ThinkVantage

Client Security Solution 8.3 Deployment Guide

Date: September 29, 2009

Includes: ThinkVantage Fingerprint Software 5.9.2 and Lenovo Fingerprint Software 3.3

ThinkVantage

Client Security Solution 8.3 Deployment Guide

Date: September 29, 2009

Third Edition (October 2009)

Contents

Preface

Information presented in this guide is to support Lenovo® computers installed with the ThinkVantage® Client Security Solution program and the Fingerprint Software program.

The goal of Client Security Solution and Fingerprint Software is to protect your systems by securing client data and to deflect security breach attempts.

The *Client Security Solution Deployment Guide* provides the information required for installing Client Security Solution and Fingerprint Software on one or more computers, and also provides instructions and scenarios on the administrator tools that can be customized to support IT and corporate policies.

This guide is intended for IT administrators, or those responsible for deploying ThinkVantage Client Security Solution and Fingerprint Software to computers throughout their organizations. If you have suggestions or comments, communicate with your Lenovo authorized representative. This guide is updated periodically, and you can check the latest publication on the Lenovo Web site at: http://www-307.ibm.com/pc/support/site.wss/TVAN-ADMIN.html

For questions and information about using the various components in the Client Security Solution and Fingerprint Software workspaces, refer to the online help system and user guides that come with Client Security Solution and Fingerprint Software.

Chapter 1. Overview

This chapter provides an overview of Client Security Solution and Fingerprint Software. The technologies presented in this deployment guide can directly and indirectly help IT professionals because they help make personal computers easier to use, more self-sufficient, and provide powerful tools that facilitate and simplify rollouts. With the help of ThinkVantage Technologies, IT professionals spend less time solving individual computer problems and more time on their core tasks.

Client Security Solution

The primary purpose of Client Security Solution software is to help you protect your computer as an asset, protect confidential data on your computer, and protect network connections accessed by your computer. (For Lenovo-branded systems that contain a Trusted Computing Group (TCG) compliant Trusted Platform Module (TPM), Client Security Solution software will leverage the hardware as the root of trust for the system. If the system does not contain an embedded security chip, Client Security Solution will leverage software based cryptographic keys as the root of trust for the system.)

Features of Client Security Solution 8.3 include:

- **Secure user authentication with Windows® password or Client Security Solution passphrase**

  Client Security Solution can be configured to accept a user's Windows password or a Client Security Solution passphrase for authentication. The Windows password provides convenience and manageability through Windows while the Client Security Solution passphrase provides additional security. The administrator can choose which authentication method is used, and this setting can be changed even after users are enrolled with Client Security Solution.
- **Fingerprint user authentication**

  Leverages the integrated and USB-attached fingerprint technology to authenticate users to password protected applications.
- **Smart card user authentication**

  Leverages a registered smart card for user authentication.
- **Multi-factor user authentication for Windows logon and various Client Security Solution operations**

  Defines multiple authentication devices (Windows password/Client Security passphrase, fingerprint, and smart card) for various security related operations.
- **Password management**

  Securely manages and stores sensitive logon information, such as user IDs and passwords.
- **Password and passphrase recovery**

  Password and passphrase recovery allows users to log into Windows and access their Client Security Solution credentials even if they forget their Windows password or Client Security Solution passphrase, by answering preconfigured security questions.
- **Audit security settings**

  Allows users to view a detailed list of workstation security settings and make changes to comply to defined standards.

- **Digital certificates transfer**

  Client Security Solution protects the private key of user and machine certificates. Use Client Security Solution to protect the private key of your existing certificates.
- **Policy Management for authentication**

  An administrator can choose which devices (Windows password, Client Security Solution passphrase, fingerprint, or smartcard) are required to authenticate for the following actions: Windows logon, Password Manager, and certificate operations.

Client Security Solution passphrase

The Client Security Solution passphrase is an optional feature of user authentication that will provide enhanced security to Client Security Solution applications. The Client Security Solution passphrase has the following requirements:

- Be at least eight characters long
- Contain at least one digit
- Be different from the last three passphrases
- Contain no more than two repeating characters
- Not begin with a digit
- Not end with a digit
- Not contain the user ID
- Not be changed if the current passphrase is less than three days old
- Not contain three or more identical consecutive characters as the current passphrase in any position
- Not be the same as the Windows password

The Client Security Solution passphrase is only known by the individual user. The only way to recover from a forgotten Client Security Solution passphrase is to execute the Client Security Solution password recovery function. If the user has forgotten the answers to his or her recovery questions, then there is no way to recover the data protected by the Client Security Solution passphrase.

Client Security password recovery

This optional feature allows Client Security enrolled users to recover a forgotten Windows password or Client Security passphrase by answering three questions correctly. If this feature is enabled, you will select three answers to ten pre-chosen questions. If the you forget your Windows password or Client Security passphrase, you will have the option to answer these three questions to reset your password or passphrase.

Notes:

1. When using the Client Security passphrase, Client Security password recovery is the only option for recovering a forgotten passphrase. If the you forget the answer to your three questions, you will be forced to rerun the enrollment wizard and lose all previous Client Security protected data.
2. When using Client Security to protect the Rescue and Recovery® Predesktop Area, the Password Recovery option will actually display your Client Security passphrase and/or Windows password. Passphrase or password is displayed because the Predesktop Area does not have the ability to automatically perform

a Windows password change. The passphrase or password is displayed when a wireless (non-network attached locally cached domain) user performs this function at the Windows logon.

Client Security Password Manager

Client Security Password Manager enables you to manage easy-to-forget application and web site information, such as user IDs, passwords, and other personal information. Client Security Password Manager protects your personal information through Client Security Solution so that access to your application and web sites remain totally secure. The Client Security Password Manager program also saves time and effort because you only have to remember one password or passphrase, provide your fingerprint, or smart card.

Client Security Password Manager enables to perform the following functions:

- **Encrypt all stored information through the Client Security Solution Software:**

  Automatically encrypts all of your information through Client Security Solution. Your sensitive password information is secured by the Client Security Solution encryption keys.
- **Autofill user IDs and passwords:**

  Automates your login process when you access an application or web site. If your logon information has been entered into Client Security Password Manager, then Client Security Password Manager can automatically fill in the required fields and submit the web site or application.
- **Edit entries using the Client Security Password Manager interface:**

  Enables you to edit your account entries and set up all optional features in one easy-to-use interface. This interface makes managing your passwords and personal information quick and easy. However, most entry related changes can be detected automatically by Client Security Password Manager and allows the user to update their entries with even less work.
- **Save your information without any extra steps:**

  Client Security Password Manager can automatically detect when sensitive information is being sent to a given web site or application. When such a detection is made, Client Security Password Manager prompts the user to save the information, thus simplifying the process of storing sensitive information.
- **Save any information into a Secure Scratch Pad:**

  With Client Security Password Manager, the user can save any textual data in secure scratch pads. The user's secure scratch pads can be protected with the same level of security as any of their other web site or application entries.
- **Export and import login information**

  Enables you to export your sensitive personal information so that you can securely carry it from one computer to another. When you export your login information from the Client Security Password Manager, a password-protected export file is created that can be stored on removable media. Use this file to access your personal information anywhere you go, or to import your entries into another computer with Client Security Password Manager.

  Note:

  – Full import support is available for Client Security Solution Versions 7.0 and 8.*x* export files. Limited import support is available for Client Security Solution Version 6.0 (application entries are not imported). Client Security Software Solution Versions 5.4*x* and previous versions will not import into the Client Security Solution Version 8.*x* Password Manager.

Security Advisor

The Security Advisor tool allows you to view a summary of security settings currently set on your computer. You can use these settings to view your current security status or to enhance your system security. The displayed category default values can be changed through the Windows registry. An example of the security categories included are:

- Hardware passwords
- Windows users passwords
- Windows password policy
- Protected screen saver
- File sharing

Certificate Transfer wizard

The Client Security Certificate Transfer wizard guides you through the process of transferring the private keys associated with your certificates from the software-based Microsoft® cryptographic service provider (CSP) to the hardware-based Client Security Solution CSP. After the transfer, operations using the certificates are more secure because the private keys are protected by Client Security Solution.

Hardware password reset

This tool creates a secure environment that runs independently of Windows and helps you reset forgotten power-on and hard-disk-drive passwords. Your identity is established by answering a set of questions that you create. Create this secure environment as soon as possible, before a password is forgotten. You cannot reset a forgotten hardware password until this secure environment is created on your hard drive and after you have enrolled. This tool is available on select computers only.

Support for systems without Trusted Platform Module

Client Security Solution 8.3 supports Lenovo-branded systems that do not have a compliant embedded security chip. This support allows a standard installation across the entire enterprise in order to create a consistent and secure environment. The systems that have the embedded security chip are more robust against an attack; however, for the systems without the embedded security chip, Client Security Solution will leverage software based cryptographic keys as the root of trust for the system, and the system can also benefit from the additional security and functionality.

Fingerprint Software

The objective of biometric fingerprint technologies offered by Lenovo is to help customers reduce the costs associated with managing passwords, enhance the security of their systems, and help address regulatory compliance. Fingerprint Software enables fingerprint authentication on individual computers and networks by working with the Lenovo fingerprint readers. Fingerprint Software combined with Client Security Solution 8.3 offers expanded functionality. Client Security Solution 8.3 supports both ThinkVantage Fingerprint Software 5.9.2 and Lenovo Fingerprint Software 3.3 that might be available for different machine types. You can find out more about Lenovo fingerprint technologies and download the Fingerprint Software from the Lenovo Web site.

Fingerprint Software offers these functions:

- **Client software capabilities**
  - **Microsoft Windows password replacement:**

    Replaces your password with your fingerprint for easy, fast, and secure system access.
  - **BIOS password (also known as power-on password) and hard drive passwords replacement:**

    Replaces passwords with your fingerprint to enhance logon security and convenience.
  - **Pre-boot fingerprint authentication for SafeGuard Easy full-drive encryption**:

    Utilizes fingerprint authentication to decrypt your hard drive before starting Windows.
  - **Single swipe to access BIOS and Windows:**

    Saves valuable time by swiping your finger at start up to gain access to BIOS and Windows, saving valuable time.
  - **Integration with Client Security Solution:** Use with the Client Security Solution Password Manager and leverage the Trusted Platform Module. Users can swipe their finger to access Web sites and select applications.
- **Administrator features**
  - **Security mode toggle:**

    Allows an administrator to toggle between secure and convenient modes to modify access rights of limited users.
- **Security capabilities**
  - **Software security:**

    Protects user templates through strong encryption when stored on a system and when transferred from the reader to the software.
  - **Hardware security:**

    Provides a security reader with a co-processor that stores and protects fingerprint templates, BIOS passwords, and encryption keys.

Chapter 2. Installation

This chapter contains instructions for installing Client Security Solution, and Fingerprint Software. Before installing Client Security Solution or Fingerprint Software, you should understand the architecture of the application you are installing. This chapter provides the architecture of each application, as well as additional information you need before installing either program.

Client Security Solution

The Client Security Solution installation package was developed with InstallShield 10.5 Premier as a Basic MSI project. InstallShield uses the Windows Installer to install applications, which gives administrators many capabilities to customize installations, such as setting property values from the command line. This chapter describes ways to use and execute the Client Security Solution setup package. For a better understanding, read the entire chapter before you begin to install these packages.

Note: When installing these packages, refer to the Client Security Solution readme file from the Lenovo Web site. The readme file contains up-to-date information on software versions, supported systems, system requirements, and other considerations to help you with the installation.

Installation requirements

The information in this section provides system requirements for installing the Client Security Solution package. For best results, go to the following Web site to make sure that you have the latest version of the software:
http://www.lenovo.com/support

Lenovo-branded computers must meet or exceed the following requirements to install Client Security Solution:

- Operating system: Windows 7
- Memory: 256 MB
  - In shared memory configurations, the BIOS setting for maximum shared memory must be set to no less than 8 MB.
  - In non-shared memory configurations, 120 MB of non-shared memory is required.
- Internet Explorer® 5.5 or later must be installed.
- 300 MB of free space on your hard disk drive.
- VGA-compatible video that supports a resolution of 800 x 600 and 24-bit color.
- The user must have administrative privileges to install Client Security Solution.

Note: It is not supported to deploy Client Security Solution installation package on Windows Server® 2003. However, it is supported to request a certificate from the Windows Server 2003. See “Generating a certificate using key generation in the TPM” on page 71.

Custom public properties

The installation package for the Client Security Software program contains a set of custom public properties that can be set on the command line when running the installation. The following table provides the custom public properties for Windows operating system:

Table 1. Public properties

Property	Description
EMULATIONMODE	Specify to force the installation in Emulation mode even if a TPM exists. Set EMULATIONMODE=1 on the command line to install in Emulation mode.
HALTIFTPMDISABLED	If the TPM is in a disabled state and the installation is running in silent mode, the default is for the installation to proceed in emulation mode. Use the HALTIFTPMDISABLED=1 property when running the installation in silent mode to halt the installation if the TPM is disabled.
NOCSSWIZARD	Set NOCSSWIZARD=1 on the command line to prevent the Client Security Solution enrollment dialog from being displayed automatically after installing Client Security Solution. This property is configured for an administrator who wants to install Client Security Solution, but use scripting later when configuring the system.
CSS_CONFIG_SCRIPT	Set CSS_CONFIG_SCRIPT="*filename*" or "*filename password*" to have a configuration file run after the user completes the install and reboots.
SUPERVISORPW	Set SUPERVISORPW="*password*" on the command line to supply the supervisor password to enable the chip in silent or non-silent install mode. If the chip is disabled and the installation is running in silent mode, the correct supervisor password must be supplied to enable the chip, otherwise the chip is not enabled.
PWMGRMODE	Set PWMGRMODE=1 on the command line to install Password Manager only.
NOSTARTMENU	Set NOSTARTMENU=1 on the command line to prevent generating shortcut in the start menu.
CREATESHORTCUT	Set CREATESHORTCUT=1 on the command line to add an entry into the **Start** Menu.

Trusted Platform Module support

Client Security Solution 8.3 includes support for the computer embedded security chip, the Trusted Platform Module (TPM). If your Lenovo computer includes a TPM supported by the Windows operating system, Client Security Solution will use the drivers integrated with the Windows operating system.

It might require a reboot to enable the TPM, as the TPM is enabled by the system BIOS. If your are running Windows 7, you may be asked to confirm whether to enable the TPM during system startup.

Before any functions can be carried out by the Trusted Platform Module, ownership must first be initialized. Each system will have one Client Security Solution administrator that will control the Client Security Solution options. This administrator must have Windows administrator privileges. The administrator can be initialized using XML deployment scripts.

After ownership of the system is configured, each additional Windows user that logs into the system is automatically prompted with the Client Security Setup wizard in order to enroll and initialize the user's security keys and credentials.

Software emulation of the Trusted Platform Module

Client Security Solution has the option to run without a Trusted Platform Module on qualified systems. The functionality will be the same except it will use software-based keys instead of using hardware-protected keys. The software can also be installed with a switch to force it to always use software-based keys instead of leveraging the Trusted Platform Module. The use of this switch is an installation-time decision, and cannot be reversed without un-installing and reinstalling the software.

The syntax to force a software emulation of the Trusted Platform Module is:

```
InstallFile.exe "/v EMULATIONMODE=1"
```

Installation procedures and command-line parameters

The Microsoft Windows Installer provides several administrative functions through command-line parameters. The Windows Installer can perform an administrative installation of an application or product to a network for use by a workgroup or for customization. Command-line options that require a parameter must be specified with no space between the option and its parameter. For example:

```
setup.exe /s /v"/qn REBOOT="R""
```

is valid, while

```
setup.exe /s /v "/qn REBOOT="R""
```

is not.

Note: The default behavior of the installation when executed alone (running setup.exe without any parameters) is to prompt the user to reboot at the end of the installation. A reboot is required for the program to function properly. The reboot can be delayed through a command line parameter for a silent installation as documented in the preceding section and in the example section.

For the Client Security Solution installation package, an administrative installation unpacks the installation source files to a specified location.

To run an administrative installation, run the setup package from the command line using the /a parameter:

```
setup.exe /a
```

An administrative installation presents a wizard that prompts the administrative user to specify the locations for unpacking the setup files. The default extract location is C:\. You can choose a new location that may include drives other than C:\ (for example, other local drives or mapped network drives). You can also create new directories during this step.

To run an administrative installation silently, you can set the public property TARGETDIR on the command line to specify the extract location:

```
setup.exe /s /v"/qn TARGETDIR=F:\TVTRR"
```

or

```
msiexec.exe /i "Client Security - Password Manager.msi" /qn TARGERDIR=F:\TVTRR
```

Note: If you are not using the latest version of Windows Installer, the setup.exe file will be configured to update the Windows Installer engine to the latest version. The update of the Windows Installer engine will prompt you to reboot the system even in an administrative extract installation. To prevent a reboot in this situation, you can use the REBOOT property of the Windows Installer. If the Windows Installer is the latest version, the setup.exe file will not attempt to update the Windows Installer engine.

Once and administrative installation has been completed, the administrative user can make customizations to the source files, such as adding settings to the registry.

The following parameters and descriptions are documented in the InstallShield developer help documentation. Parameters that do not apply to Basic MSI projects were removed.

