



October, 2009

DigitalPersona Pro v4.4.1 Upgrade Notes

Table of Contents

Important Upgrade Recommendations.....	3
Version Supportability Information	4
False Accept Rate Considerations	5
Important Information for all Upgrades.....	6
OTS "show clear text password" Setting .adm Issue.....	7
Upgrading Stand Alone Workstation	8
Upgrade from 4.x Server and 4.x Kiosk	9
Upgrade from 3.x Server and 1.x Kiosk	10
Upgrade from 4.x Server and 4.x Workstation	11
Upgrade from 4.x Server and 3.x Workstation	13
Upgrade from 3.x Server and 3.x Workstation	15
Converting OTS Templates	17
Converting Win32 OTI Logon Screens	18
Fingerprint Logon Retraining	20
Re-Registering User's Fingerprints	22
Extended Server Policy Module (ESPM)	23

Important Upgrade Recommendations

While we strive to ensure safe and trouble-free system upgrades, we cannot guarantee performance in every IT environment. It is therefore strongly recommended that you carefully plan and perform reasonable precautions before any system upgrade:

- Review the Readme.txt file included with each DigitalPersona Pro product.
- It is also strongly recommended that you review the product's Administrator Guide and identify potential changes to the system administration settings.
- Perform a lab test of the upgrade that approximates your particular IT environment.
- Incrementally deploy and test your system upgrade (i.e. Server(s) then workstations).
- Prepare a software rollback plan to reverse any potential problems. Note that rollback to a previous release may require un-installation of a later revision of software.

Notebooks with Built-in Readers

If you are upgrading from an earlier version of the DigitalPersona Pro Workstation software or installing DigitalPersona Pro software product for the first time on a supported notebook with a built-in swipe reader, it is strongly recommended that you review the Readme.txt file included with the product being installed.

Support for Previous Versions

DigitalPersona Technical Support is available for the previous two (major/minor) software releases. To be eligible for technical support and to ensure optimal software upgradeability to future releases, we recommend that all versions of DigitalPersona Pro client software prior to version v4.4.1 be upgraded.

Adjustments in the default False Accept Rate settings

The DigitalPersona Pro Solution ships with a new default FAR (False Accept Rate) setting to enhance support for notebooks with built-in fingerprint readers. With the DigitalPersona Pro 4.3 Solution, the default FAR setting is now 1 in 10,000 rather than 1 in 100,000 as in versions shipped prior to Pro 4.3.0. If your enterprise contains DigitalPersona client or server versions older than Pro 4.3.0, it is best to maintain a consistent level of FARs across Pro by setting the GPO setting for "False Accept Rate used for fingerprint verification" under the Fingerprint Recognition section. Please see the False Accept Rate Considerations section of this document.

End of Support for Pro v1.x and 2.x

Effective with the release of DigitalPersona Pro Software v4.0, DigitalPersona no longer provided technical support for versions 1.x and 2.x of DigitalPersona Pro.

Customers who have not upgraded should contact their DigitalPersona Partner or DigitalPersona Account Manager for information regarding upgrading.

Upgrading Your Pro Installation

Please contact sales@digitalpersona.com for information & pricing to upgrade your DigitalPersona Pro installation.

Maintenance & Support Plans

Please contact sales@digitalpersona.com for details and pricing for our Maintenance & Support plans.

Version Supportability Information

Pro WORKSTATION and KIOSK versions to OS table

Version	Win7 64b	Win7 32b	2008(+) 64b	2008(+) 32b	Vista(++) 64b	Vista(++) 32b	XP 64b	XP 32b	XPe	2003(+) 64b	2003(+) 32b	SBS 2003(+) R2 32b	2000(+) 32b
4.4.1	X	X	X	X	X	X	X	X	X	X	X	X	X
4.4.0	-	-	X	X	X	X	X	X	X	X	X	X	X
4.3.2	-	-	X	X	X	X	X	X	X	X	X	X	X
4.3.1	-	-	X	X	X	X	X	X	X	X	X	X	X
4.3.0	-	-	X	X	X	X	-	X	X	X	X	X	X
4.2.5	-	-	-	-	X	X	-	X	X	-	X	X	X
4.2.4	-	-	-	-	X	X	-	X	X	-	X	X	X
4.2.1	-	-	-	-	X	X	-	X	X	-	X	X	X
4.2.0	-	-	-	-	-	X	-	X	X	-	X	X	X
4.1.0	-	-	-	-	-	-	-	X	-	-	X	-	X
4.0.1	-	-	-	-	-	-	-	X	-	-	X	-	X
4.0.0	-	-	-	-	-	-	-	X	-	-	X	-	X
3.5.1	-	-	-	-	-	-	-	X	-	-	X	-	X
3.5.0	-	-	-	-	-	-	-	X	-	-	X	-	X

++ = Vista Home is *not* supported

+ = *Not* configured as a domain controller

Pro SERVER version to OS table

Version	2008 64b	2008 32b	2003 64b	2003 32b	SBS 2003 SP1 32b	2000 32b
4.3.0	X +++	X	X +++	X	X	X
4.2.4	-	-	(++++)	X	X	X
4.2.1	-	-	-	X	X	X
4.2.0	-	-	-	X	X	X
SBS 4.2.0	-	-	-	-	X	-
4.1.0	-	-	-	X	-	X
4.0.1	-	-	-	X	-	X
4.0.0	-	-	-	X	-	X
3.5.1	-	-	-	X	-	X
3.5.0	-	-	-	X	-	X

