

# PINsafe Authentication for SharePoint 2010

Documentation by R. Withey, version 1.3

This documentation describes how to install and configure the PINsafe authentication filter for SharePoint 2010, version 1.3.

## Change History

The main change for version 1.3 of the PINsafe SharePoint Filter is integrated change PIN support. Additionally, it has better support for connection using mobile devices.

Version 1.2 of the filter includes a number of improvements over the previous version, although the basic functionality remains the same.

The following new features have been implemented:

* The filter and associated configuration applications are installed under Program Files, rather than within a specific SharePoint web application.
* The filter can be deployed to multiple web applications. Earlier versions were restricted to a single application.
* A single SharePoint server can be configured, and settings copied to other servers in the farm.
* The login page can be customized to a certain extent.
* Older versions of the filter can be upgraded without uninstalling, and settings will be retained.

## Prerequisites

This guide assumes you already have a SharePoint 2010 server, with at least one web application set up with claims-based authentication enabled. You also need to create a site collection.

You may also wish to enable forms-based authentication and a membership provider, but this is not necessary at this stage: the PINsafe filter installation will check that you have a membership provider installed, and will configure it if necessary. However, you will need to enable forms-based authentication using this provider after filter installation. See post-installation instructions.

You need to ensure that you run the installation program as an administrator user. That user must have write access to the folders containing the web applications, the one containing the central administration web application, and the web.config file for the security token service. By default, this file is in “C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\WebServices\SecurityToken”.

## How the PINsafe Authentication Works

The PINsafe authentication package consists of the following parts:

* A custom login page
* An ASP.Net HTTP module
* A configuration program

The login page manages the actual authentication process, both to PINsafe and to Active Directory. The HTTP module ensures that users cannot access SharePoint without authenticating via the login page.

## PINsafe Configuration

In order to use the PINsafe SharePoint filter, you will need to configure the SharePoint server as an Agent for PINsafe. Do this as follows:

1. Log into the PINsafe administration console. It is assumed you know how to do this.
2. In the menu at the left-hand side, click “Server”, then from the sub-menu, “Agents”.
3. Create a new Agent for the SharePoint server:

* In the blank entries at the bottom of the screen, enter a name for the agent. Any name can be used, as long as it is unique.
* Under Hostname/IP, enter the SharePoint server hostname or IP address.
* Enter a Shared secret. Make sure you have a record of this value, as you will need it to configure the SharePoint filter.
* Leave the remaining settings as default and click Apply.

## Installation

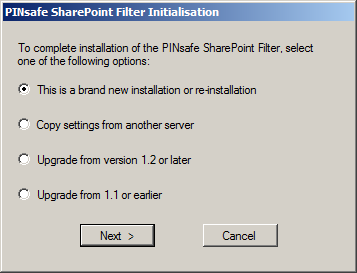
If you have not already done so, download the software from <http://kb.swivelsecure.com/wiki/images/c/cd/SharepointFilter.1.3.zip>.

NOTE: you do not need to uninstall previous versions of the filter before installing this one. However, if you are installing on top of version 1.1 or earlier, you need to ensure that you are installing with the same user account as the previous version to ensure a complete upgrade. Installing as a different user will mean that some of the settings cannot be imported from the old version.

Run the installation program, SharePointFilter.exe. It will prompt you for the destination directory, with a default of C:\Program Files\Swivel Secure Ltd\PINsafe SharePointFilter. Unlike version 1.1 of this application, the filter is not installed directly into the SharePoint web application folder, so you can generally accept the default location.

### Initialization

The first time you run the filter configuration program, which will normally be immediately after installation, you will see the following dialog:



This allows you to import filter settings either from an existing SharePoint server that already has the filter installed, or an old version of the filter, which is already installed on this server. Upgrading from version 1.1 or earlier requires more work than upgrading from 1.2 or later, as the files need to be moved from the SharePoint application itself, hence the distinction.