Table 2. Parameters

Parameter	Description
/a : Administrative installation	The /a switch causes setup.exe to perform an administrative installation. An administrative installation copies (and uncompresses) your data files to a directory specified by the user, but does not create shortcuts, register COM servers, or create an uninstallation log.
/x : Uninstall mode	The /x switch causes setup.exe to uninstall a previously installed product.
/s : Silent mode	The command setup.exe /s suppresses the setup.exe initialization window for a Basic MSI installation program, but does not read a response file. Basic MSI projects do not create or use a response file for silent installations. To run a Basic MSI product silently, run the command line setup.exe /s /v/qn. (To specify the values of public properties for a silent Basic MSI installation, you can use a command such as setup.exe /s /v"/qn INSTALLDIR=D:\Destination".)

Table 2. Parameters (continued)

Parameter	Description
/v : pass arguments to Msiexec	The /v argument is used to pass command line switches and values of public properties through to msiexe.exe.
/L : Setup language	Users can use the /L switch with the decimal language ID to specify the language used by a multi-language installation program. For example, the command to specify German is setup.exe /L1031.
/w : Wait	For a Basic MSI project, the /w argument forces setup.exe to wait until the installation is complete before exiting. If you are using the /w option in a batch file, you may want to precede the entire setup.exe command line argument with start /WAIT. A properly formatted example of this usage is as follows: `start /WAIT setup.exe /w`

Using msiexec.exe

To install from the unpacked source after making customizations, the user calls msiexec.exe from the command line, passing the name of the unpacked *.MSI file. msiexec.exe is the executable program of the Windows Installer used to interpret installation packages and install products on target systems.

```
msiexec /i "C:\WindowsFolder\Profiles\UserName\
Personal\MySetups\project name\product configuration\release name\
DiskImages\Disk1\product name.msi"
```

Note: Enter the preceding command as a single line with no spaces following the slashes.

The following table describes the available command line parameters that can be used with msiexec.exe and examples of how to use it.

Table 3. Command line parameters

Parameter	Description

/I *package*
or
product code
	Use this format to install the product:
	`Othello:msiexec /i "C:\WindowsFolder\Profiles\`
	`UserName\Personal\MySetups`
	`\Othello\Trial Version\`
	`Release\DiskImages\Disk1\`
	`Othello Beta.msi"`
	
	Product code refers to the Globally Unique Identifier (GUID) that is automatically generated in the product code property of your product's project view.

/a *package*	The **/a** option allows users with administrator privileges to install a product onto the network.
/x *package* or *product code*	The **/x** option uninstalls a product.

Table 3. Command line parameters (continued)

Parameter	Description
/L [i|w|e|a|r|u|c|m|p|v|+] *log file*	Building with the **/L** option specifies the path to the log file; these flags indicate which information to record in the log file: • **i** logs status messages • **w** logs non-fatal warning messages • **e** logs any error messages • **a** logs the commencement of action sequences • **r** logs action-specific records • **u** logs user requests • **c** logs initial user interface parameters • **m** logs out-of-memory messages • **p** logs terminal settings • **v** logs the verbose output setting • **+** appends to an existing file • * is a wildcard character that allows you to log all information (excluding the verbose output setting)
/q [n|b|r|f]	The /q option is used to set the user interface level in conjunction with the following flags: • **q** or qn creates no user interface • **qb** creates a basic user interface The user interface settings below display a modal dialog box at the end of installation: • **qr** displays a reduced user interface • **qf** displays a full user interface • **qn+** displays no user interface • **qb+** displays a basic user interface
/? or /h	Either command displays Windows Installer copyright information

TRANSFORMS	The **TRANSFORMS** command line parameter specifies any transforms that you would like applied to your base package.
	`msiexec /i "C:\WindowsFolder\`
	`Profiles\UserName\Personal`
	`\MySetups\`
	`Your Project Name\Trial Version\`
	`My Release-1`
	`\DiskImages\Disk1\`
	`ProductName.msi" TRANSFORMS="New Transform 1.mst"`
	
	You can separate multiple transforms with a semicolon. Do not use semicolons in the name of your transform, as the Windows Installer service will interpret those incorrectly.

Table 3. Command line parameters (continued)

Parameter	Description

Properties	All public properties can be set or modified from the command line. Public properties are distinguished from private properties and are all capital letters. For example, *COMPANYNAME* is a public property.
	
	To set a property from the command line, use the following syntax:
	`PROPERTY=VALUE`
	
	If you wanted to change the value of *COMPANYNAME*, you would enter the following:
	`msiexec /i "C:\WindowsFolder\`
	`Profiles\UserName\Personal\`
	`MySetups\Your Project Name\`
	`Trial Version\My Release-1\`
	`DiskImages\Disk1\ProductName.msi"`
	`COMPANYNAME="InstallShield"`

Standard Windows Installer public properties

The Windows Installer has a set of standard built in public properties that can be set on the command line to specify certain behavior during the installation. The following table provides most common public properties used in the command line.

For additional information, refer to the Microsoft Web site at: http://msdn2.microsoft.com/en-us/library/aa367437.aspx

The following table shows the commonly used Windows Installer properties:

Table 4. Windows Installer properties

Property	Description
TARGETDIR	Specifies the root destination directory for the installation. During an administrative installation this property is the location to copy the installation package.
ARPAUTHORIZEDCDFPREFIX	URL of the update channel for the application.
ARPCOMMENTS	Provides Comments for the Add or Remove Programs on Control Panel.
ARPCONTACT	Provides Contact for the Add or Remove Programs on Control Panel.
ARPINSTALLLOCATION	Fully qualified path to the application's primary folder.
ARPNOMODIFY	Disables functionality that would modify the product.
ARPNOREMOVE	Disables functionality that would remove the product.
ARPNOREPAIR	Disables the Repair button in the Programs wizard.

Table 4. Windows Installer properties (continued)

Property	Description
ARPPRODUCTICON	Specifies the primary icon for the installation package.
ARPREADME	Provides a ReadMe for the Add or Remove Programs on Control Panel.
ARPSIZE	Estimated size of the application in kilobytes.
ARPSYSTEMCOMPONENT	Prevents display of application in the Add or Remove Programs list.
ARPURLINFOABOUT	URL for an application's home page.
ARPURLUPDATEINFO	URL for application-update information.
REBOOT	The REBOOT property suppresses certain prompts for a reboot of the system. An administrator typically uses this property with a series of installations to install several products at the same time with only one reboot at the end. Set REBOOT="R" to disable any reboots at the end of an install.

Installation log file

The installation log file of Client Security Solution is named as cssinstall83xx.log, and is created in the %temp% directory if the setup is launched by the setup.exe file (double-click the install.exe file, run the executable without parameters, or extract the MSI package and run the setup.exe file). This file contains log messages that can be used to debug installation problems. The log file includes any activities performed by the **Add/Remove** applet in Control Panel. The log file is not created when you are running the setup.exe file directly from the MSI package. To create a log file for all MSI actions, you can enable the logging policy in the registry. To do this, create the following value:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer]
"Logging"="voicewarmup"
```

Installation examples

The following table shows examples of installations using the setup.exe file.

Table 5. Installation examples using the setup.exe file

Description	Example
Silent installation with no reboot	`setup.exe /s /v"/qn REBOOT="R""`
Administrative installation	`setup.exe /a`
Silent administrative installation specifying the extract location for Client Security Software.	`setup.exe /a /s /v"/qn TARGETDIR="F:\CSS83""`
Silent uninstallation.	`setup.exe /s /x /v/qn`
Installation with no reboot (Create an installation log in temp subdirectory for Client Security Software.)	`setup.exe /v"REBOOT="R" /L*v %temp%\cssinstall83.log"`
Installation without installing the Predesktop Area	`setup.exe /vPDA=0`

The following table provides installation examples using Client Security - Password Manager.msi:

Table 6. Installation examples using Client Security - Password Manager.msi

Description	Example
Installation	`msiexec /i "C:\CSS83\Client Security Solution - Password Manager.msi"`
Silent installation with no reboot	`msiexec /i "C:\CSS83\Client Security Solution - Password Manager.msi" /qn REBOOT="R"`
Silent uninstallation	`msiexec /x "C:\CSS83\Client Security Solution - Password Manager.msi" /qn`

Installing ThinkVantage Fingerprint Software

The setup.exe file of the ThinkVantage Fingerprint Software program can be installed through the following methods:

Silent installation

To silently install ThinkVantage Fingerprint Software, run the setup.exe file located in the installation directory on your CD-ROM drive.

Use the following syntax:

`Setup.exe` *`PROPERTY=VALUE`* `/q /i`

where *q* is for silent installation and *i* is for installation. For example:

```
setup.exe INSTALLDIR="C:\Program Files\ThinkVantage fingerprint software" /q /i
```

To uninstall the software, use the /x parameter instead of /i:

```
setup.exe INSTALLDIR="C:\Program Files\ThinkVantage fingerprint software" /q /x
```

Options

The following options are supported by the ThinkVantage Fingerprint Software.

Table 7. Options supported by the ThinkVantage Fingerprint Software

Parameter	Description
CTRLONCE	Displays the Control Center only once. The default value is 0.
CTLCNTR	• 0 = Do not display Control Center at startup. • 1 = Display Control Center at startup. The default value is 1.
DEFFUS	• 0 = Do not use Fast User Switching (FUS) settings. • 1 = Use FUS settings. The default value is 0.

Table 7. Options supported by the ThinkVantage Fingerprint Software (continued)

Parameter	Description
DEVICEBIO	Configures the device type that will be used by the user. • DEVICEBIO=#3 - Use the device sensor to save the first enrollment. • DEVICEBIO=#0 - Use the hard disk drive to save the enrollment. • DEVICEBIO=#1 - Use the Companion Chip to save the enrollment.
INSTALLDIR	Set the installation directory.
OEM	• 0 = Install with support to server passports or server authentication. • 1 = Install only standalone-computer mode with local passports. The default value is 1.
PASSPORT	Set the default passport type. • 1 = Local passport • 2 = Server passport The default value is 1.
POSSSO	• 1 = Enable single sign-on. • 0 = Disable single sign-on. The default value is 1.
PSLOGON	• 0 = Disable the fingerprint logon. • 1 = Enable the fingerprint logon. The default value is 0.
REBOOT	Suppresses all reboots including prompts during installation by setting to `Really Suppress`.
SECURITY	• 1 = Install in the secure mode. • 0 = Install in the convenient mode.
SHORTCUT	• 0 = Do not display Control Center shortcut at startup. • 1 = Enable the display of Control Center shortcut at startup. The default value is 0.
SHORTCUTFOLDER	Set the default name of the shortcut folder in the **Start** menu.
Non-administrator user privileges	
DELETESELF	• 1 = Enable the fingerprint deletion. • 0 = Disable the fingerprint deletion. The default value is 1.
ENROLLSELF	• 1 = Enable the fingerprint enrollment. • 0 = Disable the fingerprint enrollment. The default value is 1.

Table 7. Options supported by the ThinkVantage Fingerprint Software (continued)

Parameter	Description
ENROLLTBX	• 1 = Enable the selection of fingerprint for power-on. • 0 = Disable the selection of fingerprint for power-on. The default value is 1.
IMPORTSELF	• 1 = Enable the fingerprint import/export for non-administrator users. • 0 = Disable the fingerprint import/export for non-administrator users. The default value is 1.
REVEALPWD	• 1 = Enable the Windows password recovery. • 0 = Disable the Windows password recovery. The default value is 1.
Anti-hammering protection (Lockout Settings)	
LOCKOUT	• 1 = Enable the anti-hammering protection. • 0 = Disable the anti-hammering protection. The default value is 1.
LOCKOUTCOUNT	Maximum retries. The default value is 5, and you can use any value.
LOCKOUTTIME	Timeout in milliseconds. The default value is 120 000, and you can use any value up to 360 000.
Authentication timeout (Inactivity Settings)	
GUITMENABLE	• 1 = Enable the authentication timeout in milliseconds. • 0 = Disable the authentication timeout in milliseconds. The default value is 1.
GUITMTIME	Authentication timeout duration. The default value is 120 000, and you can use any value up to 360 000.
PWDLOGON	• 1 = Enable the fingerprint-only logon for non-administrator users. • 0 = Disable the fingerprint-only logon for non-administrator users. The default value is 1.
NOPOPPAPCHECK	• 0 = Do not show the power-on security options. • 1 = Always show the power-on security options. The default value is 0.

Table 7. Options supported by the ThinkVantage Fingerprint Software (continued)

Parameter	Description
CSS	• 0 = Assume that Client Security Solution has not been installed. • 1 = Assume that Client Security Solution has been installed. The default value is 0.

Note: All options are optional.

To uninstall the Fingerprint Software, use the `/x` parameter instead of `/i`. During the standard uninstall from the user interface, dialogs for selecting whether to delete existing passports and disable the boot security feature are displayed. In the silent uninstall mode, you can use the DELPAS parameter. Set the DELPAS value to "1" to delete existing passports. If these options are not defined, or have any other value, passports are left on the computer and the boot security remains enabled. If you leave the boot security on, you will not be able to edit fingerprints in the boot security memory unless you re-install the product. For example, running the following syntax:

```
msiexec /i Setup.msi DELPAS="1" /q
```

would uninstall the product, delete all existing passports, and leave the boot security on the computer.

Installing Lenovo Fingerprint Software

The setup32.exe file of the Lenovo Fingerprint Software program can be installed by using the following procedure.

Silent installation

To silently install the Fingerprint Software, run the setup32.exe file located in the installation directory on your CD-ROM drive.

Use the following syntax:

```
setup32.exe /s /v"/qn REBOOT ="R""
```

To uninstall the software, use the following syntax:

```
setup32.exe /x /s /v"/qn REBOOT="R""
```

Options

The following options are supported by the Lenovo Fingerprint Software.

Table 8. Options supported by the Lenovo Fingerprint Software

Parameter	Description
SHORTCUT	Displays Control Center shortcut in the **Start** menu. • 0 = Do not display the Control Center shortcut. • 1 = Display the Control Center shortcut. The default value is 0.

Table 8. Options supported by the Lenovo Fingerprint Software (continued)

Parameter	Description
SWAUTOSTART	• 0 = Do not start fingerprint software at startup. • 1 = Start fingerprint software at startup. The default value is 1.
SWFPLOGON	• 0 = Do not use the fingerprint logon (GINA or Credential Provider). • 1 = Use the fingerprint logon (GINA or Credential Provider). The default value is 0.
SWPOPP	• 0 = Disable power-on password protection. • 1 = Enable power-on password protection. The default value is 0.
SWSSO	• 0 = Disable the single sign-on function. • 1 = Enable the single sign-on function. The default value is 0.
SWALLOWENROLL	• 0 = Disable the fingerprint enrollment for non-administrator users. • 1 = Enable the fingerprint enrollment for non-administrator users. The default value is 1.
SWALLOWDELETE	• 0 = Disable the fingerprint deletion for non-administrator users. • 1 = Enable the fingerprint deletion for non-administrator users. The default value is 1.
SWALLOWIMEXPORT	• 0 = Disable the fingerprint import/export for non-administrator users. • 1 = Enable the fingerprint import/export for non-administrator users. The default value is 1.
SWALLOWSELECT	• 0 = Disable the selection of using fingerprint to replace power-on password for non-administrator users. • 1 = Enable the selection of using fingerprint to replace power-on password for non-administrator users. The default value is 1.
SWALLOWPWRECOVERY	• 0 = Disable the Windows password recovery. • 1 = Enable the Windows password recovery. The default value is 1.

Table 8. Options supported by the Lenovo Fingerprint Software (continued)

Parameter	Description
SWANTIHAMMER	• 0 = Disable the anti-hammering protection. • 1 = Enable the anti-hammering protection. The default value is 1.
SWANTIHAMMERRETRIES	Specifies the maximum retries. The default value is 5. **Note:** This setting works only when `SWANTIHAMMER` is enabled.
SWANTIHAMMERTIMEOUT	Specifies the timeout duration in seconds. The default value is 120. **Note:** This setting works only when `SWANTIHAMMER` is enabled.
SWAUTHTIMEOUT	• 0 = Disable the authentication timeout. • 1 = Enable the authentication timeout. The default value is 1.
SWAUTHTIMEOUTVALUE	Specifies the period of inactivity before authentication timeout in seconds. The default value is 120. **Note:** This setting works only when `SWAUTHTIMEOUT` is enabled.
SWNONADMIFPLOGONONLY	• 0 = Disable the fingerprint-only logon for non-Administrator users. • 1 = Enable the fingerprint-only logon for non-Administrator users. The default value is 1.
SWSHOWPOWERON	• 0 = Do not show the power-on security options. • 1 = Always show the power-on security options. The default value is 0.
CSS	• 0 = Assume that Client Security Solution has not been installed. • 1 = Assume that Client Security Solution has been installed. The default value is 0.

Systems Management Server

Systems management server (SMS) installations are also supported. Open the SMS administrator console. Create a new package and set package properties in a standard way. Open the package and select New-Program in the Programs item. At the command line type:

```
Setup.exe /m yourmiffilename /q /i
```

You can use the same parameters as used for the silent installation.

Setup normally reboots at the end of installation process. If you want to suppress all reboots during installation and reboot later (after installing more programs), add REBOOT="ReallySuppress" to the list of properties.

Chapter 3. Working with Client Security Solution

Before you install Client Security Solution, you should understand the customization available for Client Security Solution. This chapter provides customization information about Client Security Solution, as well as information regarding the Trusted Platform Module. The terms used in this chapter referencing the Trusted Platform Module are defined by the Trusted Computing Group (TCG). For more information about the Trusted Platform Module refer to the following Web site:
http://www.trustedcomputinggroup.org/

Using the Trusted Platform Module

The Trusted Platform Module is an embedded security chip designed to provide security-related functions for the software utilizing it. The embedded security chip is installed on the motherboard of a system and communicates through a hardware bus. Systems that incorporate a Trusted Platform Module can create cryptographic keys and encrypt them so that they can only be decrypted by the same Trusted Platform Module. This process is often called *wrapping* a key, and helps protect the key from disclosure. On a system with a Trusted Platform Module, the master wrapping key, called the Storage Root Key (SRK), is stored within the Trusted Platform Module itself, so the private portion of the key is never exposed. The embedded security chip can also store other storage keys, signing keys, passwords, and other small units of data. Because of the limited storage capacity in the Trusted Platform Module, the SRK is used to encrypt other keys for off-chip storage. The SRK never leaves the embedded security chip, and forms the basis for protected storage.

Using the embedded security chip is optional and requires a Client Security Solution administrator. Whether for individual user or a corporate IT department, the Trusted Platform Module must be initialized. Subsequent operations, such as the ability to recover from a hard drive failure or replaced system board, are also restricted to the Client Security Solution administrator.

Note: If you are changing the authentication mode and attempt to unlock the security chip, you must log out and then log back in as the master administrator. This will enable you to unlock the chip. You can also log on as a secondary user and continue to convert the authentication mode. This is done automatically when the secondary user logs on. Client Security Solution will prompt for the secondary user password or passphrase. Once Client Security Solution is done processing the change, the secondary user can proceed with unlocking the chip.

Using the Trusted Platform Module with Windows 7

If the Windows 7 logon is enabled and the Trusted Platform Module is disabled, you must disable the Windows logon feature before disabling the Trusted Platform Module in F1 BIOS. Doing this will prevent a security message that states: **Security chip has been deactivated, the logon process cannot be protected**.

In addition, if you are upgrading the operating system of a client system, you must clear the security chip to avoid enrollment failure of Client Security. To clear the chip in F1 BIOS, the system must be started from a cold boot. You will not be able to clear the chip if you attempt this process after a warm reboot.

Managing Client Security Solution with cryptographic keys

Client Security Solution is described by the two main deployment activities; Take Ownership and Enroll User. While running the Client Security Solution Setup Wizard for the first time, the Take Ownership and Enroll User processes are both performed during the initialization. The particular Windows user ID that completed the Client Security Solution Setup Wizard is the Client Security Solution Administrator and is enrolled as an active user. Every other user that logs into the system will be automatically requested to enroll into Client Security Solution.

- **Take Ownership**

  A single Windows administrator user ID is assigned as the sole Client Security Solution Administrator for the system. Client Security Solution administrative functions must be performed through this user ID. The Trusted Platform Module authorization is either this user's Windows password or Client Security passphrase.

  Note: The only way to recover from a forgotten Client Security Solution Administrators password or passphrase is to either uninstall the software with valid Windows permissions or to clear the security chip in BIOS. Either way, the data protected through the keys associated with the Trusted Platform Module will be lost. Client Security Solution also provides an optional mechanism that allows self-recovery of a forgotten password or passphrase based on a question and answer challenge response. The Client Security Solution Administrator makes the decision whether to use the feature or not.

- **Enroll User**

  Once the Take Ownership process is completed and a Client Security Solution Administrator is created, a User Base Key can be created to securely store credentials for the currently logged on Windows user. This design allows for multiple users to enroll into Client Security Solution and leverage the single Trusted Platform Module. User keys are protected through the security chip, but actually stored off the chip on the hard drive. This design creates hard drive space as the limiting storage factor instead of actual memory built into the security chip. The number of users that can leverage the same secure hardware is vastly increased.

Take Ownership

The root of trust for Client Security Solution is the System Root Key (SRK). This non-migratable asymmetric key is generated within the secure environment of the Trusted Platform Module and never is exposed to the system. The authorization to leverage the key is derived through the Windows Administrator account during the TPM_TakeOwnership command. If the system is leveraging a Client Security passphrase, then the Client Security passphrase for the Client Security Solution Administrator will be the Trusted Platform Module authorization, otherwise it will be the Client Security Solution Administrator's Windows password.

With the SRK created for the system, other key pairs can be created and stored outside of the Trusted Platform Module, but wrapped or protected by the hardware-based keys. Since the Trusted Platform Module, which includes the SRK is hardware and hardware can be damaged, a recovery mechanism is needed to make sure damage to the system does not prevent data recovery.

In order to recover a system, a System Base Key is created. This asymmetric storage key enables the Client Security Solution Administrator to recover from a system board swap or planned migration to another system. In order to protect the System Base Key, but allow it to be accessible during normal operation or recovery, two instances of the key is created and protected by two different methods. First, the System Base Key is encrypted with an AES Symmetric Key that is derived from knowing the Client Security Solution Administrator's password or Client Security passphrase. This copy of the Client Security Solution Recovery Key is solely for the purpose of recovering from a cleared Trusted Platform Module or replaced system board because of hardware failure.

The second instance of the Client Security Solution Recovery Key is wrapped by the SRK to import it to the key hierarchy. This double instance of the System Base Key allows the Trusted Platform Module to protect secrets bound to it below in normal usage and allows for a recovery of a failed system board through the System Base Key that is encrypted with an AES Key unlocked by the Client Security Solution Administrator password or Client Security passphrase. Next, a System Leaf Key is created. This key is created to protect system level secrets such as the AES Key.

The following diagram provides the structure for the System Level Key:

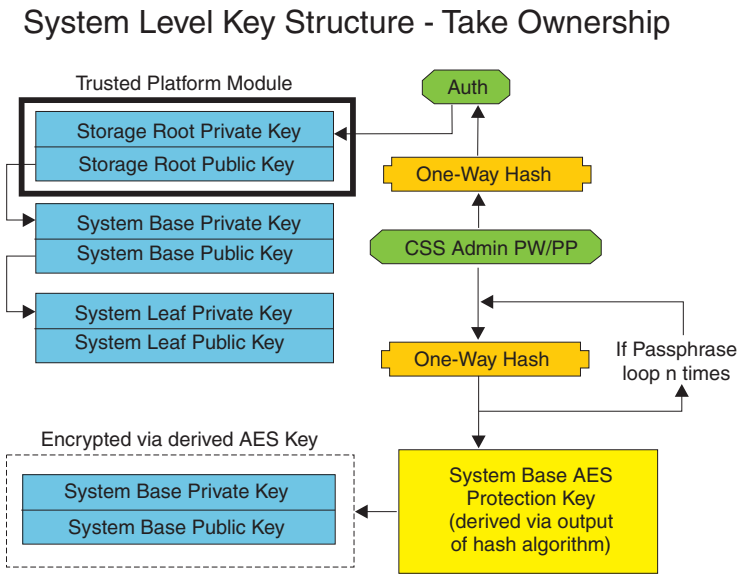

Figure 1. System Level Key Structure - Take Ownership

Enroll User

In order to have each user's data protected by the same Trusted Platform Module, each user will have their own user base key created. This asymmetric storage key can be migrated and is also created twice and protected by a symmetric AES Key generated from each user's Windows password or Client Security passphrase.

The second instance of the User Base Key is then imported into the Trusted Platform Module and protected by the system SRK. With the User Base Key created, a secondary asymmetric key called the User Leaf Key is created. The User Leaf Key protects individual secrets such as the Password Manager AES Key used to protect internet logon information, password used to protect data, and the Windows password AES Key used to protect the access to the operating system.

Access to the User Leaf Key is controlled by the user's Windows password or Client Security Solution passphrase and is automatically unlocked during logon.

The following diagram provides the structure for the user level key:

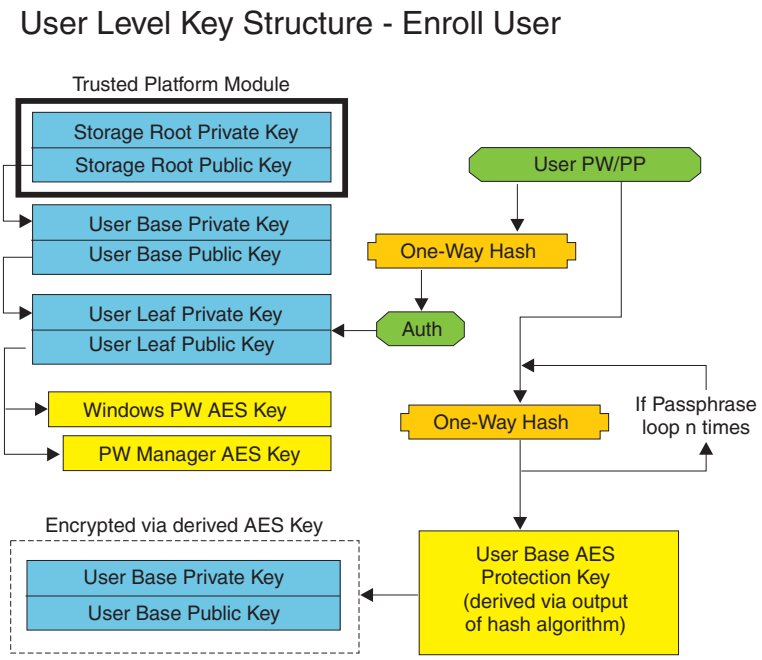

Figure 2. User Level Key Structure - Enroll User

Background enrollment

Client Security Solution 8.3 supports background enrollment for user enrollment that is started automatically. The enrollment process runs in the background without displaying any notifications.

Note: The background enrollment is only available for user enrollment that is started automatically. For user enrollment that is started manually, from the start menu or from the **Reset Security Settings**, a dialog indicating the user to wait for the user enrollment will still be displayed.
Local administrator or domain administrator can also force the waiting dialog to be displayed by editing the following policy as below:

```
CSS_GUI_ALWAYS_SHOW_ENROLLMENT_PROCESSING
```

Or by editing the following registry key as below:

```
HKLM\software\policies\lenovo\client security solution\GUI options\
AlwaysShowEnrollmentProcessing
```

The default value of `AlwaysShowEnrollmentProcessing` is 0. When the above registry key is set to 0, the waiting dialog is not displayed for user enrollment started automatically. When this policy is set to 1, the waiting dialog will always be displayed during user enrollment regardless of how the enrollment is started.

Software emulation

To provide a consistent experience for the user whose computer does not have a TPM, CSS supports the TPM emulation mode.

The TPM emulation mode is a software-based root of trust. The same functionalities provided by the TPM, including digital signature, symmetric key decryption, RSA key import, protection, and random number generation, are available to the user, except there is decreased security because the root of trust is software based keys.

The TPM emulation mode cannot be used as a secure substitute for the TPM. The TPM provides the following two key protection methods that are more secure than the TPM emulation mode.

- All keys used by the TPM are protected by a unique root-level key. The unique root-level key is created inside the TPM and cannot be seen or used outside of the TPM. In the TPM emulation mode, the root-level key is a software-based key stored on the hard disk drive.
- All private key operations are performed within the TPM, so that the private key material for any key is never exposed outside of the TPM. In the TPM emulation mode, all private key operations are performed in the software, so there is no protection of the private key material.

The TPM emulation mode is primarily for the user who is less concerned about the security and more concerned about the system logon speed.

System board swap

A system board swap infers that the old SRK to which keys were bound to is no longer valid, and another SRK is needed. This can also happen if the Trusted Platform Module is cleared through the BIOS.

The Client Security Solution Administrator is required to bind the system credentials to a new SRK. The System Base Key will need to be decrypted through the System Base AES Protection Key derived from the Client Security Solution Administrator's authorization credentials.

If a Client Security Solution Administrator is a domain user ID and the password for that user ID was changed on a different machine; the password that was last used when logged onto the system needing recovery will need to be known in order to decrypt System Base Key for recovery. For example, during deployment a Client Security Solution Administrator user ID and password will be configured, if the password for this user changes on a different machine, then the original password set during deployment will be the required authorization in order to recovery the system.

Follow these steps to perform the system board swap:

1. Client Security Solution Administrator logs on to operating system.
2. Logon-executed code (cssplanarswap.exe) recognizes the security chip is disabled and requires reboot to enable. (This step can be avoided by enabling the security chip through the BIOS.)
3. System is rebooted and security chip is enabled.
4. The Client Security Solution Administrator logs on; the new Take Ownership process is completed.
5. System Base Key is decrypted using system base AES Protection Key that is derived by the Client Security Solution Administrator's authentication. System Base Key is imported to the new SRK and re-establishes the System Leaf Key and all credentials protected by it.
6. The system is now recovered.

Note: System board swap is not needed when using Emulation Mode.

The following diagram provides the structure for the motherboard swap - take ownership:

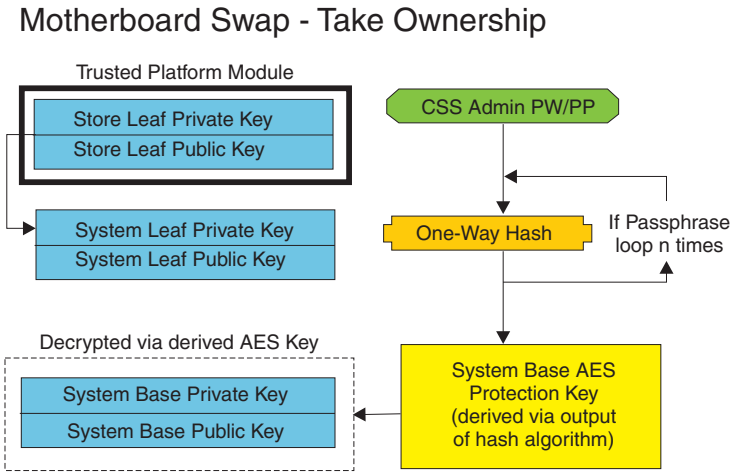

Figure 3. Motherboard Swap - Take Ownership

As each user logs onto the system, the User Base Key is automatically decrypted through the User Base AES Protection Key derived from user authentication and imported to the new SRK created through the Client Security Solution Administrator. The following diagram provides the structure for the motherboard swap - enroll user:

To login a second user after the chip has been cleared or after you replace the motherboard, you must login as the master administrator. The master administrator will be prompted to restore the keys. Once the key restoration has been completed, use Policy Manager to disable the Client Security Windows logon. The remaining users will be able to restore their respective keys. Once all secondary users have restored their keys, the master administrator can enable the Client Security Solution Windows logon feature.

The following diagram provides the structure for the motherboard swap - enroll user:

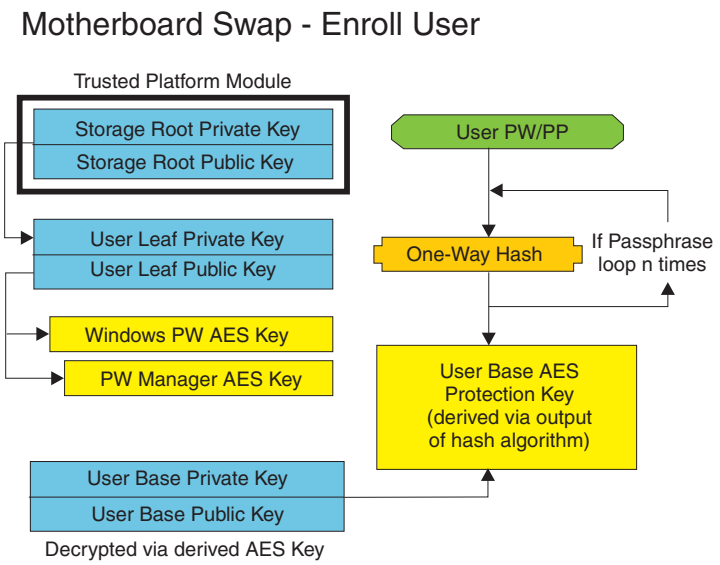

Figure 4. Motherboard Swap - Enroll User

EFS protection utility

Client Security Solution provides a command line utility that enables TPM-based protection of encryption certificates used by the Encrypting File System (EFS) to encrypt files and folders. This utility supports transfer of third party certificates (certificates generated by a Certificate Authority) and also supports generation of self-signed certificates.

Protection of the EFS certificate by Client Security Solution means that the private key associated with the EFS certificate is protected by the TPM. Access to the certificate is granted after the user has authenticated to Client Security Solution.

If no TPM is available, the EFS certificate is protected using the TPM emulator provided by Client Security Solution. You must be enrolled with Client Security Solution to be able to have the EFS certificates protected by Client Security Solution.

CAUTION:
If you use Client Security Solution and the Encrypting File System (EFS) to encrypt files and folders, then anytime Client Security Solution or the Trusted Platform Module is not available, you cannot access the encrypted files.

If the Trusted Platform Module becomes non-responsive, Client Security Solution will restore access to encrypted data after the motherboard is replaced.

Using the EFS command line utility

The following table provides the command line parameters that are supported for EFS:

Table 9. Command line parameters supported for EFS

Parameter	Description
/generate:<size>	Generates a self-signed cert and associates the certificate with EFS. If <size> is specified, the key generated will be of the specified bit size. Valid values include 512, 1024 and 2048. If no value, or an invalid value, is specified, the default will be the generation of 1024-bit keys.
/sn:xxxxxx	Specifies the serial number of an existing certificate to transfer and associate with EFS.
/cn:yyyyyy	Specifies the name (″issued to″) of an existing certificate to transfer and associate with EFS.
/firstavail	Transfers the first available existing EFS certificate and associate with EFS.
/silent	Does not display any output. Return codes provided by the value when the program exits.
/? or /h or /help	Displays the help information.

When not run in silent mode, the utility will return one of the following errors:

```
0 - "Command completed successfully"
1 - "This utility requires Windows XP"
2 - "This utility requires Client Security Solution version 8.0"
3 - "The current user is not enrolled with Client Security Solution"
4 - "The specified certificate could not be found"
5 - "Unable to generate a self-signed certificate"
6 - "No EFS certificates were found"
7 - "Unable to associate the certificate with EFS"
```

When run in silent mode, the output of the program will be an error level corresponding to the errors numbers shown above.

Using the XML Schema

The purpose of the XML scripting is to enable IT administrators to create custom scripts that can be used to deploy and configure Client Security Solution. The scripts can be protected by the xml_crypt_tool executable with a password such as AES encryption. Once created, the virtual machine (vmserver.exe) accepts the scripts as input. The virtual machine calls the same functions as the Client Security Solution Setup Wizard to configure the software.

All of the scripts consist of one tag to specify the XML encoding type, the XML schema, and at least one function to perform. The schema is used to validate the XML file and check to see that the required parameters are present. The use of schema is not currently enforced. Each function is enclosed in a function tag. Each function contains an order, this specifies in what order the command will be executed by the virtual machine (vmserver.exe). Each function has a version number as well; currently all of the functions are at version 1.0. Each of the example scripts below only contain one function. However, a practice a script

would most likely contain multiple functions. The Client Security Solution Setup Wizard can be used to create such a script. For additional information about creating scripts with the setup wizard, see "Client Security Solution setup wizard" on page 42.

Note: If the parameter <DOMAIN_NAME_PARAMETER> is left out in any of the functions that require a domain name, then the default computer name of the system will be used.

Examples

The following commands are examples of the XML Schema:

ENABLE_TPM_FUNCTION

This command enables the Trusted Platform Module and uses the argument SYSTEM_PAP. If the system already has a BIOS administrator or supervisor password set, then this argument must be provided. Otherwise, this command is optional.

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment >
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>ENABLE_TPM_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
          <SYSTEM_PAP>PASSWORD</SYSTEM_PAP>
         </FUNCTION>
</CSSFile>
```

Note: This command is not supported in the emulation mode.

