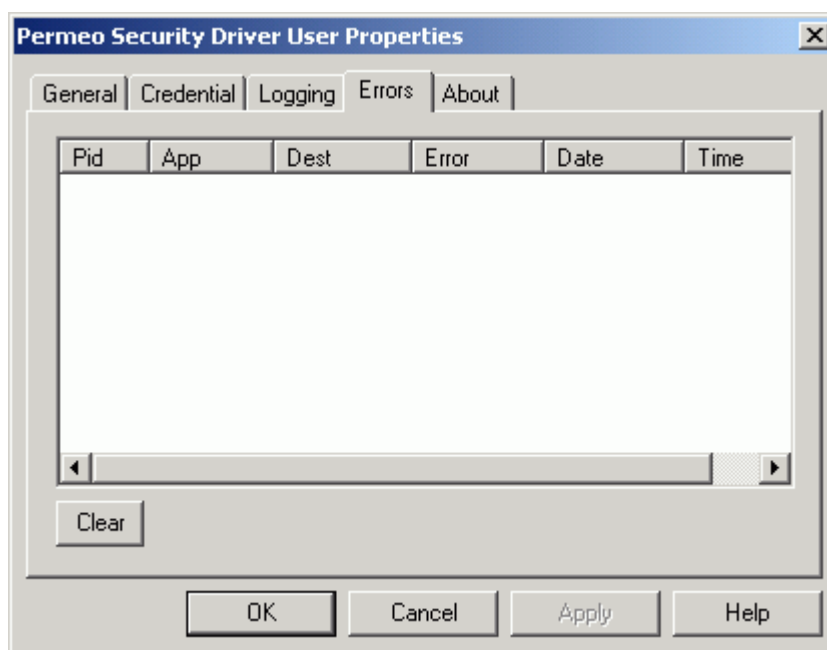
The **Clear** button erases all errors from the list.



The **Errors** tab contains the following fields. You can horizontally scroll or resize the columns on the **Errors** tab to display all of the fields.

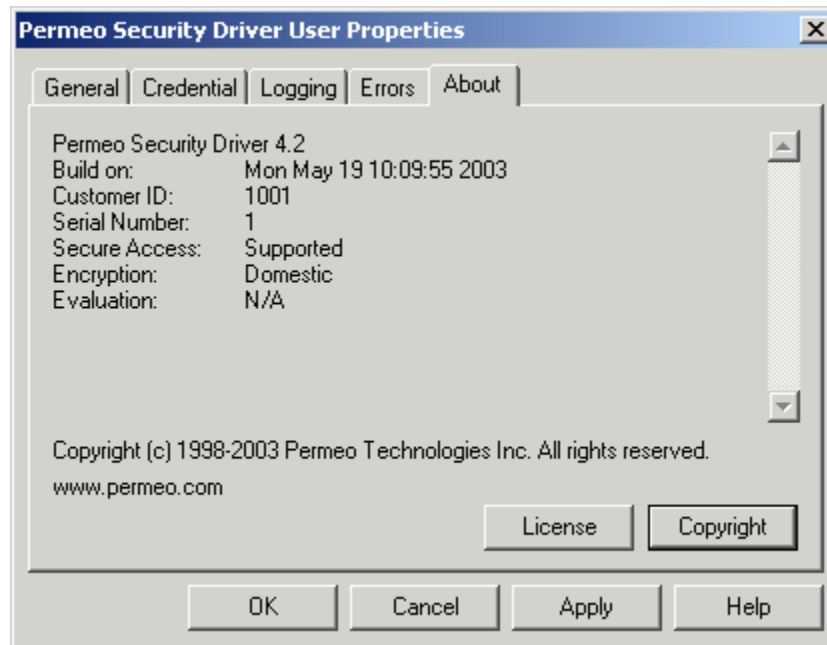
Pid Process ID
App Application
Dest Destination IP
Error Error message
Date Date of error
Time Time of error

Note: When **Show icon on the taskbar** is selected and an error occurs, the system tray icon will show a red exclamation mark  when new errors occur. The user must open the Security Driver User Properties window to view the error descriptions. The tooltip over the taskbar icon will say "Permeo Security Driver encountered errors!". The exclamation point will change back to the normal icon after the user interacts with the taskbar icon or the User Properties GUI.



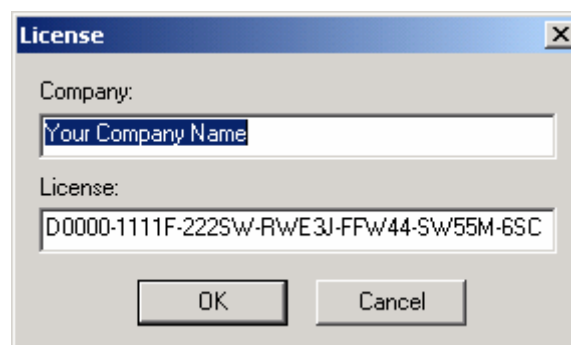
6.2.5 About Tab

The **About** tab allows users to view product version information, view/edit the license key, and read the **Permeo Security Driver** software license.



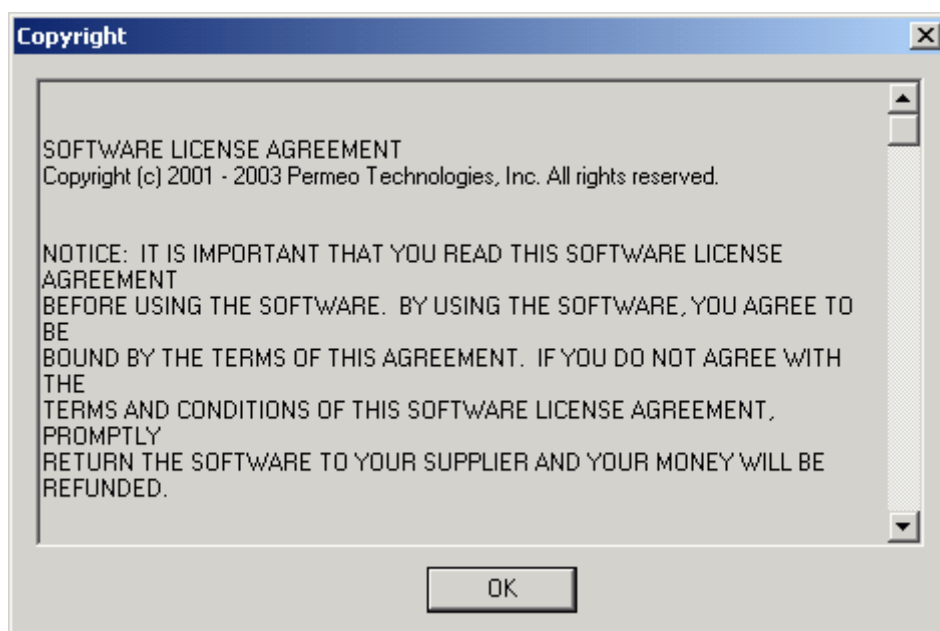
6.2.5.1 View/Enter License Key

- Click the **License** button to view or enter a license key.



6.2.5.2 View Copyright / License Agreement

- Click the **Copyright** to view the software license/copyright agreement.

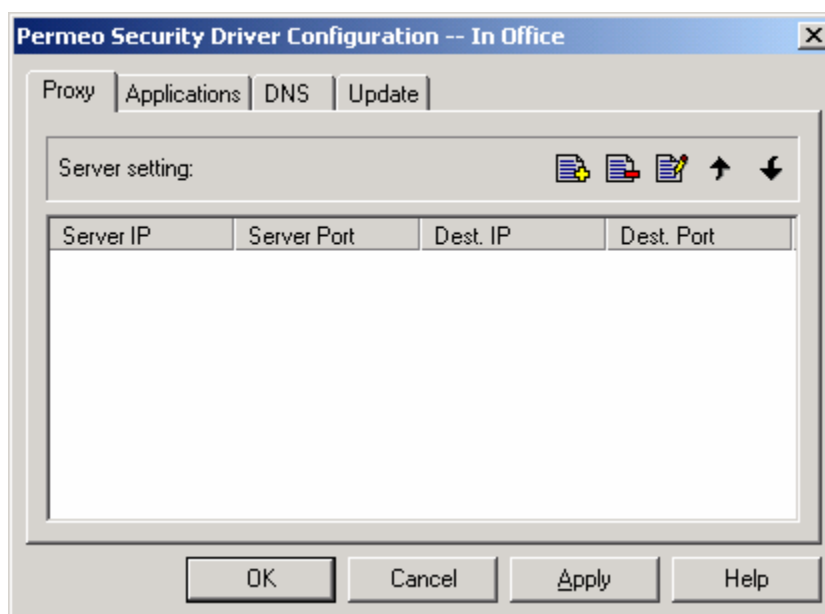


6.3 Configuration Window

The **Security Driver Configuration** window allows administrators and users to configure and view proxy, application, DNS, and update settings.

This window can be invoked from the:

- Security Driver **User Properties** window, **General** tab
(For users to view/edit their configuration settings)
- Security Driver **System Properties** window, **Advanced** tab
(For an advanced user or administrator to create a shared system configuration for multiple users on one machine)



There are four tabs accessible from the **Configuration** window:

Tab	Description
Proxy	The Proxy tab contains the Security Server settings and the proxy requirements to connect to specified destination addresses.
Applications	The Applications tab allows the user to tell the Security Driver which applications to proxy, and to enable/disable Windows Networking Services.
DNS	The DNS tab defines how the Security Driver resolves domain names.
Update	The Update tab can be used to specify a remote configuration file located on a Web server or Security Server – to download preconfigured settings on-demand, or upon every user logon.

6.3.1 Proxy tab

The Proxy tab allows you to add, edit, delete, and reorder your Server proxy entries using the following buttons:



The **New** button opens the **Proxy Properties** window, adding a blank entry under the highlighted entry.



The **Remove** button deletes the highlighted entry.



The **Edit** button opens the **Proxy Properties** window, allowing changes to be made to the highlighted entry.

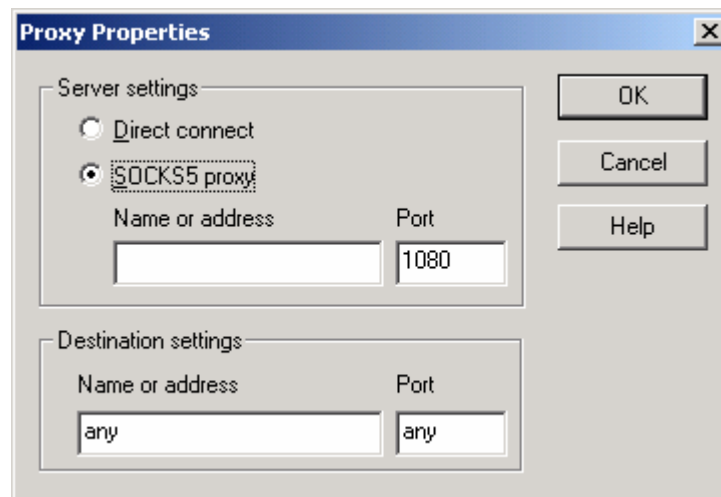


The **Up** button moves the highlighted entry up one line, raising the rule's precedence, or rule order.



The **Down** button moves the highlighted entry down one line, lowering the rule's precedence, or rule order.

Note: To learn about proxy rule precedence, please see section 6.3.1.5 - [Proxy Rule Order with Multiple Servers](#).



To proxy applications, the Security Driver must know:

- The Server host(s) and port(s)
- Server authentication requirements
- Applications for which the Driver requires a proxy Server


Security Driver configuration settings can be set:

- **Manually** – by typing all Server and Destination settings directly into the Driver **User Properties** panel
- or-
- **Automatically** – by downloading a remote configuration file from a Web server or Security Server, or importing a configuration file using the **Administrator's Tool**. Automatic configuration must be setup by a network administrator.

For information on enabling and configuring the **Remote Configuration Download** feature, see section 6.3.4 - [Update tab](#), and section 9.2 - [Remote Configuration Download](#).

For information on importing and exporting Driver configuration files, see section 6.4 - [Administrator's Tool](#).

6.3.1.1 Entering Server Settings

From the **Proxy** tab in the **Configuration** window, click the **New**  button to add a new proxy rule entry. The **Proxy Properties** window appears.