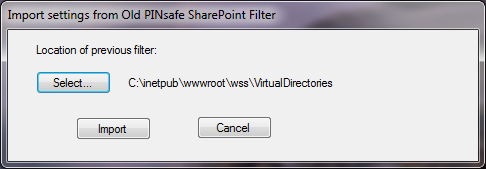
If you choose the first option, no existing settings will be imported, and the main configuration form will be displayed.

The second option allows you to make changes to PINsafe filter settings on a single server, and then import them to other servers. This option will be discussed later.

The third option allows you to upgrade the filter from version 1.2 or later, and requires no further interaction. Settings from the previous filter will be used.

The final option allows you to upgrade the filter from version 1.1 (or earlier) and maintain the existing settings. You should always choose this option if you have version 1.1 or earlier of the filter installed, or else files and menu shortcuts from the old version will not be properly removed. The alternative is to uninstall the old version before installing this one.

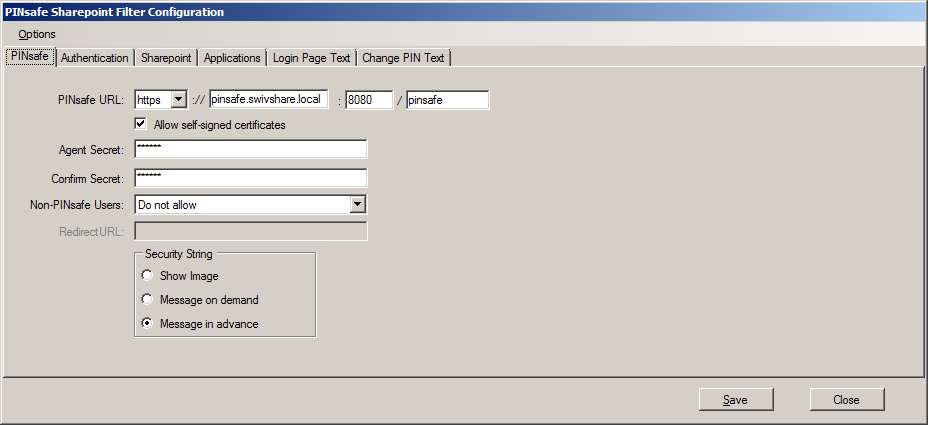
Assuming you are upgrading, you will see the following dialog when you click Next:



Select the directory in which the old filter was installed. Note that the next step will stop IIS temporarily on the SharePoint Server, while the changes are being made. Click Import and the old files and menu shortcuts will be removed, and the PINsafe filter settings will be imported. As noted above, if you are installing the filter as a different user from the old version, some settings will not be imported. Specifically, these are the settings which appear on the “SharePoint” tab of the main dialog, which you will see later. You will see a warning message if not all settings can be imported.

### Filter Configuration

The following dialog will be displayed after importing settings. When you subsequently run the configuration program, this dialog will be displayed immediately:

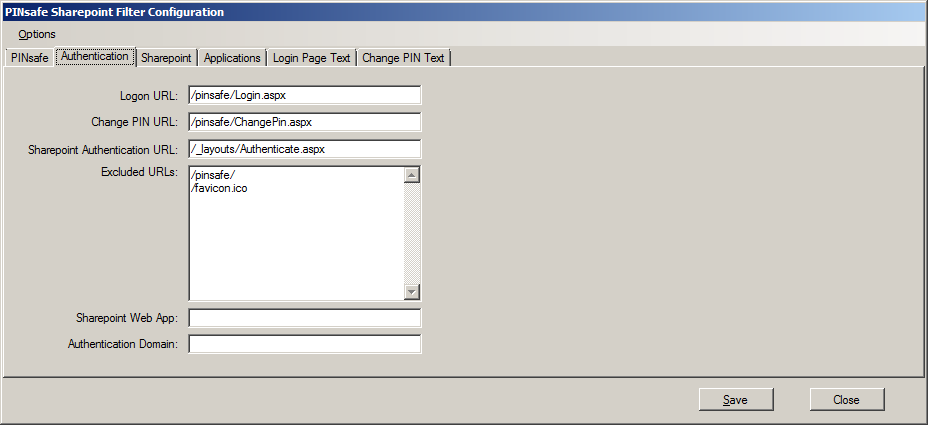


The settings on the first tab relate to the PINsafe connection. If you are upgrading, these settings will already be entered. Otherwise, enter the URL for connecting to the PINsafe server. If you are using SSL (i.e. https) connections to PINsafe, and you do not have a valid commercial certificate for the PINsafe server, or you are using the IP address rather than the host name, make sure you check the option to Allow self-signed certificates.

Enter the secret that you configured for the PINsafe agent twice.

The next option allows you to specify how users not known to PINsafe are handled. The default is to reject them. The second option is to allow them through using AD credentials only. This is a good solution for introducing PINsafe gradually. Users without PINsafe accounts can authenticate as before. The third option is to redirect unknown users to a different URL (e.g. another SharePoint site), which can be specified.

The radio buttons determine how you will receive your security string. The first option will show a TURing image on the page when you enter your username. The second option will show a button on the page to request a security string to be sent via SMS or email, depending on your PINsafe settings. The third option will not show additional options or images. This assumes that your security strings are sent to you in advance.

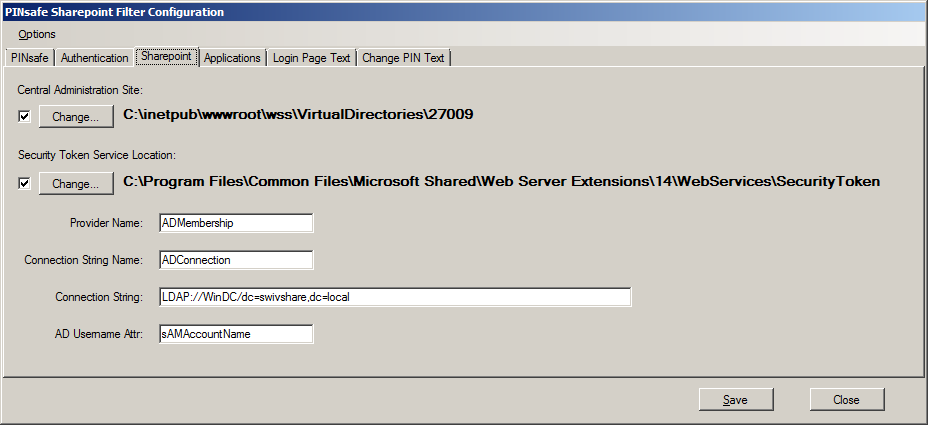


The second tab contains settings related to the authentication process. Normally, you will not need to change any of these, unless you choose to customize the login page, which is discussed later.

If you have upgraded from version 1.1 or earlier of the filter, you will notice that the path for the login files has changed. The previous path, “/\_forms/” coincided with the default path for SharePoint pages, and it was felt that it was better to have a different path. If you have not upgraded, you will only see two entries in the excluded URLs box: “/pinsafe/” and /favicon.ico. The other entries from the old version are unnecessary, as the first path includes all files under that directory, so if you prefer, you can remove all but the first path from Excluded URLs.

The setting for SharePoint Web App can normally be left blank. This gives a hint to the filter as to which SharePoint web application you are authenticating to. The filter will always try the URL used to access SharePoint initially. It will only try this entry if there is no web application or Alternate Access Mapping in SharePoint that corresponds to that URL. If you do enter a value, it must be either the default web application URL, or an alternative access mapping configured in SharePoint Central Administration. Be aware of one particular caveat here: if the public URL for your application is https, for example https://SharePoint.company.com, but the application is mapped internally to a non-SSL server, the filter will search for http://SharePoint.company.com. Therefore, you will need to add a corresponding internal URL for the public URL to match this, in the AAM collection.