DISABLE_TPM_FUNCTION

This command uses the argument SYSTEM_PAP. If the system already has a BIOS administrator or supervisor password set, then this argument must be provided. Otherwise, this command is optional.

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>DISABLE_TPM_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
          <SYSTEM_PAP>password</SYSTEM_PAP>
         </FUNCTION>
</CSSFile>
```

Note: This command is not supported in the emulation mode.

ENABLE_PWMGR_FUNCTION

This command enables the password manager for all Client Security Solution users.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
  <CSSFile xmlns="www.lenovo.com/security/CSS">
          <FUNCTION>
          <ORDER>0001</ORDER>
```

```
         <COMMAND>ENABLE_PWMGR_FUNCTION</COMMAND>
         <VERSION>1.0</VERSION>
        </FUNCTION>
</CSSFile>
```

ENABLE_CSS_GINA_FUNCTION

For Windows XP, Windows Vista, and Windows 7, this command enables the Client Security Solution logon:

```
- <tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
         <FUNCTION>
         <ORDER>0001</ORDER>
         <COMMAND>ENABLE_CSS_GINA_FUNCTION</COMMAND>
         <VERSION>1.0</VERSION>
        </FUNCTION>
</CSSFile>
```

ENABLE_UPEK_GINA_FUNCTION

Notes:

1. This command is for ThinkVantage Fingerprint Software only.
2. This command is not supported in the emulation mode.

The following command enables the ThinkVantage fingerprint Windows logon and disables the Client Security Solution Windows logon.

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment >
        <FUNCTION>
         <ORDER>0001</ORDER>
         <COMMAND>ENABLE_UPEK_GINA_FUNCTION</COMMAND>
         <VERSION>1.0</VERSION>
        </FUNCTION>
</CSSFile>
```

ENABLE_UPEK_GINA_WITH_FUS_FUNCTION

Notes:

1. This command is for ThinkVantage Fingerprint Software only.
2. This command is not supported in the emulation mode.

The following command enables the logon with fast user switching support and disables the Client Security Solution Windows logon. The fast user switching is not enabled when the computer is in a domain environment. This is a design from Microsoft.

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
     <FUNCTION>
         <ORDER>0001</ORDER>
         <COMMAND>ENABLE_UPEK_GINA_WIH_FUS_FUNCTION</COMMAND>
         <VERSION>1.0</VERSION>
        </FUNCTION>
</CSSFile>
```

ENABLE_AUTHENTEC_GINA_FUNCTION

Notes:

1. This command is for Lenovo Fingerprint Software only.
2. This command is not supported in the emulation mode.

The following command enables the Lenovo fingerprint Windows logon and disables the Client Security Solution Windows logon.

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment >
         <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>ENABLE_AUTHENTEC_GINA_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_AUTHENTEC_GINA_WITH_FUS_FUNCTION

Notes:

1. This command is for Lenovo Fingerprint Software only.
2. This command is not supported in the emulation mode.

The following command enables the logon with fast user switching support and disables the Client Security Solution Windows logon. The fast user switching is not enabled when the computer is in a domain environment. This is a design from Microsoft.

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
     <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>ENABLE_AUTHENTEC_GINA_WIH_FUS_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_NONE_GINA_FUNCTION

If the GINA or CP (Credential Provider) of one of the related ThinkVantage Technologies components, such as ThinkVantage Fingerprint Software, Client Security Solution, or Access Connections, is enabled, this command disables both the ThinkVantage Fingerprint Software logon and the Client Security Solution logon.

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>ENABLE_CSS_NONE_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

Note: This command is not supported in the emulation mode.

SET_PP_FLAG_FUNCTION

This command writes a flag that Client Security Solution reads to determine whether to use the Client Security passphrase or a Windows password.

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
         <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>SET_PP_FLAG_FUNCTION</COMMAND>
         <PP_FLAG_SETTING_PARAMETER>USE_CSS_PP</PP_FLAG_SETTING_PARAMETER>
         <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

Note: This command is not supported in the emulation mode.

SET_ADMIN_USER_FUNCTION

This command writes a flag that Client Security Solution reads to determine who the administrator is. The parameters are:

- **USER_NAME_PARAMETER**

  The user name of the administrator.

- **DOMAIN_NAME_PARAMETER**

  The domain name of the administrator.

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>SET_ADMIN_USER_FUNCTION</COMMAND>
          <USER_NAME_PARAMETER>sabedi</USER_NAME_PARAMETER>
          <DOMAIN_NAME_PARAMETER>IBM-2AA92582C79<DOMAIN_NAME_PARAMETER>
          <VERSION>1.0</VERSION>
          <SYSTEM_PAP>PASSWORD</SYSTEM_PAP>
         </FUNCTION>
</CSSFile>
```

Note: This command is not supported in the emulation mode.

INITIALIZE_SYSTEM_FUNCTION

This command initializes the Client Security Solution system function. The system-wide keys are generated through this function call. The following list of parameters explain each function:

- **NEW_OWNER_AUTH_DATA_PARAMETER**

  This parameter is used to set the new owner password for the system. For the new owner password, the value for this parameter is controlled by the current owner password. If the current owner password is not set, then the value in this parameter is passed, and becomes the new owner password. If the current owner password is already set and the administrator uses the same current owner password, then that value in this parameter is passed. If the administrator uses a new owner password, then the new owner password will be passed in this parameter.

- **CURRENT_OWNER_AUTH_DATA_PARAMETER**

  This parameter is the current owner password of the system. If the system already has an existing owner password, then this parameter should pass the

previous password. If a new owner password is requested, then the current owner password is passed in this parameter. If no password change is configured, then the value NO_CURRENT_OWNER_AUTH is passed.

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
         <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>INITIALIZE_SYSTEM_FUNCTION</COMMAND>
          <NEW_OWNER_AUTH_DATA_PARAMETER>pass1word</NEW_OWNER_AUTH_DATA_
              PARAMETER>
          <CURRENT_OWNER_AUTH_DATA_PARAMETER>No_CURRENT_OWNER_AUTH</CURRENT
              _OWNER_AUTH_DATA_PARAMETER>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

CHANGE_TPM_OWNER_AUTH_FUNCTION

This command changes the Client Security Solution Administrator authorization, and updates the system keys accordingly. The system-wide keys are regenerated through this function call. The parameters are:

- NEW_OWNER_AUTH_DATA_PARAMETER

  The new owner password of the Trusted Platform Module.

- CURRENT_OWNER_AUTH_DATA_PARAMETER

  The current owner password of the Trusted Platform Module.

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>CHANGE_TPM_OWNER_AUTH_FUNCTION</COMMAND>
          <NEW_OWNER_AUTH_DATA_PARAMETER>newPassWord</NEW_OWNER_AUTH_DATA_
              PARAMETER>
          <CURRENT_OWNER_AUTH_DATA_PARAMETER>oldPassWord</CURRENT_OWNER_AUTH
              _DATA_PARAMETER>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

Note: This command is not supported in the emulation mode.

ENROLL_USER_FUNCTION

This command enrolls a particular user to use Client Security Solution. This function creates all of the user specific security keys for a given user. The parameters are:

- **USER_NAME_PARAMETER**

  The user name of the user to enroll.

- **DOMAIN_NAME_PARAMETER**

  The domain name of the user to enroll.

- **USER_AUTH_DATA_PARAMETER**

  The Trusted Platform Module passphrase Windows password to create the user's security keys with.

- **WIN_PW_PARAMETER**

The Windows password.

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>ENROLL_USER_FUNCTION</COMMAND>
          <USER_NAME_PARAMETER>sabedi</USER_NAME_PARAMETER>
          <DOMAIN_NAME_PARAMETER>IBM-2AA92582C79<DOMAIN_NAME_PARAMETER>
          <USER_AUTH_DATA_PARAMETER>myCssUserPassPhrase</USER_AUTH_DATA_PARAMETER>

          <WIN_PW_PARAMETER>myWindowsPassword</WIN_PW_PARAMETER>
          <VERSION>1.0</VERSION>
          </FUNCTION>
</CSSFile>
```

USER_PW_RECOVERY_FUNCTION

This command sets up a particular user's password recovery. The parameters are:

- **USER_NAME_PARAMETER**

  The user name of the user to enroll.

- **DOMAIN_NAME_PARAMETER**

  The domain name of the user to enroll.

- **USER_PW_REC_QUESTION_COUNT**

  The number of questions the user must answer.

- **USER_PW_REC_ANSWER_DATA_PARAMETER**

  The stored answer to a particular question. The actual name of this parameter is connected with a number corresponding to which question it answers.

- **USER_PW_REC_STORED_PASSWORD_PARAMETER**

  The stored password that is presented to the user when all of the questions are answered correctly.

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>USER_PW_RECOVERY_FUNCTION</COMMAND>
          <USER_NAME_PARAMETER>sabedi</USER_NAME_PARAMETER>
          <DOMAIN_NAME_PARAMETER>IBM-2AA92582C79<DOMAIN_NAME_PARAMETER>
          <USER_PW_REC_ANSWER_DATA_PARAMETER>Test1</USER_PW_REC_ANSWER_DATA_PARA
              METER>
          <USER_PW_REC_ANSWER_DATA_PARAMETER>Test2</USER_PW_REC_ANSWER_DATA_PARA
              METER>
          <USER_PW_REC_ANSWER_DATA_PARAMETER>Test3</USER_PW_REC_ANSWER_DATA_PARA
              METER>
          <USER_PW_REC_QUESTION_COUNT>3</USER_PW_REC_QUESTION_COUNT>
          <USER_PW_REC_QUESTION_LIST>20000,20001,20002</USER_PW_REC_QUESTION_LIST>
         </USER_PW_REC_STORED_PASSWORD_PARAMETER>Pass1word</USER_PW_REC_STORED_PASS
              WORD_PARAMETER>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

GENERATE_MULTI_FACTOR_DEVICE_FUNCTION

This command generates the Client Security Solution multi-factor devices used for authentication. The parameters are:

- USER_NAME_PARAMETER - The user name of the administrator.
- DOMAIN_NAME_PARAMETER - The domain name of the administrator.
- MULTI_FACTOR_DEVICE_USER_AUTH - The Client Security passphrase or Windows password to create the user's security keys.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
<FUNCTION>
<ORDER>0001</ORDER>
<COMMAND>GENERATE_MULTI_FACTOR_DEVICE_FUNCTION</COMMAND>
<USER_NAME_PARAMETER>myUserName</USER_NAME_PARAMETER>
<DOMAIN_NAME_PARAMETER>domainName</DOMAIN_NAME_PARAMETER>
<MULTI_FACTOR_DEVICE_USER_AUTH>myCssUserPassPhrase</MULTI_FACTOR_DEVICE_USER_AUTH>
<VERSION>1.0</VERSION>
</FUNCTION>
</CSSFile>
```

SETUP_PDA_FUNCTION

This command sets up the Predesktop Area for use with Client Security Solution:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
<FUNCTION>
<ORDER>0001</ORDER>
<COMMAND>SETUP_PDA_FUNCTION</COMMAND>
<VERSION>1.0</VERSION>
</FUNCTION>
</CSSFile>
```

SET_USER_AUTH_FUNCTION

This command sets the Client Security Solution user authentication:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
<FUNCTION>
<ORDER>0001</ORDER>
<COMMAND>SET_USER_AUTH_FUNCTION</COMMAND>
<VERSION>1.0</VERSION>
</FUNCTION>
</CSSFile>
```

Using Smart Cards

Smart cards provide an additional level of security. Designed to support enterprises that use smart cards to authenticate identity, Client Security Solution 8.3 has smart card support and capabilities. You can use a smart card to log on to a system at instances when Client Security Solution requires user authentication, such as the Windows logon and Password Manager.

Installing the smart card package

The smart card middleware is available on the Lenovo Web site. Alternatively, you can get the latest release of the smart card middleware from the manufacturer of the smart card.

Requirements

The following list provides the requirements for Client Security Solution with smart card capabilities:

- A smart card reader must be installed internally or connected through a Universal Serial Bus (USB) port.
- The smart card must be enrolled for use by Client Security Solution. The smart card enrollment can be accessed through Client Security Solution.

- Only one smart card per user may be enrolled.
- There must be at least one certificate on the smart card for digital signatures. If more than one valid certificate is detected on the card, then you will be prompted to select one of the certificates.
- The smart card must be configured with a PIN.

How it works

A smart card is the size of credit card and has an embedded chip inside the card. When you insert a smart card into a card reader, the card reader reads the data stored on the embedded chip of the smart card.

Enrolling the smart card

If a smart card reader is detected, you can enroll the smart card with Client Security Solution. If a smart card reader is not detected, the option will be disabled. Smart cards can be enrolled and un-enrolled without loosing Client Security Solution credentials.

PINs

When prompted, you must enter the smart card's PIN. When you insert the card, the PIN will be validated. After you validate the PIN, the original registered certificate will be used to authenticate your identity. Maximum retries of the smart cards PIN is not enforced by Client Security Solution. If your PIN fails, you will be prompted to re-enter your PIN.

Policy Manager support

Policy Manager will allow the selection of a smart card to be used as an authentication device. If you choose to use a password or passphrase, you can override the smart card by setting the policies in Policy Manager.

If you un-enroll smart cards for all users, it is recommended that you turn off the smart card policy option in the Client Security Solution Policy Manager.

Using RSA SecurID tokens

Levering the encryption algorithm method of encrypting data, using RSA SecurID tokens in addition to Client Security Solution will provide your enterprise with multi-factor security. Using RSA SecurID tokens, users authenticate into networks and software using their user ID or PIN and a token device. The token device displays a string of numbers that change every sixty seconds. This method of authentication provides a much more reliable level of user authentication than reusable passwords.

Installing the RSA SecurID Software Token

Complete the following steps to install the RSA SecurID software:

1. Go to the following Web site:
   http://www.rsasecurity.com/node.asp?id=1156
2. Complete the registration process.
3. Download and install the RSA SecurID Software.

Requirements

1. Each Windows user must be enrolled with Client Security Solution for the RSA software to work properly after it has been associated with Client Security Solution.

2. The RSA software will get into an endless loop of trying to authenticate with a non-Client Security Solution enrolled Windows user. Enroll the user with Client Security Solution to resolve this issue.

Setting the Smart Card Access Options

To set the Smart Card Access Options, complete the following steps:

1. From the RSA SecurID main menu, click **Tools** and then click **Smart Card Access Options**.
2. From the Smart Card Communication panel, select the radio button for **Access the Smart Card through a PKCS #11 module**.
3. Click the **Browse** button and navigate to the following path:

   `C:\Program Files\LENOVO\Client Security Solution\csspkcs11.dll`
4. Click the **csspkcs11.dll** file and then click **Select**.
5. Click **OK**.

Installing the RSA SecurID Software Token manually

To leverage Client Security Solution protection with the RSA SecurID Software Token complete the following steps:

1. From the RSA SecurID Software Token main menu, click **File** and then click **Import Tokens**.
2. Navigate to the location of the SDTID file and then click **Open**.
3. From the **Select Token(s) to Install** panel, highlight the serial numbers of the desired software tokens.
4. Click **Transfer Selected Tokens Smart Card**.

   Note: If a token has a distribution password, enter the password when prompted.
5. Click **OK**.

Active Directory Support

The following path provides the directory path for the PKCS #11 module for Client Security Solution:

`C:\Program Files\Lenovo\Client Security Solution\csspkcs11.dll`

To leverage the PKCS #11 module of Client Security Solution, the following policies must be set for Active Directory:

1. PKCS #11 Signature
2. PKCS #11 Decryption

The following table provides the modifiable field and description of policies for PKCS# 11:

Table 10. ThinkVantage\Client Security Solution\Authentication Policies\PKCS# 11 Signature\Custom Mode

Fields	**CSS.ADM**
Modifiable field	Required
Field Description	Controls whether password, passphrase or smart card is required.

Table 10. ThinkVantage\Client Security Solution\Authentication Policies\PKCS# 11 Signature\Custom Mode (continued)

Fields	CSS.ADM
Possible values	• Enabled – Every time – Once per logon • Disabled • Not configured

Settings and policies for the fingerprint reader authentication

Enforced fingerprint bypass option

The fingerprint bypass option enables a user to bypass the fingerprint authentication and use a windows password to log on. The user can select or deselect this option on the Password Manager user interface when adding a new entry.

However, by default, the fingerprint bypass is enabled even if this option is not selected. This is to allow the user to log on to Windows when the fingerprint sensor is not functional. To disable the enforced fingerprint bypass option, edit the following registry key:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Lenovo\Client Security Solution\CSS Configuration]
"GinaDenyLogonDeviceNonEnrolled"=dword:00000001
```

When the registry key is set as above, the user can not bypass fingerprint authentication when the fingerprint sensor is not working.