The **Proxy Properties** window is divided into two boxes:

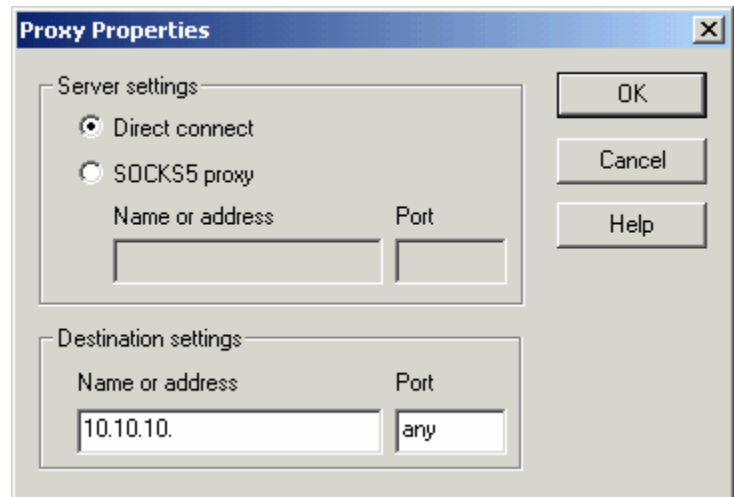
- **Server settings**
- **Destination settings**

Server settings allows the user to indicate whether the Driver bypasses (**Direct connect**) or uses a Security Server (**SOCKS5 proxy**) to connect to an application server. You must enter a specific Server IP address or name in Server settings. Do not use a subnet or port ranges in Server settings.

You must enter data in both the **Server settings** and **Destination settings** boxes to create a proxy rule entry. Click **OK** to create the proxy rule. You can create as many entries as necessary to customize the Security Driver to your environment. After an entry is created, use the **Proxy** tab buttons to add, remove, edit, and reorder entries.

6.3.1.1.1 Connecting Directly to an Address

1. Click Direct connect.
2. Enter destinations to which you directly connect – destinations that do not require a proxy connection. This option connects directly to the specified address, by-passing the **Permeo Security Server**. See section 6.3.1.2 - [Entering Destination Settings](#), for valid entries.



6.3.1.1.2 Using the Security Server to connect to an Application Server

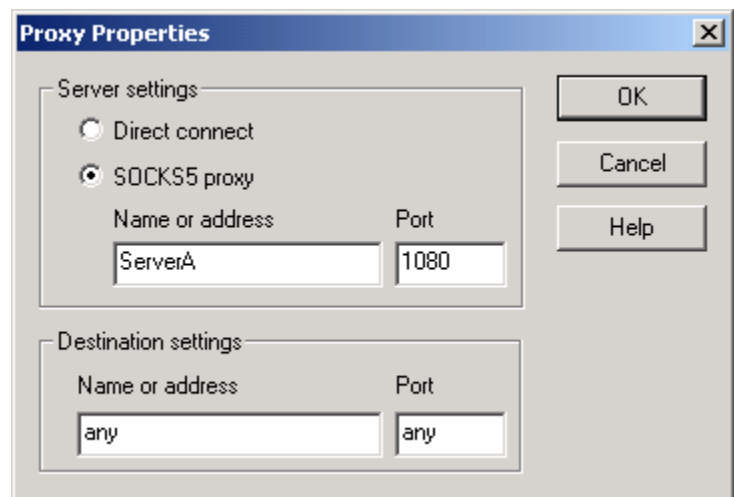
1. Click **SOCKS5 proxy**.
2. Enter the Security Server's IP address or host name in the **Name or address** box. **Server Name or Address** identifies the Server the Driver uses to connect to the application server.

Note: When specifying a **SOCKS5 proxy**, you must enter a specific Server name or IP address. Do not use a subnet.

3. Enter the Security Server's port in the **Port** box.

Note: When specifying a SOCKS5 proxy, you must enter a single port.

4. Enter Destination settings. See section 6.3.1.2 - [Entering Destination Settings](#), for valid entries.

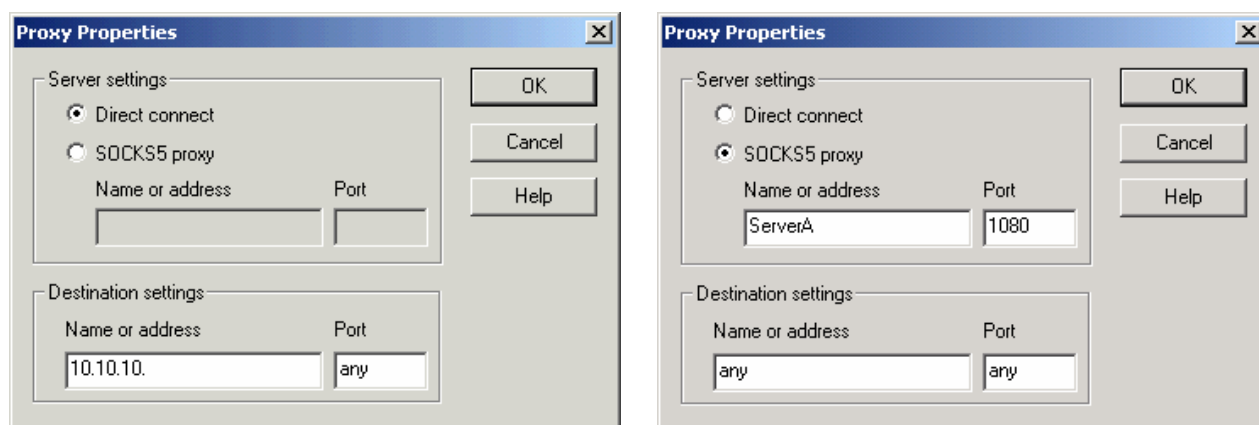


6.3.1.2 Entering Destination Settings

The **Destination settings Name or address** and **Port** identify a specific address, subnet, or domain, and port or range of ports that you can connect to using the Security Server. Enter a specific host name or IP address, or enter a **Dash (-)** or **any** to connect to any address or any port using the Server. After entering both Server settings and Destination settings, click **OK** to complete the entry and return to the Configuration Window's **Proxy** tab.

You can create as many entries as necessary to customize the Security Driver to your environment. After an entry is created, use the **Proxy** tab's buttons to add, remove, edit, and reorder entries.

Please see the following sections for acceptable use of Server host names, IP addresses, Server ports, and proxy rule order.



To enter a Destination:

1. Enter the destination name or IP address in the **Name or address** box. **Destination Name or address** identifies the specific address to which the Security Driver connects using the Security Server.

- or -

Type a **Dash (-)** or **any** to allow the Security Driver to connect to any address on the destination Server.

See section 6.3.1.3 - [Entering Destination Server Host Names and IP Addresses](#), for valid host and IP address syntax.

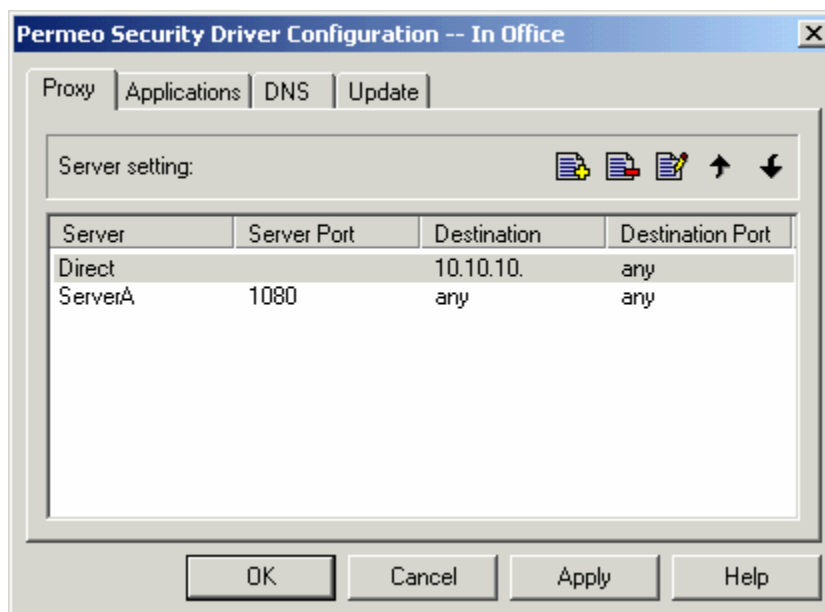
2. Enter the destination port in the **Port** box. **Destination Port** identifies the specific port to which the **Security Driver** connects using the **Security Server**.





- or -


Type a **Dash (-)** or **any** to allow the Security Driver to connect to any port on the destination Server.

See section 6.3.1.4 - [Entering Destination Server Ports](#), for valid port syntax.

- Click **OK** to save the settings and return to the **Proxy** tab of the Security Driver **Configuration** window. All proxy entries are displayed. The order of the entries indicates the order that the Security Driver processes the proxy rules.



- If desired, use the **Proxy** tab buttons to **Remove** , **Edit** , or re-order   highlighted proxy rule entries. For more information on changing rule order with multiple servers, see section 6.3.1.5 - **Proxy Rule Order with Multiple Servers**.
- or -

Click the **New**  button to add another proxy entry below the current entry.

- Click **Apply**, then **OK** to save the current entries.

6.3.1.3 Entering Destination Server Host Names and IP Addresses

The Server recognizes a **Dash (-)** or **any** to indicate any host, or IP addresses and host names using these patterns:

hostip/mask	Use the hostip/mask to mask the host portion of the address from the network or subnetwork portion.
n1.	all hosts in the <i>n1</i> . subnet
n1.n2.	all hosts in the <i>n1.n2</i> . subnet
n1.n2.n3.	all hosts in the <i>n1.n2.n3</i> . subnet
n1.n2.n3.n4	specific IP address
.domain.com	wildcard domain; host must end with <i>.domain.com</i>
host.domain.com	full host name; host must match exactly with <i>host.domain.com</i>

Using Domain Names vs. IP Addresses

The Security Driver uses the following conventions when resolving IP addresses and Domain names used in proxy rules and connections:

Domain names:

When using Domain names in **Direct** and **Proxy** rules, it is important to consistently use Domain names when making connections, not IP addresses.

IP addresses:

When using IP addresses in **Direct** and **Proxy** rules, you can use either IP addresses or Domain names when making connections, as long as the domains can be resolved using DNS.

The following table shows all Domain name and IP address usage combinations, and whether the usage is valid and/or requires DNS to work:

Used in Rule	Used in Connection	DNS Requirement
Domain name	Domain name	Valid usage – No DNS required to work
IP address	IP address	Valid usage – No DNS required to work
IP address	Domain name	Valid usage – Must have DNS to work
Domain name	IP address	Invalid usage – Will not work

6.3.1.4 Entering Destination Server Ports

The Server recognizes a **Dash (-)** or **any** to indicate any port, or the following port syntax:

port number	for example, port 80
service port	for example, Telnet, usually port 23
a range of ports	separated by a comma and enclosed in square brackets, for example [100,1000] specifies ports 100 through 1000, inclusive

Note: Avoid using service port names because some systems lack the ability to convert the service port name to the correct port number.

6.3.1.5 Proxy Rule Order with Multiple Servers

When your Driver uses more than one Server, or when you specify addresses to which you connect directly, you can specify the conditions, or rules, under which the Driver uses each Server.

Proxy rules allow you to:

- Prioritize the order in which the Driver attempts to connect to Servers
- Use specific Servers for different applications
- Use specific Servers for different destinations
- Achieve load-balancing by randomly choosing a Server from a list of Servers

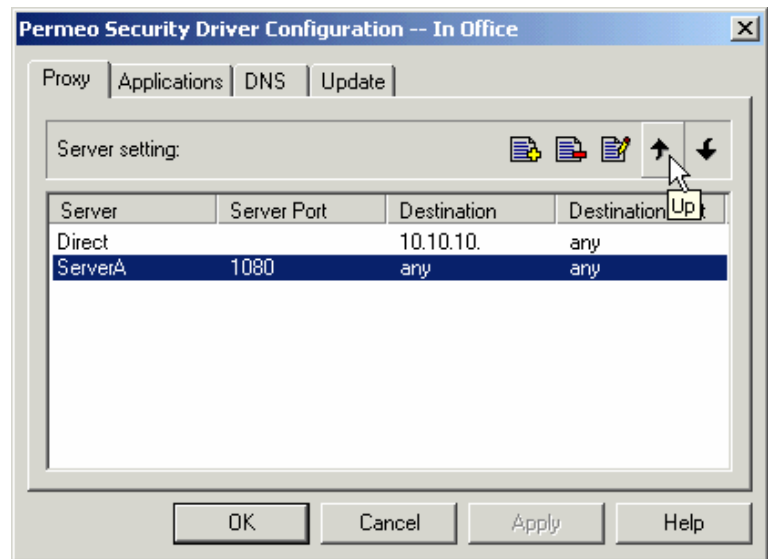
The following sections show how to change the proxy rule order and examples of multiple proxy rule entries, and how rule order impacts Security Driver behavior.

