

DigitalPersona® One Touch SignOn for Active Directory v4.x

Quick Start Installation Guide

Process Overview

Step	Description
1. Review the overview and configuration documentation for One Touch SignOn.	One Touch SignOn (OTS) allows you to log on to a password-protected program or Web site by simply touching the reader.
2. Create a shared folder on the network drive to store OTS templates and assign appropriate permissions to the users	Create a shared folder on the network drive to store OTS templates and assign appropriate permissions to the users
3. Deploy & configure the DigitalPersona One Touch SignOn GPO to allow workstations to acquire preconfigured logon and change password templates at user logon.	To allow users to acquire OTS templates, using the Group Policy Management console, configure the appropriate DigitalPersona GPOs with the UNC path of the newly created shared folder that contains your OTS templates.
4. Install & configure the One Touch SignOn Administration tool.	<ul style="list-style-type: none"> To install the One Touch SignOn Administration tool, navigate to the One Touch SignOn folder of the Pro for AD distribution and click the Setup.exe file. Create a container for OTS template management. The container should point to your newly created shared folder.
5. Create OTS Logon Templates.	Administrators can pre-train websites and programs facilitating ease of use and user roaming.
6. Setup Change Password Screen Templates.	Keep passwords in sync by changing passwords.
7. Logging on with One Touch SignOn	
8. Changing Passwords with One Touch SignOn	

One Touch SignOn Overview

One Touch SignOn and the One Touch SignOn Administration Tool allow administrators to control access to a Web site or program by adding fingerprint authentication to logon screens. Attributes such as user name, password and other files are specified in the template. The administrator can also automate the process of changing passwords, by adding the attributes of the change password screen to the template for the Web site or program.

One Touch SignOn templates contain the specifications for a logon screen and a change password screen for a particular Web site or program. Templates are stored in containers, and are deployed to DigitalPersona Pro Workstations or Kiosks using the One Touch SignOn Group Policy Object.

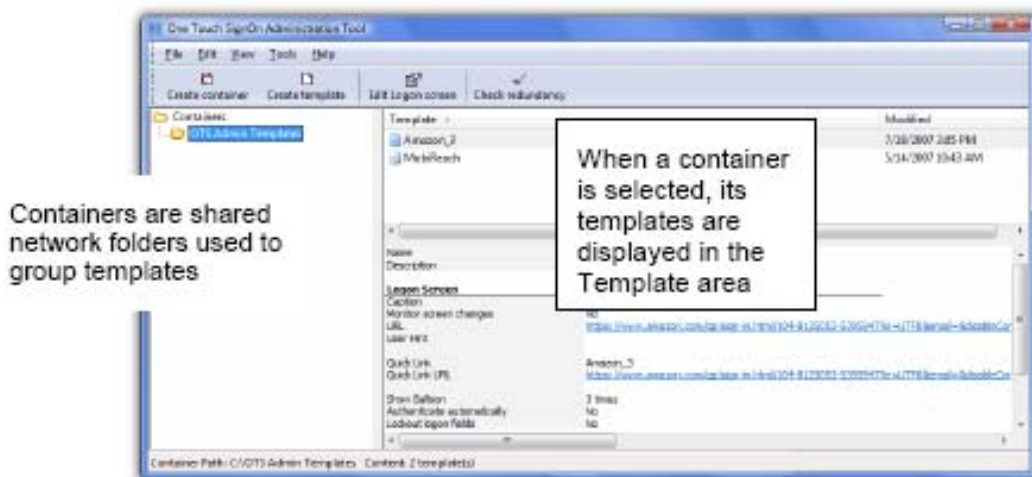
After templates are deployed to a computer, One Touch SignOn recognizes that logon or change password screens are fingerprint-enabled by using the attributes specified in the templates.



The fingerprint logon icon in the upper left corner of the logon screen for a Web site or program indicates that touching the reader with any enrolled finger will log the user on to the Web site or program.

The user is then guided through the process of logging on or changing the password with One Touch SignOn. Depending on the settings applied by the administrator, the user may be prompted for account data, such as username, password, and other information during the first logon. After the first logon, the account data is provided by One Touch SignOn after the user identity is confirmed with a fingerprint.