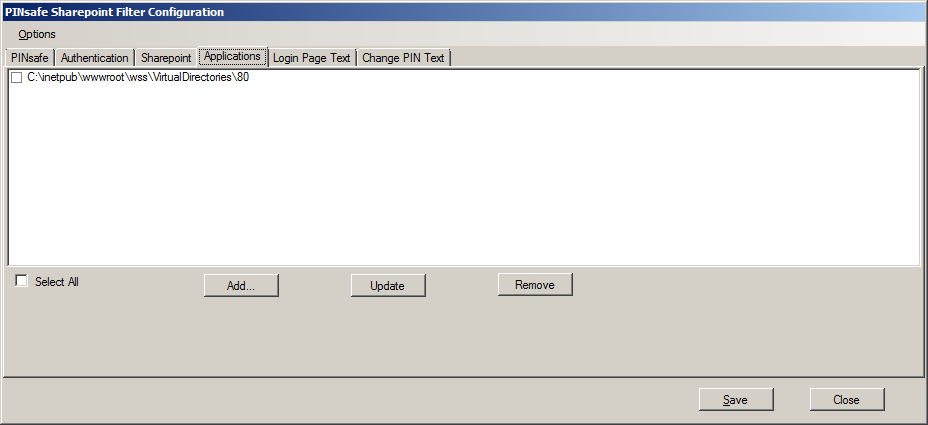
The Authentication Domain should be left blank. This is provided for future development. It sets the domain for the PINsafe authentication cookie.



The third tab relates to SharePoint settings. These may be imported on upgrade, but as explained, if the new filter was installed as a different user from the old one, these will not have been imported.

The first folder is the location of the SharePoint Central Administration. On a new installation, this is guessed by determining the URL for Central Administration, and assuming that the folder matches the port number. If this is incorrect, change it to the correct location. If this is a web front-end, and central administration is not running on this server, uncheck the checkbox next to the Central Administration site entry. The second folder is the root folder for the security token service, assuming a default installation for SharePoint. If this was installed in a different location, you may need to change this. Confirm that the target location exists before continuing.

The final 4 values are the names for the membership provider and corresponding connection string, the provider connection string itself, and the attribute from AD used for the username. If you have already configured a membership provider, make sure you use the values already entered. Otherwise, you can enter any valid names for the provider and connection string: the names should not contain any spaces. The connection string itself needs to be a valid LDAP URL for your Active Directory server, i.e. LDAP://server/domain, where server is the domain controller server name (or the domain name itself), and domain is the fully-qualified LDAP name for the domain, typically something like dc=companyname,dc=com – check with your Active Directory administrators for details. The username attribute should normally only be changed if you have used a different attribute within PINsafe. These must match, or else you will not be able to authenticate.

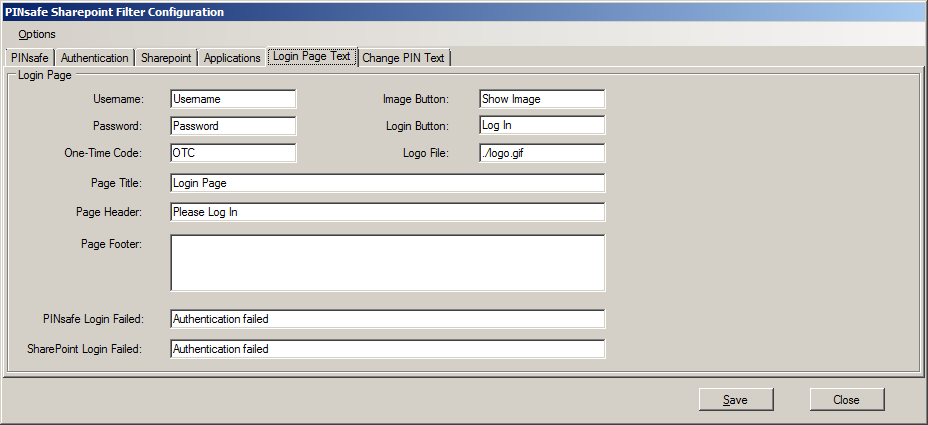


This tab lists the SharePoint web applications that are protected by PINsafe authentication. If you have upgraded from 1.1 or earlier, the single application the old filter was installed in will be listed.