6.3.1.5.1 Changing Rule Order

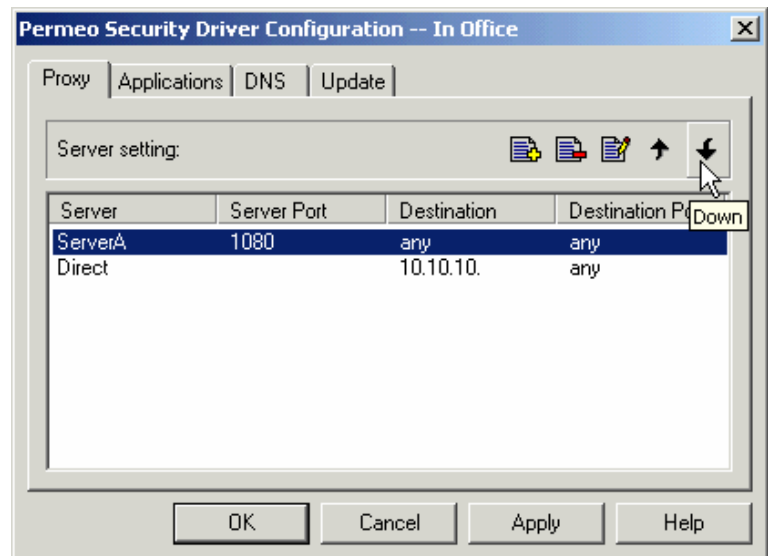
The **Security Driver** sequentially reads and processes each rule in the **Proxy** box in the order listed. The Driver provides an easy method to reorder the rules displayed in the **Proxy** tab.



To raise the priority of a rule, select the rule and click the **Up** button until the rule is in the correct position.



To lower the priority of a rule, select the rule and click the **Down** button until the rule is in the correct position.

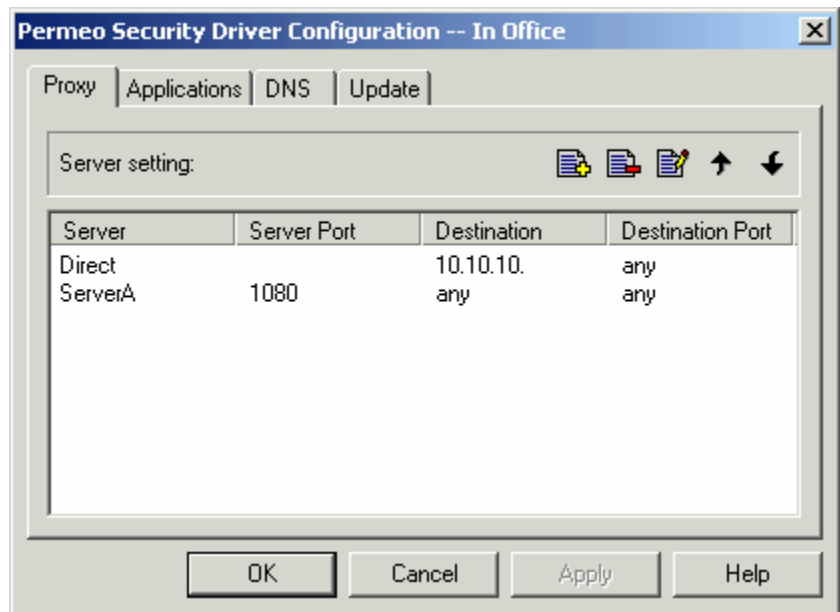


6.3.1.5.2 Proxy Rule Examples

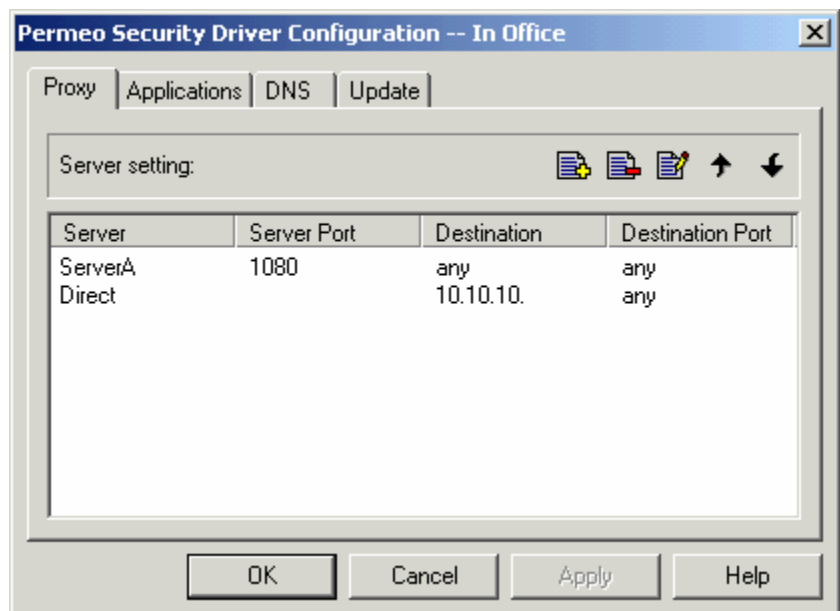
The order of rules in the proxy list is crucial to achieving desired results. The **Security Driver** sequentially reads and processes each rule in the **Proxy** box in the order listed. When a proxy rule matches the Driver's request, it stops checking rules. The following examples show how the order of rules determines how proxy requests are processed.

Proxy Rules Example 1

- The first rule specifies that all requests go Direct (by-passing the Security Server) for any host in the 10.10.10 network, while all other requests use ServerA.



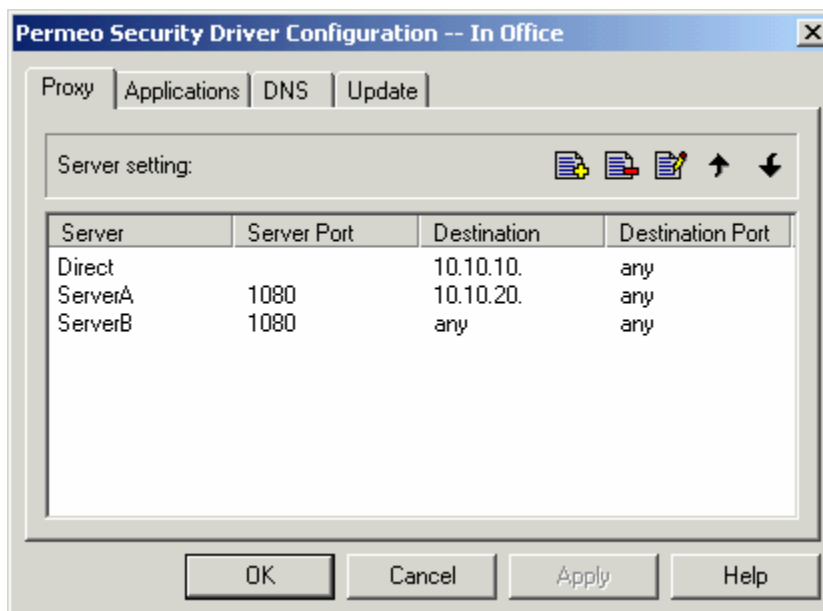
- If the same rules were in the reverse order, the first rule would satisfy the Driver's request, and it would never process the second rule. ServerA would process all requests.



Proxy Rules Example 2

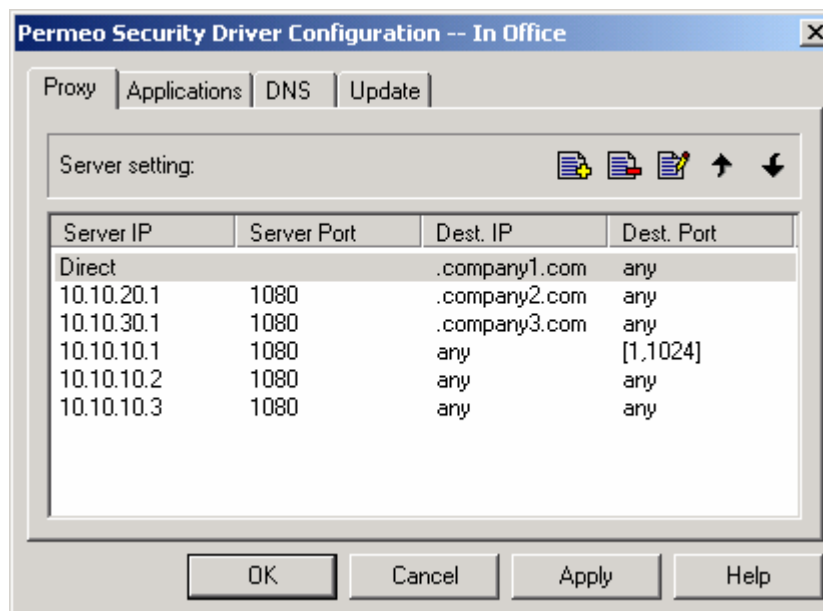
This example describes how the Security Driver processes these rules, assuming your local subnet is 10.10.10.:

- **Rule 1:** Specifies that all requests go Direct (by-passing the Security Server) for any host in the 10.10.10 network.
- **Rule 2:** Specifies that all traffic bound for the 10.10.20 network uses ServerA.
- **Rule 3:** Specifies that all other requests (not covered by rules 1 and 2) use ServerB.



Proxy Rules Example 3

- **Rule 1:** Connection requests to any host in the **.company1.com** domain connect directly – without using the Security Server. When the Driver processes a request to connect to a host in **.company1.com**, it does not process the remaining rules. The Driver stops evaluating rules when it finds a match.
- **Rule 2:** Traffic bound for the **.company2.com** network goes via Server 10.10.20.1.



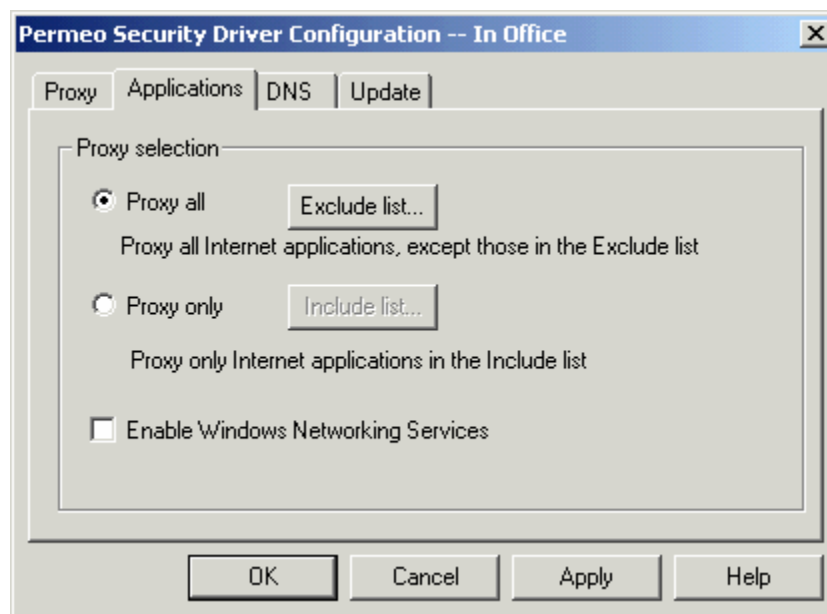
- **Rule 3:** Traffic bound for the **.company3.com** network goes via Server 10.10.30.1.
- **Rule 4:** All traffic bound for ports in the range 1 through 1024 uses Server 10.10.10.1.
- **Rules 5 and 6:** For all other traffic, the Security Driver load-balances between Servers 10.10.10.2 and 10.10.10.3.