+++ = For legacy 3.x Pro client support install the 32b Pro Server onto 64 OSs

++++ = While this OS is *not* supported, the Pro Server 4.2.4 32b *will* install on Windows Server 2003 64b **and** Pro Server Kiosk Add-On 4.2.4 32b *will* install on Windows Server 2003 64b

Pro client to Supported Web Browser Table

Supported in version	IE 8	IE 7	IE 6	FF 3.5	FF 3.0
4.4.0 and higher	X	X	X	X	X
4.3.0 and higher	-	X	X	-	X
Prior to 4.3.0	-	X	X	-	-

Pro does NOT support: Safari, Opera, Chrome, non-Firefox (FF) Mozilla, Netscape, AOL or any other browser not listed.

False Accept Rate Considerations

False Accept Rate Recommendations

We recommend explicitly setting the False Accept Rate (FAR) for your environment via AD GPO to between 100,000 and 10,000.

If your DigitalPersona deployment uses solely DigitalPersona branded fingerprint readers, it is recommended that the FAR in your environment is set to 1 in 100,000 (one hundred thousand) as this will provide a high level of security. Conversely, to ensure a positive user experience, if your environment contains notebooks with built-in swipe readers with DigitalPersona software installed, it is recommended that the FAR in your environment is set to 1 in 10,000 (ten thousand). The FAR can then be tweaked over time, preferably between 100,000 and 10,000, based on behavior in the environment.

Default by Pro versions:

- If not defined by GPO for *Pro 4.3.0 and higher*, the FAR setting is 1 in 10,000 - the newer 1 in 10,000 FAR setting is optimized to accommodate notebooks with built-in swipe fingerprint readers
- If not defined by GPO for *Pro versions prior to 4.3.0*, the FAR setting is 1 in 100,000

It is strongly recommended that the FAR value for DigitalPersona Servers and DigitalPersona clients are set to the same value.

False Accept Rate Management by GPO Settings Locations

The False Accept Rate (FAR) is managed via DigitalPersona Active Directory Group Policy Administrative Templates settings. Server, Workstation, and Kiosk setting locations:

- Computer configuration / Administrative Templates / DigitalPersonaPro / DigitalPersonaPro Server / Fingerprint Recognition / False Accept Rate used in fingerprint verification
- Computer configuration / Administrative Templates / DigitalPersonaPro / DigitalPersonaPro Workstation / Fingerprint Recognition / False Accept Rate used in fingerprint verification
- Computer configuration / Administrative Templates / DigitalPersonaPro / DigitalPersonaPro Kiosk / Fingerprint Recognition / False Accept Rate used in fingerprint verification

False Accept Rate Settings Explained

The False Accept Rate (FAR) specifies the False Accept Rate for fingerprint verification. The FAR is the mathematical probability (1:n) of two different fingerprints being falsely matched.

The value of n, which is specified in the Value: (one in) text box, indicates the likelihood of false fingerprint verification. The higher the value of n, the less likely a fingerprint will be falsely accepted as verified. For example, setting n to 10,000 indicates that it is probable that one in every 10,000 fingers will be falsely accepted as verified; setting n to 100,000 sets the probability to one in 100,000.

Particularly high values of n may cause false rejection of good fingerprint scans.

If this setting is not configured, the default values of one in 10,000 (Pro 4.3.0 and higher) or 100,000 (Pro versions prior to 4.3.0) are used. The maximum value for n is one in 1,000,000; the minimum is one in 1,000. In an environment with mixed pre-4.3.0 and post-4.3.0 and no FAR GPOs set, a FAR mismatch can result!

False Reject Rates and False Accept Rates are only probabilistic estimates and not indicators of actual performance in a given deployment.

Important Information for all Upgrades

For the following upgrade scenarios these are important and relevant considerations:

- Upgrading Stand Alone Workstation (no Pro Server)
- Upgrade from 4.x Server and 4.x Kiosk
- Upgrade from 3.x Server and 1.x Kiosk
- Upgrade from 4.x Server and 4.x Workstation
- Upgrade from 4.x Server and 3.x Workstation
- Upgrade from 3.x Server and 3.x Workstation

DigitalPersona Pro v4.4.1 Clients Require the Presence of DigitalPersona Pro 4.x Server

Please note that DigitalPersona Pro 4.x clients cannot be deployed with DigitalPersona Pro Server 3.x or earlier. You must install DigitalPersona Pro Server 4.x prior to installing DigitalPersona Pro v4.4.1 clients in an existing DigitalPersona Pro deployment.

Pro Server 64-bit(x64) Interoperability

DigitalPersona Pro Server v4.3.0 (and higher) 64 bit (x64) does NOT provide support for DigitalPersona Pro 3.x Workstation at all. If you wish to install DigitalPersona Pro Server v4.3.0 (or higher) onto a 64 bit server platform, be sure to install the 32 bit (x86) Pro Server software onto your 64 bit OS to enable backwards compatibility support for Pro 3.x Workstation.

.\Pro Server\Setup.exe	installs 32b or 64b, matching the bits of the OS
.\Pro Server\Bin\Setup.exe	installs 32b
.\Pro Server\Bin\x64\Setup.exe	installs 64b

Upgrading Pro Server

While recommended, it is not necessary that Pro Servers are upgraded along with Pro clients. DigitalPersona Pro Workstation v4.4.1 & DigitalPersona Pro Kiosk v4.4.1 are supported by DigitalPersona Pro Server 4.x and higher.