The One Touch SignOn Administration Tool is used to create and manage templates for password-protected Web sites and programs.



Create a Shared Folder that will contain One Touch SignOn Templates

Create a shared folder on the network drive to store OTS templates and assign appropriate permissions to the users. This newly created shared folder will be the **container** used for your newly created OTS templates.

- Create a folder on the server you will use to store the OTS templates.
- Share the folder that you just created to allow users to access it.
- Right click on the folder and click on Properties in the context menu.
- Click on the Sharing tab.
- Verify the permissions by clicking on the Permissions button.

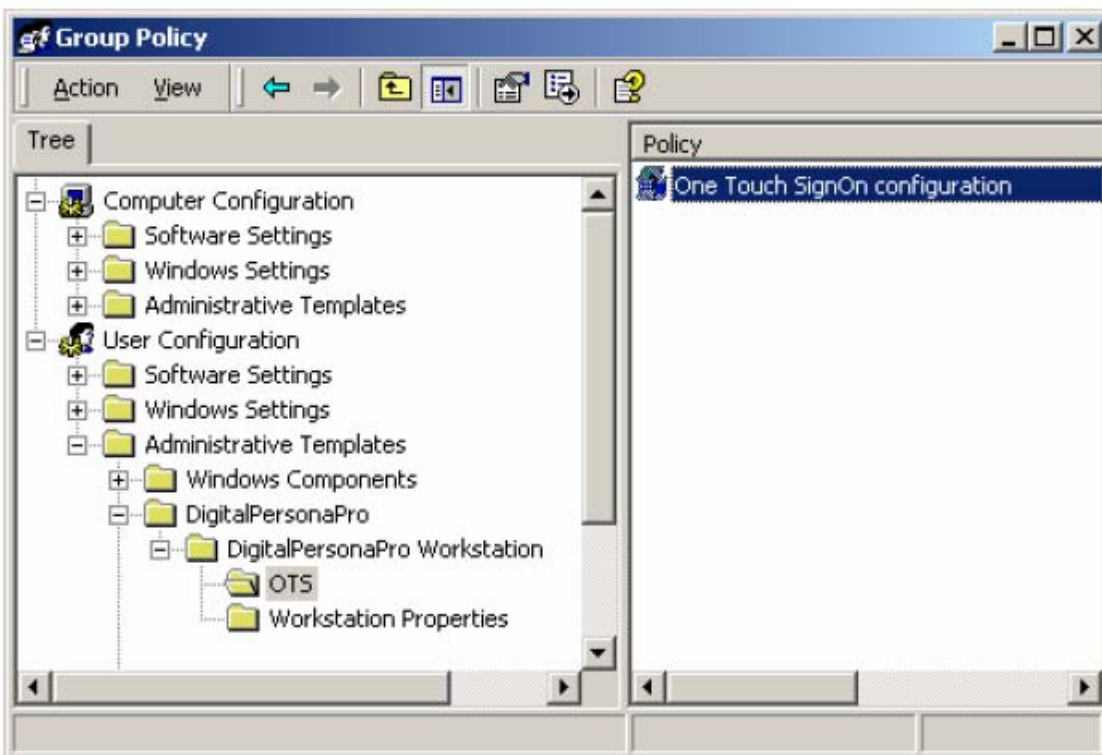
Note: A Best Practice tip would be to simply create a folder beneath the already shared Netlogon folder. The Netlogon folder is pre-shared by default for administrative purposes and is automatically replicated throughout the domain. As such, it is optimized to reduce traffic across sites, eliminates the need for a new share and thanks to the File Replication Service, (FRS) provides failover and redundancy.

e.g. \\fully qualified domain name\netlogon\OTSSHARED

Deploying & Configuring the DigitalPersona One Touch SignOn Group Policy Object

To make One Touch SignOn templates accessible to computers running DigitalPersona Pro Workstation & Pro Kiosk, add the One Touch SignOn GPO to the appropriate Active Directory OU.