Note: If the last rule were first, the Driver would use 10.10.10.3 for all connection requests and would never process the other rules.

6.3.2 Applications tab

The **Applications** tab allows the user to tell the Security Driver which applications to proxy, and to enable/disable Windows Networking Services.

In the **Proxy selection** box, you must choose between **Proxy all** and **Proxy only**, then indicate which applications you want to **Exclude** or **Include**.



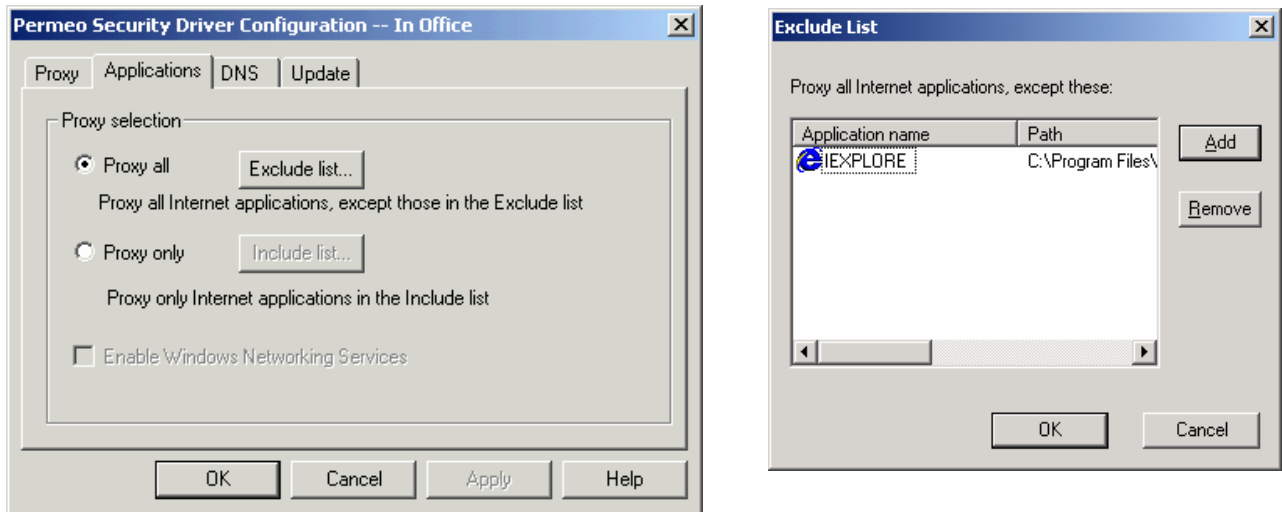
- Select **Proxy All** to proxy all applications, except those listed in the **Exclude list**.
- Select **Proxy Only** to proxy only those applications listed in the **Include List**.

Note: When adding applications to either the **Include** or **Exclude** list, make sure to add all necessary executables (files ending with .exe) for that application – since some applications have more than one executable file.

- Click **Enable Windows Networking Services** to access remote files and printers on a Windows network.

6.3.2.1 Proxy All applications except those in Exclude List

Select **Proxy All** to proxy all applications, except those listed in the **Exclude list**.



To add applications to the **Exclude List**:

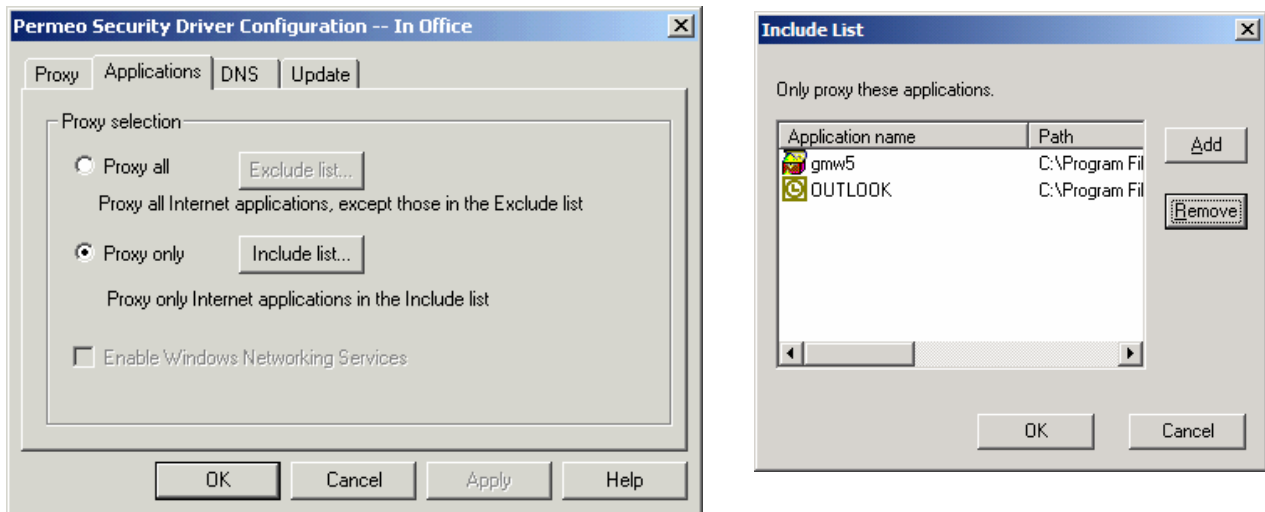
1. Select **Proxy all**.
2. Click the **Exclude list** button to open the **Exclude List** window.
3. Click **Add** and navigate to and select the executable file for the application.
- or -
Drag application icons from the Windows Desktop to the **Exclude List** window.
4. Repeat step 3 to exclude as many applications as needed.
5. Click **OK** when finished adding applications.

To delete an application from the **Exclude List**:

1. Select **Proxy all**.
2. Click the **Exclude list** button to open the **Exclude List** window.
3. Select the application to remove.
4. Click **Remove**.
5. Click **OK** when finished removing applications.

6.3.2.2 Proxy Only applications specified in Include list

Select **Proxy Only** to proxy only those applications listed in the **Include List**.



To add applications to the **Include List**:

1. Select **Proxy only**.
2. Click the **Include list** button to open the **Include List** window.
3. Click **Add** and navigate to the executable file for the application.
- or -
Drag application icons from the Windows Desktop to the **Include List** box.
4. Repeat step 3 to include as many applications as needed.
5. Click **OK** when finished adding applications.

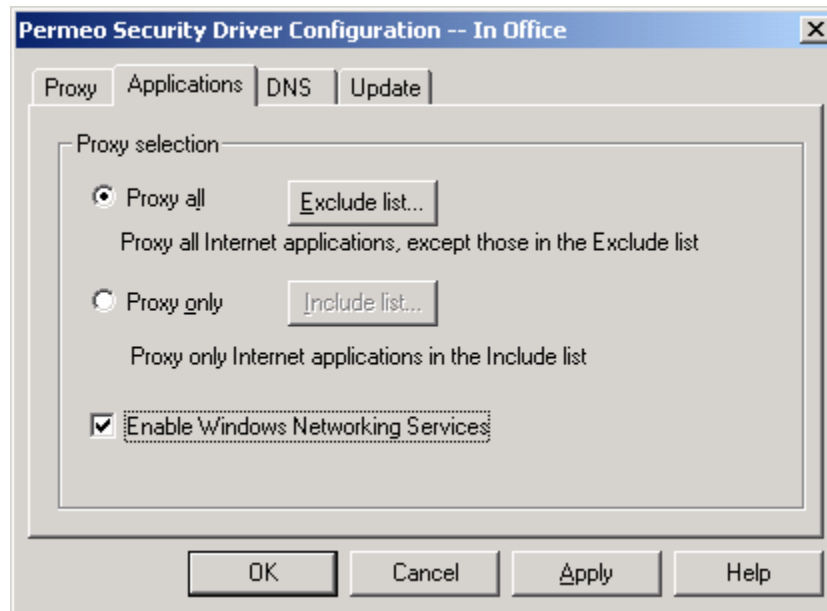
Note: Some applications, including Netscape® Navigator and Communicator, and Microsoft® Internet Explorer include built-in SOCKS capability. If you are using the built-in SOCKS capability, do not SOCKS-enable those applications with the **Permeo Security Driver**.

To delete an application from the **Include List**:

1. Select **Proxy only**.
2. Click the **Include list** button to open the **Include List** window.
3. Select the application to remove.
4. Click **Remove**.
5. Click **OK** when finished removing applications.

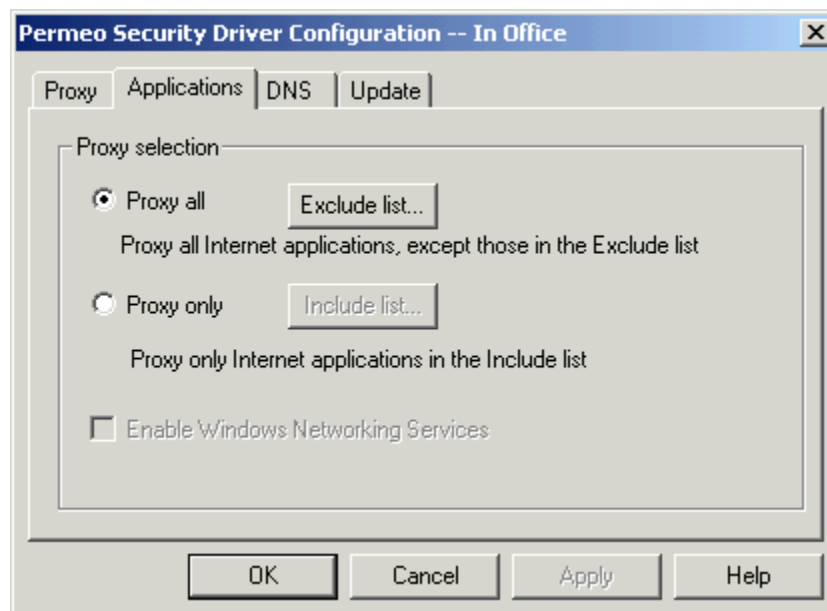
6.3.2.3 Enable Windows Networking Services

Click **Enable Windows Networking Services** to enable the Security Driver to access remote files and printers on a Windows network.



Note: This feature is only available through the **Permeo Driver Secure Access** package, and is supported only on Windows 2000 and XP platforms.

If you have not installed the **Driver Secure Access** package, the **Enable Windows Networking Services** feature will be unavailable (grayed out) as shown below:



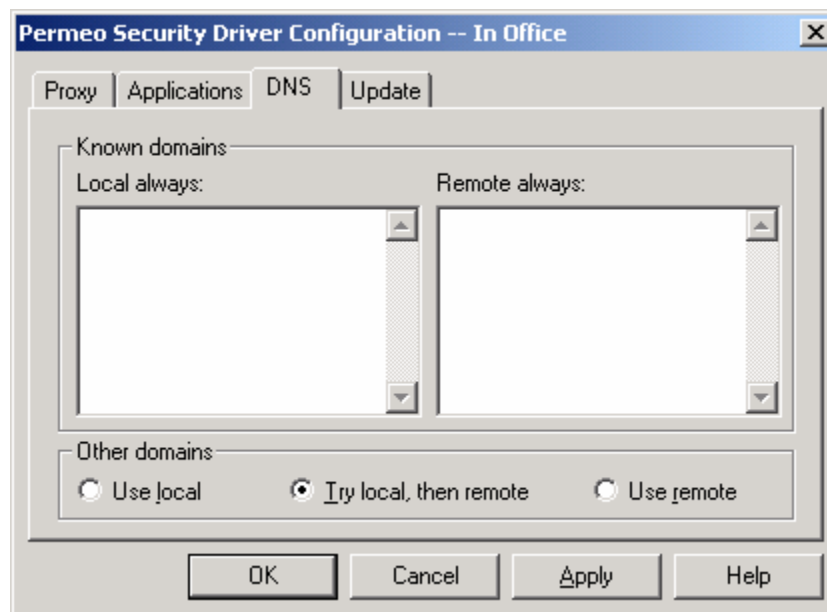
To configure Microsoft Networking Services support on the client, you must:

- Install the **Driver Secure Access** package
- Have a valid WINS server configured on a Windows host
- Obtain the required credential, account, and workgroup information on the client.
- Set your client computer to use the WINS server
- Enable the **Microsoft Networking Services** feature in the Security Driver's Configuration window Applications tab
- Restart your Windows system

Note to Administrators: Detailed information on server requirements and configuring the client to run Microsoft Networking Services is available in section 8 - [Configuring Remote File and Printer Sharing for Administrators](#) later in this document. In addition, a network administrator must configure the **Permeo Security Server** to support Microsoft Networking Services.