Click the Add button to add PINsafe authentication to a new SharePoint web application. You will be prompted to select an existing web application within the SharePoint virtual directories folder. Make sure you do not select the Central Administration website, as this may have undesirable consequences. When you select an application, the PINsafe login page and associated files are copied to the web application (under /pinsafe), as are the required DLLs to handle PINsafe authentication (under /bin). It also copies the PINsafe settings to the web.config file in that application.

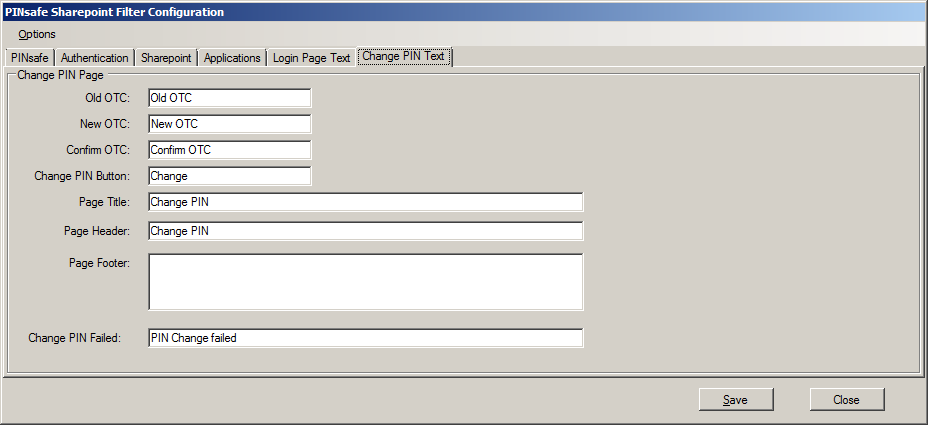
To remove PINsafe authentication from applications, check each application you want to remove, then click the Remove button. Note that this does not remove the application itself, only removes PINsafe authentication. It also removes the PINsafe login pages and DLLs.

The Update button will restore the files and settings from the central filter location on the server. It will apply these changes to all applications that are checked. You will not normally need to do this, as importing from an old filter, or from a central server, will do this automatically, as will adding a new application.



This tab allows you to customize the text displayed on the login page. This includes the page title, header and footer (the footer is empty by default), and labels for the identification fields and buttons. It also allows you to change the logo displayed on the page (see login page customization for more information), and the messages displayed when authentication fails. By default, the messages for PINsafe and SharePoint authentication are different, which might be considered a security risk, so you can make them the same if you prefer.

Note that the text can include limited html formatting if required.



The final tab allows you to customize the text displayed on the Change PIN page.

The Options menu will be discussed in a later section.

## Post-Installation Actions

After installing the PINsafe filter, if you have not already enabled forms-based authentication for the protected sites, you will need to do so. The advantage of doing it at this stage is that the PINsafe filter installer will make the necessary changes to the web.config files for the membership provider. It will not, however, enable forms-based authentication, which you must do at some point.

## Sharing Configurations

Although the PINsafe filter needs to be installed on each member of a SharePoint server farm individually, it is possible to distribute the configuration from a single server to all other servers.

To initiate the process, on the first configured server, select the “Share Configuration” item from the “Options” menu of the configuration program. This creates a share on that server (called PINsafeSP) mapped to the folder containing the PINsafe filter settings.

To import settings from the central server, you can either select the Import option when initializing the filter, or select the “Load from Shared Config” option from the Options menu. You will be prompted for the name of the central server (the last server used will be remembered), and then all settings from the central server will be copied to the local server.

Note that Central Administration is not installed on all servers. Therefore, when importing settings, the Central Administration option is unchecked if the corresponding folder does not exist on the target server.

