ThinkVantage

Client Security Solution 6.0 User's Guide

ThinkVantage

Client Security Solution 6.0 User's Guide

Note: Before using this information and the product it supports, read the information in "Notices," on page A-1.

First Edition (August 2005)

Contents

Chapter 1. English

The Client Security Solution application is a suite of ThinkVantage™ Technology tools designed to help protect access to your computer operating system and your sensitive data. The Client Security Solution integrates the hardware protection of its embedded chip with the protection afforded by its secure software. By combining dedicated hardware with its software protection, the Client Security Solution powerfully enhances the security features built into the operating system of your computer.

Who should read this guide

The *ThinkVantage Client Security Solution User's Guide* is intended for individual end users and end users working within a business environment. This guide provides information on the following areas:

- Client Security Solution components
- Client Security Solution installation considerations
- Client Security Solution features

This guide supplements the Client Security Solution help system, which provides step-by-step instructions on how to perform specific tasks within the program.

Additional information

If you are a system administrator, system engineer, network administrator or customer engineer seeking to implement the Client Security Solution across a large enterprise, you can obtain detailed information by reading the *ThinkVantage Rescue and Recovery™ and Client Security Solution Deployment Guide* located at the following Web site:

`http://www.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-54502`

Client Security Solution components

The Client Security Solution is designed for computers that come equipped with an embedded security chip, which helps provide additional levels of security to your computer data and processes. However, the Client Security Solution software can now be configured to enhance the security of computers that are not equipped with a security chip.

The Client Security Solution is divided into the following hardware and software components.

- **Embedded security chip**

  The Client Security Solution is designed for computers that come equipped with an embedded security chip. An embedded security chip is built-in cryptographic hardware technology that provides an extra level of security to your computer. The security chip enables the encryption and authentication processes to be transferred from vulnerable software to the secure environment of dedicated hardware. The increased security that this provides is tangible.

- **Client Security Setup Wizard**

  The Client Security Setup Wizard helps guide you through the process of configuring your security options. The wizard helps you enable the embedded security chip, select an authentication and login method, create password recovery questions, establish fingerprint authentication (optional), and configure additional Client Security Solution components.

- **Password Manager**

  The Client Security Password Manager enables you to securely and conveniently manage your sensitive and easy-to-forget application and Web site login information, such as user IDs, passwords, and other personal information. The Client Security Password Manager stores all information through the embedded security chip so that access to your applications and Web sites remain totally secure.
- **PrivateDisk**

  PrivateDisk sets up an encrypted virtual disk drive which automatically encrypts any data that you store within the secure confines of this ″electronic safe.″ Use your own virtual drive to encrypt and store all your critical data. Data is automatically encrypted when stored in any PrivateDisk volume.
- **Client Security Solution application**

  The Client Security Solution application provides a single interface which enables users to perform basic and advanced security functions, such as enabling the embedded security chip, changing a passphrase, or using fingerprint software. For a list of complete Client Security Solution features, see "Client Security Solution features" on page 1-3
- **ThinkVantage fingerprint software**

  ThinkVantage fingerprint software enable users to establish fingerprint authentication. This convenient security feature is available on select ThinkPad and ThinkCentre models and options.

Before you install the Client Security Solution

Before you install the Client Security Solution application, it is important that the following prerequisites are met:

- Windows XP or Windows 2000 with Service Pack 3. If you are installing this program on a hard disk that has a capacity of greater than 137 GB, Service Pack 1 is required for Windows XP.
- Internet Explorer 5.5 (or higher).
- 128 MB of memory of which no more than 8 MB can be designated as shared memory under the video setup in BIOS.
- 800 MB of free disk space.

If you have a previous version of Client Security Solution, Client Security Software, or Rescue and Recovery, see "Using the Client Security Solution with Rescue and Recovery" on page 1-5 for specific instructions.

Setting up the Client Security Solution

The Client Security Solution application is available at the `http://www.pc.ibm.com/thinkvantage` Web site. Downloading, installing, and configuring the Client Security Solution can be done in the matter of minutes.

Downloading and installing the Client Security Solution

Complete the following installation process to download and install the Client Security Solution program:

1. Start your computer and close any open programs.
2. Go to the `http://www.pc.ibm.com/thinkvantage` Web site.

3. Click the **Support and downloads** link in the Resources section.
4. Scroll down to the Embedded Security Subsystem and Client Security Solution section and click **Software download**.
5. Follow the instructions on the screen.
6. Run the installation executable file and follow the instructions on the screen. You will be given the option to install the Password Manager and PrivateDisk components of the Client Security Solution.
7. After you have made your selections, you will be prompted to restart your computer.
8. When the computer restarts, the Client Security Setup Wizard will open. If the setup wizard does not open, see "Opening the Client Security Setup Wizard"
9. Complete the Client Security Setup Wizard to complete the configuration process.

Opening the Client Security Setup Wizard

Complete the following procedure to configure the Client Security Solution program using the Client Security Setup Wizard:

1. From the Windows desktop click **Start**, click **All Programs**, select **ThinkVantage**, and then double-click **Client Security Solution**.
2. When the Client Security Solution window opens, click the **Advanced** menu item.
3. When the Client Security Solution window opens, click **Set security and backup preferences**. The Client Security Setup Wizard will open.
4. Complete the Client Security Solution Setup Wizard steps and then click **Finish**. For detailed information, click **Help** within the Client Security Setup Wizard.

Using the Client Security Solution

Complete the following procedure to access the Client Security Solution application:

1. From the Windows desktop, click **Start**.
2. Select **All Programs**.
3. Select **ThinkVantage**.
4. Click **Client Security Solution**.

Client Security Solution features

The following information details the various tasks that can be accomplished using the Client Security Solution application.

Note: If some of the tools mentioned below are not available to you, it might be because you do not have the proper software installed, your computer does not support the application, or the application requires administrator or supervisor access.

Basic features

The following information details basic tasks that can be accomplished using the Client Security Solution application.

Changing a passphrase: The Change passphrase tool enables you to establish a new Client Security passphrase. Passphrases must adhere to Client Security passphrase requirements.

Configuring password recovery: The Configure password recovery tool enables you to establish a means to recover a forgotten Windows password or Client Security passphrase, depending upon the authentication methodology that you use.

Managing logon information: The Password Manager application enables you to use the Client Security Solution to manage your sensitive and easy-to-forget login information, such as user IDs, passwords, and other personal information. The Password Manager application stores all information through the embedded security chip so that your user-authentication policy controls access to your secure applications and Web sites. This means that rather than having to remember and provide a plethora of individual passwords-- all subject to different rules and expiration dates-- you only have to remember one passphrase or, when fingerprint software is installed, provide your fingerprint.

Using fingerprint software: The integrated fingerprint reader enables you to enroll and associate your fingerprint with your power-on password, hard disk password, and Windows password so that fingerprint authentication can replace passwords and enable simple and secure user access. A fingerprint reader keyboard is available with select computers and can be purchased as an option. This option is supported on select ThinkCentre and ThinkPad computers only.

Protecting data: The PrivateDisk tool generates an encrypted virtual disk drive, which automatically encrypts any data that you store within the secure confines of this ″electronic safe.″

Advanced features

The following information details advanced tasks that can be accomplished using the Client Security Solution application.

Note: You must have administrator rights to perform the following operations.

Monitoring security settings: The Security Advisor tool enables you to view a summary of security settings currently set on your computer. Review these settings to either view your current security status or to enhance your system security. Some of the security topics included are hardware passwords, Windows users passwords, Windows password policy, protected screen saver, and file sharing.

Note: The Security Advisor tool only provides a summary of security settings and suggestions to help enhance your system security. Not all aspects of security are addressed, such as using and maintaining antivirus and firewall programs. Many of the settings require supervisor or administrator access.

Transferring digital certificates: 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 the embedded security chip.

Establishing a hardware password reset mechanism: 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. It is a good idea to 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 ThinkCentre and ThinkPad computers only.

Note: It is a good idea to set an administrator or supervisor password before using this tool. If you have not set an administrator or supervisor password, your environment will not be as secure as possible. When you complete this procedure, your power-on password and hard-disk drive password will match. This procedure is designed to help you complete the task of creating the secure environment and to help you reset your forgotten passwords after the secure environment is created.

Activating the embedded security chip: This tool initiates a BIOS setting change that is used to activate or disactivate the embedded security chip. You must restart the computer for this change to take effect.

Changing logon settings: This tool displays your current logon settings and enables an administrator to change how users log on to the Windows operating system and to the ThinkVantage Rescue and Recovery workspace.

Clearing the fail safe counter: This tool resets the authentication fail counter that monitors how many incorrect authentication attempts have been passed to the embedded security chip. After a certain number of failed attempts, the chip locks itself for a period of time. The lockout period grows with continued failed attempts.

Setting security and backup preferences: The Client Security Setup Wizard enables you to configure a variety of security software tools. This wizard provides configuration options which enable you to set a variety of security features, such as enabling the Client Security embedded security chip, selecting how you want to authenticate to the Windows environment, choosing to use Rescue and Recovery to back up your sensitive data, or electing to use fingerprint authentication.

Using the Client Security Solution with Rescue and Recovery

Both the Rescue and Recovery program and the Client Security Solution application are ThinkVantage Technologies that have been developed with you in mind. That is, they are designed to work separately or together, depending upon your needs. The following information is intended to help you design your strategy for using these programs, and to highlight how these programs enhance each other.

There are important considerations to take into account when installing the Rescue and Recovery program, the Client Security Solution application, or both together. The following tables provide information to help you determine the correct procedure for your desired configuration:

Table 1-1. The following table provides information to help you change your Rescue and Recovery and Client Security configuration. Client Security Solution standalone means that the installation package was acquired from the Web or CD.