Upgrading OneTouch SignOn Administration Tool

To ensure the compatibility of One Touch SignOn templates across all DigitalPersona Pro clients and to maximize the utilization of the new features available in Pro Solution v4.4.1, we recommend that all DigitalPersona Pro clients be upgraded to v4.4.1. The OneTouch SignOn Administration Tool should also be upgraded to the latest version (or to the version matching the Pro clients.)

Current Versions of Pro Components

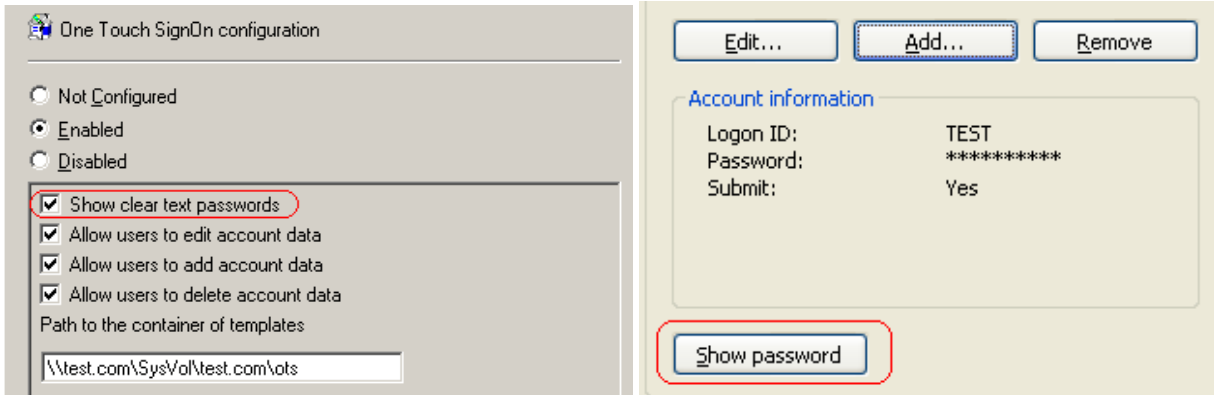
Pro Solution	Additional Optional Components
Server..... 4.3.0	Extended Server Policy Module 4.3.0
License Control Manager Tool..... 4.4.1	OneTouch Access (SSO) 4.3.0
User Query Tool..... 4.4.1	Kiosk ID Server Add-on..... 4.4.1
Attended Fingerprint Registration Tool 4.4.1	Kiosk for ID Server 4.4.1
Fingerprint logon for DCs 4.4.1	
Workstation 4.4.1	
OTS Admin Tool..... 4.4.1	
Kiosk Server Add-on 4.4.0	
Kiosk (workstation)..... 4.4.1	

OTS "show clear text password" Setting .adm Issue

If "**Show clear text passwords**" is enabled in your environment (the recommended state is to enable all four checkboxes) there is no issue for you and the reader can ignore this page.

Expected Behavior

The screenshot on the left is from the OTS configuration GPO setting in the User Configuration node under DigitalPersona Pro Workstation, OTS. The screenshot on the right is from the Fingerprint Logon Manager (FLM). (Not show is) if "**Show clear text passwords**" is unchecked, then the "**Show password**" button should be grayed out and in-accessible.



Symptom

The "**Show password**" button is not properly grayed out. End users can view their OTS (One-Touch Signon) passwords in cleartext even though administrators intended and configured for this not to be the case.

Solutions (Each bullet is a complete solution.)

- Do nothing as this issue is not applicable to your deployment
- **Upgrade to 4.4.1** instead of to 4.4.0 or 4.3.2 or 4.3.1 or 4.3.0.
- Do nothing as the window of this issue manifesting will be short and users will not even notice this
- Upgrade clients and Administrative Templates over the 4.3.0 threshold all at once
- Use separate OUs. Create two sub OUs below where users currently are in AD. One OU will named the Pre-4.3.0 OU. This will have the (existing) pre-4.3.0 adm imported into the DigitalPersona GPO linked to it. AD users using pre Pro 4.3.0 clients will be in this OU. The second OU will be named Post-4.3.0 OU. This will have the new 4.3.0 or higher adm imported into the DigitalPersona GPO linked to it. AD users using Pro 4.3.0 and higher clients will be in this OU. (There are obviously variations, for example a single Post-4.3.0 sub OU would work too.)

FOR THE COMPLETE TECH NOTE INCLUDING CAUSE AND SOLUTION GO TO:

http://www.digitalpersona.com/downloads/OTS_GPO_Tech_Notes2009-10.pdf

Effectuated Products

- Pro client 4.4.0
- Pro client 4.3.2
- Pro client 4.3.1
- Pro client 4.3.0

Upgrading Stand Alone Workstation

Upgrading DigitalPersona Pro Workstations

To ensure the compatibility of One Touch SignOn templates across all DigitalPersona Pro Workstations and to maximize the utilization of the new features available in DigitalPersona Pro Workstation v4.4.1, we recommend that all DigitalPersona Pro Workstations be upgraded to v4.4.1. The OneTouch SignOn Administration Tool should also be upgraded to the latest version.