6.3.3 DNS tab

The **DNS** tab defines how the **Security Driver** resolves domain names. The window is divided into **Known domains** and **Other domains**. Enter the **Known domains** by typing domain names in the appropriate columns. Use space to separate multiple domain names. The DNS tab is most useful when the Driver machine and Server machine use different DNS servers.



6.3.3.1 Resolving Domain Names

- **Local always:** To define domain and host names the Driver resolves. The Driver attempts to resolve domain names and fails connection attempts it cannot resolve. Enter all the domains that you know can be resolved by the local machine in the **Local always** list.
- **Remote always:** To define domain and host names the Security Server resolves for the Driver. Enter all the domains that you know can be resolved by the remote machine in the **Remote always** list.
- **Other domains:** For domains that are not in either **Local always** or **Remote always** categories, the Driver uses **Other domains** to define the priority to resolve domain names.
 - When you choose **Use local**, the Driver attempts to resolve domain names and fails connection attempts it cannot resolve.
 - When you choose **Try local, then remote**, the Driver attempts resolution. If the Driver fails to resolve the name, the Server attempts resolution.
 - When you choose **Use remote**, the Driver requests that the Server resolve domain and host names.

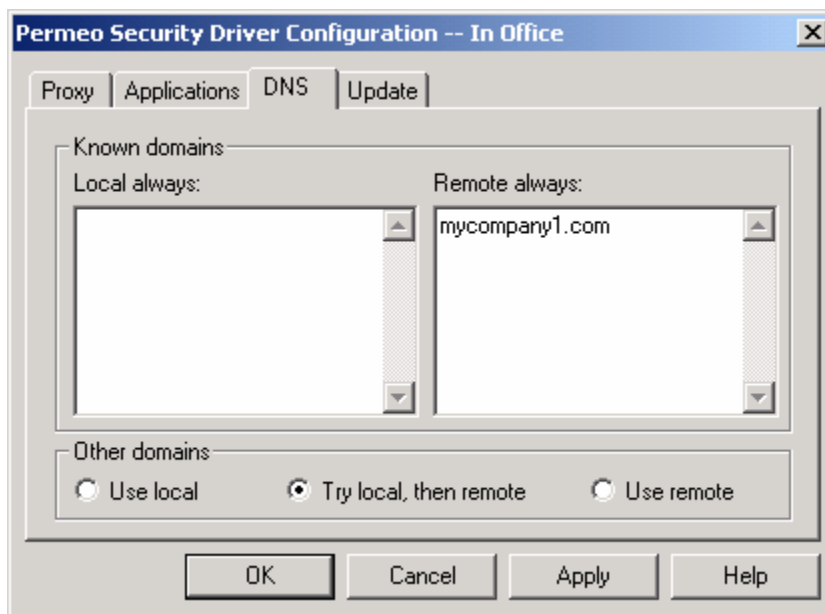
Note: It is no longer required to have a DNS Server entry in the Windows Internet Protocol (TCP/IP) Properties window. The Driver will function without it. However, if you do not have a DNS Server, then you must configure the Driver with a remote option, such as **local then remote**, or **remote always** on the Security Driver Configuration **DNS** tab.

6.3.3.2 DNS Examples

DNS Example 1

This examples assumes you work from home to access your company resources (**mycompany1.com**) via the **Permeo Security Server**. Since your Driver machine's DNS server is provided by your ISP, it cannot resolve internal machines in your company network.

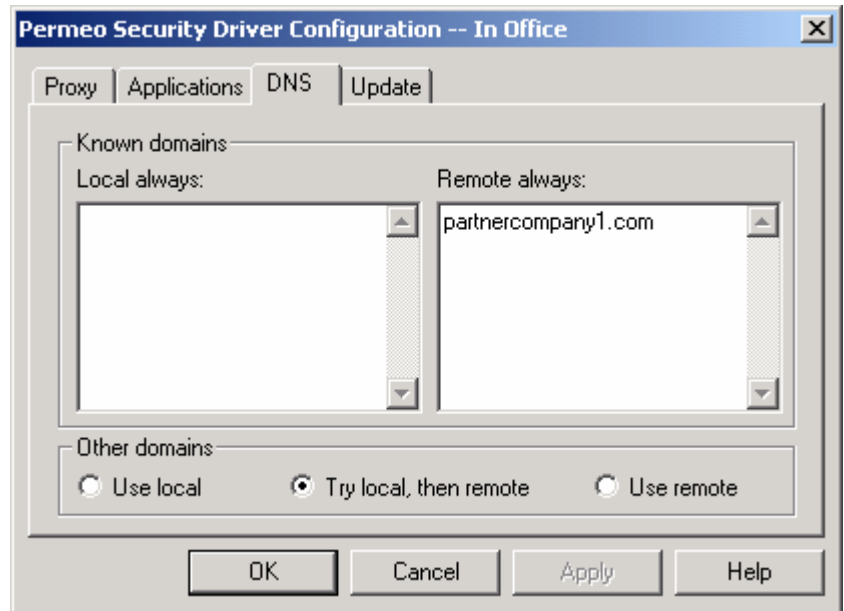
In this case, you would specify **mycompany1.com** as **Remote always**.



DNS Example 2

Now you are back at the office, working on **mycompany1.com**, but you are using your partner company's **Permeo Security Server** to access their resources.

In this case, you would specify **partnercompany1.com** as **Remote always**.



6.3.4 Update tab

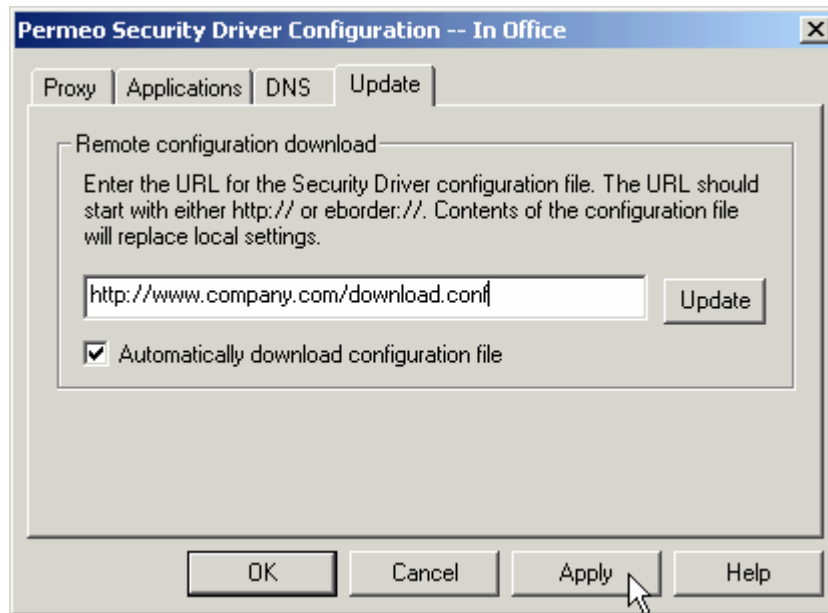
The **Update** tab provides a **Remote Configuration Download** option that allows network administrators to create a Driver configuration file and store it on a Web server or Security Server in a centralized location. The **Security Driver** can connect to the URL or Security Server, copy the file locally, and activate (and override) the settings for the Driver on the client machine.

This option simplifies Security Driver setup in a networking environment where groups of Driver users require the same configuration. The configuration file can be set to download on-demand, or to download every time the user logs on.

The following sections detail the **Remote Configuration Download** feature. For other advanced configuration options and more detail on the **Remote Configuration Download**, please see section 9 - [Advanced Configuration Options for Administrators](#) later in this document.

The **Remote Configuration Download** feature allows a network administrator to:

- Create one Security Driver configuration file for use by several machines
- Centrally manage and control Security Driver settings
- Easily make changes to settings for many users by changing one file
- Provide users with consistent and immediate configuration updates
- Allow users to update their configuration on-demand, or automatically upon logon



6.3.4.1 Remote Configuration Download – On-demand

A remote configuration file can be downloaded on-demand whenever a network administrator wants to distribute a standardized configuration, or when users want to restore their configuration back to the network standard. The advantage of the on-demand update is that users can update whenever they want, and choose to use the downloaded settings as is, or further customize their settings by making changes to their configuration through the **Configuration** window. Administrators can put a **Security Driver** configuration file either on a Web server or a **Permeo Security Server**.

Note: When the **Update** is performed, only the settings for the selected **Zone of Service** are updated. Before you **Update**, be sure to **Edit** the configuration in the **Zone of Service** that you want to update (**In Office**, **Out of office**, or **Wireless**) from the User Properties **General** tab.

To specify the configuration file and download settings on-demand:

1. From the **Update** tab, type the **URL** or **Security Server** name that contains the pre-configured **Security Driver** configuration file. (See entry examples below.)
2. Click **Update** to copy the remote configuration file, overriding the local Driver settings for the selected **Zone of Service**.
3. Downloaded configuration data will override all local settings in Proxy, Application, DNS, and Update tabs. Upon updating, it is even possible that the URL or Server name on the Update tab could change. The Security Driver displays a prompt to indicate that the update was successful. Click **OK**.

Note: Users must obtain the URL of the configuration file or the Security Server name from their network administrator for the initial update. If the path, name, or syntax is invalid, the Security Driver displays an error prompt indicating the update failed. Click **OK** and try again.

Examples

- **To enter a URL:** You must enter the complete URL for the configuration file, for example: **http://www.company.com/download.conf**
- **To enter a Security Server:** You only need to specify **eborder://** followed by the name of the Security Server where the file is located. It is not necessary to enter a filename, as it must be specified by your administrator in the Server configuration, for example: **eborder://SecurityServer1**

Notes to Administrators:

- When preparing the remote configuration file, you must be sure to enter the target URL or Security Server name for the remote configuration file location. When users initially perform the **Update** function, they must enter the same target URL or Security Server name. Each subsequent time the **Update** is performed (upon user logon), the URL or Server Name is provided by the remote configuration file.
- To create a configuration file that users automatically download each time they logon, enable **Automatically download configuration file** when you are preparing the remote configuration file. Please see the following section.

6.3.4.2 Remote Configuration Download – Automatic

This option is for advanced users and network administrators who are configuring the Security Driver for other users. Use this option to automatically update the configuration file each time the user logs on – guaranteeing that all designated users are using the same configuration. This option ensures uniformity of settings – any changes users make to their local Security Driver settings will be overwritten the next time they logon.

To specify that the configuration file be downloaded each time a user logs on:

1. Perform steps 1-3 listed under **Remote Configuration Download – On-demand** above. A valid configuration file URL or Security Server name must be properly entered and successfully updated.
2. Check **Automatically download configuration file**.
3. Click **Apply** for the setting to take effect.

Note to Administrators: When preparing the remote configuration file for users to automatically download each time they logon, you must enable **Automatically download configuration file**. If you do not enable **Automatically download configuration file** in the source file, the configuration file will be updated only one time – when the user clicks **Update**. When the remote configuration file updates the current settings, if the box is not checked in the remote configuration file, the Driver will not download the next time the user logs on.

6.4 Administrator's Tool

The **Permeo Security Driver** provides an **Administrator's Tool** to manually export and import configuration settings to and from a file, and Ping and Traceroute diagnostics to verify connectivity to a Security Server. Generally, this tool is used by network administrators to create centralized configuration files to be used by groups of users, as well as troubleshoot Server problems. The Import/Export functions of the **Administrator's Tool** lend flexibility to advanced users and administrators who configure the Security Driver for others.