Software installed is...	And you want...	Follow this process	Comments
Client Security Software 5.4x	Client Security Software 5.4x and Rescue and Recovery 3.0	1. Install Rescue and Recovery 3.0 program. 2. When prompted, indicate that you want to keep the Client Security Software 5.4x application installed.	Backups cannot be protected using Client Security Software 5.4x application, and any use of Client Security Software features by the Rescue and Recovery 3.0 program will be done using an emulated version of Client Security Software. The master password feature is added to your security features. A master password is typically used in an enterprise environment. For more information see, "Additional information" on page 1-1
Client Security Software 5.4x	Client Security Solution 6.0 Standalone installation package	1. Uninstall the Client Security Software 5.4x. application. 2. Install the Client Security Solution 6.0 (Standalone) application.	• You must decrypt any encrypted files and export any Password Manager information before uninstalling. Otherwise, this information will be lost. • You must uninstall the IBM® File and Folder Encryption software before installing the Client Security Solution application.

Table 1-1. The following table provides information to help you change your Rescue and Recovery and Client Security configuration. Client Security Solution standalone means that the installation package was acquired from the Web or CD. (continued)

Software installed is...	And you want...	Follow this process	Comments
Client Security Software 5.4x	Client Security Solution 6.0 and Rescue and Recovery 3.0	1. Uninstall the Client Security Software 5.4x application. 2. Install the Rescue and Recovery 3.0 program. (Make sure the Client Security Solution 6.0 component is selected.)	• Installing Rescue and Recovery 3.0 over Client Security Software 5.4x without first uninstalling Client Security Software will result in Rescue and Recovery only. • Before you uninstall the Client Security Software 5.4x application, you must decrypt any encrypted files and export any Password Manager information before uninstalling. Otherwise, this information will be lost. • You must uninstall the IBM File and Folder Encryption software before installing the Client Security Solution 6.0 application.
Rescue and Recovery 3.0	Client Security Software 5.4x and Rescue and Recovery 3.0	1. Uninstall the Rescue and Recovery 3.0 program. 2. Install the Client Security Software 5.4x application. 3. Install the Rescue and Recovery 3.0 program. 4. When prompted, indicate that you want to keep the Client Security Software 5.4x application installed.	• The Client Security Software 5.4x application cannot be installed over the Rescue and Recovery 3.0 program. • Local backups are deleted when uninstalling the Rescue and Recovery 3.0 program.

Table 1-1. The following table provides information to help you change your Rescue and Recovery and Client Security configuration. Client Security Solution standalone means that the installation package was acquired from the Web or CD. (continued)

Software installed is...	And you want...	Follow this process	Comments
Rescue and Recovery 3.0	Client Security Solution 6.0 Standalone install package	1. Uninstall the Rescue and Recovery 3.0 program. 2. Install the Client Security Solution 6.0 (Standalone) application.	• Uninstalling Rescue and Recovery will delete user files and Client Security Solution registry settings. • Rescue and Recovery backups protected by Client Security Solution will no longer be accessible. • Local backups are deleted when uninstalling Rescue and Recovery 3.0. • Client Security Solution 6.0 (Standalone) cannot be installed over Rescue and Recovery 3.0.
Rescue and Recovery 3.0	Rescue and Recovery 3.0 and Client Security Solution 6.0	1. Select the **Modify** option from Add/Remove programs. 2. Complete the modify operation by adding the Client Security Solution application and any desired subcomponents.	• Local backups are deleted when the Client Security Solution application is added. • After adding the Client Security Solution application, create a new base backup as soon as possible. • Client Security Solution settings and data files are deleted. • The Client Security Solution 6.0 (Standalone) application cannot be installed over the Rescue and Recovery 3.0 program.
Client Security Solution 6.0 Standalone installation package	Client Security Software 5.4x	1. Uninstall the Client Security Solution 6.0 (Standalone) application. 2. Install the Client Security Software 5.4x application.	• Deleting Client Security Solution 6.0 data files and settings at the prompt will not affect Client Security Software 5.4x operations.

Table 1-1. The following table provides information to help you change your Rescue and Recovery and Client Security configuration. Client Security Solution standalone means that the installation package was acquired from the Web or CD. (continued)

Software installed is...	And you want...	Follow this process	Comments
Client Security Solution 6.0 Standalone installation package	Rescue and Recovery 3.0	1. Uninstall the Client Security Solution 6.0 application. 2. Install the Rescue and Recovery 3.0 program. 3. During the install, choose to install the Rescue and Recovery program only.	When uninstalling the Client Security Solution 6.0 application, you must delete Security Solution 6.0 files and settings. Failure to remove these at the prompt will terminate the Rescue and Recovery 3.0 install.
Client Security Solution 6.0 Standalone	Rescue and Recovery 3.0 and Client Security Solution 6.0	1. Install the Rescue and Recovery 3.0 program. 2. Select any subcomponents of the Client Security Solution 6.0 application that you would like installed.	• Client Security Solution 6.0 data files and settings are preserved. • To choose to protect backups using the Client Security Solution 6.0 application, use the Rescue and Recovery program.
Rescue and Recovery 3.0 and Client Security Solution 6.0	Client Security Software 5.4x	1. Uninstall the Rescue and Recovery - Client Security Solution application. 2. Install the Client Security Software 5.4x application.	• The Client Security Software 5.4x application cannot install over the Client Security Solution 6.0 application. • Deleting data files and settings at the prompt will not affect Client Security Software 5.4x operations. • By uninstalling the Rescue and Recovery 3.0 program, the Client Security Solution 6.0 application is automatically uninstalled.
Rescue and Recovery 3.0 and Client Security Solution 6.0	Rescue and Recovery 3.0	1. Select **Modify** from Add/Remove programs. 2. Remove the Client Security Solution 6.0 application.	• Local backups are deleted when the Client Security Solution 6.0 application is removed. • Uninstalling the Client Security Solution 6.0 application will result in not having Password Manager or PrivateDisk. • The Rescue and Recovery 3.0 backups protected with the Client Security Solution 6.0 application are no longer accessible. Create a new backup as soon as possible.

Table 1-1. The following table provides information to help you change your Rescue and Recovery and Client Security configuration. Client Security Solution standalone means that the installation package was acquired from the Web or CD. (continued)

Software installed is...	And you want...	Follow this process	Comments
Rescue and Recovery 3.0 and Client Security Solution 6.0	Client Security Solution 6.0	1. Uninstall the Rescue and Recovery 3.0 program. 2. When prompted, choose to keep current Client Security Solution 6.0 settings only if you want to keep your current security configuration. 3. Install the Client Security Solution 6.0 (Standalone) application.	1. Rescue and Recovery 3.0 backups protected with Client Security Solution 6.0 are no longer accessible. 2. Local backups are deleted when uninstalling the Rescue and Recovery 3.0 application.

Rescue and Recovery passwords and passphrases

You can use passwords or passphrases can be used to protect the Rescue and Recovery workspace, thereby protecting critical data from unauthorized access. You can specify to protect the Rescue and Recovery workspace by using the Client Security Setup wizard to set security preferences or by changing your logon settings using the Client Security Solution application. The Client Security Solution application also enables you to establish password recovery options within the Rescue and Recovery workspace.

Notes:

1. This feature is available only if the Client Security Solution 6.0 program is installed. To use this feature you must have completed the Client Security 6.0 Setup wizard and specified that you want to use either a password or passphrase to log on to your computer.
2. Both the Client Security Setup 6.0 wizard and the Client Security Solution 6.0 application are accessible in the Windows environment only. If you choose to use Rescue and Recovery without Client Security Solution, then the Rescue and Recovery workspace will not be protected by a password or passphrase.
3. The Client Security Solution application enables you to establish password recovery options within the Rescue and Recovery workspace.

Use the following methods to protect the Rescue and Recovery workspace using a password or passphrase.

Method 1: If you have not completed the Client Security Setup Wizard, do the following to protect the Rescue and Recovery workspace with either a password or passphrase:

1. From the Windows desktop click **Start**, click **All Programs**, select **ThinkVantage**, and then double-click **Client Security Solution**.
2. When the Client Security Solution window opens, click the **Advanced** menu item.
3. Click the **Set security and backup preferences** icon. The Client Security Setup Wizard opens.
4. Set your security preferences. When prompted choose one of the following:

- If you want to protect the Rescue and Recovery workspace using your Windows logon password, mark the **Use Windows password to gain access to the Rescue and Recovery workspace** check box.
- If you want to protect the Rescue and Recovery workspace using your Client Security Solution logon passphrase, mark the **Use the Client Security Solution passphrase to gain access to the Rescue and Recovery workspace** check box.

5. Complete the Client Security Solution Setup wizard, then click **Finish**. For more information, click **Help** within the Client Security Setup Wizard.

Method 2: If you have completed the Client Security Setup Wizard, do the following to protect the Rescue and Recovery workspace with a password or passphrase:

1. From the Windows desktop click **Start**, click **All Programs**, select **ThinkVantage**, and then double-click **Client Security Solution**.
2. When the Client Security Solution window opens, click the **Advanced** menu item.
3. Click **Change logon settings**.
4. Follow the instructions on the screen. For detailed information click **Help** within the Client Security Solution application.

Setting backup preferences using the Client Security Setup Wizard

The Client Security Solution Setup Wizard provides configuration options that enable you to set a variety of security features, such as enabling the embedded security chip, selecting how you want to authenticate to the Windows environment, choosing to use Rescue and Recovery to back up your sensitive data, or electing to use fingerprint authentication.