Administrators must specify the path to the previously created shared folder in the One Touch SignOn GPO using the **UNC path**. One Touch SignOn will copy templates from the shared folder to the user computers as specified by the policy during logon.



To Set up the GPO policy for OTS

- The Workstation Administrative Template, DigitalPersonaProWksta.adm (or kiosk template if appropriate) file must be added to the Active Directory Computer Configuration folder in the Administrative Templates folder of the Group Policy editor. The ADM file is located in the inf directory on the hard drive where DigitalPersona Pro AD Server or Workstation was installed.
- Open the GPO where the DigitalPersona template was added.
- Go to User Configuration\Administrative Templates\DigitalPersonaPro. Double click on One Touch SignOn Configuration policy (in the right pane).
- The default setting is "Not Configured". Click on Enable to enable this policy, and then type in the path to the shared folder that you previously created.
- The new setting will be applied to all DigitalPersona Pro Workstations during the usual refresh interval or the next time they restart Windows.

Install and Configure the One Touch SignOn Administration Tool

The OTS Administration Tool manages access to password-protected Web sites and programs through the creation and administration of templates that contain the specifications for:

- **Logon screen template** - This template specifies attributes that are utilized during the logon, such as a user name, password, and Submit button.
- **Password Change screen template** - This template defines how a password for an OTS-enabled program or Web site is changed, specifying details such as whether the password can be changed by the user at will, or must be changed at prescribed intervals, and any format restrictions that are enabled.

These OTS templates are created in the One Touch SignOn Administration Tool, and then deployed to users through a setting in the Active Directory GPO governing the workstations. (For further information, see “Deploying Templates” in the *DigitalPersona Pro Administrator Guide*.

After the templates are created and deployed, the One Touch SignOn application uses the templates to recognize which logon and change password screens are fingerprint-enabled, displaying the DigitalPersona fingerprint logon icon in the upper left corner of the Web site or program window to indicate that the user can log on with their fingerprint, as well as a balloon prompting the user to touch the reader to log on.

Install the One Touch SignOn Administration Tool

The OTS Administration Tool is located in the One Touch SignOn folder. To install the Administration Tools, navigate to the One Touch SignOn folder on the DigitalPersona for AD distribution and click the **Setup.exe** file.

Configure the One Touch SignOn Administration Tool

To configure the One Touch SignOn Administration Tool, you must create a container to manage OTS templates. The container is simply a shared folder that is accessible to One Touch SignOn users.

To create an OTS Container

- Open the OTS Administration Tool from Start/Programs/DigitalPersona Pro.
- On the toolbar, click the New Container icon.
- In the Create New Container dialog box, type a name for the container in the Name text box.
- Specify the path of the container in the Path field. To browse for a path using the standard Windows file browser dialog box, click the Browse button.
- Click OK to create the container.

Once a container is created, you are ready to create templates for password protected programs your users may access locally, over the network, or over the Internet.

Creating One Touch SignOn Logon Templates

The Logon Screen Wizard provides administrators with two different ways to create logon templates:

- **Automatically** –The Logon Screen Wizard detects the fields on the logon screen. Administrators can then specify which fields are required for logon and what type of information should be provided in the fields.
- **Manually** – More complex logon screens can be created manually. Please refer to the *DigitalPersona Pro Administrator Guide* for more information on creating manual logon screens.

The following procedure has been simplified for this guide. For more detailed instructions, please refer to the *DigitalPersona Pro for Active Directory Administrator Guide*.

To create a logon screen automatically:

- Launch the password-protected Web site or program for which you want to create the logon template.
- In the OTS Administration Tool, select the container to which you want to add the new template.
- Click **Create Template** to launch the Logon Screen wizard.
- Make sure the title of the desired program is accurately displayed on the first screen of the wizard, and then click **Next** to display the Logon Fields page. This page will contain all the fields on the program's logon screen, and may include some fields that are not used during logon.
- Complete the Logon Fields page and click **Next** to display the Submit Option page.
- Select the button from the list that submits the logon data. You can type a new button name by typing over the current name. If you want the user to submit the logon data themselves, select **Do Not Submit**.
- To continue, click **Next** to display the Logon Screen Properties page.
- Complete the Logon Screen Template page and click **Next**.
- On the Setup Complete page, click **Finish** to save the changes and exit the wizard.