Note also that the import process is on demand only. If you make any changes to the central configuration after importing to the other servers, you will need to import the settings again on each server.

Note on upgrading: if you are upgrading from version 1.1 or earlier of the PINsafe filter, it is recommended that you select the Upgrade option on ALL servers that have the old filter installed. If you upgrade the first one, then import settings on all others, the old filter will not be fully removed. This should not affect anything, but unnecessary files and menu shortcuts will not be removed. You can still import settings from the Options menu later. Alternatively, you can uninstall the filter from all but one of the servers, in which case you can use the Import option.

## Customizing the Login Page

It has already been explained how you can change the text included in the login page. Provided that you are careful, you can customize the page further.

The Text tab on the configuration program allows you to change the URL for the logo displayed on the page. However, if you do this, you will need to include the new logo within the filter deployment files. You will need to copy your image file to C:\Program Files\Swivel Secure Ltd\ PINsafe SharePointFilter\Web\pinsafe (assuming a default installation). You will need to do this on each server within a farm individually: files are not copied when importing the configuration. However, once the file is within this folder, it will be automatically copied to the relevant web applications (you will need to click Update on the Applications tab if the application is added before the file is uploaded). Make sure that the URL for the logo starts with “./” for it to display properly.

You can also change the look and feel of the page by editing the stylesheet, styles.css.

To customize the login page further, you can edit the file Login.aspx within this directory, as long as you are familiar with HTML. Make sure that you do not remove or alter any items with the attribute runat=“server”, other than to relocate them within the file. In particular, do not change the ID attribute. There is no point in changing the Text attributes of these items either, since the content of these is overwritten by the values on the configuration.

If you need to add further external files (images, stylesheets etc.), the recommended method is to copy the relevant file into the same folder as the login page. However, if you refer to files outside this folder, you will need to add them to the list of excluded URLs on the Authentication tab, or else they will not display properly. Files within the pinsafe folder do not need to be explicitly added, as they are covered by the “/pinsafe/” entry.

Entries within the excluded URLs are processed as follows: if the entry starts with “./”, then the end of the URL must match. Otherwise, the beginning must match. So, for example, “/pinsafe/” will match anything within the /pinsafe folder, while “./picture.jpg” will match any file called picture.jpg within any folder.

## Troubleshooting

Under normal circumstances, this filter will work with a newly-created web application using claims-based authentication. However, certain non-default SharePoint settings can cause problems with this filter. Additionally, the filter requires some non-obvious changes to SharePoint under certain circumstances.

For example, as mentioned above, the login page will determine the web application name by reading the protocol, host name and port from the request. There must be an Alternate Access Mapping (AAM) entry to match this web application for this to work. Normally, this just requires that you define a public URL that corresponds to the URL users are required to use to access SharePoint, with the same internal URL. However, if the protocol or host name is changed by a proxy server before it reaches SharePoint, the internal URL that the PINsafe login page sees will not be the same as the public URL. For example, if an external https request is mapped internally to http, then you will need to define an internal URL in the AAM entries using http, rather than https.

You must ensure that the SharePoint login page is set to default under Authentication settings. Once the PINsafe filter has successfully authenticated a user, control is passed to the SharePoint login page. Normally, since SharePoint authentication has already been carried out by the PINsafe filter, this would automatically forward to the SharePoint home page. However, if the default page has been changed, this may not happen: most likely, the page will not be found.

If you are running a load-balanced SharePoint server farm, ensure that the PINsafe filter is installed on ALL the web front-end servers. It must be separately configured on each one. It is not normally necessary to install it on back end servers that do not received unauthenticated requests directly, but it IS necessary that the relevant membership provider is configured under Central Administration and Security Token Service on all servers, so it is simplest to install the filter on all servers.

Make sure that installation is done by a user with sufficient rights to modify all the relevant files: ideally, by an administrator. Also, check that none of the files modified, i.e. the web.config files in the Web Application, Central Administration and Security Token Service, are marked as read-only.