Data Migration Notes		
Application/Policy	Changes	Actions
One Touch SignOn (OTS) Templates	To ensure compatibility with Internet Explorer, Firefox and DigitalPersona Pro 4.4.1, new templates should be created using Internet Explorer and the DigitalPersona Pro One Touch SignOn Administration Tool. A small percentage of the existing OTS templates may not be compatible with DigitalPersona Pro v4.4.1 and will need to be converted using the DigitalPersona One Touch SignOn Administration Tool. To ensure compatibility with Firefox, existing templates will may to be retrained using Internet Explorer and the DigitalPersona One Touch SignOn Administration Tool.	See the Converting OTS Templates & Fingerprint Logon Retraining section of this document.
Web site One Touch Internet (OTI) logon screens	All existing web site OTI logon screens will continue to work with Internet Explorer after upgrading to DigitalPersona Pro Workstation v4.4.1. To ensure Firefox compatibility, fingerprint logons created prior to 4.3.0 should be deleted and recreated.	See the Converting Win32 OTI Logon Screens section of this document.
One Touch Crypto (OTC)	This application is no longer included with the DigitalPersona Pro. Please contact sales@digitalpersona.com for additional information.	All files encrypted with OTC must be unencrypted before uninstalling or upgrading prior versions of DigitalPersona Pro Workstation software.

To upgrade existing standalone DigitalPersona Pro Workstations (non-networked) to DigitalPersona Pro Workstation v4.4.1:

1. Notify users to decrypt any files encrypted with One Touch Crypto if applicable.
2. Upgrade all existing DigitalPersona Pro Workstations to v4.4.1.
3. Deploy additional DigitalPersona Pro Workstations v4.4.1.
4. Remove previously added DigitalPersonaProWksta.adm from the Local Computer Policy and add the new DigitalPersonaProWksta.adm file.

Upgrade from 4.x Server and 4.x Kiosk

If Your Current Version Is:

DigitalPersona Pro Server version	4.0.0 4.0.1 4.1.0 4.2.1 4.2.4
DigitalPersona Pro Kiosk version	4.1.0 4.2.1 4.2.4 4.2.5 4.3.0 4.3.1 4.3.2

Data Migration Notes:

Application/Policy	Changes	Actions
One Touch SignOn (OTS) Templates	To ensure compatibility with Internet Explorer, Firefox and DigitalPersona Pro 4.4.1, new templates should be created using Internet Explorer and the DigitalPersona Pro One Touch SignOn Administration Tool. A small percentage of the existing OTS templates may not be compatible with DigitalPersona Pro v4.4.1 and will need to be converted using the DigitalPersona One Touch SignOn Administration Tool. To ensure compatibility with Firefox, existing templates may need to be retrained using Internet Explorer and the DigitalPersona One Touch SignOn Administration Tool.	See the Converting OTS Templates & Fingerprint Logon Retraining section of this document.
One Touch Crypto (OTC)	This application is no longer included with the DigitalPersona Pro. Please contact sales@digitalpersona.com for additional information.	All files encrypted with OTC must be unencrypted before uninstalling or upgrading prior versions of Pro Kiosk software.

Recommended Upgrade Steps:

1. Uninstall all existing DigitalPersona Pro Servers (no restart is required).
2. Install DigitalPersona Pro Server v4.3.0 (no restart is required) on all DigitalPersona Pro Servers.
3. Install the DigitalPersona Pro Kiosk Server Add-on located in the DigitalPersona Server **DigitalPersona Pro Kiosk Server Add-on\Install** folder on all DigitalPersona Pro Servers.
4. Remove previously added DigitalPersonaProKiosk.adm from the Computer Policy and add the new DigitalPersonaProKiosk.adm file.
5. Ensure the FAR (False Accept Rate) is set by GPO to 100,000 (or some custom value) constantly for Pro Server and clients.
6. Upgrade all existing DigitalPersona Pro Kiosk to v4.4.1.
7. Deploy additional DigitalPersona Pro Kiosk Workstations v4.4.1.

Upgrade from 3.x Server and 1.x Kiosk

If Your Current Version Is:

DigitalPersona Pro Server version	3.5.0 3.5.1
DigitalPersona Pro Kiosk version	1.0.2

Data Migration Note:

<i>Application/Policy</i>	<i>Changes</i>	<i>Actions</i>
One Touch SignOn (OTS) Templates	To ensure compatibility with Internet Explorer, Firefox and DigitalPersona Pro 4.4.1, new templates should be created using Internet Explorer and the DigitalPersona Pro One Touch SignOn Administration Tool. A small percentage of the existing OTS templates may not be compatible with DigitalPersona Pro v4.4.1 and will need to be converted using the DigitalPersona One Touch SignOn Administration Tool. To ensure compatibility with Firefox, existing templates will need to be retrained using Internet Explorer and the DigitalPersona One Touch SignOn Administration Tool.	See the Converting OTS Templates & Fingerprint Logon Retraining section of this document.