The fingerprint logon icon in the upper left corner of the logon screen for a Web site or program indicates that touching the reader with any enrolled finger will log you on to the Web site or program.

Setting Up Change Password Screen Templates Automatically

The Change Password Screen Wizard provides administrators with two different ways to create change password screen templates:

Automatically – See the procedure below. The Wizard detects the fields on the change password screen. You can then specify which fields are required for logon and what type of information should be provided in the fields.

Manually - Change Password screens can also be created manually. Please refer to the *DigitalPersona Pro Administrator Guide* for more information on creating manual change password screens.

To set up a change password screen automatically:

- ❑ Launch the password-protected Web site or program for which you want to automate the change password operation and then navigate to the Change Password screen.
- ❑ In the OTS Administration Tool, select the template which was created for that Web site or program.
- ❑ Right-click on the template name to display that template's context menu and select **Add Change Password Screen** to display the Change Password Screen wizard.
- ❑ Click **Next** to display the Change Password Screen Field page. Select the fields used for the change password process.
- ❑ Click Next to display the Password Policy page.

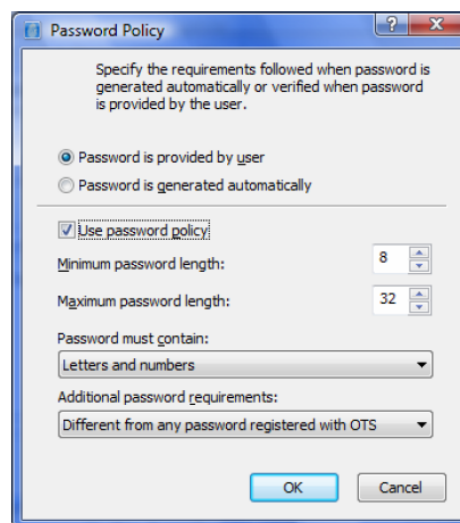


- ❑ If desired, specify the password policy for a protected field by selecting the corresponding Field Policy item, and then click the [...] button which is shown on the right side, to display the Password Policy dialog.

- ❑ In the Password Policy dialog box, the following options are available:

Password is provided by user - Allows the user to specify the new password for the Web site or program.

Password is generated automatically - Generates a randomized password for the user. By selecting this option, you can ensure that the user can only log on using a fingerprint.



Use password policy - To specify the constraints on the password format, length and uniqueness, check the **Use password policy** checkbox. These requirements will be followed when the password is generated, and verified when the password is provided by the user.

The following standard options are available for the password:

Minimum password length - Specifies the minimum number of characters allowed in the password

Maximum password length - Specifies the maximum number of characters allowed in the password

Password must contain - The following options are available for the password content:

- **Letters and numbers** - Allows any combination of letters and/or numbers.
- **Letters only** - Allows letters only.
- **Numbers only** - Allows numbers only.
- **Letters and numbers with special characters** - Allows passwords that contain at least one number or at least one letter, and at least one special character is required. Special characters include symbols such as !"#%&'()*+,-./:;<=>?[\]^_`{|}~@. Spaces are not allowed.
- **Letters and numbers with at least one number** - Allows passwords containing any combination of letters and numbers, but both types must be present.

Additional password requirements – You can select any one of the following constraints:

- **None** - No other constraints are applied to the password.
- **Different from Windows password** - The new password must be different from the current Windows password.
- **Different from any password registered with OTS** - The new password must be different from all passwords registered for fingerprint-enabled Web sites or programs by the current Windows user.
- **Different from current password** - The new password must be different from the current password for this Web site or program.

- Click **OK** to save the changes in the Password Policy dialog box.

Note - The password policy applied in the wizard should be the same as, or at least compatible with, the password policy of the Web site or program.

- On the Password Policy page, click **Next**.

- On the Submit Selection page, select the button which submits the data on the Change Password screen, and then click **Next**.