Fingerprint swipe result

During the fingerprint authentication, the below policy controls the display of fingerprint swipe results.

```
HKLM\Lenovo\TVT Common\Client Security Solution\FPSwipeResult
```

- FPSwipeResult=0: Show all messages.
- FPSwipeResult=1: Show failure messages only(default value).
- FPSwipeResult=2: Do not show any messages.

Command-line tools

ThinkVantage Technologies features can also be implemented locally or remotely by corporate IT administrators through the command-line interface. Configuration settings can be maintained through remote text file settings.

Client Security Solution has the following command-line tools:

Security Advisor

To use the Security Advisor function, launch the Client Security Solution program, click the **Advanced** menu, and click **Security Advisor** button in the Client Security Solution workspace. The system will run the wst.exe file that is located in the C:\Program Files\Lenovo\Common Files\WST\ directory for a default installation.

The parameters are:

Table 11. Parameters

Parameters	Description
HardwarePasswords	Sets the value for the hardware password. 1 will show this section, 0 will hide. The default value is 1.
PowerOnPassword	Sets value that a PowerOn password should be enabled, or setting will be flagged.
HardDrivePassword	Sets value that a hard drive password should be enabled, or setting will be flagged.
AdministratorPassword	Sets value where an administrator password should be enabled, or setting will be flagged.
WindowsUsersPasswords	Sets the value for the Windows user password. 1 will show this section, 0 will hide. If not present then it is shown by default.
Password	Sets value that the users password should be enabled, or setting will be flagged.
PasswordAge	Sets value of what Windows password age should be on this machine, or setting will be flagged.
PasswordNeverExpires	Sets value that windows password can never expire, or setting will be flagged.
WindowsPasswordPolicy	Sets the value for the Windows password policy. 1 will show this section, 0 will hide. If not present then it is shown by default.
MinimumPasswordLength	Sets value of what password length should be on this machine, or setting will be flagged.
MaximumPasswordAge	Sets value of what password age should be on this machine, or setting will be flagged
ScreenSaver	Sets the value for the screensaver. 1 will show this section, 0 will hide. If not present then it is shown by default.
ScreenSaverPasswordSet	Sets value that screen saver should have password, or setting will be flagged.
ScreenSaverTimeout	Sets value of what the screensaver time-out should be on this machine, or setting will be flagged.
FileSharing	Sets the value for the file sharing. 1 will show this section, 0 will hide. If not present then it is shown by default.

Table 11. Parameters (continued)

Parameters	Description
AuthorizedAccessOnly	Sets value that authorized access should be set for file-sharing, or setting will be flagged.
ClientSecurity	Sets the value for Client Security. 1 will show this section, 0 will hide. If not present then it is shown by default.
EmbeddedSecurityChip	Sets value that security chip should be enabled, or setting will be flagged.
ClientSecuritySolution	Sets value of what version Client Security Solution should be on this machine, or setting will be flagged.

Client Security Solution setup wizard

The Client Security Solution setup wizard is used to generate deployment scripts through XML files. The following command displays the different functions of the wizard:

```
"C:\Program Files\Lenovo\Client Security Solution\css_wizard.exe" /?
```

The following table provides the commands for the Client Security Solution setup wizard.

Table 12. Commands for the Client Security Solution setup wizard

Parameter	Result
/h or /?	Displays the help message box
/name:*FILENAME*	Precedes the fully qualified path and filename for the generated deployment file. The file will have an .xml extension.
/encrypt	Encrypts the script file using AES encryption. The filename will be appended with .enc if it is encrypted. If the /pass command is not used, a static passphrase is used to obscure the file.
/pass:	Precedes the passphrase for protection of the encrypted deployment file.
/novalidate	Disables the password and passphrase checking capabilities of the wizard so a script file can be created on a already configured machine. For example, the administrator password on the current machine might not be the administrator password desired across the enterprise. Use the `/novalidate` command to allow you to type a different administrator password it into the css_wizard GUI during xml file creation.

Example:

```
css_wizard.exe /encrypt /pass:my secret /name:C:\DeployScript /novalidate
```

Deployment file encrypt or decrypt tool

This tool is used to encrypt or decrypt Client Security XML deployment files. The following command displays the different functions of the tool:

```
"C:\Program Files\Lenovo\Client Security Solution\xml_crypt_tool.exe" /?
```

The parameters are shown in the following table:

Table 13. Parameters for encrypting or decrypting Client Security XML deployment files

Parameters	Results
/h or /?	Displays the help message.
FILENAME	Displays path name and filename with either .xml or .enc extension.
/encrypt or /decrypt	Selects /encrypt for XML files and /decrypt for ENC files.
PASSPHRASE	Displays the optional parameter that is required if a passphrase is used to protect the file.

Examples:

```
xml_crypt_tool.exe "C:\DeployScript.xml" /encrypt "my secret"
```

and

```
xml_crypt_tool.exe "C:\DeployScript.xml.enc" /decrypt "my secret"
```

Deployment file processing tool

The tool vmserver.exe processes the Client Security Solution XML deployment scripts. The following command displays the different functions of the wizard:

```
"C:\Program Files\Lenovo\Client Security Solution\vmserver.exe" /?
```

The following table provides the parameters for file processing.

Table 14. Parameters for file processing

Parameter	Result
FILENAME	The FILENAME parameter must have either an XML or ENC file extension
PASSPHRASE	The PASSPHRASE parameter is used to decrypt a file with the ENC extension

Example:

```
Vmserver.exe  C:\DeployScript.xml.enc "my secret"
```

TPMENABLE.EXE

The tpmenable.exe file is used to turn the security chip on or off.

Table 15. Parameters for the tpmenable.exe file

Parameter	Description
/enable or /disable	Turns the security chip on or off.
/quiet	Hides prompts for BIOS password or errors.

Table 15. Parameters for the tpmenable.exe file (continued)

Parameter	Description
sp:*password*	For Windows 2000 and XP only, BIOS administrator/supervisor password, do not use quotes around the password.

Example:

```
tpmenable.exe /enable /quiet /sp:My BiosPW
```

Certificate Transfer tool

The following table provides the command line switches of the Certificate Transfer tool for Client Security Solution:

Table 16. css_cert_transfer_tool.exe <cert_store_type> <filter_type>:<name | size> | all_access | usage

Parameter		Description
<cert_store_type>		This is the first required parameter. It must be used as the first switch and include one of the following examples:
Examples:	cert_store_user	Transfers user certificates only. User certificates are assigned to the current user.
	cert_store_machine	Transfers machine certificates only. Machine certificates may be used by all authorized users on a machine.
	cert_store_all	Transfers both user and machine certificate types.
<filter_type>:<name | size>		This is the second required parameter. It must be used after the required <cert_store_type> parameter. Each filter type (except as noted below) must have a colon ':' after it and must have the name of the certificate subject, authority, or key size that is being searched for immediately after the colon. This utility is case-sensitive and if the name you are searching for is a compound name, such as "CA Authority", you must use double-quote marks "" around your search criteria (see examples).

Table 16. css_cert_transfer_tool.exe <cert_store_type> <filter_type>:<name | size> | all_access | usage (continued)

Parameter		Description
Examples:	subject_simple_name:<name>	Transfers all of the certificates that match the name the certificate is issued to, where the name of the subject is <name>.
	subject_friendly_name:<name>	Transfers all of the certificates that match the friendly name that the certificate is issued to, where the friendly name is <name>.
	issuer_simple_name:<name>	Transfers all of the certificates that match the name of the certificate authority that issued them, where the name of the authority is <name>.
	ssuer_friendly_name:<name>	Transfers all of the certificates that match the friendly name of the certificate authority that issued them, where the friendly name of the authority is <name>.
	key_size:<size>	Transfers all certificates that are encrypted with the key size <size> in bits. Note that this is an exact match criteria; the program will not search for certificates encrypted with a key size of at least or at most that size.
The following two switches are standalone; they do not have a second argument to them:		
all_access	Transfers all certificates, do not filter.	
usage	Does not provide information on the command line, but the function used to determine correct usage will return true or false if the commands passed in are correct or not.	

TPM activate tool

The tpm_activate_cmd.exe file is used to activate or deactivate the TPM on the Lenovo system.

Note: You need administrator privileges to run this command.

Table 17. Parameters for activating or deactivating the TPM on the Lenovo system

Parameter	Description
/help or /?	Displays the list of parameters.
/biospw:*password*	Specifies the BIOS supervisor or administrator password if one is set.
/deactivate	Deactivates the TPM. **Note:** If you run tpm_activate_cmd.exe without parameter `/deactivate`, it will activate the TPM by default.
/verbose	Displays a text output.

Example:

```
tpm_activate_cmd.exe /?
tpm_activate_cmd.exe /verbose
tpm_activate_cmd.exe /biospw:pass
```

Active Directory Support

Active Directory is a directory service. The directory is where information about users and resources is stored. The directory service allows access so you can manipulate those resources.

Active Directory provides a mechanism that gives administrators the ability to manage computers, groups, users, domains, security policies, and any type of user-defined objects. The mechanism used by Active Directory to accomplish this is known as Group Policy. With Group Policy, administrators define settings that can be applied to computers or users in the domain.

ThinkVantage Technology products currently use a variety of methods for gathering settings used to control program settings, including reading from specific application-defined registry entries.

The following examples are settings that Active Directory can manage for Client Security Solution:

- Security policies.
- Custom security policies; such as whether to use a Windows password or Client Security Solution passphrase.

Administrative (ADM) template files

The ADM (Administrative) template file defines policy settings used by applications on the client computers. Policies are specific settings that govern the application behavior. Policy settings also define whether the user will be allowed to set specific settings through the application.

Settings defined by an administrator on the server are defined as policies. Settings defined by a user on the client computer for an application are defined as preferences. As defined by Microsoft, policy settings take precedence over preferences.

For example, a user may put a background image on his desktop. This is the user's preference setting. An administrator may define a setting on the server that dictates that a user must use a specific background image. The administrators policy setting will override the preference set by the user.

When a ThinkVantage Technology product checks for a setting, it will look for the setting in the following order:

- Computer policies
- User policies
- Default user policies
- Computer preferences
- User preferences
- Default user preferences

As described previously, computer and user policies are defined by the administrator. These settings can be initialized through the XML configuration file or through a Group Policy in the Active Directory. Computer and user preferences are set by the user on the client computer through options in the applications

interface. Default user preferences are initialized by the XML configuration script. Users do not change the values directly. Changes made to these settings by a user will be updated in the user preferences.

Customers not using Active Directory can create a default set of policy settings to be deployed to client systems. Administrators can modify XML configuration scripts and specify that they be processed during the installation of the product.

Defining manageable settings

The following example shows settings in the Group Policy editor using the following hierarchy:

```
Computer Configuration>Administrative Templates>ThinkVantage Technologies>
Client Security Solution>Authentication Policies>Max Retries>
Password number of retries
```

The ADM files indicate where in the registry the settings will be reflected. These settings will be in the following registry locations:

```
Computer policies:
HKLM\Software\Policies\Lenovo\Client Security Solution\

User policies:
HKCU\Software\Policies\Lenovo\Client Security Solution\

Default user policies:
HKLM\Software\Policies\Lenovo\Client Security Solution\User defaults

Computer preferences:
HKLM\Software\Lenovo\Client Security Solution\

User preferences:
HKCU\Software\Lenovo\Client Security Solution\

Default user preferences:
HKLM\Software\Lenovo\Client Security Solution\User defaults
```

Group Policy settings

The tables in this section provide policy settings for the Computer Configuration and the User Configuration for Client Security Solution.

Max retries

The following table provides policy settings for Authentication policies, Max retries.

Table 18. Computer Configuration > ThinkVantage > Client Security Solution > Authentication policies > Max retries

Policy	Enabled Setting	Description
Password number of retries	Maximum number of retries is 20.	Controls the maximum number of times that a user can use Windows password for authentication before falling back to the override policy.
Passphrase number of retries	Maximum number of retries is 20.	Controls the maximum number of times a user can use Client Security passphrase for authentication before falling back to the override policy.

Secure Mode

The following table provides policy settings for Authentication policies, Secure mode.

Table 19. Computer Configuration > Administrative templates > ThinkVantage > Client Security Solution > Authentication policies > Secure mode

Policy	Enabled settings	Description
Password	Set the frequency to either **Every time**, or **Once per logon**.	Controls whether password is required.
Passphrase	Set the frequency to either **Every time**, or **Once per logon**.	Controls whether passphrase is required.
Fingerprint	Set the frequency to either **Every time**, or **Once per logon**.	Controls whether fingerprint is required.
Override	Set to override the password, passphrase, or fingerprint.	Defines "fallback" authentication requirements if normal authentication fails.

Default mode

The following table provides policy settings for Authentication policies, Default mode.

Table 20. Computer Configuration > Administrative templates > ThinkVantage > Client Security Solution > Authentication policies > Default mode

Policy	Enabled settings	Description
Password	You can set the frequency to either **Every time**, or **Once per logon**.	Controls whether password is required.
Passphrase	You can set the frequency to either **Every time**, or **Once per logon**.	Controls whether passphrase is required.
Fingerprint	You can set the frequency to either **Every time**, or **Once per logon**.	Controls whether fingerprint is required.
Smart card	You can set the frequency to either **Every time**, or **Once per logon**.	Controls whether smart card is required.
Override	Set to override the password, passphrase, or fingerprint.	Defines "fallback" authentication requirements if normal authentication fails.

Authentication Policies

The following list of policies contain enabled settings that define the authentication level of each policy:

- Windows logon authentication level
- System unlock authentication level
- Password manager authentication level
- CSP signature authentication level
- CSP decryption authentication level
- PKCS#11 signature authentication level
- PKCS#11 decryption authentication level
- PKCS#11 logon authentication level

The following table provides values and settings for the preceding authentication levels:

Table 21. Computer Configuration > Administrative templates > ThinkVantage > Client Security Solution > Authentication policies

Policy	Enabled settings	Description
Password	Set the frequency to either **Every time**, or **Once per logon**.	Controls whether password is required.
Passphrase	Set the frequency to either **Every time**, or **Once per logon**.	Controls whether passphrase is required.
Fingerprint	Set the frequency to either **Every time**, or **Once per logon**.	Controls whether fingerprint is required.
Smart card	Set the frequency to either **Every time**, or **Once per logon**.	Controls whether smart card is required.
Override	Set to override the password, passphrase, or fingerprint.	Defines "fallback" authentication requirements if normal authentication fails.

Password manager

The following table provides policy settings for Password manager.

Table 22. Computer Configuration > ThinkVantage > Client Security Solution > Password manager

Policy setting	Description
Disable Password manager	Controls whether Password manager will start when the system starts.
Disable Internet Explorer support	Controls whether Password manager will be able to store passwords from Internet Explorer.
Disable Mozilla support	Controls whether Password manager will be able to store passwords from Mozilla-based browsers, including Firefox and Netscape.
Disable support for Windows applications	Controls whether Password manager will be able to store passwords from Windows applications.
Disable Auto-fill	Controls whether Password manager will auto-fill data into Web sites and Windows applications.
Disable Hotkey support	Controls whether Password manager will support use of hotkeys for filling in data into Web sites and Windows applications.
Use Domain filtering	Controls whether Password manager will filter Web sites based on domains.
Prohibited Domains	Controls which domains Password manager is prohibited from storing passwords for.
Prohibited URLs	Controls which URLs Password manager is prohibited from storing passwords for.
Prohibited Modules	Controls which Windows applications Password manager is prohibited from storing passwords for.
Auto-fill Hotkey	Controls the Auto-fill Hotkey Ctrl+F2.
Type and Transfer Hotkey	Controls the Type and Transfer Hotkey Ctrl+Shift+H.
Manage Hotkey	Controls the Hotkey Ctrl+Shift+B.

User Interface

The following table provides policy settings for the User interface.