Complete the following procedure to use the Client Security Setup wizard:

1. From the Windows desktop click **Start**, click **All Programs**, select **ThinkVantage**, and then double-click **Client Security Solution**.
2. When the Client Security Solution window opens, click the **Advanced** menu item.
3. When the Client Security Solution window opens, click **Set security and backup preferences**. The Client Security Setup Wizard opens.
4. Set your security preferences.
5. Complete the Client Security Solution Setup wizard, then click **Finish**. For detailed information, click **Help** within the Client Security Setup Wizard.

More information about the Client Security Solution

For detailed information about the Client Security Solution application and its features, see the *Client Security Solution User Guide* on the Web at:

`http://www.ibm.com/pc/support/site.wss/`

If you have the Client Security Solution application already installed, you can read more detailed information from the User Guide by completing the following procedure:

1. From the Windows desktop, click **Start**.
2. Select **All Programs**.
3. Select **ThinkVantage**.
4. Click **Client Security Solution**.
5. From the Client Security Solution menu bar click **Help**.

6. Click **User’s Guide**.

Chapitre 2. Français

L'application Client Security Solution est une suite d'outils de technologie ThinkVantage conçus pour vous aider à protéger l'accès au système d'exploitation de votre ordinateur et à vos données sensibles. Client Security Solution intègre la protection matérielle de son processeur intégré grâce à la protection fournie par son logiciel sécurisé. En combinant le matériel dédié avec sa protection logicielle, Client Security Solution améliore de façon significative les fonctions de sécurité figurant dans le système d'exploitation de votre ordinateur.

A qui s'adresse ce manuel

Le manuel *ThinkVantage Client Security Solution User's Guide* s'adresse aux particuliers et aux utilisateurs finaux qui travaillent dans un environnement métier. Le présent manuel fournit des informations sur les domaines suivants :

- Composants Client Security Solution
- Considérations relatives à l'installation de Client Security Solution
- Fonctions de Client Security Solution

Le présent manuel complète le système d'aide Client Security Solution, qui fournit des instructions détaillées sur l'exécution de tâches spécifiques dans le programme.

Informations supplémentaires

Si vous êtes un administrateur système, un ingénieur système, un administrateur de réseau ou un technicien de maintenance cherchant à mettre en oeuvre Client Security Solution dans une grande entreprise, vous pouvez obtenir des informations plus détaillées en consultant le manuel *ThinkVantage Rescue and Recovery and Client Security Solution Deployment Guide* sur le site Web suivant :

`http://www.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-54502`

Composants Client Security Solution

Client Security Solution est conçu pour les ordinateurs équipés d'un processeur de sécurité intégré, qui aide à fournir des niveaux de sécurité supplémentaires à vos données informatiques et à vos processus. Toutefois, le logiciel Client Security Solution peut désormais être configuré pour améliorer la sécurité des ordinateurs non équipés d'un processeur de sécurité.

Client Security Solution se subdivise en composants matériels et logiciels, qui sont présentés ci-dessous.

- **Processeur de sécurité intégré**

  Client Security Solution est conçu pour les ordinateurs équipés d'un processeur de sécurité intégré. Un processeur de sécurité intégré est un élément matériel de chiffrement intégré qui offre un niveau de sécurité supplémentaire à votre ordinateur. Le processeur de sécurité permet aux processus de chiffrement et d'authentification d'être transférés d'un logiciel vulnérable à l'environnement sécurisé du matériel dédié. Il fournit une sécurité supplémentaire significative.
- **Assistant d'installation du logiciel Client Security**

  L'assistant d'installation du logiciel Client Security vous guide lors du processus de configuration de vos options de sécurité. Il vous aide à activer le processeur de sécurité intégré, à sélectionner une méthode d'authentification et de connexion, à créer des questions permettant de récupérer un mot de passe, à établir une authentification par empreintes digitales (facultatif) et à configurer des composants Client Security Solution supplémentaires.

- **Gestionnaire de mots de passe**

  Client Security Password Manager permet de gérer de façon sécurisée et pratique vos informations de connexion aux applications et aux sites Web, confidentielles, sensibles et faciles à oublier, telles que les ID utilisateur, les mots de passe et les autres informations personnelles. Client Security Password Manager stocke toutes les informations à l'aide du processeur de sécurité intégré, sécurisant ainsi l'accès aux applications et aux sites Web sécurisés.
- **PrivateDisk**

  PrivateDisk permet de configurer un disque virtuel privé chiffré qui chiffre automatiquement les données stockées dans les emplacements sécurisés de ce ″coffre-fort électronique″. Utilisez votre propre unité virtuelle pour chiffrer et stocker toutes vos données essentielles. Les données sont automatiquement chiffrées lors de leur stockage sur un volume PrivateDisk.
- **Application Client Security Solution**

  L'application Client Security Solution fournit une interface unique qui permet aux utilisateurs d'exécuter des fonctions de sécurité de base et avancées, telles que l'activation du processeur de sécurité intégré, la modification d'un mot de passe composé ou l'utilisation d'un logiciel d'identification par empreintes digitales. Pour obtenir la liste complète des fonctions Client Security Solution, voir «Fonctions de Client Security Solution», à la page 2-3.
- **Logiciel d'identification par empreintes digitales ThinkVantage**

  Le logiciel d'identification par empreintes digitales ThinkVantage permet aux utilisateurs d'établir une authentification par empreintes digitales. Cette fonction de sécurité pratique est disponible sur certains modèles et options d'ordinateurs ThinkPad et ThinkCentre.

Avant l'installation de Client Security Solution

Avant d'installer l'application Client Security Solution, il est important de respecter les conditions prérequises suivantes :

- Windows XP ou Windows 2000 avec Service Pack 3. Si vous installez ce programme sur un disque dur dont la capacité est supérieure à 137 Go, le Service Pack 1 est requis pour Windows XP.
- Internet Explorer 5.5 (ou version suivante).
- 128 Mo de mémoire, dont 8 Mo au maximum peuvent être désignés comme de la mémoire partagée dans les paramètres de configuration vidéo du BIOS
- 800 Mo d'espace disque disponible

Si vous disposez d'une version précédente de Client Security Solution, Client Security Software ou Rescue and Recovery, voir «Utilisation de Client Security Solution avec Rescue and Recovery», à la page 2-6 pour des instructions spécifiques.

Configuration de Client Security Solution

L'application Client Security Solution est disponible sur le site Web `http://www.pc.ibm.com/thinkvantage`. Le téléchargement, l'installation et la configuration de Client Security Solution peuvent s'effectuer en quelques minutes.

Téléchargement et installation de Client Security Solution

Exécutez la procédure d'installation suivante pour télécharger et installer le logiciel Client Security Solution :

1. Démarrez votre ordinateur et fermez tous les programmes ouverts.
2. Accédez au site Web `http://www.pc.ibm.com/thinkvantage`.
3. Cliquez sur le lien **Support and downloads** dans la section Resources.
4. Faites défiler la page jusqu'à la section Embedded Security Subsystem and Client Security Solution et cliquez sur **Software download**.
5. Suivez les instructions qui s'affichent à l'écran.
6. Exécutez le fichier d'installation et suivez les instructions qui s'affichent à l'écran. Vous aurez la possibilité d'installer les composants Password Manager et PrivateDisk de Client Security Solution.
7. Après avoir effectué vos sélections, vous serez invité à redémarrer votre ordinateur.
8. Une fois que l'ordinateur redémarre, l'assistant d'installation du logiciel Client Security s'ouvre. Si l'assistant ne s'affiche pas, voir «Ouverture de l'assistant d'installation du logiciel Client Security»
9. Exécutez l'assistant d'installation du logiciel Client Security pour terminer le processus de configuration.

Ouverture de l'assistant d'installation du logiciel Client Security

Procédez comme suit pour configurer le programme Client Security Solution à l'aide de l'assistant d'installation du logiciel Client Security :

1. A partir du bureau Windows, sélectionnez **Démarrer**, **Tous les programmes**, **ThinkVantage**, puis cliquez deux fois sur **Client Security Solution**.
2. Lorsque la fenêtre Client Security Solution s'ouvre, cliquez sur l'option de menu **Avancé**.
3. Lorsque la fenêtre Client Security Solution s'ouvre, cliquez sur **Configuration des préférences de sécurité et de sauvegarde**. L'assistant d'installation du logiciel Client Security s'ouvre.
4. Exécutez l'assistant d'installation de Client Security Solution, puis cliquez sur **Terminer**. Pour plus d'informations, cliquez sur **Aide** dans l'assistant d'installation de Client Security.

Utilisation de Client Security Solution

Procédez comme suit pour accéder à l'application Client Security Solution :

1. A partir du bureau Windows, cliquez sur **Démarrer**.
2. Sélectionnez **Tous les programmes**.
3. Sélectionnez **ThinkVantage**.
4. Cliquez sur **Client Security Solution**.

Fonctions de Client Security Solution

Les informations suivantes détaillent les diverses tâches que vous pouvez exécuter à l'aide de l'application Client Security Solution.

Remarque : Certains outils mentionnés ci-dessous peuvent ne pas être disponibles ; c'est le cas si le logiciel n'est pas installé, si l'ordinateur ne prend pas en charge l'application, ou si l'application requiert des droits administrateur ou superviseur.

Fonctions de base

Les informations suivantes détaillent les tâches de base que vous pouvez exécuter à l'aide de l'application Client Security Solution.

Modification d'un mot de passe composé : L'outil de changement du mot de passe composé vous permet d'établir un nouveau mot de passe composé Client Security. Les mots de passe composés doivent répondre aux conditions requises pour les mots de passe composés Client Security.