Potential uses for Import/Export are:

- Export a configuration file that will later be shared with (imported by) other users, or put on a Web server or Security Server for users to download. For more information on the **Remote Configuration Download** feature, see section 6.3.4 - [Update tab](#), and section 9 - [Advanced Configuration Options for Administrators](#).
- Import a configuration file to override current settings
- Export a configuration file to have as a backup
- Import a backup file to restore settings to original configuration

To start the Security Driver **Administrator's Tool**:

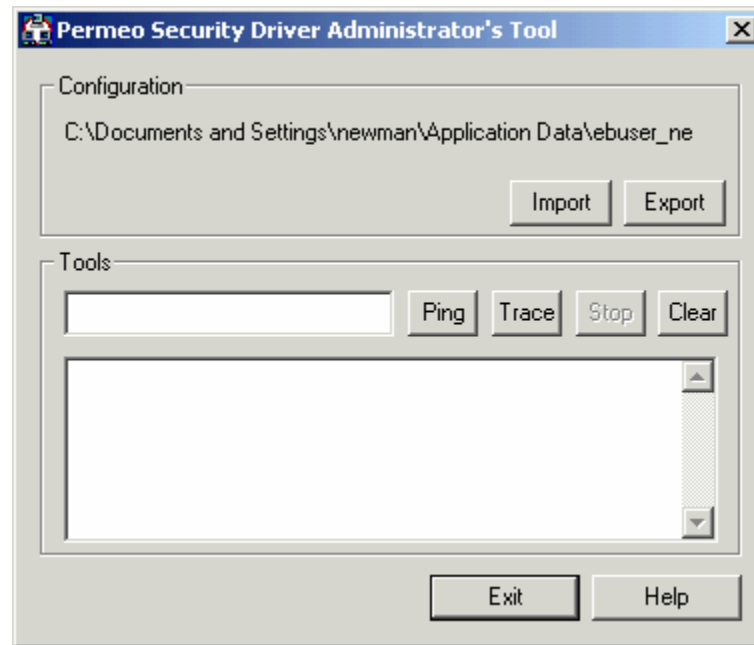
1. Run the **Administrator's Tool** from the **Start** menu:

Click **Start > Programs > Permeo Security Driver > Administrator's Tool**

- or -

From Windows Explorer, go to your **Permeo Security Driver** INSTALLDIR (the default installation directory is c:\Program Files\Permeo\Security Driver) and run **EBAdmin.exe**.

2. The **Administrator's Tool** window appears, displaying the current configuration file.

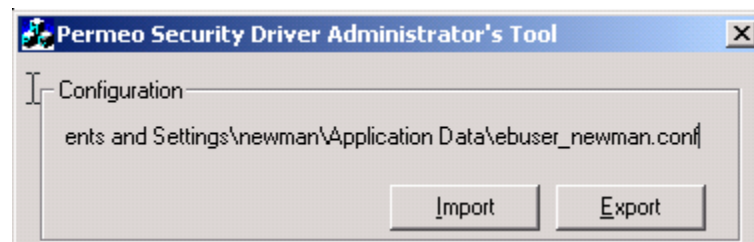


6.4.1 Configuration Filenames

Upon loading, the **Administrator's Tool** automatically shows the Security Driver configuration file that is currently in use:

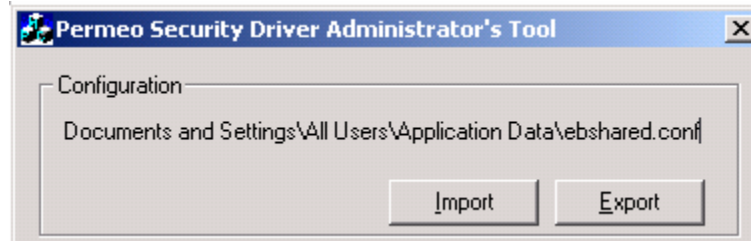
- If the **Allow non-administrator users to change configuration** feature is ENABLED in the System Properties window, a separate Driver configuration file is stored for each user in the Windows application data directory.

The user configuration file is named **ebuser_username.conf**, where *username* is the User's logon name.



- If the **Allow non-administrator users to change configuration** feature is DISABLED in the System Properties window, one shared system configuration file is stored in the Windows application data directory on that machine for use by all users on that machine.

The shared system configuration file is named **ebshared.conf**.

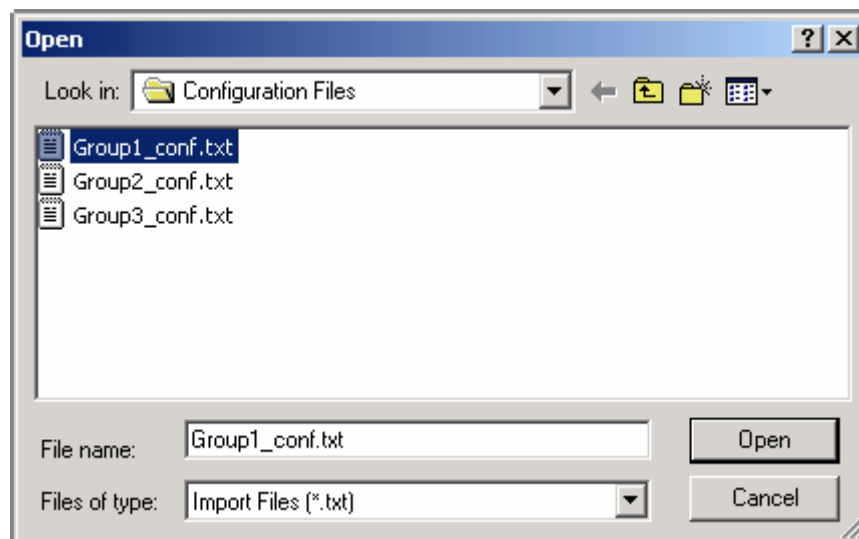


6.4.2 Importing a Configuration File

In some environments, an administrator may give users a Security Driver configuration file directly, for example, as an e-mail attachment, or place it on a network server. Users can manually import the configuration file to override their local Driver settings.

Note: When importing a configuration file, all configurations (**In Office**, **Out of office**, and **Wireless**) will be imported.

1. Make sure your Permeo Security Driver **User Properties** window is closed.
2. Click the **Import** button in the **Administrator's Tool** window.
3. Enter the filename, or browse to locate the file to import.
4. Click the **Open** button or press **Enter** to import the file and override the current Security Driver settings. The active Driver configuration file will be updated.



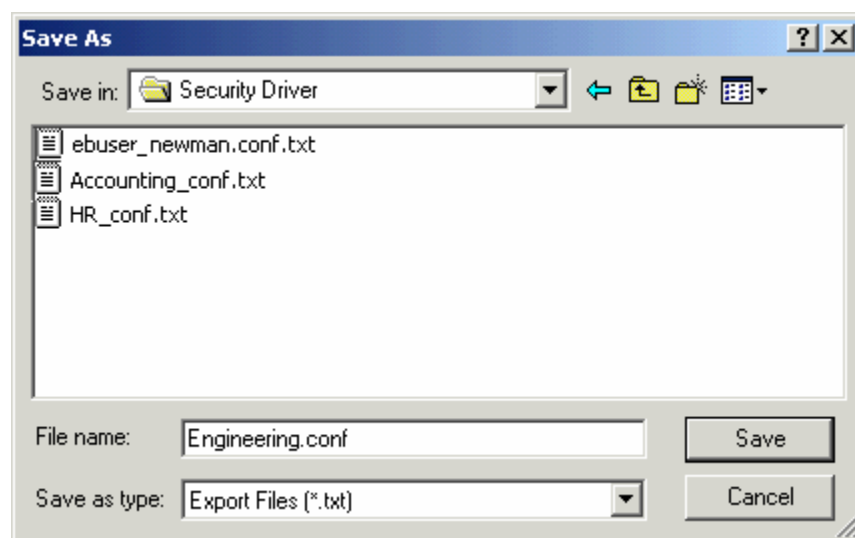
6.4.3 Exporting a Configuration File

An administrator can configure the Security Driver and export the configuration settings to a specific filename and location.

Note: When exporting a configuration file, all configurations (**In Office**, **Out of office**, and **Wireless**) will be exported. Exported configuration file does not include user credential information or any settings contained in the Driver System Properties.

1. Make sure you have all sections for all service zones configured as desired.
2. Click the **Export** button in the **Administrator's Tool** window.
3. Browse to a location where you want to save the Driver configuration file, and enter a filename.
4. Click **Save**. The file can then be sent to users to **Import**, or put on a Web server or Security Server for users to download.

For more information on the **Remote Configuration Download** feature, please see section 6.3.4 - [Update tab](#), and section 9 - [Advanced Configuration Options for Administrators](#).



6.4.4 Driver Diagnostics

The Administrator's tool offers Ping and Traceroute diagnostics that could be helpful while diagnosing network connectivity issues. The Ping and Trace tools allow users to run ping and trace functions provided by the **Permeo Security Server**.

Ping	Executes a ping command to the host in the Destination box and displays the result in the message window
Trace	Executes a traceroute command to the host identified in the Destination box and displays the result in the message window
Stop	Cancels the ping or traceroute command
Clear	Clears the diagnostic message window

7 Wireless LAN Solution

Permeo offers a Wireless LAN (WLAN) solution through the combined use of the Security Server and Security Driver. In addition to the “in office” and “out of office” configurations, users can choose to create a “wireless” configuration on the client to ensure secure wireless connections between the Driver and the Security Server.

7.1 Security Server Requirements

To use the Wireless LAN solution, the Security Server requires the following:

- The **Server Encrypt SSL** plug-in must be properly installed, configured, and enabled on the Security Server. When the **Wireless** setting is active on the Driver, all connections are protected by SSL, even when the Security Server's policy does not require SSL authentication. Meaning that an **auth** rule in the Policy editor is not required for the Wireless LAN solution to function. However, if you do use an **auth** rule, it will be combined with ssl.

For example, if you specify:

```
auth - - u
```

it will function as if you specified:

```
auth - - su
```

- If the Driver is set to use the wireless **Auto-Detect** option, then the SERVER_DETECT global variable must be set to **on**. From **Server Manager**, click the **Properties** button, select the **Advanced** tab, then change SERVER_DETECT to the desired value.

7.2 Client Requirements & Options

To use the Wireless LAN solution, the **Security Driver** and the **Driver Encrypt SSL** plug-in module must be installed on the client machine. If the Encrypt SSL plug-in module is not installed on the client machine, the **Wireless** option will not be available.

7.2.1 Wireless Auto-Detect Server Option

The wireless configuration has two options for connecting to a Security Server: **Auto-Detect** mode and the standard **Proxy** rules.

- If **Auto-Detect** is selected, the Driver will automatically locate a Security Server. Auto-detect is done per connection. When you make a connection, the Driver will actively search for an available Security Server. The Driver will use the first Server it detects to make a connection. On the Driver side, there is no way to control or specify which Server to use when **Auto-Detect** is in effect.

Note: When **Auto-Detect** is selected, any rules previously defined in the **Proxy** tab are preserved, but not used.

- If **Auto-Detect** is not selected, rules defined in the **Proxy** tab will be used.

All other wireless configuration options (on Applications, DNS, Update tabs) function the same as **in office** and **out of office** configurations.

8 Configuring Remote File and Printer Sharing for Administrators

The **Permeo Security Driver Secure Access** package provides support for Microsoft Networking Services. After you have installed the Permeo **Secure Access** package, the **Configuration** window **Applications** tab displays a check box labeled **Enable Windows Networking Services**. This is an advanced feature that allows a user to securely browse files and share printers in their office network from a computer in a remote location. However, this capability will require some setup by a network administrator on the network to be browsed, and some setup by the user on the client machine.

The Windows Networking Services feature requires a client and a server component. The client component is the Security Driver, and is only supported on Windows 2000 and XP. The server component may be a Windows or UNIX Security Server.

This section outlines:

- Network requirements for Microsoft Networking Services
- Client requirements for Microsoft Networking Services
- How to change the client computer's workgroup
- How to set the client computer to use the network WINS server
- How to enable Microsoft Networking Services on the Security Driver
- How to disable/enable NetBIOS on the client

8.1 Network Requirements

The Security Driver will support Microsoft Networking Services only if the network to be browsed meets the following requirements:

- The network has a domain.
- The network is running a Microsoft WINS server on the Primary Domain Controller (PDC).
- The PDC must grant the user access to the WINS server.
- The network is running a Permeo Security Server on a Windows 2000 or UNIX system.
- The Security Server must run on a different machine than the PDC.
- The machine the Security Server is on must have NetBIOS disabled.
- The Security Server must grant the user access for remote file and printer sharing (ports UDP 137, UDP 138, and TCP 139).