Table 23. Computer Configuration > ThinkVantage > Client Security Solution > User interface

Policy setting	Description
Fingerprint software option	Show, gray, or hide the Fingerprint software option in the Client Security Solution application. Default: Show.
File encryption option	Show, gray, or hide the File encryption option in the Client Security Solution application. Default: Show.
Security settings audit option	Show, gray, or hide the Security settings audit option in the Client Security Solution application. Default: Show.
Digital certificate transfer option	Show, gray, or hide the Digital certificate transfer option in the Client Security Solution application. Default: Show.
Change security chip status option	Show, gray, or hide the security chip status option in the Client Security Solution application. Default: Show.
Clear security chip lockout option	Show, gray, or hide the Clear security chip lockout option in the Client Security Solution application. Default: Show.
Policy manager option	Show, gray, or hide the Policy manager option in the Client Security Solution application. Default: Show.
Reset/Configure settings option	Show, gray, or hide the Configuration wizard option in the Client Security Solution application. Default: Show
Password manager option	Show, gray, or hide the Password manager option in the Client Security Solution application. Default: Show.
Hardware Password Reset option	Show, gray, or hide the Hardware Password Reset option in the Client Security Solution application. Default: Show.
Windows password recovery option	Show, gray, or hide the Windows password recovery option in the Client Security Solution application. Default: Show.
Change authentication mode option	Show, gray, or hide the Change authentication mode option in the Client Security Solution application. Default: Show
Set up smart card option	Show, gray, or hide the Setup smart card option in the Client Security Solution application. Default: Show
Enable/disable Windows password recovery option	Show, gray, or hide the option to enable or disable Windows password recovery in the Client Security Solution application. Default: Show
Enable/disable Password Manager option	Show, gray, or hide the option to enable or disable Password Manager in the Client Security Solution application. Default: Show

Workstation security tool

The following table provides policy settings for the Workstation security tool.

Table 24. Computer Configuration > ThinkVantage > Client Security Solution > Workstation security tool

Policy	Setting	Description
Hardware Passwords	Hardware Passwords	Enable or disable hardware passwords information from being displayed.
Hardware Passwords	Power-On Password	Select the recommended value as enable or disable or select to ignore this setting.

Table 24. Computer Configuration > ThinkVantage > Client Security Solution > Workstation security tool (continued)

Policy	Setting	Description
Hardware Passwords	Hard Drive Password	Select the recommended value as enable or disable or select to ignore this setting.
Hardware Passwords	Administrator Password	Select the recommended value as enable or disable or select to ignore this setting.
Windows Users Passwords	Windows Users Passwords	Enable or disable Windows users password information from being displayed.
Windows Users Passwords	Password	Select the recommended value as enable or disable or select to ignore this setting.
Windows Users Passwords	Password Age	Max number of days the password is allowed to be.
Windows Users Passwords	Password never expires	Recommended value can be set to `True`, `False`, or `Ignore`.
Windows Password Policy	Windows Password Policy	Enable or disable Windows password policy information from being displayed.
Windows Password Policy	Minimum number of characters in the password	Minimum number of characters the password can be, or 'Ignore' this value.
Windows Password Policy	Maximum password age	Maximum password age setting - number of days or 'Ignore' this value in your results.
Screen Saver	Screen Saver	Enable or disable Windows password policy information from being displayed.
Screen Saver	Screen Saver password set	Minimum number of characters the password can be, or 'Ignore' this value.
Screen Saver	Screen Saver timeout	Maximum password age setting - number of days or 'Ignore' this value in your results.
File Sharing	File Sharing	Enable or disable file sharing information from being displayed.
File Sharing	Authorized access	Recommended value can be set to `True`, `False`, or `Ignore`.
Client Security	Client Security	Enable or disable Client Security information from being displayed.
Client Security	Embedded Security Chip	Select the recommended value as enable or disable or set to ignore this setting.
Client Security	Client Security Solution Version	Set the minimum recommended version of Client Security Solution or set it as `Ignore`.

Chapter 4. Working with ThinkVantage Fingerprint Software

The fingerprint console must be run from the ThinkVantage Fingerprint Software installation folder. The basic syntax is FPRCONSOLE [USER | SETTINGS]. The USER or SETTINGS command specifies which mode of operation will be used. The full command is then “fprconsole user add TestUser”. When the command is not known or not all parameters are specified, the short command list is shown together with the parameters.

The ThinkVantage Fingerprint Software, installation instructions, management console and all related documentation are available at the following Web: http://www-307.ibm.com/pc/support/site.wss/TVAN-EAPFPR.html

Management console tool

This section provides information about user-specific commands and global setting commands.

User-specific commands

To enroll or edit users, the USER section is used. When the current user does not have administrator rights, the console behavior depends on the security mode of the Fingerprint Software. Secure mode: no commands are allowed. Convenient mode: ADD, EDIT and DELETE commands are possible for standard user. However, the user can modify only his own passport (enrolled with his user name). The following is the syntax:

`FPRCONSOLE USER command`

where *command* is one of the following commands: ADD, EDIT, DELETE, LIST, IMPORT, EXPORT.

Table 25. User-specific commands

Command	Syntax	Description

Enroll new user
Example:
`fprconsole user add domain0\testuser`
 	
`fprconsole user add testuser`
	`ADD [username [| domain\ username]]`	If the user name is not specified, then the current user name is used.

Edit enrolled user
Example:
`fprconsole user edit domain0\testuser`
 	
`fprconsole user edit testuser`
	`EDIT [username [| domain\ username]]`	If the user name is not specified, then the current user name is used.
		Note: The enrolled user must verify his fingerprint first.

Table 25. User-specific commands (continued)

Command	Syntax	Description

Delete a user
Example:
`fprconsole user delete domain0\testuser`
 	
`fprconsole user delete testuser`
 	
`fprconsole user delete /ALL`
	`DELETE [`*`username`* `[| `*`domain`*`\ `*`username`* `| /ALL]]`	The /ALL flag will delete all users enrolled on this computer. If the user name is not specified then the current user name is used.

Enumerate enrolled users	`List`	Lists the enrolled users.
Export enrolled user to a file	`Syntax: EXPORT username [| domain\username] file`	This command will export an enrolled user to a file on the hard disk drive. The user then can be imported using the IMPORT command on other computer or on the same computer, if the user is deleted.
Import enrolled user	`Syntax: IMPORT `*`file`*	The command will import the user from the specified file. **Note:** If the user in the file is already enrolled on the same computer using the same fingerprints then it is not guaranteed which user will have a precedence in the identification operation.

Global settings commands

The global settings of the Fingerprint Software can be changed by the SETTINGS section. All the commands in this section need administrators rights. The syntax is:

`FPRCONSOLE SETTINGS `*`command`*

where *command* is one of the following commands: SECUREMODE, LOGON, CAD, TBX, SSO.

Table 26. Global settings commands

Command	Syntax	Description
Security mode **Example:** `To set to convenient mode: fprconsole settings securemode 0`	`SECUREMODE 0|1`	This setting switches between Convenient and Secure mode of the Fingerprint Software.
Logon type	`LOGON 0|1 [/FUS]`	This setting enables (1) or disables (0) the logon application. If the /FUS parameter is used the logon is enabled in Fast User Switching mode if the computer configuration allows this.

Table 26. Global settings commands (continued)

Command	Syntax	Description
CTRL+ALT+DEL message	`CAD 0|1`	This setting enables(1) or disables(0) the "Press Ctrl+Alt+Delete" text in logon.
Power-on security	`TBX 0|1`	This setting globally turns off (0) power-on security support in the fingerprint software. When the power-on security support is turned off no power-on security wizards or pages are shown and it does not matter what are the BIOS settings.
Power-on security single sign-on	`SSO 0|1`	This setting enables(1) or disables(0) the usage of fingerprint used in BIOS in logon to automatically logon user when the user was verified in BIOS.

Secure mode and convenient mode

Fingerprint Software can be run in two security modes, a secure mode and a convenient mode. The secure mode is intended for situations when you want to achieve higher security. Special functions are reserved for administrators only. Only administrators can log on using password without additional authentication.

The convenient mode is intended for home computers where a high security level is not so important. All the users can perform all operations, including editing passports of other users and possibility to log on to the system using password (without fingerprint authentication).

An *administrator* is any member of local administrators group. After you set the secure mode, only the administrator can toggle it back to the convenient mode.

Secure mode - administrator

To enhance security, if the wrong user name or password is typed at logon, the secure mode displays the following message: ″Only administrators can log on this computer with user name and password.″

Table 27. Options for administrators in the secure mode

Fingerprints	Description
Create a new passport	Administrators can create their own passport and they can also create the passport of a limited user.
Edit Passports	Administrators can edit *only* their own passport.
Delete Passport	Administrators can delete all limited user and other administrator passports. If other users are using power-on security, the administrator will have the option to remove user templates from power-on security at this time.

Table 27. Options for administrators in the secure mode (continued)

Fingerprints	Description
Power-on Security	Administrators can delete Limited user and administrator fingerprints used in power-on. **Note:** There must at least be one fingerprint present when power-on mode is enabled.
Settings	
Logon settings	Administrators can make changes to all logon settings.
Protected screen saver	Administrators can access.
Passport type	Administrators can access - only relevant with server.
Security mode	Administrators can toggle between secure and convenient modes.
Pro Servers	Administrators can access - only relevant with server.

Secure mode - limited user

During a Windows logon, a limited user must use a fingerprint to logon. If the limited user fingerprint reader is not working, an administrator will need to change the fingerprint software setting to convenient mode to enable user name and password access.

Table 28. Options for limited users in the secure mode

Setting	Description
Create a new passport	Limited user cannot access.
Edit Passports	Limited user can edit only their own passport.
Delete Passport	Limited user can delete only their own passport.
Power-on Security	Limited user cannot access.
Logon settings	Limited user cannot modify logon settings.
Protected screen saver	Limited user can access.
Passport type	Limited user cannot access.
Security mode	Limited user cannot modify security modes.
Pro Servers	Limited user can access - only relevant with server.

Convenient mode - administrator

During a Windows logon, administrators can logon using either their user name and password or their fingerprint.

Table 29. Options for administrators in the convenient mode

Settings	Description
Create a new passport	Administrators can create *only* their own passport.
Edit Passports	Administrators can edit *only* their own passport.

Table 29. Options for administrators in the convenient mode (continued)

Settings	Description
Delete Passport	Administrators can delete *only* their own passport.
Power-on Security	Administrators can delete Limited user and administrator fingerprints used in power-on. **Note:** There must be at least one fingerprint present when power-on mode is enabled.
Logon settings	Administrators can make changes to all logon settings.
Protected screen saver	Administrators can access.
Passport type	Administrators can access - only relevant with server.
Security mode	Administrators can toggle between secure and convenient modes.
Pro Servers	Administrators can access - only relevant with server.

Convenient mode - limited user

During a Windows logon, limited users can logon using either their user name and password or their fingerprint.

Table 30. Options for limited users in the convenient mode

Settings	Description
Create a new passport	Limited users can create only their own password.
Edit Passports	Limited users can edit only their own passport.
Delete Passport	Limited users can delete only their own passport.
Power-on Security	Limited users can delete only their own fingerprints.
Logon settings	Limited users cannot modify logon settings.
Protected screen saver	Limited users can access.
Passport type	Limited users cannot access - only relevant with server.
Security mode	Limited users cannot modify security modes.
Pro Servers	Limited users can access - only relevant with server.

Configurable settings

Some fingerprint software options can be configured through registry settings.

- **Preboot/power-on software interface**: The mechanism for enabling fingerprint preboot or power-on support and storing fingerprints on the companion chip is not normally displayed in the fingerprint software unless there are BIOS or hard drive passwords set on the system.

In order to override this behavior and force these options to be shown without the existence of BIOS or hard drive passwords, add one of the following, that apply to your computer machine type, to the registry:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Protector Suite QL\1.0]


REG_DWORD "BiosFeatures" = 2
```

or,

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Protector Suite QL\1.0]


REG_DWORD "BiosFeatures" = 4
```

This setting is useful when SafeGuard Easy is installed on a system without BIOS passwords and is utilizing fingerprint authentication to decrypt the hard drive.

- **Sounds**: The fingerprint software can be configured to play a sound contained in a .wav file under various circumstance during the fingerprint authentication process. The registry settings for these sounds are as follows:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Protector Suite QL\1.0\settings]
'Success'
REG_SZ "sndSuccess" = [path to sound file]
The file designated will play whenever a successful swipe is registered.

'Failure'
REG_SZ "sndFailure" = [path to sound file]
The file designated will play whenever an unsuccessful swipe is attempted.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\fingerprint

'Scan'
REG_SZ "sndScan" = [path to sound file]
The file designated will play whenever the fingerprint verification
 dialog is displayed for Client Security Solution-related operations.
If the value is not present or is empty then no sound is played.

'Quality'
REG_SZ "sndQuality" = [path to sound file]
The file designated will play whenever an unreadable swipe has occurred.
If the value is not present or is empty then no sound is played.
```

- **Password validation during system unlock**: By default, the fingerprint software validates stored password during system unlock. The validation requires contacting the domain controller and might cause delay. To avoid the delay, disable the password validation during system unlock and by editing the registry as follows:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Protector Suite QL\1.0\settings]
REG_DWORD "DoNotTestUnlock"=1
```

The fingerprint software will continue to validate the password at system logon.

Note: When the above registry key is set to 1, if the domain administrator changes the user's when the user's system is locked, the fingerprint software will have the old password stored until the user logs off and logs on again.

Fingerprint Software and Novell Netware Client

To prevent conflicts, Fingerprint Software and Novell Netware Client user names and passwords must match. If you have Fingerprint Software installed on your computer and then install the Novell Netware Client, some items in the registry might be overwritten. If you encounter problems with Fingerprint Software logon, go to the logon settings screen and re-enable the Logon Protector.

If you have the Novell Netware Client installed on your computer but have not logged on to the client before installing Fingerprint Software, the Novell Logon screen will display. Provide the information requested by the screen.

Note: The information in this section is for ThinkVantage Fingerprint Software only.

To change Logon Protector Settings:

- Start the Control Center.
- Click **Settings.**
- Click **Logon settings.**
- Enable or disable Logon Protector.

  If you want to use fingerprint logon, check the Replace Windows logon with fingerprint-protected logon check box.

  Note: Enabling and disabling Logon Protector requires a reboot.
- Enable or disable fast user switching, when supported by your system.
- (Optional feature) Enable or disable automatic logon for a user authenticated by power-on boot security.
- Set Novell logon settings. The following settings are available when logging on to a Novell network:
  - **Activated**

    Fingerprint Software automatically provides known credentials. If the Novell logon fails, the Novell Client logon screen is displayed along with a prompt to enter the correct data.
  - **Ask during logon**

    Fingerprint Software displays the Novell Client logon screen and a prompt to enter the logon data.
  - **Disabled**

    Fingerprint Software does not attempt a Novell logon.

Authenticating

Complete the following steps to pass Novell to Fingerprint Software:

1. Install Fingerprint Software.
2. Install Novell Netware Client.
3. When prompted, click **Yes** to logon.
4. Reboot.
5. When prompted, click Yes to logon to Fingerprint Software.
6. Start the Novell Netware Client.
7. Authenticate to the server.
8. Log onto Windows.
9. Reboot.

Note: Your authentication ID and password for Windows and Novell must be identical.

ThinkVantage Fingerprint Software service

The upeksvr.exe service is added to the system after the ThinkVantage fingerprint software is installed. It starts running while startup, and then runs all the time the user is logging on. The upeksvr.exe service is the core of the ThinkVantage fingerprint software and runs all the operations with the device and user's data. It also shows all the biometric verification GUI and provides secure access to the user's data.

Chapter 5. Working with Lenovo Fingerprint Software

The fingerprint console must be run from the Lenovo Fingerprint Software installation folder. The basic syntax is FPRCONSOLE [USER | SETTINGS]. The USER or SETTINGS command specifies what set of operation will be used. The full command is “fprconsole user add TestUser”. When the command is not known or not all parameters are specified, the short command list is shown together with the parameters.

The Lenovo Fingerprint Software, installation instructions, management console and all related documentation are available on the Lenovo Web site at: http://www.lenovo.com/support

Management console tool

For information about the management console tool of the Lenovo Fingerprint Software, see “Management console tool” on page 53 for reference.

Lenovo Fingerprint Software service

Note: The Lenovo Fingerprint Software requires the terminal service on the system. If you turn off the terminal service, some unexpected results might occur in the Lenovo Fingerprint Software.

The following services are added to the system after the Lenovo Fingerprint Software is installed:

- ATService.exe (on by default)

  You must turn on the ATService.exe service to use the fingerprint system. This service manages requests from applications using the fingerprint sensor.
- Data Transfer Service (on by default)

  When Data Transfer Service or the ATService.exe service is abnormally terminated, Lenovo Fingeprint Software will not work as expected.
- ADMonitor.exe (off by default)

  You must turn on the ADMonitor.exe service to support Active Directory Administration. This service monitors the registry for changes propagated down from Active Directory and reflects the changes locally.

Active Directory support for Lenovo Fingerprint Software

The following table shows the policy settings for the Lenovo Fingerprint Software.