Configuration de la récupération du mot de passe : L'outil de configuration de la récupération du mot de passe vous permet d'établir un moyen de récupération d'un mot de passe Windows ou d'un mot de passe composé Client Security oublié, en fonction de la méthode d'authentification utilisée.

Gestion des informations de connexion : L'application Password Manager vous permet d'utiliser Client Security Solution pour gérer vos informations de connexion sensibles et difficilement mémorisables, telles que les ID utilisateur, les mots de passe et d'autres informations personnelles. Password Manager stocke toutes les informations à l'aide du processeur de sécurité intégré et permet ainsi à votre méthode d'authentification des utilisateurs de contrôler l'accès aux applications et aux sites Web sécurisés. Cela signifie qu'il n'est plus nécessaire de fournir et de mémoriser de nombreux mots de passe -- associés à des conditions et à des dates d'expiration diverses -- il suffit de mémoriser un mot de passe composé ou, si le logiciel d'identification par empreintes digitales est installé, de fournir son empreinte digitale.

Utilisation d'un logiciel d'identification par empreintes digitales : Le lecteur d'empreintes digitales intégré vous permet d'enregistrer votre empreinte et de l'associer à votre mot de passe utilisateur, à votre mot de passe d'accès au disque dur et à votre mot de passe Windows afin que l'authentification par empreintes digitales puisse remplacer l'utilisation de mots de passe et permettre un accès simple et sécurisé aux utilisateurs. Un clavier avec lecteur d'empreintes digitales est disponible en option pour certains ordinateurs. Cette option est prise en charge sur certains ordinateurs ThinkCentre et ThinkPad uniquement.

Protection des données : L'outil PrivateDisk permet de générer un disque virtuel privé chiffré qui chiffre automatiquement les données stockées dans les emplacements sécurisés de ce ″coffre-fort électronique″.

Fonctions avancées

Les informations suivantes détaillent les tâches avancées que vous pouvez exécuter à l'aide de l'application Client Security Solution.

Remarque : Vous devez disposer des droits administrateur pour effectuer les opérations suivantes :

Contrôle des paramètres de sécurité : L'outil Security Advisor vous permet d'afficher un récapitulatif des paramètres de sécurité définis sur l'ordinateur. Vérifiez ces paramètres pour connaître l'état actuel de la sécurité du système ou pour améliorer cette sécurité. Parmi les paramètres de sécurité fournis : les mots de passe matériel, les mots de passe utilisateur Windows, les règles régissant les mots de passe Windows, les fonctions d'économiseur d'écran et le partage des fichiers.

Remarque : L'outil Security Advisor fournit un récapitulatif des paramètres de sécurité et de suggestions dans le but de vous aider à améliorer la sécurité de votre système. Tous les aspects de la sécurité ne sont pas abordés (comme par exemple l'utilisation et la maintenance d'un programme antivirus et d'un pare-feu). De nombreux paramètres exigent des droits superviseur ou administrateur.

Transfert de certificats numériques : L'Assistant de transfert de certificats Client Security vous guide tout au long du processus de transfert des clés privées associées aux certificats à partir du fournisseur de service cryptographique Microsoft (logiciel) vers le fournisseur de service cryptographique de Client Security Solution. Une fois le transfert effectué, les opérations utilisant les certificats sont plus sécurisées car les clés privées sont protégées par le processeur de sécurité intégré.

Définition d'un mécanisme de réinitialisation des mots de passe matériel : Cet outil génère un environnement sécurisé qui s'exécute indépendamment de Windows et qui vous aide à redéfinir des mots de passe à la mise sous tension et d'accès au disque dur oubliés. Votre identité est établie lorsque vous répondez à des questions que vous créez. Il est judicieux de créer cet environnement sécurisé dès que possible, avant tout oubli de mot de passe. Il n'est pas possible de redéfinir un mot de passe matériel tant que cet environnement sécurisé n'est pas créé sur le disque dur et tant que vous ne vous êtes pas enregistré. Cet outil est disponible sur certains ordinateurs ThinkCentre et ThinkPad uniquement.

Remarque : Avant d'utiliser cet outil, il est judicieux de définir un mot de passe superviseur ou administrateur. Si vous n'avez pas défini de mot de passe administrateur ou superviseur, votre environnement ne sera pas sécurisé de manière optimale. A l'issue de cette procédure, vos mots de passe à la mise sous tension et d'accès au disque dur correspondent. Cette procédure est conçue pour vous aider à créer un environnement sécurisé et à redéfinir vos mots de passe oubliés une fois cet environnement sécurisé créé.

Activation du processeur de sécurité intégré : Cet outil permet de modifier l'état du paramètre BIOS servant à activer ou à désactiver le processeur de sécurité intégré. Vous devez redémarrer l'ordinateur pour que cette modification prenne effet.

Modification des paramètres de connexion : Cet outil affiche les paramètres de connexion en cours et permet à un administrateur de modifier le mode de connexion des utilisateurs à Windows et à l'espace de travail ThinkVantage Rescue and Recovery.

Vidage du compteur d'échecs : Cet outil permet de réinitialiser le compteur d'échecs d'authentification qui contrôle le nombre de tentatives incorrectes transmises au processeur de sécurité intégré. A partir d'un certain nombre de tentatives, le processeur se verrouille pendant une durée déterminée. La période de verrouillage augmente au fil des échecs continus.

Configuration des préférences de sécurité et de sauvegarde : L'assistant d'installation de Client Security vous permet de configurer divers outils de sécurité. Cet assistant fournit des options de configuration qui vous permettent de configurer diverses fonctionnalités de sécurité, telles que le processeur de sécurité intégré de Client Security, la méthode d'authentification sous Windows, l'utilisation de Rescue and Recovery pour sauvegarder vos données confidentielles, ou encore le recours à l'authentification par empreintes digitales.

Utilisation de Client Security Solution avec Rescue and Recovery

Le programme Rescue and Recovery et l'application Client Security Solution sont tous deux des technologies ThinkVantage qui ont été développées en pensant à vous. Ils sont donc conçus pour fonctionner séparément ou conjointement, en fonction de vos besoins. Les informations suivantes sont destinées à vous aider à mettre au point votre stratégie en ce qui concerne l'utilisation de ces programmes et à mettre en évidence la façon dont ces programmes peuvent s'améliorer mutuellement.

Des considérations importantes doivent être prises en compte lors de l'installation du programme Rescue and Recovery et/ou de l'application Client Security Solution. Les tableaux suivants fournissent des informations qui vous aident à déterminer la procédure correcte pour votre configuration :

Tableau 2-1. Le tableau suivant fournit des informations pour vous aider à modifier votre configuration Rescue and Recovery et Client Security. Client Security Solution autonome signifie que le module d'installation a été obtenu à partir du Web ou d'un CD.

Logiciel installé	Logiciel souhaité	Procédure à suivre	Commentaires
Client Security Software 5.4x	Client Security Software 5.4x et Rescue and Recovery 3.0	1. Installez le programme Rescue and Recovery 3.0. 2. Lorsque vous y êtes invité, indiquez que vous souhaitez conserver l'application Client Security Software 5.4x installée.	Les sauvegardes ne peuvent pas être protégées à l'aide de l'application Client Security Software 5.4x et toute utilisation des fonctions Client Security Software par le programme Rescue and Recovery 3.0 sera effectuée à l'aide d'une version émulée de Client Security Software. La fonction de mot de passe maître est ajoutée à vos fonctions de sécurité. Un mot de passe maître est généralement utilisé dans un environnement d'entreprise. Pour plus d'informations, voir «Informations supplémentaires», à la page 2-1
Client Security Software 5.4x	Module d'installation Client Security Solution 6.0 autonome	1. Désinstallez l'application Client Security Software 5.4x. 2. Installez l'application Client Security Solution 6.0 (autonome).	• Vous devez déchiffrer les fichiers chiffrés et exporter les informations Password Manager avant de procéder à la désinstallation, sous peine de perdre ces informations. • Vous devez désinstaller le logiciel IBM File and Folder Encryption avant d'installer l'application Client Security Solution.

Tableau 2-1. Le tableau suivant fournit des informations pour vous aider à modifier votre configuration Rescue and Recovery et Client Security. Client Security Solution autonome signifie que le module d'installation a été obtenu à partir du Web ou d'un CD. (suite)

Logiciel installé	Logiciel souhaité	Procédure à suivre	Commentaires
Client Security Software 5.4x	Client Security Solution 6.0 et Rescue and Recovery 3.0	1. Désinstallez l'application Client Security Software 5.4x. 2. Installez le programme Rescue and Recovery 3.0. (Assurez-vous que le composant Client Security Solution 6.0 est sélectionné.)	• L'installation de Rescue and Recovery 3.0 sur Client Security Software 5.4x sans désinstaller au préalable Client Security Software résultera dans la seule installation de Rescue and Recovery. • Avant de désinstaller l'application Client Security Software 5.4x, vous devez déchiffrer les fichiers chiffrés et exporter les informations Password Manager, sous peine de perdre ces informations. • Vous devez désinstaller le logiciel IBM File and Folder Encryption avant d'installer l'application Client Security Solution 6.0.
Rescue and Recovery 3.0	Client Security Software 5.4x et Rescue and Recovery 3.0	1. Désinstallez le programme Rescue and Recovery 3.0. 2. Installez l'application Client Security Software 5.4x. 3. Installez le programme Rescue and Recovery 3.0. 4. Lorsque vous y êtes invité, indiquez que vous souhaitez conserver l'application Client Security Software 5.4x installée.	• L'application Client Security Software 5.4x ne peut pas être installée sur le programme Rescue and Recovery 3.0. • Les sauvegardes locales sont supprimées lors de la désinstallation de Rescue and Recovery 3.0.