Recommended Upgrade Steps:

1. Uninstall all existing DigitalPersona Pro Servers (no restart is required).
2. Launch the Domain Configuration Wizard (included with your DigitalPersona Server installation files) in all domains where users will be authenticated. (This step should only be performed once, prior to the first DigitalPersona Pro 4.x Server installation.)
3. Install DigitalPersona Pro Server v4.3.0 (no restart is required) on all DigitalPersona Pro Servers.
4. Install the DigitalPersona Pro Kiosk Server Add-on located in the DigitalPersona Server **DigitalPersona Pro Kiosk Server Add-on\Install** folder on all DigitalPersona Pro Servers.
5. Remove previously added DigitalPersonaProKiosk.adm from the Computer Policy and add the new DigitalPersonaProKiosk.adm file.
6. Install the License file using the License Control Manager. (This step need only be performed once per domain.)
7. Convert existing OTS templates using the OTS Administration Tool; the Conversion Utility will check for and convert older templates that need to be made compatible with Pro Kiosk v4.4.1.
8. Ensure the FAR (False Accept Rate) is set by GPO to 100,000 (or some custom value) constantly for Pro Server and clients.
9. Upgrade all existing DigitalPersona Pro Kiosk workstations to v4.4.1.
10. Deploy additional DigitalPersona Pro Kiosk workstations v4.4.1.

Upgrade from 4.x Server and 4.x Workstation

If Your Current Version Is:

Pro Server versions	4.0.0
	4.0.1
	4.1.0
	4.2.1
	4.2.4
Pro Workstation versions	4.0.0
	4.0.1
	4.1.0
	4.2.1
	4.2.4
	4.2.5
	4.3.0
	4.3.1
	4.3.2

Data Migration Notes:

Application/Policy	Changes	Actions
One Touch SignOn (OTS) Templates	To ensure compatibility with Internet Explorer, Firefox and DigitalPersona Pro 4.4.1, new templates should be created using Internet Explorer and the DigitalPersona Pro One Touch SignOn Administration Tool. A small percentage of the existing OTS templates may not be compatible with DigitalPersona Pro v4.4.1 and will need to be converted using the DigitalPersona One Touch SignOn Administration Tool. To ensure compatibility with Firefox, existing templates may need to be retrained using Internet Explorer and the DigitalPersona One Touch SignOn Administration Tool.	See the Converting OTS Templates & Fingerprint Logon Retraining section of this document.
Web site One Touch Internet (OTI) logon screens	All existing web site OTI logon screens will continue to work with Internet Explorer after upgrading to DigitalPersona Pro Workstation v4.4.1. To ensure Firefox compatibility, fingerprint logons created prior to 4.3.0 should be deleted and recreated.	See the Converting Win32 OTI Logon Screens section of this document.
One Touch Crypto (OTC)	This application is no longer included with the DigitalPersona Pro. Please contact sales@digitalpersona.com for additional information.	All files encrypted with OTC must be unencrypted before uninstalling or upgrading prior versions of Pro Workstation software.
Pro User & Computer Policies	These policies have been changed with the release of DigitalPersona Pro v4.3.	See the Extended Server Policy Module section of this document

Recommended Upgrade Steps:

10/20/2009

1. Uninstall all existing Pro Servers (no restart is required).
2. Install Pro Server 4.3 (no restart is required)
3. Remove previously added DigitalPersonaProWksta.adm from the Computer Policy and add the new DigitalPersonaProWksta.adm file.
4. Ensure the FAR (False Accept Rate) is set by GPO to 100,000 (or some custom value) constantly for Pro Server and clients.
5. Upgrade all existing DigitalPersona Pro Workstations to v4.4.1.
6. Deploy additional Pro 4.4.1 workstations.

Upgrade from 4.x Server and 3.x Workstation

If Your Current Version Is:

Pro Server versions	4.0.0
	4.0.1
	4.1.0
	4.2.1
	4.2.4
Pro Workstation versions	3.5.0
	3.5.1

Data Migration Note:

Application/Policy	Changes	Actions
One Touch SignOn (OTS) Templates	To ensure compatibility with Internet Explorer, Firefox and DigitalPersona Pro 4.4.1, new templates should be created using Internet Explorer and the DigitalPersona Pro One Touch SignOn Administration Tool. A small percentage of the existing OTS templates may not be compatible with DigitalPersona Pro v4.4.1 and will need to be converted using the DigitalPersona One Touch SignOn Administration Tool. To ensure compatibility with Firefox, existing templates may need to be retrained using Internet Explorer and the DigitalPersona One Touch SignOn Administration Tool.	See the Converting OTS Templates & Fingerprint Logon Retraining section of this document.
Web site One Touch Internet (OTI) logon screens	All existing web site OTI logon screens will continue to work with Internet Explorer after upgrading to DigitalPersona Pro Workstation v4.4.1. To ensure Firefox compatibility, fingerprint logons created prior to 4.3.0 should be deleted and recreated.	See the Converting Win32 OTI Logon Screens section of this document.
One Touch Crypto (OTC)	This application is no longer included with the DigitalPersona Pro. Please contact sales@digitalpersona.com for additional information.	All files encrypted with OTC must be unencrypted before uninstalling or upgrading prior versions of Pro Workstation software.
Pro User & Computer Policies	These policies have been changed with the release of DigitalPersona Pro v4.3.	See the Extended Server Policy Module section of this document

Recommended Upgrade Steps:

1. Uninstall all existing DigitalPersona Pro Servers (no restart is required).
2. Install DigitalPersona Pro Server v4.3.0 (no restart is required) on all DigitalPersona Pro Servers.
3. Remove previously added DigitalPersonaProWksta.adm from the Computer Policy and add the new DigitalPersonaProWksta.adm file.
4. Install the License file using the License Control Manager. (This step need only be performed once per DigitalPersona Pro Server installation.)
5. Ensure the FAR (False Accept Rate) is set by GPO to 100,000 (or some custom value) constantly for Pro Server and clients.
6. Upgrade all existing DigitalPersona Pro Workstations to v4.4.1.
7. Deploy additional DigitalPersona Pro Workstations v4.4.1.