8.2 Client Requirements

The Security Driver requires the following to be set up on the client machine before a user can browse the remote network.

- A credential (username and password) for the network PDC.
- A credential for the remote resources to be accessed. This usually is, but may not be, the same credential as the domain login.
- A local account and local workgroup to match the domain login and network domain, respectively.
- Set the client computer to use the network WINS server.
- Enable Microsoft Networking Services on the Security Driver.

8.3 Changing the Workgroup

Before a user can browse the remote network, the Security Driver requires a local account and local workgroup be set up to match the domain login and network domain, respectively. When the user's computer is in a remote location from the network to be browsed, they may not login to the remote domain. This would be insecure, because joining a domain is only secure when the client computer is physically connected to the local network of the domain controllers. Remote domain login attempts will fail after a long timeout. This means that when the user's computer is removed from the company network, they must login to a local account and local workgroup. It is best to create a local account with the same username and password as the user's domain login, and a local workgroup with the same name as the network domain.

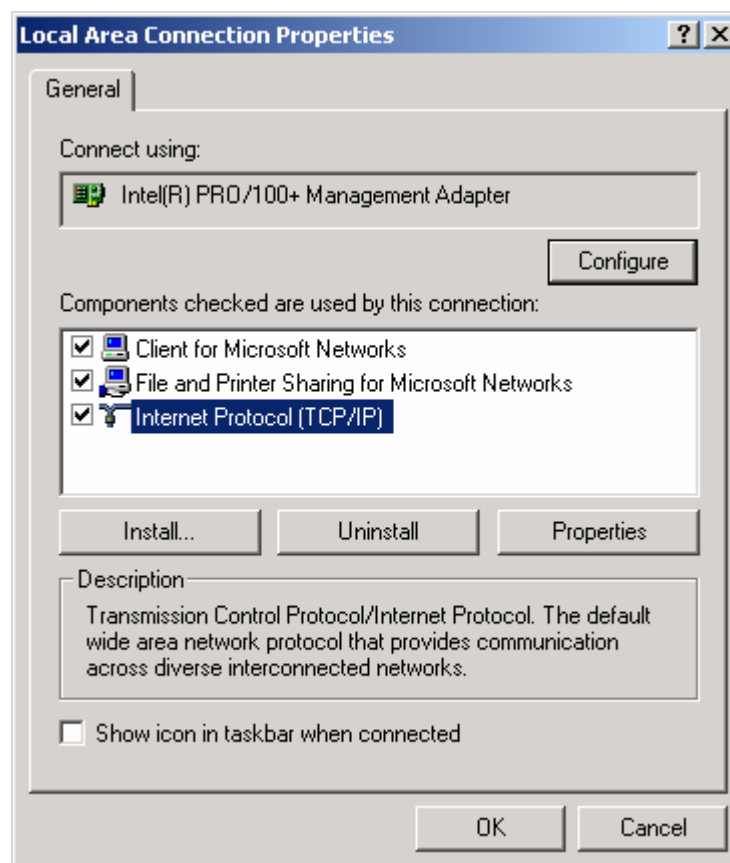
To change your computer's workgroup on Windows 2000:

1. Login to an account with administrator privileges.
2. From the system taskbar, click:
Start > Settings > Control Panel
3. From the **Control Panel**, double-click the **Network and Dial-up Connections** applet.
4. Select the **Advanced** menu, then the **Network Identification...** menu item.
5. From the **Network Identification** tab, click the **Properties** button
6. Select the **Workgroup:** radio button, and set the workgroup name as desired.
7. Click the **OK** button on the dialog.
8. After a few seconds, you will see a "**Welcome to the ... workgroup**" message box. Click **OK** and read the warning that states: "**You must reboot this computer for the changes to take effect.**"
9. Click **OK** for another message box that asks, "**You must restart your computer before the new settings will take effect. Do you want to restart your computer now?**" You may answer **No** if you do not wish to wait for a reboot. For Windows 2000 and Windows XP, you do not need to reboot before Microsoft Networking Services will work.

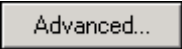
8.4 Setting the client computer to use the network WINS server

To set the WINS server on Windows 2000:

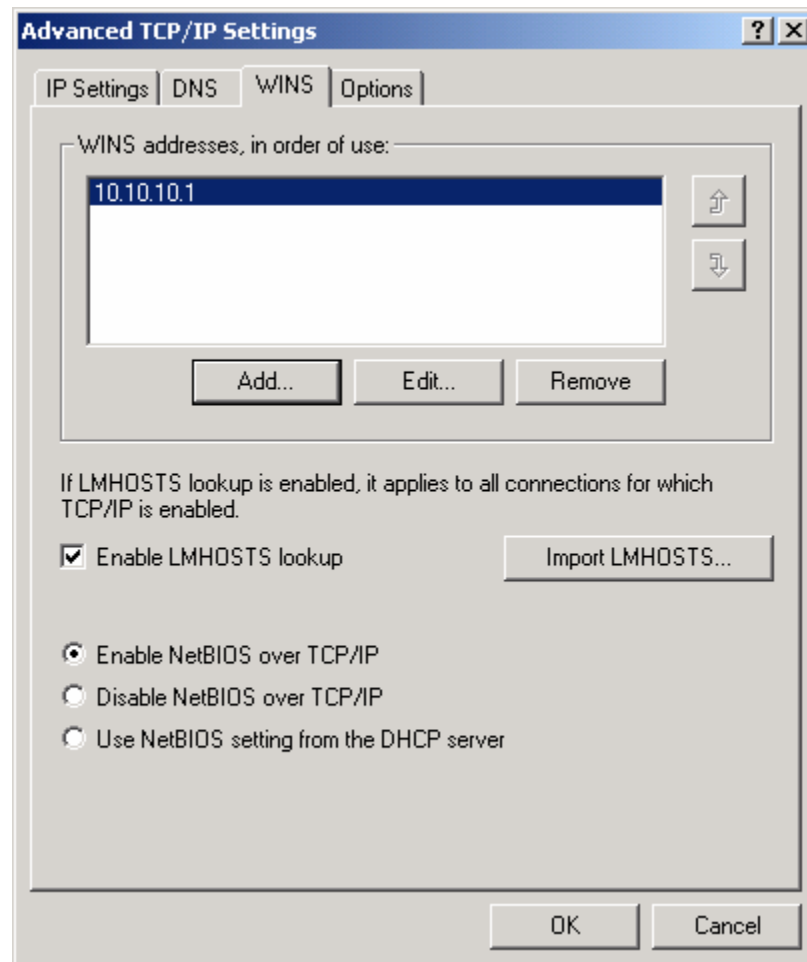
1. From the system taskbar, click:
Start > Settings > Control Panel
2. From the **Control Panel**, double-click the **Network and Dial-up Connections** applet.
3. Right-click the **Local Area Connection** icon, and select the **Properties** menu item.
4. Select **Internet Protocol (TCP/IP)** from the list, and click the **Properties** button.



- From the **General** tab of the **Internet Protocol (TCP/IP) Properties** window, click the **Advanced** button, and select the **WINS** tab page.



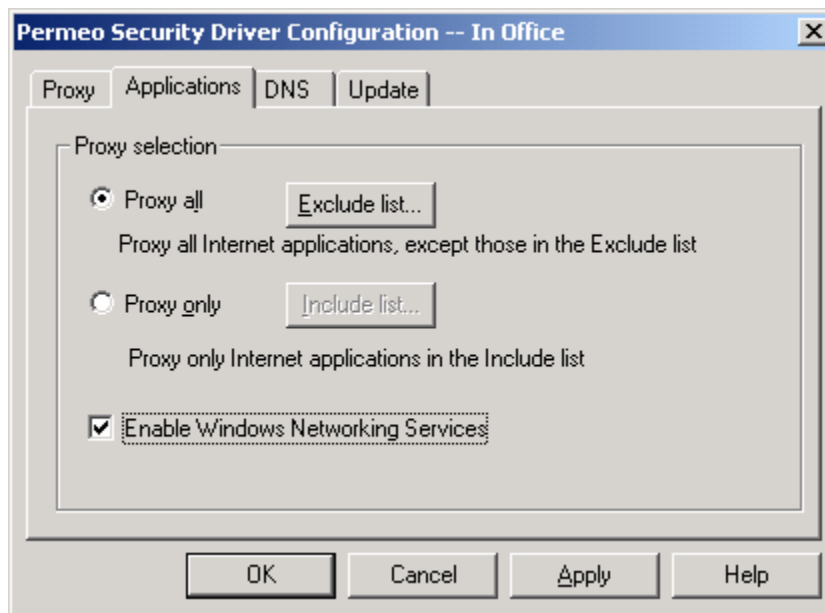
- Click the **Add** button and enter the internal IP address of the WINS server.



8.5 Enabling Microsoft Networking Services

To enable Windows Networking Services on the Security Driver, you must check the **Enable Windows Networking Services** checkbox in the **Applications** tab of the Security Driver **Configuration** window.

See also: Section 6.3.2.3 - [Enable Windows Networking Services](#).



After enabling Windows Networking Services, you may not immediately see the remote network in the Windows Explorer browse list. At the time you booted the machine, Microsoft Networking could not retrieve the browse list for the remote network, because you were not logged in to enter your Security Driver credential.

Unfortunately, Microsoft Networking may take up to 15 minutes to refresh the Windows Explorer browse list after you log in. Activating the **View**, then **Refresh** menu on the **Network Neighborhood** window will not make Microsoft Networking refresh its browse list.

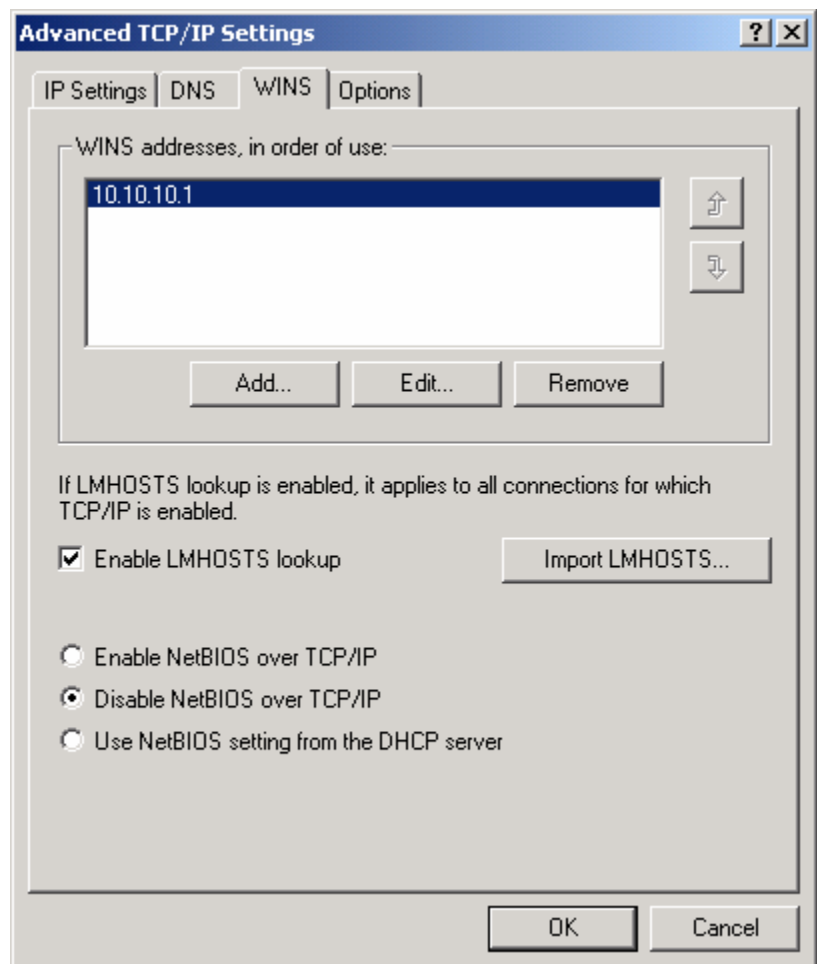
Tip: If you do not wish to wait, you may login with administrator privileges, then disable and re-enable NetBIOS (see the following section.) This workaround should cause the remote network computers to appear immediately in your Network Neighborhood.