Tableau 2-1. Le tableau suivant fournit des informations pour vous aider à modifier votre configuration Rescue and Recovery et Client Security. Client Security Solution autonome signifie que le module d'installation a été obtenu à partir du Web ou d'un CD. (suite)

Logiciel installé	**Logiciel souhaité**	**Procédure à suivre**	**Commentaires**
Rescue and Recovery 3.0	Module d'installation Client Security Solution 6.0 autonome	1. Désinstallez le programme Rescue and Recovery 3.0. 2. Installez l'application Client Security Solution 6.0 (autonome).	• La désinstallation de Rescue and Recovery supprimera les fichiers utilisateur et les paramètres de la base de registre Client Security Solution. • Les sauvegardes Rescue and Recovery protégées par Client Security Solution ne seront plus accessibles. • Les sauvegardes locales sont supprimées lors de la désinstallation de Rescue and Recovery 3.0. • Client Security Solution 6.0 (autonome) ne peut pas être installé sur Rescue and Recovery 3.0.
Rescue and Recovery 3.0	Rescue and Recovery 3.0 et Client Security Solution 6.0	1. Sélectionnez l'option **Modifier** dans le panneau Ajout/Suppression de programmes. 2. Terminez l'opération de modification en ajoutant l'application Client Security Solution et les sous-composants souhaités.	• Les sauvegardes locales sont supprimées lorsque l'application Client Security Solution est ajoutée. • Après avoir ajouté l'application Client Security Solution, créez une nouvelle sauvegarde de base dès que possible. • Les paramètres Client Security Solution et les fichiers de données sont supprimés. • L'application Client Security Solution 6.0 (autonome) ne peut pas être installée sur le programme Rescue and Recovery 3.0.
Module d'installation Client Security Solution 6.0 autonome	Client Security Software 5.4x	1. Désinstallez l'application Client Security Solution 6.0 (autonome). 2. Installez l'application Client Security Software 5.4x.	• La suppression des paramètres et des fichiers de données Client Security Solution 6.0 à l'invite n'affectera pas les opérations Client Security Software 5.4x.

Tableau 2-1. Le tableau suivant fournit des informations pour vous aider à modifier votre configuration Rescue and Recovery et Client Security. Client Security Solution autonome signifie que le module d'installation a été obtenu à partir du Web ou d'un CD. (suite)

Logiciel installé	Logiciel souhaité	Procédure à suivre	Commentaires
Module d'installation Client Security Solution 6.0 autonome	Rescue and Recovery 3.0	1. Désinstallez l'application Client Security Solution 6.0. 2. Installez le programme Rescue and Recovery 3.0. 3. Lors de l'installation, choisissez d'installer uniquement le programme Rescue and Recovery.	Lors de la désinstallation de l'application Client Security Solution 6.0, vous devez supprimer les paramètres et fichiers Security Solution 6.0. Si vous ne parvenez pas à les supprimer à l'invite, l'installation de Rescue and Recovery 3.0 prendra fin.
Client Security Solution 6.0 autonome	Rescue and Recovery 3.0 et Client Security Solution 6.0	1. Installez le programme Rescue and Recovery 3.0. 2. Sélectionnez les sous-composants de l'application Client Security Solution 6.0 que vous souhaitez installer.	• Les paramètres et fichiers de données Client Security Solution 6.0 sont conservés. • Pour protéger des sauvegardes à l'aide de l'application Client Security Solution 6.0, utilisez le programme Rescue and Recovery.
Rescue and Recovery 3.0 et Client Security Solution 6.0	Client Security Software 5.4x	1. Désinstallez l'application Rescue and Recovery - Client Security Solution. 2. Installez l'application Client Security Software 5.4x.	• L'application Client Security Software 5.4x ne peut pas être installée sur l'application Client Security Solution 6.0. • La suppression des fichiers de données et des paramètres à l'invite n'affectera pas les opérations Client Security Software 5.4x. • La désinstallation du programme Rescue and Recovery 3.0 entraîne automatiquement la désinstallation de l'application Client Security Solution 6.0.

Tableau 2-1. Le tableau suivant fournit des informations pour vous aider à modifier votre configuration Rescue and Recovery et Client Security. Client Security Solution autonome signifie que le module d'installation a été obtenu à partir du Web ou d'un CD. (suite)

Logiciel installé	Logiciel souhaité	Procédure à suivre	Commentaires
Rescue and Recovery 3.0 et Client Security Solution 6.0	Rescue and Recovery 3.0	1. Sélectionnez **Modifier** dans le panneau Ajout/Suppression de programmes. 2. Retirez l'application Client Security Solution 6.0.	• Les sauvegardes locales sont supprimées lorsque l'application Client Security Solution 6.0 est supprimée. • Si l'application Client Security Solution 6.0 est désinstallée, Password Manager ou PrivateDisk ne seront pas installés. • Les sauvegardes Rescue and Recovery 3.0 protégées à l'aide de l'application Client Security Solution 6.0 ne sont plus accessibles. Créez une nouvelle sauvegarde dès que possible.
Rescue and Recovery 3.0 et Client Security Solution 6.0	Client Security Solution 6.0	1. Désinstallez le programme Rescue and Recovery 3.0. 2. Lorsque vous y êtes invité, choisissez de conserver les paramètres Client Security Solution 6.0 en cours, uniquement si vous souhaitez garder votre configuration de sécurité actuelle. 3. Installez l'application Client Security Solution 6.0 (autonome).	1. Les sauvegardes Rescue and Recovery 3.0 protégées à l'aide de Client Security Solution 6.0 ne sont plus accessibles. 2. Les sauvegardes locales sont supprimées lors de la désinstallation de Rescue and Recovery 3.0.

Mots de passe et mots de passe composés Rescue and Recovery

Vous pouvez utiliser des mots de passe ou des mots de passe composés pour protéger l'espace de travail Rescue and Recovery, protégeant ainsi les données essentielles contre les accès non autorisés. Vous pouvez choisir de protéger l'espace de travail Rescue and Recovery en utilisant l'assistant d'installation de Client Security pour définir les préférences de sécurité ou en modifiant les paramètres de connexion à l'aide de l'application Client Security Solution. L'application Client Security Solution vous permet également de définir des options de récupération du mot de passe dans l'espace de travail Rescue and Recovery.

Remarques :

1. Cette fonction est disponible uniquement si le programme Client Security Solution 6.0 est installé. Pour l'utiliser, vous devez avoir exécuté l'assistant d'installation de Client Security 6.0 et indiqué que vous souhaitez utiliser un mot de passe ou un mot de passe composé pour vous connecter.

2. L’assistant d’installation de Client Security 6.0 et l’application Client Security Solution 6.0 sont accessibles dans l’environnement Windows uniquement. Si vous choisissez d’utiliser Rescue and Recovery sans Client Security Solution, l’espace de travail Rescue and Recovery ne sera pas protégé par un mot de passe ni un mot de passe composé.
3. L’application Client Security Solution vous permet de définir des options de récupération du mot de passe dans l’espace de travail Rescue and Recovery.

Utilisez les méthodes suivantes pour protéger l’espace de travail Rescue and Recovery à l’aide d’un mot de passe ou d’un mot de passe composé.

Méthode 1 : Si vous n’avez pas exécuté l’assistant d’installation de Client Security, procédez comme suit pour protéger l’espace de travail Rescue and Recovery à l’aide d’un mot de passe ou d’un mot de passe composé :

1. A partir du bureau Windows, sélectionnez **Démarrer**, **Tous les programmes**, **ThinkVantage**, puis cliquez deux fois sur **Client Security Solution**.
2. Lorsque la fenêtre Client Security Solution s’ouvre, cliquez sur l’option de menu **Avancé**.
3. Cliquez sur l’icône **Configuration des préférences de sécurité et de sauvegarde**. L’assistant s’affiche.
4. Définissez vos préférences en matière de sécurité. A l’invite, choisissez l’un des éléments suivants :
   - Si vous souhaitez protéger l’espace de travail Rescue and Recovery à l’aide de votre mot de passe de connexion Windows, cochez la case d’**utilisation du mot de passe Windows pour accéder à l’espace de travail Rescue and Recovery**.
   - Si vous souhaitez protéger l’espace de travail Rescue and Recovery à l’aide de votre mot de passe composé Client Security Solution, cochez la case d’**utilisation du mot de passe composé Client Security Solution pour accéder à l’espace de travail Rescue and Recovery**.
5. Exécutez l’assistant d’installation de Client Security Solution, puis cliquez sur **Terminer**. Pour plus d’informations, cliquez sur **Aide** dans l’assistant d’installation de Client Security.

Méthode 2 : Si vous avez exécuté l’assistant d’installation de Client Security, procédez comme suit pour protéger l’espace de travail Rescue and Recovery à l’aide d’un mot de passe ou d’un mot de passe composé :

1. A partir du bureau Windows, sélectionnez **Démarrer**, **Tous les programmes**, **ThinkVantage**, puis cliquez deux fois sur **Client Security Solution**.
2. Lorsque la fenêtre Client Security Solution s’ouvre, cliquez sur l’option de menu **Avancé**.
3. Cliquez sur **Modification des paramètres de connexion**.
4. Suivez les instructions qui s’affichent à l’écran. Pour plus de détails, cliquez sur **Aide** dans l’application Client Security Solution.