Table 31. Policy settings

Setting	Description
Enable/disable fingerprint logon	Specifies the use of fingerprints instead of Windows passwords to log in to the computer. If you enable this setting, there are two more options you can enable or disable: • **Disable CTRL+ALT+DEL dialog for logon interface** If you select this option, the message directing the user to press CTRL+ALT+DEL to log in is turned off. (Only available in Windows XP) • **Require non-administrator user logon with fingerprint authentication** If you select this option, users who are not administrators will only be able to log in using fingerprints.
Allow user to retrieve password through fingerprint authentication	If you enable this setting, users are able to view the Windows password for their account in the Lenovo Fingerprint Software after fingerprint authentication.
Always show power-on security options	If you enable this setting, users will be able to select using the Fingerprint Reader instead of power-on and hard disk drive passwords when the computer is turned on. In the Lenovo Fingerprint Software enrollment window, power-on fingerprint authentication can be enabled or disabled for each enrolled finger.
Use fingerprint authentication instead of power-on and HD passwords	If you enable this setting, the fingerprint authentication will be used instead of passwords for power-on and the hard drive.
Set number of failed attemps before lock out	Sets the number of failed attempts to log on allowed before the user is locked out, and also the duration (in seconds) the user is locked out.
Set inactive timeout	Sets the duration of system inactivity (in seconds) allowed before the user logs off.
Allow users to enroll fingerprints	If you enable this setting, the non-administrator users are able to enroll fingerprints using the Lenovo Fingerprint Software.
Allow users to delete fingerprints	If you enable this setting, the non-administrator users are able to delete previously enrolled fingerprints using the Lenovo Fingerprint Software.
Allow users to import/export fingerprints	If you enable this setting, the non-administrator users are able to import and export previously enrolled fingerprints using the Lenovo Fingerprint Software.

Table 31. Policy settings (continued)

Setting	Description
Show/Hide elements in setting tab of fingerprint software	If you enable this setting, the IT administrators are able to control fingerprint software setting GUI.

Chapter 6. Best Practices

This chapter presents scenarios to illustrate the best practices of Client Security Solution and Fingerprint Software. This scenario starts with the configuration of the hard disk drive, continues through several updates, and follows the life cycle of a deployment. Installation on both Lenovo and non-Lenovo computers is described.

Deployment examples for installing Client Security Solution

The following section provides examples of installing Client Security Solution on both desktop and notebook computers.

Scenario 1

This is an example of an installation on a desktop computer using these hypothetical customer requirements:

- **Administration**

  Use the local administrator account for administration of the computer.
- **Client Security Solution**
  - Install and run in Emulation Mode.

    Not all of the Lenovo systems have a Trusted Platform Module (security chip).
  - Enable Client Security passphrase.

    Protect Client Security Solution applications through a passphrase.
  - Enable Client Security Windows logon.

    Log in to Windows with Client Security passphrase.
  - Enable End-User Passphrase Recovery feature.

    Enable users to recover their passphrase by answering three user defined questions.
  - Encrypt Client Security Solution XML Script with password, for example, XMLscriptPW.

    Protect the Client Security Solution configuration file with password.
  - Fingerprint Software may or may not be installed.

On the preparation machine:

1. Log in to Windows with a local administrator account.
2. Install the Client Security Solution program using the following command:

   ```
   tvtcss83_xxxx.exe /s /v"/qn "EMULATIONMODE=1" "NOCSSWIZARD=1"
   ```

   (where *XXXX* is the build ID)
3. Restart the computer and log in to Windows with a local administrator account.
4. Prepare the XML script for deployment by doing the following:
   a. Run the following command:

      ```
      "C:\Program Files\Lenovo\Client Security Solution\css_wizarde.exe"
      /name:C:\ThinkCentre
      ```

   b. Configure in the wizard by doing the following:
      1) Click **Secure logon method → Next**.
      2) Type the Windows password (for example, `WPW4Admin`) for the administrator account and click **Next**.
      3) Type the Client Security passphrase (for example, `CSPP4Admin`) for the administrator account, select the **Use the Client Security passphrase to protect access to the Rescue and Recovery workspace** option, and click **Next**.
      4) Answer the three questions for the administrator account and click **Next**, for example:
         a) What was the name of your first pet?
         b) What is your favorite movie?
         c) What is your favorite athletic team?
      5) Review the summary and select **Apply** to save the XML file to the following location:
         C:\ThinkCentre.xml
      6) Click **Finish** to close the wizard.
5. Open the ThinkCentre.xml file with a text editor (an XML script editor or the Microsoft Word 2003 program that supports the XML format), remove all references to the domain setting and save the file. This will make the script use the local machine name on each system instead.
6. Use the xml_crypt_tool.exe tool in the C:\Program Files\Lenovo\Client Security Solution directory to encrypt the XML script with a password, by using the following syntax:

   ```
   xml_crypt_tool.exe C:\ThinkCentre.xml /encrypt XMLScriptPW
   ```

   The file will now be called C:\ThinkCentre.xml.enc and be protected by the password `XMLScriptPW`, and ready to be added to the deployment machine.

On the deployment machine:

1. Log in to Windows with a local administrator account.
2. Install the Rescue and Recovery and Client Security Solution programs with the following syntax:

   ```
   setup_tvtrnr40_xxxxcc.exe /s /v"/qn "EMULATIONMODE=1" "NOCSSWIZARD=1"
   ```

   (Where *xxxx* is the build ID and *cc* the country code.)

   Notes:

   a. Make sure the TVT files such as Z652ZIXxxxxyy00.tvt for Windows XP or Z633ZISxxxxyy00.tvt for Windows Vista or Windows 7 (where xxxx is the

build ID and yy is the country ID) are located in the same directory as the executable file; otherwise the installation will fail.

b. If you are performing an administrative installation, see “Scenario 1” on page 65.

3. Restart the computer and log in to Windows with a local administrator account.
4. Add the ThinkCentre.xml.enc file prepared earlier to the C:\ root directory.
5. Prepare the RunOnceEx command with the following parameters:
   a. Add a new key 0001 after the RunonceEx key. It is:

      ```
      HKEY_LOCAL_MACHINE \Software\Microsoft\Windows
      \Current Version\RunOnceEx\0001
      ```

   b. Add a string value name CSSEnroll in that key:

      ```
      "C:\Program Files\Lenovo\Client Security Solution\vmserver.exe"
      C:\ThinkCenter.xml.enc XMLscriptPW
      ```

6. Run the following commands to prepare the system for a sysprep backup:

   ```
   %rr%C:\Program Files\Lenovo\Rescue and Recovery\rrcmd.exe"
   sysprepbackup location=L name="Sysprep Backup"
   ```

   Then, you will see the following output after the system is ready to take a sysprep backup.

   ```
   ********************************************************
   ** Ready to take sysprep backup.                      **
   **                                                    **
   ** PLEASE RUN SYSPREP NOW AND SHUT DOWN.              **
   **                                                    **
   ** Next time the machine boots, it will boot          **
   ** to the Predesktop Area and take a backup.          **
   ********************************************************
   ```

7. Run your Sysprep implementation.
8. Shut down and restart the computer. It will start the backup process in Windows PE.

   Note: If the message "Restore in progress but a backup is occurring" is displayed, after the backup, shut down the computer, do not restart.
9. The Sysprep Base Backup is now complete.

Scenario 2

This is an example installation on a notebook computer using these hypothetical customer requirements:

- **Administration**
  - Install on machines where an earlier version of Client Security Solution is installed.
  - Use the domain administrator account for administration of the computer.
  - All computers have a BIOS supervisor password, BIOSpw.
- **Client Security Solution**
  - Utilize the Trusted Platform Module.

    All machines have the security chip.
  - Enable Password Manager.
  - Use the user’s Windows password as authentication to Client Security Solution.
  - Encrypt the Client Security Solution XML Script with password, for example, XMLscriptPW.

Protect the Client Security Solution configuration file with password.

- **ThinkVantage Fingerprint Software**
  - Do not use BIOS and hard disk drive passwords.
  - Log in to Windows using ThinkVantage Fingerprint Software.

    After an initial period of self-user enrollment, the user will switch to Secure Mode logon that requires a fingerprint for non-administrator users, and this would effectively enforce a dual factor authentication methodology.
  - Include the Fingerprint Software tutorial.

    The Fingerprint Software tutorial will help end-users to learn how to swipe a finger across the fingerprint reader, and will get visual feedback on their actions.

On the preparation machine:

1. From the off state, start the computer and press **F1** to go into BIOS Setup Utility and navigate to the **Security** menu and clear the security chip. Save the settings and exit BIOS.
2. Log in to Windows with a domain administrator account.
3. Install the ThinkVantage Fingerprint Software by doing the following:
   a. Run the f001zpz2001us00.exe file to extract the setup.exe file from the Web package. The setup.exe file will be automatically extracted to the following location:
   C:\SWTOOLS\APPS\TFS5.9.2-Buildxxxx\Application\0409 (where xxxx is the build ID).
   b. Double-click the extracted setup.exe file and follow the instructions on the screen to install the ThinkVantage Fingerprint Software.
4. Install the ThinkVantage Fingerprint Software tuturial by doing the following:
   a. Run the f001zpz7001us00.exe file to extract the tutess.exe file from the Web package. The tutess.exe file will be automatically extracted to the following location:
   C:\SWTOOLS\APPS\tutorial\TFS5.9.2 Buildxxxx\Tutorial\0409 (where xxxx is the build ID).
   b. Double-click the tutess.exe file to install the ThinkVantage Fingerprint Software tuturial.
5. Install the ThinkVantage Fingerprint console by doing the following:
   a. Run the f001zpz5001us00.exe to extract the fprconsole.exe file from the Web package. The fprconsole.exe file will be automatically extracted to the following location:
   C:\SWTOOLS\APPS\fpr_con\APPS\UPEK\FPR Console\TFS5.9.2-Buildxxx\Fprconsole (where xxxx is the build ID).
   b. Double-click the fprconsole.exe file to install the ThinkVantage Fingerprint console.
6. Install the Client Security Solution program with the following syntax:

   ```
   tvtcss82_xxxxcc.exe /s /v"/qn NOCSSWIZARD=1 SUPERVISORPW="BIOSpw""
   ```
7. Restart the computer and log in to Windows with a domain administrator account and prepare the XML script for deployment.
   a. Run the following commands:

   ```
   "C:\Program Files\Lenovo\Client Security Solution\css_wizard.exe"
   /name:C:\ThinkPad
   ```
   b. Configure in the wizard to match the example script by doing the following:

1) Click **Secure logon method → Next**.
2) Type the Windows password (for example, `WPW4Admin`) for the domain administrator account and click **Next**.
3) Type the Client Security passphrase for the domain administrator account.
4) Select **Ignore Password Recovery Setting** and click **Next**.
5) Review the summary and click **Apply** to save the XML file to the following location:
C:\ThinkPad.xml
6) Click **Finish** to close the wizard.

8. Use the xml_crypt_tool.exe tool in the C:\Program Files\Lenovo\Client Security Solution directory to encrypt the XML script with a password:
At a command prompt, use the following syntax:

```
xml_crypt_tool.exe C:\ThinkPad.xml /encrypt XMLScriptPW
```

The file will be called C:\ThinkPad.xml.enc and be protected by the password `XMLScriptPW`.

On the deployment machine:

1. Install the ThinkVantage Fingerprint Software on the deployment machine by doing the following:
   a. Deploy the setup.exe file that has been extracted from the preparation machine to the deployment machine, using your company's software distribution tool.
   b. Run the following command:

```
setup.exe CTLCNTR=0 /q /i
```

2. Install the ThinkVantage Fingerprint Software tuturial on the deployment machine by doing the following:
   a. Deploy the tutess.exe file that has been extracted from the preparation machine to the deployment machine, using your company's software distribution tool.
   b. Run the following command:

```
tutess.exe /q /i
```

3. Install the ThinkVantage Fingerprint console on the deployment machine by doing the following:
   a. Deploy the fprconsole.exe file that has been extracted from the preparation machine to the deployment machine, using your company's software distribution tool.
   b. Place the fprconsole.exe file to the C:\Program Files\ThinkVantage Fingerprint Software directory.
   c. Turn off BIOS power-on security support by running the following command:

```
fprconsole.exe settings TBX 0
```

4. Install the ThinkVantage Client Security Solution on the deployment machines by doing the following:
   a. Deploy the tvtvcss83_xxxx.exe (where *xxxx* is the build ID) file to the deployment machine, using your company's software distribution tool.
   b. Run the following command:

```
tvtvcss83_xxxx.exe /s /v"/qn "NOCSSWIZARD=1" "SUPERVISORPW="BIOSpw""
```

The installation of the software will automatically enable the Trusted Platform Module hardware.

5. Restart the computer and configure the system with the XML script file through the following procedure:
   a. Copy the ThinkPad.xml.enc file prepared early to the C:\ directory.
   b. Run the following command:

      ```
      "C:\Program Files\Lenovo\Client Security Solution\
      vmserver.exe" C:\ThinkPad.xml.enc XMLScriptPW
      ```
6. Restart the computer and the system is now ready for Client Security Solution user enrollment. All users can log in to the system with their user ID and Windows password. Each user who logs in to the system will automatically be prompted to enroll into Client Security Solution and then be able to enroll into the fingerprint reader.
7. After all users for the system have been enrolled in the ThinkVantage Fingerprint Software, the secure mode setting can be enabled to prompt all Windows non-administrator users to log in with their fingerprint.
   - To enable the secure mode setting, run the following command:

     ```
     "C:\Program Files\ThinkVantage Fingerprint Software\
     fprconsole.exe" settings securemode 1
     ```
   - To remove the message "Press Ctrl+Alt+Delete to log in using a password" from the logon screen, run the following command:

     ```
     "C:\Program Files\ThinkVantage Fingerprint Software\fprconsole.exe settings"
     CAD 0
     ```
8. The deployment of Client Security Solution 8.3 and ThinkVantage Fingerprint Software is now complete.

Switching Client Security Solution modes

If you switch the Client Security Solution mode from convenient to secure or if you switch from secure to convenient mode, and you are using Rescue and Recovery to backup your system, take a new base backup after you switch modes.

Corporate Active Directory rollout

For a corporate Active Directory rollout, complete the following steps:

1. Install either through Active Directory or LANDesk:
   a. Take backups and get reports through Active Directory and LANDesk of who and when they were taken.
   b. Give certain groups abilities to take backups, delete backups, schedule options, and password restrictions, then change groups and see if settings persists.
   c. Through Active Directory, enable Antidote Delivery Manager. Place packages to be run and make sure reporting is captured.

Standalone Install for CD or script files

For a standalone install for CD or script file, complete the following steps:

1. Use one batch file to silently install Client Security Solution, and Fingerprint technology.
2. Configure BIOS password recovery silently.

System Update

For System Update, complete the following steps:

1. Install Client Security Solution and Fingerprint Software technology through a customized system update server simulating how a large enterprise would have a server set up instead of going to a Lenovo server, so they can control content.
2. Over install all three different versions of older software (Rescue and Recovery 1.0/2.0/3.0, Fingerprint, Client Security Solution 5.4–6, FFE). Settings should be kept when installing the new version over the old version.

System Migration Assistant

System Migration Assistant 6.0 supports migrating from an old system to the latest Windows 7 system, and supports migrating the software settings from earlier versions of the Client Security Solution and Fingerprint Software. You can download the System Migration Assistant 6.0 from the Lenovo Web site at: http://www.lenovo.com/support

Generating a certificate using key generation in the TPM

Certificates can be generated directly by using Client Security Solution CSP, and the private keys in the certificates are generated and protected by the TPM. To request a certificate using Client Security Solution CSP, complete the following steps:

Requirements:

- The server machine should have the following installed:
  - Windows Server 2003 Enterprise or above
  - Active Directory
  - Certificate Authority service
- The client machine should meet the following requirements
  - TPM enabled
  - Client Security Solution installed

Requesting certificate from the Server

Creating template for TPM user

To create a template for TPM users, complete the following procedure:

1. Click **Start** → **Run**.
2. Type `mmc` and click **OK**. The console window displays.
3. From the **File** menu, click **Add/Remove Snap-in**, and then click **Add**. The Add Standalone snap-in window displays.
4. Double-click **Certification Authority** in the snap-in list, and click **Close**.
5. Click **OK** in the Add/Remove Snap-in window.
6. Click **Certificate Templates** from the console tree. All of the certificate templates are displayed in the left pane.
7. Click **Action** → **Duplicate Template**.
8. In the **Display Name** field, type `TPM User`.
9. Click the **Request Handling** tab, and click **CSPs**. Be sure to select **Requests can use any CSP available on the subject's computers**.

10. Click the **General** tab. Make sure that **Publish Certificate in Active Directory** is selected.
11. Click the **Security** tab, in the **Group or user names** list, click **Authenticated Users** and make sure **Enroll** is selected in the **Permissions for Authenticated Users** option.

Configuring an enterprise certification authority

To issue the TPM User certificate by configuring an enterprise certification authority, complete the following procedure:

1. Open Certification Authority.
2. In the console tree, click **Certificate Templates**.
3. From the **Action** menu, click **New → Certificate to Issue**.
4. Click **TPM** and click **OK**.

Applying certificate from the Client

To apply the certificate from the Client, complete the following procedure:

1. Connect to the Intranet, start Internet Explorer, and type in the IP address of the server where CA service is installed.
2. Input your domain user name and password in the prompt window.
3. Click **Request a certificate** under **Select a task**.
4. Click **advanced certificate request** at the bottom of the Web page.
5. On the Advanced Certificate Request page, change the following settings:
   - Select **TPM User** from the **Certificate Template** drop-down list.
   - Select **ThinkVantage Client Security Solution CSP** from the **CSP** drop-down list.
   - Make sure the **Mark keys as exportable** is not selected.
   - Click **Submit** and follow the process.
   - On the Certificate Issued page, click **Install this certificate**. The Certificate Installed page is displayed.