## Uninstalling the Filter

A link is provided on the “PINsafe Filter for SharePoint 2010” menu to uninstall the filter, or you can uninstall it from the Control Panel. Uninstalling will remove PINsafe authentication from all configured web applications.

It is possible to disable the filter temporarily, by removing it from the list on the Applications tab of the configuration program. Note that, when using a server farm, you must remove it from ALL farm members (e.g. by using central configuration).

## Appendix – Changes made by the filter installer

The filter is installed, by default, into C:\Program Files\Swivel Secure Ltd\PINsafe SharePoint Filter. You can change this on installation if you need to.

The following files are installed directly within that folder:

* PINsafeConfig.exe – the filter configuration program
* PINsafeClient.dll – manages PINsafe settings and communication with PINsafe
* Swivel.ico – the Swivel logo (used for menu shortcuts)

All files to be deployed to SharePoint web applications are installed within a sub-folder of the installation folder, called “web”. Any files you add to this will be deployed as well. However, it is recommended that you only add files within the “pinsafe” sub-folder. The deployment files are as follows:

Under the bin sub-folder:

* PINsafeSharePointFilter.dll – the filter itself
* PINsafeLogin.dll – the code behind the login pages
* PINsafeClient.dll – as described above

These 3 DLL files are also installed in the Global Assembly Cache.

Under the pinsafe sub-folder:

* Login.aspx – the login page itself
* Logoff.aspx – handles logging off from PINsafe
* ChangePin.aspx – the change PIN page
* SCImage.aspx – displays the TURing image
* CheckUser.aspx – used to check whether a user is known to PINsafe
* Ping.aspx – used to check connection between the SharePoint server and PINsafe when the login page is first displayed. This can help reduce the time taken to authenticate later.
* Pinsafe1.js, Pinsafe2.js, Pinsafe3.js – client-side JavaScript used in the 3 different scenarios for handling unknown users.
* Logo.gif – the Swivel logo, which is the default logo displayed on the login page. You can delete this file if you are using a different logo.
* Styles.css – the CSS stylesheet for the login and change PIN pages.

Two shortcuts are added to the start menu:

* Configure PINsafe SharePoint Filter – runs the configuration program.
* PINsafe SharePoint Filter Uninstaller – uninstalls the filter.

The first time the configuration program runs, it carries out the following actions:

* Registers the 3 DLLs in the Global Assembly Cache.
* Runs the Initialization wizard, allowing for upgrade or import of settings.

You can run the initialization wizard at a later stage by calling PINsafeConfig.exe from the command line with the argument “-i”. Running this application with the argument “-u” will uninstall PINsafe authentication from all applications, unregister the DLLs and remove the PINsafe share (if created). This is done automatically on uninstallation, so you should never need to do this.

In addition to the above actions, every time you save settings from the configuration program, the following actions occur:

* Check that the membership provider and connection string are configured in the security token service web.config file, and add or modify them if necessary.
* As the previous action in the Central Administration web.config.
* Register PINsafeLogin.dll and PINsafeClient.dll as safe controls for SharePoint, if required.
* Register PINsafeSharePointFilter.dll as a HTTP module (so that it is invoked on every request to the SharePoint server).
* Save any changes to settings in the central storage (see below).
* Save any relevant changes to settings in the web.config file for all registered applications.

The deployed files are normally only copied to the web applications when the application is created, either directly from the configuration program, or when importing or upgrading. If you need to re-deploy the files, use the Update button from the Applications tab.

Settings are stored in the folder C:\ProgramData\Swivel Secure\PINsafe SharePoint Filter, in 3 files:

* PINsafeSettings.data – settings relating to PINsafe. These settings are copied to each web application within web.config.
* SharePointSettings.data – settings relating to SharePoint configuration.
* Logintext.data – the text strings for the login page.

It is this folder that is shared as PINsafeSP on the central configuration server, when chosen.