Définition des préférences de sauvegarde à l’aide de l’assistant d’installation de Client Security

L’assistant d’installation de Client Security Solution fournit des options de configuration qui vous permettent de configurer diverses fonctionnalités de sécurité, telles que le processeur de sécurité intégré, la méthode d’authentification sous Windows, l’utilisation de Rescue and Recovery pour sauvegarder vos données confidentielles, ou encore le recours à l’authentification par empreintes digitales.

Procédez comme suit pour utiliser l'assistant d'installation de Client Security :

1. A partir du bureau Windows, sélectionnez **Démarrer**, **Tous les programmes**, **ThinkVantage**, puis cliquez deux fois sur **Client Security Solution**.
2. Lorsque la fenêtre Client Security Solution s'ouvre, cliquez sur l'option de menu **Avancé**.
3. Lorsque la fenêtre Client Security Solution s'ouvre, cliquez sur **Configuration des préférences de sécurité et de sauvegarde**. L'assistant s'affiche.
4. Définissez vos préférences en matière de sécurité.
5. Exécutez l'assistant d'installation de Client Security Solution, puis cliquez sur **Terminer**. Pour plus d'informations, cliquez sur **Aide** dans l'assistant d'installation de Client Security.

Informations supplémentaires sur Client Security Solution

Pour plus de détails sur l'application Client Security Solution et ses fonctions, consultez le manuel *Client Security Solution User Guide* sur le site Web suivant :

`http://www.ibm.com/pc/support/site.wss/`

Si l'application Client Security Solution est déjà installée, vous pouvez consulter des informations plus détaillées dans le Guide d'utilisation en procédant comme suit :

1. A partir du bureau Windows, cliquez sur **Démarrer**.
2. Sélectionnez **Tous les programmes**.
3. Sélectionnez **ThinkVantage**.
4. Cliquez sur **Client Security Solution**.
5. A partir de la barre de menus Client Security Solution, cliquez sur **Aide**.
6. Cliquez sur **Guide d'utilisation**.

Kapitel 3. Deutsch

Bei Client Security handelt es sich um eine Suite von ThinkVantage™-Technologietools, die Sie dabei unterstützen, das Betriebssystem Ihres Computers und sensible Daten vor unberechtigtem Zugriff zu schützen. Client Security verbindet den Hardwareschutz, den der integrierte Chip bietet, mit den Funktionen der zugehörigen Sicherheitssoftware. Durch die Kombination von dedizierter Hardware mit dem zugehörigen Softwareschutz erweitert Client Security die Sicherheitsfunktionen des Betriebssystems Ihres Computers bedeutend.

Zielgruppe

Das vorliegende Benutzerhandbuch für ThinkVantage Client Security richtet sich an einzelne Endbenutzer und an Endbenutzer aus einem Geschäftsumfeld. Es enthält Informationen zu den folgenden Bereichen:

- Komponenten von Client Security
- Installationsvoraussetzungen für Client Security
- Funktionen von Client Security

Dieses Handbuch ergänzt die Hilfefunktion von Client Security, die schrittweise Anleitungen zum Ausführen von bestimmten Tasks mit Hilfe von Client Security bietet.

Weitere Informationen

Wenn Sie als Systemadministrator, Systementwickler, Netzadministrator oder Kundendienstmitarbeiter Client Security in einem großen Unternehmen implementieren, finden Sie ausführliche Informationen im *ThinkVantage Rescue and Recovery™ and Client Security Solution Deployment Guide* auf der folgenden Website:

`http://www.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-54502`

Komponenten von Client Security

Client Security wurde für Computer entwickelt, die mit einem integrierten Security Chip ausgestattet sind, und bietet dadurch zusätzliche Sicherheitsstufen für Ihre Computerdaten und -prozesse. Jetzt kann Client Security aber auch zum Erweitern der Sicherheit auf Computern konfiguriert werden, die über keinen integrierten Security Chip verfügen.

Client Security beinhaltet die folgenden Hardware- und Softwarekomponenten:

- **Integrierter Security Chip**

  Client Security wurde für Computer entwickelt, die mit einem integrierten Security Chip ausgestattet sind. Bei einem integrierten Security Chip handelt es sich um integrierte Verschlüsselungshardwaretechnologie, die besondere Sicherheitsfunktionen für Ihren Computer bietet. Der Security Chip ermöglicht es, dass Verschlüsselungs- und Authentifizierungsprozesse aus der anfälligen Softwareumgebung in die sichere Umgebung von dedizierter Hardware übertragen werden. Dieser Ansatz bietet eine bedeutend höhere Sicherheit.

- **Konfigurationsassistent von Client Security**

  Der Konfigurationsassistent von Client Security führt Sie durch den Prozess der Konfiguration Ihrer Sicherheitsoptionen. Der Assistent unterstützt Sie beim Aktivieren des integrierten Security Chips, beim Auswählen einer Methode für Authentifizierung und Anmeldung, beim Einrichten einer Authentifizierung über Fingerabdrücke (optional), beim Erstellen von Fragen zur Kennwortwiederherstellung und beim Konfigurieren von weiteren Komponenten von Client Security.
- **Password Manager**

  Mit dem Password Manager von Client Security können Sie Ihre sensiblen und leicht zu vergessenden Anmeldedaten für Anwendungen und Websites, wie z. B. Benutzer-IDs, Kennwörter und andere persönliche Daten, sicher und einfach verwalten. Der Password Manager von Client Security speichert alle Daten über den integrierten Security Chip, so dass der Zugriff auf Ihre Anwendungen und Websites weiterhin völlig gesichert ist.
- **PrivateDisk**

  PrivateDisk richtet ein verschlüsseltes virtuelles Plattenlaufwerk ein, das automatisch alle Daten verschlüsselt, die Sie in dem sicheren Bereich dieses ″elektronischen Safes″ speichern. Verwenden Sie zum Verschlüsseln und Speichern aller Ihrer kritischen Daten Ihr eigenes virtuelles Laufwerk. Beim Speichern von Daten auf einem PrivateDisk-Datenträger werden die Daten automatisch verschlüsselt.
- **Client Security-Anwendung**

  Die Client Security-Anwendung stellt eine einzelne Schnittstelle zur Verfügung, über die Benutzer grundlegende und erweiterte Sicherheitsfunktionen ausführen können. Hierzu zählen die Aktivierung des integrierten Security Chips, das Ändern eines Verschlüsselungstexts und das Verwenden der Software zum Lesen von Fingerabdrücken. Eine Liste aller Funktionen von Client Security finden Sie im Abschnitt „Funktionen von Client Security” auf Seite 3-4.
- **ThinkVantage-Software zum Lesen von Fingerabdrücken**

  Mit der ThinkVantage-Software zum Lesen von Fingerabdrücken können Benutzer Authentifizierung über Fingerabdrücke einrichten. Diese einfache Sicherheitsfunktion ist auf bestimmten ThinkPad- und ThinkCentre-Modellen und -Zusatzeinrichten verfügbar.

Vor dem Installieren von Client Security

Bevor Sie Client Security installieren, müssen die folgenden Voraussetzungen erfüllt sein:

- Windows XP oder Windows 2000 mit Service-Pack 3. Wenn Sie dieses Programm auf einem Festplattenlaufwerk mit mehr als 137 GB installieren, ist für Windows XP das Service-Pack 1 erforderlich.
- Internet Explorer ab Version 5.5.
- 128 MB Speicher, von denen bei der Konfiguration der Grafikkarte im BIOS höchstens 8 MB als gemeinsamer Speicher festgelegt werden dürfen.
- 800 MB freier Plattenspeicherplatz.

Wenn Sie mit einer älteren Version von Client Security oder Rescue and Recovery arbeiten, finden Sie entsprechende Anweisungen im Abschnitt „Client Security mit Rescue and Recovery verwenden” auf Seite 3-6.

Client Security einrichten

Client Security steht auf der Website `http://www.pc.ibm.com/thinkvantage` zur Verfügung. Das Herunterladen, Installieren und Konfigurieren von Client Security dauert nur ein paar Minuten.

Client Security herunterladen und installieren

Führen Sie den folgenden Installationsprozess aus, um Client Security herunterzuladen und zu installieren:

1. Starten Sie den Computer, und schließen Sie alle gestarteten Programme.
2. Rufen Sie die Website `http://www.pc.ibm.com/thinkvantage` auf.
3. Klicken Sie im Abschnitt ″Resources″ auf **Support and downloads**.
4. Blättern Sie bis zum Abschnitt ″Embedded Security Subsystem and Client Security Solution″ abwärts, und klicken Sie auf **Software download**.
5. Befolgen Sie die angezeigten Anweisungen.
6. Starten Sie die ausführbare Installationsdatei, und befolgen Sie die angezeigten Anweisungen. Sie können sich für die Installation der Komponenten ″Password Manager″ und ″PrivateDisk″ von Client Security entscheiden.
7. Nachdem Sie Ihre Auswahl getroffen haben, werden Sie aufgefordert, den Computer erneut zu starten.
8. Beim Neustart des Computers wird der Konfigurationsassistent von Client Security geöffnet. Wird der Konfigurationsassistent nicht geöffnet, finden Sie Informationen im Abschnitt „Konfigurationsassistenten von Client Security öffnen".
9. Beenden Sie den Konfigurationsassistenten von Client Security, um den Konfigurationsprozess abzuschließen.