For mixed environment of Pro AD Workstation 3.x and 4.x

If you have deployed Pro software in a Windows Server 2003 SP1 environment and will continue to run a mixed environment of Pro AD Workstation versions 3.x and 4.x, please read the following notice:

http://www.digitalpersona.com/index.php?id=bus_support_refMaterial_windows2003SP1Notice

Upgrade from 3.x Server and 3.x Workstation

If Your Current Version Is:

Pro Server versions	3.5.0 3.5.1
Pro Workstation versions	3.5.0 3.5.1

Data Migration Note:

Application/Policy	Changes	Actions
One Touch SignOn (OTS) Templates	To ensure compatibility with Internet Explorer, Firefox and DigitalPersona Pro 4.4.1, new templates should be created using Internet Explorer and the DigitalPersona Pro One Touch SignOn Administration Tool. A small percentage of the existing OTS templates may not be compatible with DigitalPersona Pro v4.4.1 and will need to be converted using the DigitalPersona One Touch SignOn Administration Tool. To ensure compatibility with Firefox, existing templates will need to be retrained using Internet Explorer and the DigitalPersona One Touch SignOn Administration Tool.	See the Converting OTS Templates & Fingerprint Logon Retraining section of this document.
Web site One Touch Internet (OTI) logon screens	All existing web site OTI logon screens will continue to work with Internet Explorer after upgrading to DigitalPersona Pro Workstation v4.4.1. To ensure Firefox compatibility, fingerprint logons created prior to 4.3.0 should be deleted and recreated.	See the Converting Win32 OTI Logon Screens section of this document.
One Touch Crypto (OTC)	This application is no longer included with the DigitalPersona Pro. Please contact sales@digitalpersona.com for additional information.	All files encrypted with OTC must be unencrypted before uninstalling or upgrading prior versions of Pro Workstation software.
Pro User & Computer Policies	These policies have been changed with the release of DigitalPersona Pro v4.3.	See the Extended Server Policy Module section of this document

Recommended Upgrade Steps:

1. Uninstall all existing DigitalPersona Pro Servers (no restart is required).
2. Launch the Domain Configuration Wizard (included with your DigitalPersona Server installation files) in all domains where users will be authenticated. (This step should only be performed once, prior to the first DigitalPersona Pro 4.x Server installation.)
3. Install DigitalPersona Pro Server v4.3.0 (no restart is required) on all DigitalPersona Pro Servers.
4. Remove previously added DigitalPersonaProWksta.adm from the Computer Policy and add the new DigitalPersonaProWksta.adm file.
5. Install the License file using the License Control Manager. (This step need only be performed once per DigitalPersona Pro installation.)
6. Ensure the FAR (False Accept Rate) is set by GPO to 100,000 (or some custom value) constantly for Pro Server and clients.
7. Upgrade all existing DigitalPersona Pro Workstations to v4.4.1.
8. Deploy additional DigitalPersona Pro Workstations v4.4.1.

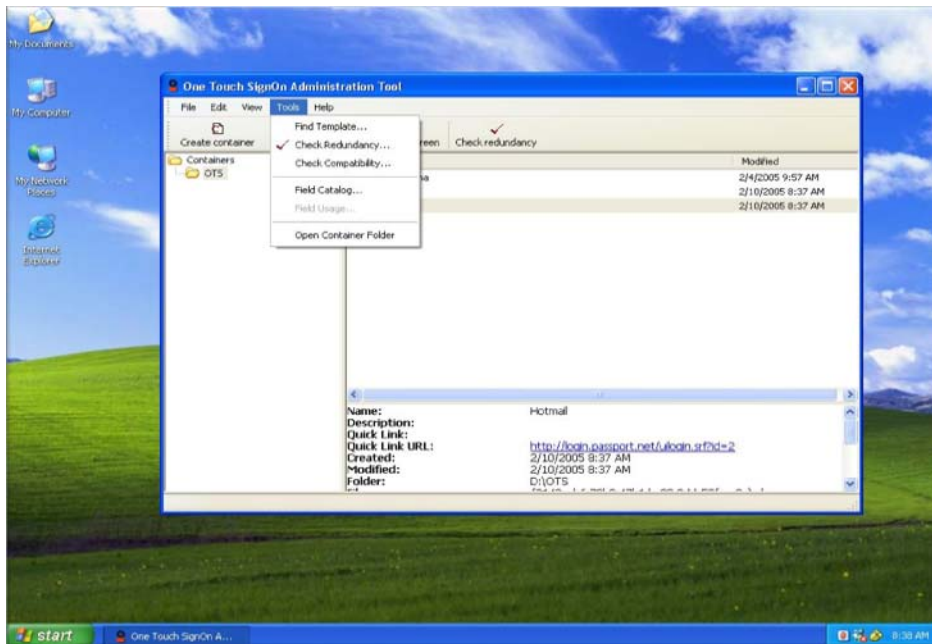
For mixed environment of Pro AD Workstation 3.x and 4.x

If you have deployed Pro software in a Windows Server 2003 SP1 environment and will continue to run a mixed environment of Pro AD Workstation versions 3.x and 4.x, please read the following notice:

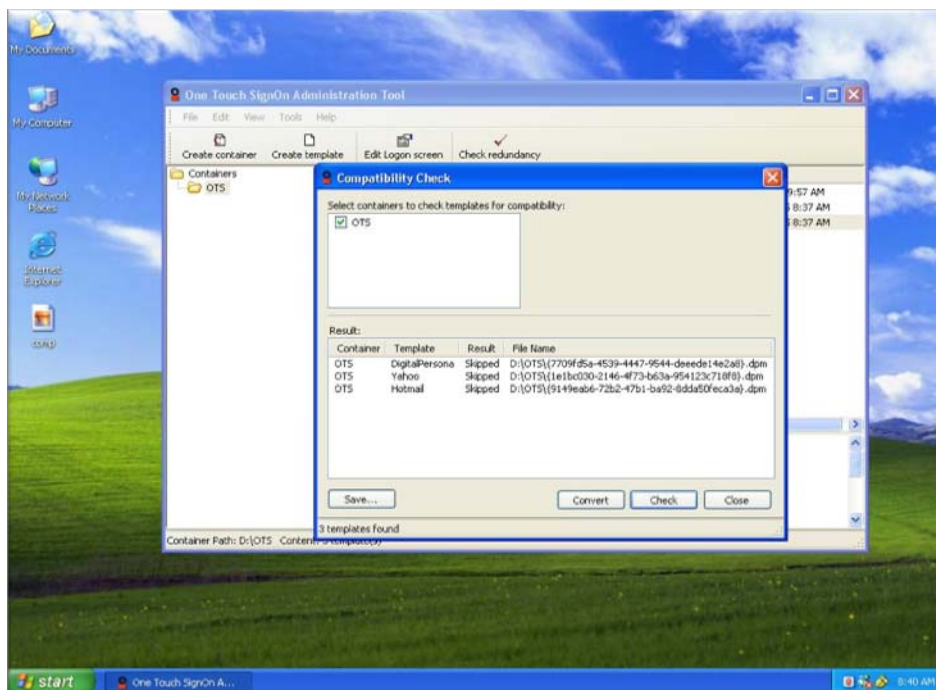
http://www.digitalpersona.com/index.php?id=bus_support_refMaterial_windows2003SP1Notice

Converting OTS Templates

1. Open the OTS Administration Tool.
2. Go to Tools menu and click on Check Compatibility



3. In the Check Compatibility window click on the Save button if you want to keep a backup of your current OTS templates before converting them.
4. Click on the Convert button to convert all OTS templates. The conversion utility will convert the templates and automatically save them in their current location.
5. Click on the Close button to close the Compatibility window.
6. Restart your workstation to automatically download the converted templates to your system.



Converting Win32 OTI Logon Screens

1. Install the One Touch SignOn Administration Tool from the Pro Solution v4.4.1 One Touch SignOn folder located in the software package.
2. Start the Tool by going to Start / DigitalPersona Pro / OTS Administration Tools
3. Create a new container that contains the path to the location where OTI templates are located.

The OTI templates you created are located in a hidden folder in your user profiles folder; this folder is located at:

C:\Documents and Settings\<>Username>\Application Data\DigitalPersona\OTS\Templates.

- a. Make sure all folders are not hidden (go to Explorer's Tools / Folder Options)
- b. Create a new container and use the browse button to set the path to YOUR USERNAME location (see screenshots):



4. From the OTS Admin Tools, go to Tools / Check Compatibility, then select the container that you created in step #3. Click on the "Check button". The Tool will check for all templates in this container.

5. Click on the "Convert" button; all templates that need to be converted will be converted.

These templates can now be used with DigitalPersona Pro v4.4.1. Simply go to the Application logon page and login with your registered finger.

Fingerprint Logon Retraining

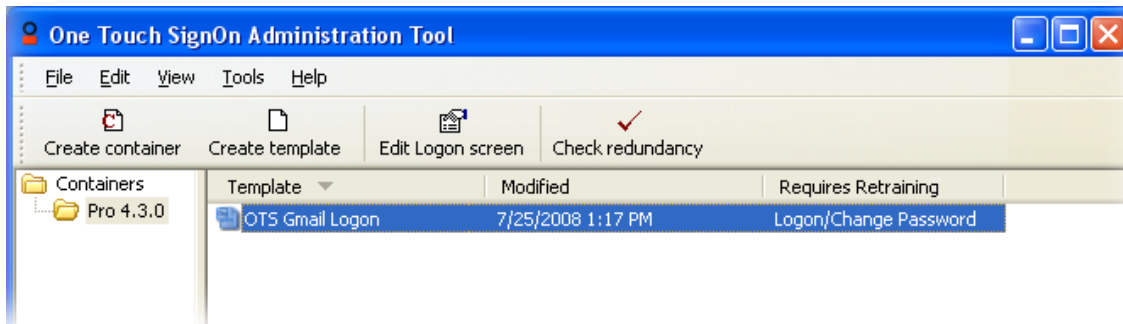
Retraining a fingerprint logon template is only necessary if BOTH of the following statements are true.

- You have fingerprint logon templates that were created in a version of the One Touch SignOn Administration Tool prior to 4.3, AND
- You will have end-users using the created fingerprint logons with the Firefox browser.

Which templates need retraining?

The OTS Administration Tool 4.3 and higher has a new Retraining Wizard that walks you through the simple steps to retrain your Logon screen and Change Password screen templates.

Also, the main window of the OTS Admin Tool has a new column titled “Requires Retraining”.



The “Requires Retraining” column heading is hidden by default, but can be displayed by right-clicking anywhere in the column headers and selecting **Requires Retraining**.