- On the Change Password Screen Properties page, you can customize the behavior of the system during the change password operation. The following settings are available:

- **User Hint** - Allows customization of the text that will be shown when the user is prompted to type data into input fields for the Change Password screen.
- **Windows Caption** - Specifies the title of the change password screen as detected by the wizard. The caption is used by One Touch SignOn to recognize a fingerprint enabled screen. You may use wildcards to specify the changeable portion of the caption.

- **Monitor Screen Changes** - Enables the fingerprint software to recognize the previously trained screen in case the screen content changes in time due to system or user activity, for example, when the screen contains some complex structure such as long-loading ActiveX, Flash, etc. Since most Web pages do not fall into this category, this setting is turned off by default.
- **URL** - Uniform Resource Locator is a unique, identifying address for any particular page on the Web. A web page's URL can be used by One Touch SignOn to recognize the previously trained screen. The dropdown menu allows you to specify the type of matching performed on the URL. By default, the URL is not used to recognize a fingerprint enabled screen.

When done configuring the Change Password Screen Properties, click **Next**.

On the Setup Complete page, click Finish to save the changes and exit the wizard.

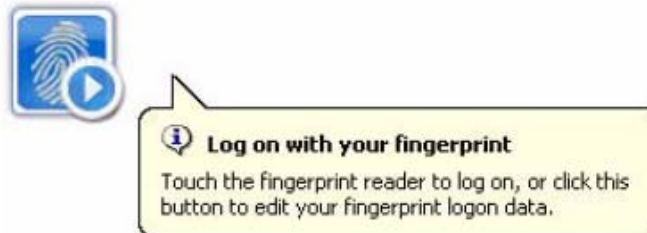


The fingerprint logon icon in the upper left corner of the logon screen for a Web site or program indicates that touching the reader with any enrolled finger will log you on to the Web site or program.

Logging On with One Touch SignOn

After templates have been created and deployed, end users can launch a logon screen and touch the fingerprint reader with a registered finger to log on. If a Quick Link was defined in the template, users can select the Quick Link from the One Touch Menu to launch the Web site logon screen. Quick Links only display in the One Touch Menu after the user has visited them and used their fingerprint to logon.

Logon screens that have a template created for them display a fingerprint logon icon in the upper left corner of the screen and a balloon informing the user to log on with a fingerprint.



Depending on the template attributes, the logon process may vary. For example, the user can be automatically logged on by touching the reader, i.e. the fields can be automatically populated and submitted.

In other cases, the user is prompted to choose a set of account data or provide logon field values. If there are multiple accounts for the same logon screen, the user is prompted to select an account in the Select Account Data dialog box. The user must click the name of the account to use and click OK to log on.

When the user is prompted to type values for logon fields, the Enter Account Data dialog box displays. This dialog box displays when the user has required fields where the values are not yet specified. In the dialog box, the user can provide the appropriate values for the fields and click OK to log on.

Providing Logon Field Values

If the template contains logon field values, the Field Values dialog box opens, listing each field needing a value and allowing the user to enter them before logging on.

The appearance of this dialog box is dependent on the Value attribute, such as Ask- Reuse, Ask-Confirm or Ask Always, for fields in a template.

If the Show Password Values in Fields option in the GPO is enabled or not configured, the user can click the “Show passwords during editing” button to display the password as they edit it. Otherwise, the characters in the password are replaced with a bullet.

Choosing an Account

If a logon screen is set up for multiple accounts, the Select Account Data dialog box is displayed, prompting the user to select the set of account data they want to use.

When the user selects the set of account data, they can click OK to log on.

Changing Passwords with One Touch SignOn

Change password screens that have a template created for them display a fingerprint logon icon in the upper left corner of the screen and a balloon informing the user to provide a fingerprint. The user is asked to provide the old password, a new password and to confirm the new password. Depending on the template attributes, the change password process may vary. For example, the user can be allowed to choose a new password with or without constraints on the password complexity.

In other cases, the new password is generated automatically by the system. In this case, the user must log on with a fingerprint