Konfigurationsassistenten von Client Security öffnen

Gehen Sie wie folgt vor, um Client Security mit Hilfe des Konfigurationsassistenten von Client Security zu konfigurieren:

1. Klicken Sie auf dem Windows-Desktop auf **Start**, **Alle Programme**, **ThinkVantage** und anschließend doppelt auf **Client Security**.
2. Wenn das Fenster für Client Security geöffnet wird, klicken Sie auf den Menüpunkt **Erweitert**.
3. Wenn das Fenster für Client Security geöffnet wird, klicken Sie auf **Sicherheits- und Sicherungseinstellungen festlegen**. Daraufhin wird der Konfigurationsassistent von Client Security geöffnet.
4. Führen Sie die erforderlichen Schritte im Konfigurationsassistenten von Client Security aus, und klicken Sie anschließend auf **Fertig stellen**. Ausführliche Informationen erhalten Sie im Konfigurationsassistenten von Client Security, indem Sie auf **Hilfe** klicken.

Client Security verwenden

Gehen Sie wie folgt vor, um auf Client Security zuzugreifen:

1. Klicken Sie auf dem Windows-Desktop auf **Start**.
2. Wählen Sie **Alle Programme** aus.
3. Wählen Sie **ThinkVantage** aus.
4. Klicken Sie auf **Client Security**.

Funktionen von Client Security

Im Folgenden erhalten Sie ausführliche Informationen zu den verschiedenen Tasks, die mit Client Security ausgeführt werden können.

Anmerkung: Wenn einige der im Folgenden erwähnten Tools Ihnen nicht zur Verfügung stehen, könnte dies daran liegen, dass Sie nicht die richtige Software installiert haben, dass Ihr Computer die Anwendung nicht unterstützt oder dass Sie für die Anwendung eine Administratorberechtigung benötigen.

Grundlegende Funktionen

Im Folgenden erhalten Sie ausführliche Informationen zu den grundlegenden Tasks, die mit Client Security ausgeführt werden können.

Verschlüsselungstext ändern: Mit dem Tool zum Ändern des Verschlüsselungstexts können Sie einen neuen Verschlüsselungstext für Client Security erstellen. Verschlüsselungstexte müssen die Anforderungen von Client Security erfüllen.

Kennwortwiederherstellung konfigurieren: Mit dem Tool zum Konfigurieren der Kennwortwiederherstellung haben Sie die Möglichkeit, ein vergessenes Windows-Kennwort oder einen Verschlüsselungstext von Client Security wiederherzustellen (abhängig von der Authentifizierungsmethode, die Sie verwenden).

Anmeldedaten verwalten: Mit dem Password Manager können Sie Client Security für die Verwaltung Ihrer sensiblen und leicht zu vergessenden Anmeldedaten, wie z. B. Benutzer-IDs, Kennwörter und andere persönliche Daten, verwenden. Der Password Manager speichert alle Daten über den integrierten Security Chip, so dass Ihre Policy für Benutzerauthentifizierung den Zugriff auf Ihre sicheren Anwendungen und Websites steuert. Dies bedeutet, dass Sie sich nicht mehr eine Vielzahl einzelner Kennwörter merken müssen, die alle unterschiedlichen Regeln, Ablaufdaten usw. unterliegen. Sie benötigen nur noch einen Verschlüsselungstext oder Ihren Fingerabdruck, wenn Software zum Lesen von Fingerabdrücken installiert ist.

Software zum Lesen von Fingerabdrücken verwenden: Mit dem integrierten Lesegerät für Fingerabdrücke können Sie Ihren Fingerabdruck registrieren und Ihrem Startkennwort, Festplattenkennwort und Windows-Kennwort zuordnen, so dass die Kennwörter durch Authentifizierung über Fingerabdrücke ersetzt werden und der Benutzerzugriff sicherer gestaltet werden kann. Eine Tastatur mit Lesegerät für Fingerabdrücke ist für bestimmte Computer verfügbar und kann als Zusatzeinrichtung erworben werden. Diese Zusatzeinrichtung wird nur von bestimmten ThinkCentre- und ThinkPad-Computern unterstützt.

Daten schützen: Das Tool ″PrivateDisk″ richtet ein verschlüsseltes virtuelles Plattenlaufwerk ein, das automatisch alle Daten verschlüsselt, die Sie in dem sicheren Bereich dieses ″elektronischen Safes″ speichern.

Erweiterte Funktionen

Im Folgenden erhalten Sie ausführliche Informationen zu den erweiterten Tasks, die mit Client Security ausgeführt werden können.

Anmerkung: Um die folgenden Operationen ausführen zu können, müssen Sie über eine Administratorberechtigung verfügen.

Sicherheitseinstellungen überwachen: Mit dem Tool ″Security Advisor″ können Sie eine Zusammenfassung der auf dem Computer festgelegten Sicherheitseinstellungen anzeigen. Überprüfen Sie diese Einstellungen, um entweder Ihren aktuellen Sicherheitsstatus anzuzeigen oder um die Systemsicherheit zu erweitern. Zu den Sicherheitseinstellungen gehören beispielsweise Hardwarekennwörter, Windows-Benutzerkennwörter, Windows-Kennwortrichtlinien, geschützte Bildschirmschoner und gemeinsamer Dateizugriff.

Anmerkung: Der Security Advisor bietet nur eine Zusammenfassung der Sicherheitseinstellungen und Vorschläge zur Verbesserung der Systemsicherheit. Es werden nicht alle Aspekte behandelt, wie z. B. die Verwendung und Wartung von Antivirenprogrammen oder Firewalls. Für viele Einstellungen benötigen Sie eine Administratorberechtigung.

Digitale Zertifikate übertragen: Der CSS-Assistent zur Übertragung von Zertifikaten führt Sie durch die einzelnen Schritte zur Übertragung der Ihren Zertifikaten zugeordneten privaten Schlüssel vom softwarebasierten Microsoft-CSP (Cryptographic Service Provider) auf den hardwarebasierten CSS-CSP. Nach der Übertragung sind Vorgänge, bei denen die Zertifikate verwendet werden, besser gesichert, da die privaten Schlüssel durch den integrierten Security Chip geschützt werden.

Mechanismus zum Zurücksetzen des Hardwarekennworts einrichten: Dieses Tool erstellt eine sichere, von Windows unabhängige Umgebung und unterstützt Sie beim Zurücksetzen von vergessenen Start- und Festplattenkennwörtern. Ihre Identität wird über die Beantwortung einer Reihe von Fragen, die Sie zuvor erstellt haben, überprüft. Es wird empfohlen, diese sichere Umgebung so schnell wie möglich einzurichten, bevor ein Kennwort vergessen wird. Sie können ein vergessenes Hardwarekennwort erst zurücksetzen, wenn diese sichere Umgebung auf Ihrer Festplatte eingerichtet wurde und Sie sich registriert haben. Dieses Tool ist nur auf bestimmten ThinkCentre- und ThinkPad-Computern verfügbar.

Anmerkung: Es wird empfohlen, vor dem Verwenden dieses Tools ein Administratorkennwort festzulegen. Nur mit einem Administratorkennwort erreichen Sie die größtmögliche Sicherheit in der Umgebung. Nach der Durchführung dieser Prozedur stimmt Ihr Startkennwort mit dem Festplattenkennwort überein. Diese Prozedur soll Sie bei der Einrichtung dieser sicheren Umgebung und beim Zurücksetzen von vergessenen Kennwörtern, nachdem die sichere Umgebung eingerichtet wurde, unterstützen.

Integrierten Security Chip aktivieren: Dieses Tool leitet eine Änderung der BIOS-Einstellung zum Aktivieren oder Inaktivieren des integrierten Security Chips ein. Sie müssen den Computer erneut starten, damit diese Änderung wirksam wird.

Anmeldeeinstellungen ändern: Über dieses Tool werden Ihre aktuellen Anmeldeeinstellungen angezeigt. Außerdem kann ein Administrator über dieses Tool einstellen, auf welche Weise sich Benutzer beim Windows-Betriebssystem und beim Arbeitsbereich von ThinkVantage Rescue and Recovery anmelden können.

Zähler für fehlgeschlagene Versuche löschen: Mit diesem Tool wird der Zähler für fehlgeschlagene Authentifizierungsversuche zurückgesetzt, der die Anzahl der fehlgeschlagenen Authentifizierungsversuche beim integrierten Security Chip überwacht. Nach einer bestimmten Anzahl an fehlgeschlagenen Versuchen sperrt sich der Chip für einen bestimmten Zeitraum selbst. Bei weiteren fehlgeschlagenen Versuchen verlängert sich dieser Zeitraum.

Sicherheits- und Sicherungseinstellungen festlegen: Mit dem Konfigurationsassistenten von Client Security können Sie eine Vielzahl an Sicherheitssoftwaretools konfigurieren. Dieser Assistent bietet Konfigurationsoptionen, mit denen Sie eine Reihe von Sicherheitsfunktionen festlegen können, wie z. B. die Aktivierung des integrierten Security Chips von Client Security, die Auswahl, wie Sie sich in der Windows-Umgebung authentifizieren möchten, die Verwendung von Rescue and Recovery zum Sichern Ihrer sensiblen Daten oder die Möglichkeit der Authentifizierung über Fingerabdrücke.

Client Security mit Rescue and Recovery verwenden

Sowohl bei Rescue and Recovery als auch bei Client Security handelt es sich um ThinkVantage-Technologien, die speziell für Ihre Bedürfnisse entwickelt wurden. Je nach Ihren Erfordernissen können sie separat oder zusammen ausgeführt werden. Die folgenden Informationen sollen Sie bei der Entwicklung Ihrer eigenen Strategie für die Verwendung dieser Programme unterstützen und Ihnen zeigen, wie sich diese beiden Programme gegenseitig ergänzen.

Es gibt einige wichtige Aspekte, die bei der Installation von Rescue and Recovery und von Client Security bzw. von beiden Programmen zusammen zu beachten sind. In den folgenden Tabellen finden Sie Informationen, die Sie bei der Entscheidung unterstützen sollen, welche Prozedur für Ihre gewünschte Konfiguration die richtige ist.