8.6 Changing NetBIOS Settings

The following workaround (disabling and re-enabling the NetBIOS on the client) may assist in expediting the refresh of your browse list – causing the remote network computers to appear in your Network Neighborhood. You must have administrator privileges to perform this procedure.

To disable or enable NetBIOS on Windows 2000:

1. From the system taskbar, click:
Start > Settings > Control Panel
2. From the **Control Panel**, double-click the **Network and Dial-up Connections** applet.
3. Right-click the **Local Area Connection** icon and select the **Properties** menu item.
4. Select **Internet Protocol (TCP/IP)** from the list, and click the **Properties** button.
5. Click the **Advanced** button on the resulting dialog, and select the **WINS** tab.
6. Select either the **Enable NetBIOS over TCP/IP**, or **Disable NetBIOS over TCP/IP** radio buttons.
7. Exit all dialogs by clicking the **OK** button.



Note: Even with Microsoft Networking Services remote file and printer sharing enabled, your mapped network drives may sometimes fail to reconnect. This is because at the time Windows attempts to reconnect your network drives, your Security Driver credential is not available to authenticate your connection to the remote network (by design). You should cancel the reconnection. When you have completed logging in, you may simply select the remote drive from Windows Explorer to reestablish the connection.

9 Advanced Configuration Options for Administrators

This section is intended for network administrators and individuals tasked with configuring and deploying the Security Driver for other users. There are several advanced configuration options that can ease the process of installing and/or configuring the Driver for other users:

- Manually import a configuration file
- Remote configuration download
- Advanced Installation Options:
 - Manual Web install program that installs all Driver components (prompted)
 - Silent desktop install program that installs all Driver components (pre-configured)
 - Automatic Web install program that installs all Driver components (pre-configured)

9.1 *Manually Import a Configuration File*

The **Permeo Security Driver** provides an **Administrator's Tool** that can import and export a Driver configuration file. An administrator can configure all Driver settings, then export the configuration file and send it to other users who require the same Driver configuration. The configuration file can be sent as an e-mail attachment, or placed on a network server. Instruct users to run the **Administrator's Tool**, and import the configuration file from wherever it is stored. Upon import, all local configuration settings (**In office**, **Out of office**, and **Wireless**) are overridden, and the user's configuration file is updated.

Please see section 6.4 - **Administrator's Tool**, for more information on running the Administrator's tool, configuration file names, and steps for importing and exporting configuration files.

9.2 Remote Configuration Download

Permeo offers two remote configuration download options that allow a network administrator to centrally manage, control, and update Security Driver settings for any size group of users – freeing users from the task of configuring their own Driver settings. The configuration file can be provided for users to download on-demand, or set to automatically download each time they logon to their machines.

Please see section 6.3.4 - **Update tab**, for more information on on-demand and automatic remote configuration download.

Note: The remote configuration download feature is accessible by users during the initial installation process or from within the Security Driver interface.

A network administrator can deploy the remote configuration download feature as follows:

1. Create a Security Driver configuration file by entering all of the configuration settings for all desired **Zones of Service (In office, Out of Office, Wireless)** for a particular target audience.
2. Export the file using the **Administrator's Tool**.
3. Copy the exported configuration file to a Web server accessible to the target group of users, and provide the users with the URL to this file. Or, copy the configuration file to a Permeo Security Server, and supply the users with the Security Server name.

Note: If your Security Server is running on a Windows system, the network administrator must enable the **Push Driver Configuration** feature, and create a **Remote Client Configuration File**, as defined in the *Permeo Security Server User's Guide for Windows Systems*. If your Security Server is running on a UNIX system, the network administrator must set the **CLIENT_CONFFILE** variable in the Server Configuration file, and create a **Remote Client Configuration File**, as defined in the *Permeo Security Server User's Guide for UNIX Systems*.

Note to Administrators:

- When users specify the URL or Security Server of the remote configuration file during the initial install process, all **Zones of Service** settings (**In office**, **Out of office**, and **Wireless**) will be downloaded.
- When users perform the remote configuration download on-demand through the **Configuration** window **Update** tab, only the selected **Zone of Service** settings (**In office**, **Out of office**, or **Wireless**) will be downloaded.

- In the **Install Wizard** window, the **Allow users to change configuration** option is initially enabled – allowing users to edit their own Security Driver configurations, including Proxy server settings, applications to proxy, and DNS settings. When this option is disabled, the **shared system configuration** feature is enabled, such that users who are sharing one computer share one configuration file, and can only view their configuration previously setup by an administrator.
4. Users who have already installed the Security Driver must manually download the configuration file on-demand, as follows:
- 1) From the Security Driver **User Properties** windows, click the **Edit** button to open the **Configuration** window for the **Zone of Service** they want to update (**In office**, **Out of office**, or **Wireless**).
 - 2) From the **Configuration** window, select the **Update** tab.
 - 3) Enter the **URL** or **Security Server** that links to the configuration file.
 - 4) Click the **Update** button, then click **OK**.
 - 5) The pre-configured remote configuration file loads, overriding all local configuration settings for the selected **Zone of Service** only (**In office**, **Out of office**, or **Wireless**).

Note to Administrators: If you want to set the Driver to automatically download the remote configuration file every time the users logon to their machines, you must enable the option to **Automatically download configuration file** when preparing the remote configuration file.

9.3 *Advanced Installation Options*

The installation program that installs the Security Driver is the standard method for installing the software on a client workstation. This method, referred to as the “Desktop install program” requires no prior configuration on the part of the user or network administrator. The user will be prompted for their product license keys and the address of their Security Server during installation.

The following automated installation options can be setup by a network administrator to simplify the distribution and/or the configuration of the Driver and all related components.

- Manual Web install program (prompted)
- Automatic Web install program (pre-configured)
- Desktop Silent install program (pre-configured)

9.3.1 **Manual Web install program (prompted)**

The manual Web install program provides an easy way for multiple users to download the Security Driver software from a Web Server. Since the manual Web install method is not pre-configured, it can be used like the standard installation program. Users will be prompted for their license keys during installation, and must know the address of their Security Server in order to configure the Security Driver.

1. Copy all distribution files to your Web Server.
2. Instruct users to use a browser to access the setup URL:
e.g. http://MY_WEB_SERVER/PSDinstall/default.html
3. Instruct users to select the manual configuration option:
“Install Permeo Security Driver and allow me to customize settings”
4. Instruct users to answer **Yes** to InstallShield prompt, and wait for InstallShield download to complete.
5. Instruct users to click **Install Now** link to start Security Driver installation.

9.3.2 Automatic Web install program (pre-configured)

The Permeo Security Driver offers an automatic installation method to simplify administration, troubleshooting, and setup of the Security Driver. The Security Driver automatic Web install allows the Administrator to create a pre-configured distribution of the Driver that can then be installed by any user through their Web browser. The advantage of the automatic install process is that it installs the Permeo Security Driver product along with a pre-configured Driver configuration file.

The user must accept the installation of the InstallShield Wizard in order for the automatic install to proceed. It is important to wait for the InstallShield download to complete before clicking the "Install Now" link.

9.3.2.1 Pre-configuring the Automatic Web install

When required, a network administrator can completely pre-configure the automatic install to include the complete Driver configuration, including the license key and the location of the remote configuration file.

Pre-configuring the automatic Web install consists of two main steps:

1. The administrator must place the pre-configured Driver configuration file on a Web server or Permeo Security Server accessible to all users. For example, a company may save a configuration file named **PSDconfig.txt** on their Web server, www.company.com.
2. The administrator then edits the Web install installation script, **auto.htm**, to specify the license key information and point to the configuration URL.

9.3.2.2 Customizing the auto.htm file

The automatic install uses JavaScript to manage the installation of the Security Driver. To configure the automatic install to include the license key and the URL to the Driver's configuration file, edit the file **auto.htm**, inserting your valid data. In addition, the administrator can specify whether to overwrite any current configuration files, or to use a system configuration file.

1. Replace the sample license key with a valid license key:

```
ether.SetProperty("LicenseKey", "1234-5678-9123-4567-ABCD");
```

2. Replace the sample Encrypt license key with a valid Encrypt license key:

```
ether.SetProperty("EncryptLicenseKey", "1234-5678-9123-4567-ABCD");
```

3. Specify the URL of the Security Driver remote configuration file:

```
ether.SetProperty("ImportURL", http://www.company.com/PSDconfig.txt");
```

4. To specify that all users use the shared system configuration, enter 1, otherwise 0, for example:

```
ether.SetProperty("shared", "0");
```

5. To use the user's current configuration, enter 1, otherwise 0, for example:

```
ether.SetProperty("preserve", "0");
```

If the user already has a configuration file, specifying 1 will preserve the configuration file, while specifying 0 will over-write the current settings with the contents of **PSDconfig.txt**.

With these options set, the user only needs to click on the link to the file and the Driver will be installed on their system with the remote configuration options set.

9.3.2.3 Running the Automatic Web Install program

1. Instruct your users to use a browser to access the setup URL:
e.g. http://MY_WEB_SERVER/PSDinstall/default.html
2. Instruct your users to select the **Automatic** configuration option:
"Install and automatically customize the Permeo Security Driver"
3. Instruct users to answer **Yes** to InstallShield prompt, and wait for InstallShield download to complete.
4. Instruct users to click **Install Now** link to start Security Driver installation.

9.3.3 Desktop Silent Install program (pre-configured)

The Security Driver Desktop Silent Install is designed to allow the network administrator to pre-configure the Driver and distribute it across an entire network. Once the Silent Install has been configured, the user runs the installation from their local machine and the Security Driver is installed on the user's computer using the configuration supplied by the administrator. No input is required by the user during the installation process.

Note: The Desktop Silent install will only work on systems that do not have the Driver currently installed. If your user already has the Driver installed on their system, instruct them to remove the Driver and all Driver-related components before proceeding with the Desktop Silent install.

9.3.3.1 Creating the Silent install response file

To configure the Security Driver Silent install, the administrator must create the InstallShield response file – a text file created by **setup.exe** that is used by InstallShield when the Silent Install is executed. The InstallShield silent install response file, **setup.iss**, should be created on a computer that does not have the Security Driver installed on it. Running **setup.exe** with the **-r** option will install the Driver on your system and create the **setup.iss** file in the process.

Note: To run the **setup.exe** program, you will need to have a valid license key available.

To create the response file, run the executable **setup.exe** at a command line with the following options:

```
setup.exe -r -f1PATH\setup.iss
```

Where **-r** creates the response file, and **-f1** (no space between **f1** and the location) specifies the path and names the target file **setup.iss**.

9.3.3.2 Modifying the setup.ini file

1. Locate the **Properties** section of your **setup.ini** file:

```
[Properties]
Licensekey=
EncryptLicensekey=
ImportURL=
Shared=
Preserve=
```

2. Replace the sample license key with a valid license key:

```
LicenseKey=1234-5678-9123-4567-ABCD
```

3. Replace the sample Encrypt license key with a valid Encrypt license key:

```
EncryptLicenseKey=1234-5678-9123-4567-ABCD
```

4. Specify the URL of the Security Driver remote configuration file:

```
ImportURL=http://www.company.com/PSDconfig.txt
```

5. To specify that all users use the shared system configuration, enter 1, otherwise 0, for example:

```
Shared=0
```

6. To use the user's current configuration, enter 1, otherwise 0, for example:

`Preserve=0`

If the user already has a configuration file, specifying 1 will preserve the configuration file, while specifying 0 will over-write the current settings with the contents of **PSDconfig.txt**.

With these options set, the user only needs to click on the link to the file and the Driver will be installed on their system with the remote configuration options set.

9.3.3.3 Running the Desktop Silent install

Distribute the **setup.exe** and **setup.iss** files along with the other accompanying files supplied by Permeo Technologies to your users.

Your users can run the Desktop Silent install from a command line by executing the following command:

```
setup.exe -s
```

Note: The program must be run from the location containing the **setup.iss** file and the other accompanying files. The entire process can be modified to work with a batch file or login script if desired.