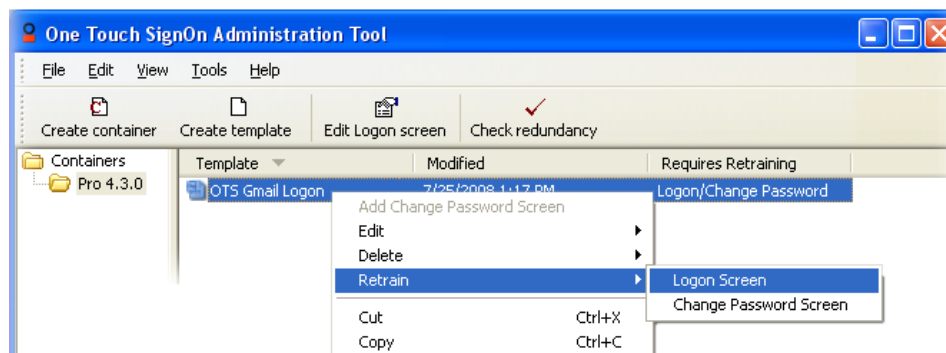
When the heading is visible, all templates with fingerprint logons requiring retraining will have an entry in that column such as Logon, Change Password or Logon/Change Password. This information tells you whether just the Logon screen needs to be retrained, or just the Change Password screen or both.

By viewing the list of templates in each of your containers, you can tell at a glance which fingerprint logons need retraining.

How do I retrain a fingerprint logon?

The easiest way to retrain a fingerprint logon for a **Logon** or **Change Password** screen is to:

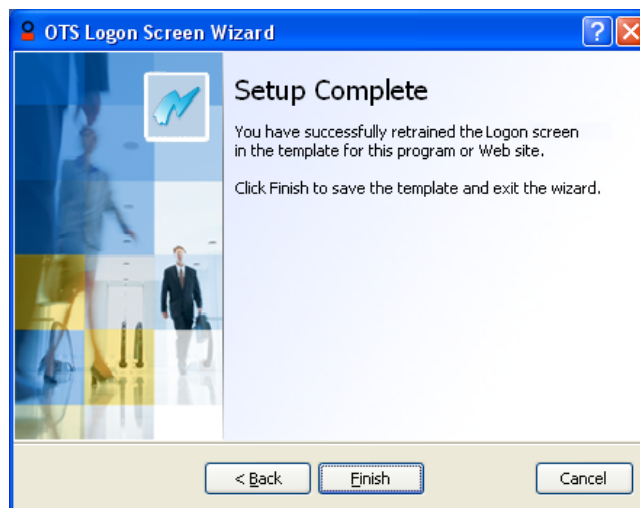
1. Right click on the template that you want to retrain.
2. Select **Retrain** from the menu and select **Logon Screen** or **Change Password Screen** from the submenu.



3. The **OTS Logon Screen Wizard** or **Change Password Screen Wizard** displays.



4. Launch the program or Web site that the Logon screen or Change Password screen is associated with.
5. Click **Next**.
6. The wizard will retrain your template and display the Setup Complete page. Click **Finish** to close the wizard.



Re-Registering User's Fingerprints

As a general, low priority, best practice, re-registering selected user's fingerprints is recommended. Re-registering users whose fingerprints have changed over time will decrease false negatives and reduce the need to raise your domains FAR (False Accept Rate.)

Users whose fingerprints have changed over time include:

- People who work with abrasive materials or solutions and whose fingerprints are damaged or worn down by this work
- Some of our people more advanced in years

The Pro User Query Tool can be used to generate a report of all users with fingerprints registered. When logged to file this can then be viewed as a tab delimited spreadsheet. There is a column for date fingerprint last modified on, which used in conjunction with the select user types above, can determine who you request re-register their fingerprints.

Extended Server Policy Module (ESPM)

DigitalPersona Pro Server v4.3.0 and higher release includes settings which are set per user and are found on the DigitalPersona tab of AD User's properties. These are added to the AD Users and Computers snap-in when DigitalPersona Pro Server is installed. Also they are added by the Pro Administration Tools install's User Properties Snap-In installation selection (not the OTS Admin Tool install.) Only machines on which the ESPM is installed will have added the ESPM's additions. (This can also be done on an administrative workstation with the Microsoft Admin Pack installed.)

Out of the box you get:

- User provides only Windows credentials to log on
- Account is locked out from use of fingerprint credentials

The Extended Server Policy Module (ESPM) contains additional DigitalPersona user policies and is available as a standalone module from DigitalPersona and its authorized Partners.

The Extended Server Policy Module (ESPM) adds:

- User must type a PIN when providing a fingerprint to log on
- User must provide a fingerprint to log on
- Randomize user's Windows password (in some limited earlier versions this policy was basic)

The following table describes the policies included in the basic Server installation and the Extended Server Policy module.

DigitalPersona Pro 4.3 User Policy text	Location of Policy
User provides only Windows credentials to log on	Basic and Extended
Account is locked out from use of fingerprint credentials	Basic and Extended
User must type a PIN when providing a fingerprint to log on	Extended
User must provide a fingerprint to log on	Extended
Randomize user's Windows password	Extended

Customers who have been using Extended Policies (shown in red) with earlier Pro Server iterations or who simply need this functionality now should contact sales@digitalpersona.com for pricing of the Extended Server Policy Module.