Using USB fingerprint keyboards with 2008 ThinkPad notebook computer models (R400/R500/T400/T500/W500/X200/X301)

Lenovo contracts with two vendors to provide fingerprint authentication in ThinkPad® notebook computer models and USB keyboards. ThinkPad notebook computer models prior to 2008 (for example, T61) use ThinkVantage fingerprint sensors. 2008 ThinkPad notebook computer models (starting with T400) use Lenovo fingerprint sensors. All Lenovo USB fingerprint keyboards use ThinkVantage fingerprint sensors. Special considerations are required if the fingerprint keyboard is used on some ThinkPad notebook models (for example, ThinkPad T400 with an external USB keyboard).

This section describes the common usage scenarios and deployment strategies for fingerprint software that is installed on the latest ThinkPad notebook computer models.

Note:

- Lenovo Fingerprint Software

  The Lenovo Fingerprint Software is the software for the AuthenTec fingerprint sensor (for example, the internal fingerprint sensor in T400).
- ThinkVantage Fingerprint Software

The ThinkVantage Fingerprint Software is the software for the UPEK fingerprint sensor (for example, the internal fingerprint sensor in T61, and the fingerprint sensor in all external USB keyboards).

Windows 7 logon

To log on to the Windows 7 operating system, you can use either the AuthenTec fingerprint sensor or the UPEK fingerprint sensor at any time.

1. Install the Lenovo Fingerprint Software version 3.2.0.275 or later.
2. Install the ThinkVantage Fingerprint Software version 5.8.2.4824 or later.
3. Restart the computer. The fingerprint enrollment wizard automatically starts.
4. Use the ThinkVantage Fingerprint Software to enroll your fingerprints with the external fingerprint sensor. If it does not automatically start, click **Start** → **Programs** (or **All Programs**) → **ThinkVantage** → **ThinkVantage Fingerprint Software** to start the enrollment.
5. Enter your Windows password when prompted and then select a finger to enroll.
6. Follow the prompts on the computer screen to enroll your finger using the external fingerprint sensor.
7. Click **Settings** at the top of the window.
8. Select the **Use fingerprint scan instead of password when logging into Windows** check box, click **OK**, and then click **Close** to close the window.
9. Restart the computer and ensure that your fingerprint can be used to log on to Windows with the external fingerprint sensor.
10. Use fingerprint enrollment to enroll your fingerprints with the internal fingerprint sensor. If it does not automatically start, click **Start** → **Programs** (or **All Programs**) → **ThinkVantage** → **Lenovo Fingerprint Software** to start the enrollment.
11. Enter your Windows password when prompted and then select a finger to enroll.
12. Follow the prompts on the computer screen to enroll your finger using the internal fingerprint sensor.
13. Click **Settings** at the top of the window.
14. Select the **Use fingerprint scan instead of password when logging into Windows** check box, click **OK**, and then click **Close** to close the window.
15. Restart the computer and ensure that your fingerprint can be used to log on to Windows with the internal fingerprint sensor.

Client Security Solution and Password Manager

Different from Windows logon, authentication requests from Client Security Solution and Password Manager only work on the preferred fingerprint sensor. For example, when a fingerprint keyboard is connected, its fingerprint sensor is the preferred device. When a fingerprint keyboard is not connected, the ThinkPad internal fingerprint sensor is the preferred device.

To change the preferred device, create a registry entry as follows:

```
[HKLM\Software\Lenovo\TVT Common\Client Security Solution]
REG_DWORD "PreferInternalFPSensor" = 1
```

Table 32. Registry keys

Name	Value	Description
PreferInternalFPSensor	0 (default)	Specifies that the external fingerprint sensor is preferred whenever the fingerprint keyboard is connected.
	1	Specifies that the internal fingerprint sensor is preferred.

Preboot Authentication – using fingerprint instead of BIOS passwords

Different from Windows logon, authentication requests for BIOS passwords only work on the fingerprint sensor when BIOS is configured to use. By default, BIOS recognizes the swipes on the fingerprint keyboard if it is connected. If the fingerprint keyboard is not connected, BIOS recognizes the swipes on the internal fingerprint device for authentication.

The BIOS setting **Reader Priority** can be changed to force the use of the internal fingerprint sensor, even when the external fingerprint keyboard is connected. The default value for **Reader Priority** is **External**. The setting can be changed to **Internal Only** to force the use of the internal fingerprint sensor.

Note: This BIOS setting applies to the fingerprint prompts on BIOS only. It does not have any effect on Windows logon or Client Security Solution fingerprint authentication requests.

Configuring Fingerprint Software to enable preboot authentication

If you have set supervisor, power-on, or hard disk drive passwords in BIOS, you can configure the Fingerprint Software for authentication instead of entering these passwords.

Lenovo Fingerprint Software – for the internal fingerprint sensor:

1. Click **Start** → **Programs** (or **All Programs**) → **ThinkVantage** → **Lenovo Fingerprint Software** to start the Lenovo Fingerprint Software.
2. Swipe your finger, or enter your Windows password when prompted.
3. Click **Settings** at the top of the window.
4. Select the **Use fingerprint scan instead of power-on and hard drive passwords** check box and the **Always show power-on security options** check box.
5. Click **OK** to close the window.
6. Choose one of the registered fingerprints to enable your fingerprint and replace the BIOS passwords.
7. Click **Close** to close the window.

ThinkVantage Fingerprint Software – for the external fingerprint sensor:

1. Start the Fingerprint Software using one of the following approaches:
   - Click **Start** → **Programs** (or **All Programs**) → **ThinkVantage** → **ThinkVantage Fingerprint Software**.

- Click the **ThinkVantage Fingerprint Software** icon in the Lenovo ThinkVantage Tools window.

2. Swipe your finger, or enter your Windows password when prompted.
3. Click **Settings** at the top of the window.
4. Select the **Use fingerprint scan instead of power-on and hard drive passwords** check box and the **Always show power-on security options** check box.
5. Click **OK** to close the window.
6. Choose one of the registered fingerprints to enable your fingerprint and replace the BIOS passwords.
7. Click **Close** to close the window.

Appendix A. Special considerations for using the Lenovo Fingerprint Keyboard with some ThinkPad notebook models

The fingerprint device used in some ThinkPad notebook models is different than the fingerprint device used in the Lenovo Fingerprint Keyboard. Special considerations might be required if the fingerprint keyboard is used on some ThinkPad notebook models.

For more information, go to the fingerprint software download page on the Lenovo Web site for a list of these ThinkPad notebook models.

Only the models listed for "Lenovo Fingerprint Software" require special consideration when used with the fingerprint keyboard. All other ThinkPad notebook models, which use "ThinkVantage Fingerprint Software," use a fingerprint device that is compatible with the device included in the fingerprint keyboard, and do not require any special consideration.

Configuration and setup

Lenovo Fingerprint Software 2.0 or later must be installed for use with the fingerprint device used in the ThinkPad notebook. Users must enroll fingerprints with the Lenovo Fingerprint Software using the integrated fingerprint device.

ThinkVantage Fingerprint Software 5.8 or later must be installed for use with the Lenovo Fingerprint Keyboard. Users must also enroll fingerprints with the ThinkVantage Fingerprint Software using the fingerprint keyboard.

Note: Fingerprints registered with one device are not interchangeable with the other device.

Pre-desktop authentication

Either the built-in fingerprint device or the fingerprint keyboard will be used for pre-desktop authentication (replacing the system power on or hard drive password with a fingerprint). The BIOS will determine which device to use when the system is powered on.

By default, the BIOS will only accept swipes on the fingerprint keyboard, if it is connected. Swipes on the integrated fingerprint device will be ignored for pre-desktop authentication if a fingerprint keyboard is connected. If the fingerprint keyboard is not connected, the integrated fingerprint device will be used for pre-desktop authentication.

The BIOS setting for "Reader Priority" can be changed to use the built-in fingerprint sensor. If the "Reader Priority" is set to "Internal only," then the integrated fingerprint sensor can be used for pre-desktop authentication. Swipes on the fingerprint keyboard will be ignored in this case.

Windows logon

Both the Lenovo fingerprint keyboard and the fingerprint device used with the ThinkPad notebook computer models provide their own interface for users to log in to Windows with an enrolled fingerprint.

Important: Compatibility problems in the process of Windows logon might occur if the fingerprint logon interfaces are not configured correctly.

When the ThinkPad notebook computer model is equipped with both the Lenovo fingerprint keyboard and the integrated fingerprint device, and installed with the Client Security Solution program, there are two approaches to log in to the Windows 7 operating system using fingerprint authentication:

- Using the Fingerprint Software logon interface

  The logon interfaces of both Lenovo Fingerprint Software and ThinkVantage Fingerprint Software must be enabled. When both fingerprint logon interfaces are enabled in the Windows 7 operating system, users can swipe their finger on either the fingerprint keyboard or the integrated fingerprint device to log in.
- Using the Client Security Solution logon interface

  The Client Security Solution logon interface can be used instead of the Fingerprint Software logon interfaces. When using the Client Security Solution logon interface to log in to the Windows operating system with fingerprint authentication, the Fingerprint Software logon is disabled from the **Settings** option in the respective Fingerprint Software workspace, and the Client Security Solution logon interface is configured in the **Manage security policies** option from the Client Security Solution **Advanced** menu.

  Notes:

  1. The BIOS Reader Priority setting does not apply in this situation. Either device can be used for logon if both devices are available.
  2. Only Client Security Solution 8.3 or later supports this function. For more information, see “Authentication with Client Security Solution.”

Authentication with Client Security Solution

Note: The following information applies only to Client Security Solution 8.3 and later. Previous versions of Client Security Solution do not support the use of the integrated fingerprint device with the fingerprint keyboard.

When performing an action with Client Security Solution that requires fingerprint authentication, such as auto-filling a password into a Web site with Password Manager, users must swipe a finger on the fingerprint keyboard, if it is connected, when prompted. Swipes on the built-in fingerprint device will be ignored if the fingerprint keyboard is connected. If the fingerprint keyboard is not connected, the integrated fingerprint sensor must be used.

A registry setting is available to require users to use the built-in fingerprint sensor for authenticating with Client Security Solution. If this registry entry is set, fingerprint authentication with Client Security Solution must be done with the built-in sensor, and swipes from the fingerprint keyboard will be ignored.

The registry entry is as below:

```
[HKLM\Software\Lenovo\TVT Common\Client Security Solution]
REG_DWORD "PreferInternalFPSensor" = 1
```

The default value of the above registry entry is 0, when fingerprint authentication with Client Security Solution must be done with the fingerprint keyboard, and swipes on the built-in fingerprint device will be ignored.

This setting may also be changed by using the Client Security Solution Administrative Template file with group policies for Active Directory.

Notes:

1. When the BIOS Reader Priority setting is set to **Internal only**, it is recommended to set the registry entry value to 1. This will enable authentication with Client Security Solution to simulate the setting for BIOS pre-desktop authentication.
2. The BIOS setting and this registry setting are independent.

Appendix B. Synchronizing password in Client Security Solution after the Windows password is reset

After the Windows password is reset, Client Security Solution continually prompts you for a new Windows password, but then displays an error message indicating that the password is incorrect. Windows security is designed this way so that your security credentials are invalidated when your Windows password is reset. Windows will prompt a warning message at each attempt to reset your password. Also, not only is Client Security Solution affected by resetting your Windows password, but you will also lose access to your certificates and files that are encrypted by Windows EFS. When Client Security Solution can no longer access your Windows security credentials (as a result of the password reset), Client Security Solution will continually prompt you for the new password and then display an error message indicating that the password you entered is invalid. Client Security Solution cannot function when the Windows security credentials are invalidated in this way. If your Windows password has been changed (for example, you are prompted to specify both the old and the new password), your security credentials are preserved and protected by the new password.

To synchronize password in CSS after the Windows password is reset, do the following:

1. Restore a backup of your system prior to resetting the Windows password.
2. Reset your Windows password back to what it was originally. This should restore access to your Windows security credentials.
3. Create a new Windows account and start using it instead of the original account with corrupted credentials.
4. Follow this method to recover your system:
   a. Launch the Password Manager.
   b. Click **Import/Export** and select **Export entry list**.
   c. Specify a location to save the file and enter a file name.
   d. Enter a password for the Entries file.
   e. Close the Password Manager.
   f. Launch Client Security Solution.
   g. Click **Advanced → Reset security settings**.
   h. Enter the new Windows password when prompted.
   i. Client Security Solution will prompt you to restart the system.
   j. After the system restarts, launch the Password Manager.
   k. Click **Import/Export** and select **Import entry list**.
   l. Browse the file that was saved earlier.
   m. Enter the password when prompted.

Appendix C. Using Client Security Solution on a reinstalled Windows operating system

If your Windows operating system installed with Client Security Solution has been reinstalled, to use Client Security Solution on the newly installed Windows operating system, you need to clear the installation data of Client Security Solution and reinstall Client Security Solution.

The best practice is:

1. Uninstall Client Security Solution from the current Windows operating system.
2. Restart the computer.
3. Clear the following data in the registry:
   - [HKEY_LOCAL_MACHINE\SOFTWARE\Lenovo\TVT Common\Client Security Solution]
   - [HKEY_LOCAL_MACHINE\SOFTWARE\Lenovo\Client Security Solution]
   - [HKEY_LOCAL_MACHINE\SOFTWARE\Lenovo\Logs]
   - [HKEY_LOCAL_MACHINE\SOFTWARE\IBM\Security\Debug]
4. Clear the data related with Client Security Solution in the C partition. It is recommended to search the data in the whole C partition, with the option of viewing all hidden files in the File Option window enabled. The result can be found in, but not limited to, the following locations:
   - C:\Users\All Users\AppData\Roaming\Client Security Solution
   - C:\Users\%USER%\AppData\Roaming\Client Security Solution
5. Clear the security chip in BIOS Setup Utility and activate the security chip by doing the following:
   a. Shut down the computer.
   b. Turn on the computer and press F1 to enter BIOS Setup Utility.
   c. Select **Security**.
   d. Press Enter and select **Clear Security Chip**.
   e. Press Enter and select **Yes** to clear encryption keys.
   f. Select **Security Chip** and press Enter to select **Active**.

      Note: If you do not want to set Client Security Solution into hardware TPM mode, set the security chip to **Disabled**.
6. Restart the computer and reinstall the Client Security Solution program.

Note: When you change Client Security Solution installation mode from software emulation mode to hardware TPM-based mode, or after clearing the security chip, Client Security Solution will try to recover existing data when it detects the TPM change, and will fail because the encrypted data cannot be decrypted by new TPM data. In this case, Client Security Solution will fail to be launched.

Appendix D. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to an Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc
1009 Think Place
Building One
Morrisville, NC 27560
USA
Attention: Lenovo Director of Licensing

LENOVO GROUP LTD. PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk

Any performance data contained herein was determined in a controlled environment. Therefore, the result in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Trademarks

The following terms are trademarks of Lenovo in the United States, other countries, or both:

Lenovo
Rescue and Recovery
ThinkCentre
ThinkPad
ThinkVantage

IBM is a trademark of International Business Machines Corporation in the United States, other countries, or both.

Microsoft, Internet Explorer, Windows Server, and Windows are trademarks of the Microsoft group of companies.

Other company, product, or service names may be trademarks or service marks of others.

Glossary

Administrator (ThinkCentre)/Supervisor (ThinkPad) BIOS Password. The administrator or supervisor password is used to control the ability to change BIOS settings. This includes the capability to enable or disable the embedded security chip and to clear the Storage Root Key stored within the Trusted Platform Module.

Advanced Encryption Standard (AES). *Advanced Encryption Standard* is a *symmetric key* encryption technique. The U.S. Government adopted the algorithm as its encryption technique in October 2000, replacing the DES encryption it used. AES offers higher security against brute-force attack than the 56-bit DES keys, and AES can use 128, 192 and 256-bit keys, if necessary.

Cryptography systems. Cryptography systems can be broadly classified into symmetric-key encryption that use a single key that both encrypts and decrypts the data, and Public-key encryption that use two keys, a public key known to everyone and a private key that only the owner of the key pair has access to.

Embedded Security Chip. The embedded security chip is another name for a Trusted Platform Module.

Public-key/Asymmetric-key encryption. Public-key algorithms typically use a pair of two related keys — one key is private and must be kept secret, while the other is made public and can be widely distributed; it should not be possible to deduce one key of a pair given the other. The terminology of ″public-key cryptography″ derives from the idea of making part of the key public information. The term asymmetric-key cryptography is also used because not all parties hold the same information. In a sense, one key ″locks″ a lock (encrypts); but a different key is required to unlock it (decrypt).

Storage Root Key (SRK). The storage root key (SRK) is a 2,048-bit (or larger) public key pair. It is initially empty and is created when the TPM owner is assigned. This key pair never leaves the embedded security chip. It is used to encrypt (wrap) private keys for storage outside the Trusted Platform Module and to decrypt them when they are loaded back into the Trusted Platform Module. The SRK can be cleared by anyone that has access to the BIOS.

Symmetric-key encryption. Symmetric key encryption ciphers use the same key for encryption and decryption of data. Symmetric key ciphers are simpler and faster, but their main drawback is that the two parties must somehow exchange the key in a secure way. Public-key encryption avoids this problem because the public key can be distributed in a non-secure way, and the private key is never transmitted. Advanced Encryption Standard is an example of a symmetric-key.

Trusted Platform Module (TPM). Trusted Platform Modules are special-purpose integrated circuits built into systems to enable strong user authentication and machine verification. The main purpose of the TPM is to prevent inappropriate access to confidential and sensitive information. The TPM is a hardware based root of trust that can be leveraged to provide a variety of cryptographic services on a system. Another name for TPM is the embedded security chip.

ThinkVantage™

Printed in USA