Tabelle 3-1. Die folgende Tabelle enthält Informationen, mit deren Hilfe Sie Ihre Konfiguration von Rescue and Recovery und Client Security ändern können. "Client Security (Standalone)" bedeutet, dass das Installationspaket vom Web oder von CD installiert wurde.

Installierte Software	Gewünschte Software	Gehen Sie wie folgt vor	Kommentare
Client Security 5.4x	Client Security 5.4x und Rescue and Recovery 3.0	1. Installieren Sie Rescue and Recovery 3.0. 2. Geben Sie bei entsprechender Aufforderung an, dass Sie die Installation von Client Security 5.4x beibehalten möchten.	Sicherungen können nicht über Client Security 5.4x geschützt werden. Außerdem erfolgt die Verwendung von Funktionen von Client Security durch Rescue and Recovery 3.0 über eine emulierte Version von Client Security. Die Hauptkennwortfunktion wird zu Ihren Sicherheitseinstellungen hinzugefügt. Ein Hauptkennwort wird gewöhnlich in einer Unternehmensumgebung verwendet. Weitere Informationen finden Sie im Abschnitt „Weitere Informationen" auf Seite 3-1.

Tabelle 3-1. Die folgende Tabelle enthält Informationen, mit deren Hilfe Sie Ihre Konfiguration von Rescue and Recovery und Client Security ändern können. "Client Security (Standalone)" bedeutet, dass das Installationspaket vom Web oder von CD installiert wurde. (Forts.)

Installierte Software	Gewünschte Software	Gehen Sie wie folgt vor	Kommentare
Client Security 5.4x	Client Security 6.0 (Standalone-Installationspaket)	1. Deinstallieren Sie Client Security 5.4x. 2. Installieren Sie Client Security 6.0 (Standalone).	• Sie müssen vor der Deinstallation alle verschlüsselten Dateien entschlüsseln und alle Password Manager-Daten exportieren. Andernfalls gehen diese Daten verloren. • Sie müssen vor der Installation von Client Security das IBM® Dienstprogramm für die Verschlüsselung von Dateien und Ordnern (IBM FFE, IBM File and Folder Encryption) deinstallieren.
Client Security 5.4x	Client Security 6.0 und Rescue and Recovery 3.0	1. Deinstallieren Sie Client Security 5.4x. 2. Installieren Sie Rescue and Recovery 3.0. (Stellen Sie sicher, dass die Komponente für Client Security 6.0 ausgewählt ist.)	• Die Installation von Rescue and Recovery 3.0 über Client Security 5.4x, ohne zuvor Client Security deinstalliert zu haben, führt dazu, dass anschließend nur Rescue and Recovery installiert ist. • Sie müssen vor der Deinstallation von Client Security 5.4x alle verschlüsselten Dateien entschlüsseln und alle Password Manager-Daten exportieren. Andernfalls gehen diese Daten verloren. • Sie müssen vor der Installation von Client Security 6.0 das IBM Dienstprogramm für die Verschlüsselung von Dateien und Ordnern (IBM FFE, IBM File and Folder Encryption) deinstallieren.

Tabelle 3-1. Die folgende Tabelle enthält Informationen, mit deren Hilfe Sie Ihre Konfiguration von Rescue and Recovery und Client Security ändern können. "Client Security (Standalone)" bedeutet, dass das Installationspaket vom Web oder von CD installiert wurde. (Forts.)

Installierte Software	Gewünschte Software	Gehen Sie wie folgt vor	Kommentare
Rescue and Recovery 3.0	Client Security 5.4x und Rescue and Recovery 3.0	1. Deinstallieren Sie Rescue and Recovery 3.0. 2. Installieren Sie Client Security 5.4x. 3. Installieren Sie Rescue and Recovery 3.0. 4. Geben Sie bei entsprechender Aufforderung an, dass Sie die Installation von Client Security 5.4x beibehalten möchten.	• Client Security 5.4x kann nicht über Rescue and Recovery 3.0 installiert werden. • Lokale Sicherungen werden bei der Deinstallation von Rescue and Recovery 3.0 gelöscht.
Rescue and Recovery 3.0	Client Security 6.0 (Standalone-Installationspaket)	1. Deinstallieren Sie Rescue and Recovery 3.0. 2. Installieren Sie Client Security 6.0 (Standalone).	• Durch die Deinstallation von Rescue and Recovery werden alle Benutzerdateien und Registry-Einstellungen von Client Security gelöscht. • Auf Sicherungen von Rescue and Recovery, die von Client Security geschützt werden, kann nicht mehr zugegriffen werden. • Lokale Sicherungen werden bei der Deinstallation von Rescue and Recovery 3.0 gelöscht. • Client Security 6.0 (Standalone) kann nicht über Rescue and Recovery 3.0 installiert werden.

Tabelle 3-1. Die folgende Tabelle enthält Informationen, mit deren Hilfe Sie Ihre Konfiguration von Rescue and Recovery und Client Security ändern können. "Client Security (Standalone)" bedeutet, dass das Installationspaket vom Web oder von CD installiert wurde. (Forts.)

Installierte Software	Gewünschte Software	Gehen Sie wie folgt vor	Kommentare
Rescue and Recovery 3.0	Rescue and Recovery 3.0 und Client Security 6.0	1. Wählen Sie unter der Option zum Hinzufügen/Entfernen von Programmen die Option zum Ändern aus. 2. Führen Sie die Änderungen aus, indem Sie Client Security und alle gewünschten Unterkomponenten hinzufügen.	• Lokale Sicherungen werden beim Hinzufügen von Client Security gelöscht. • Erstellen Sie nach dem Hinzufügen von Client Security so schnell wie möglich eine neue Basissicherung. • Einstellungen und Datendateien von Client Security werden gelöscht. • Client Security 6.0 (Standalone) kann nicht über Rescue and Recovery 3.0 installiert werden.
Client Security 6.0 (Standalone-Installationspaket)	Client Security 5.4x	1. Deinstallieren Sie Client Security 6.0 (Standalone). 2. Installieren Sie Client Security 5.4x.	• Das Löschen der Datendateien und Einstellungen von Client Security 6.0 bei entsprechender Aufforderung hat keine Auswirkungen auf die Funktionen von Client Security 5.4x.
Client Security 6.0 (Standalone-Installationspaket)	Rescue and Recovery 3.0	1. Deinstallieren Sie Client Security 6.0. 2. Installieren Sie Rescue and Recovery 3.0. 3. Wählen Sie während der Installation aus, dass Sie nur Rescue and Recovery installieren möchten.	Sie müssen bei der Deinstallation von Client Security 6.0 die Dateien und Einstellungen von Client Security 6.0 bei entsprechender Aufforderung löschen. Andernfalls wird die Installation von Rescue and Recovery 3.0 abgebrochen.
Client Security 6.0 (Standalone)	Rescue and Recovery 3.0 und Client Security 6.0	1. Installieren Sie Rescue and Recovery 3.0. 2. Wählen Sie alle Unterkomponenten von Client Security 6.0 aus, die Sie installieren möchten.	• Datendateien und Einstellungen von Client Security 6.0 bleiben erhalten. • Verwenden Sie Rescue and Recovery, um festzulegen, dass Sicherungen mit Client Security 6.0 geschützt werden sollen.

Tabelle 3-1. Die folgende Tabelle enthält Informationen, mit deren Hilfe Sie Ihre Konfiguration von Rescue and Recovery und Client Security ändern können. "Client Security (Standalone)" bedeutet, dass das Installationspaket vom Web oder von CD installiert wurde. (Forts.)

Installierte Software	Gewünschte Software	Gehen Sie wie folgt vor	Kommentare
Rescue and Recovery 3.0 und Client Security 6.0	Client Security 5.4x	1. Deinstallieren Sie Rescue and Recovery und Client Security. 2. Installieren Sie Client Security 5.4x.	• Client Security 5.4x kann nicht über Client Security 6.0 installiert werden. • Das Löschen der Datendateien und Einstellungen bei entsprechender Aufforderung hat keine Auswirkungen auf die Funktionen von Client Security 5.4x. • Bei der Deinstallation von Rescue and Recovery 3.0 wird Client Security 6.0 automatisch deinstalliert.
Rescue and Recovery 3.0 und Client Security 6.0	Rescue and Recovery 3.0	1. Wählen Sie unter der Option zum Hinzufügen/Entfernen von Programmen die Option zum Ändern aus. 2. Entfernen Sie Client Security 6.0.	• Lokale Sicherungen werden beim Entfernen von Client Security 6.0 gelöscht. • Nach der Deinstallation von Client Security 6.0 sind der Password Manager und PrivateDisk nicht mehr verfügbar. • Auf die Sicherungen von Rescue and Recovery 3.0, die durch Client Security 6.0 geschützt werden, kann nicht mehr zugegriffen werden. Erstellen Sie so bald wie möglich eine neue Sicherung.
Rescue and Recovery 3.0 und Client Security 6.0	Client Security Solution 6.0	1. Deinstallieren Sie Rescue and Recovery 3.0. 2. Wählen Sie bei entsprechender Aufforderung nur dann die Option zum Beibehalten der aktuellen Einstellung von Client Security 6.0 aus, wenn Sie die aktuelle Sicherheitskonfiguration beibehalten möchten. 3. Installieren Sie Client Security 6.0 (Standalone).	1. Auf die Sicherungen von Rescue and Recovery 3.0, die durch Client Security 6.0 geschützt werden, kann nicht mehr zugegriffen werden. 2. Lokale Sicherungen werden bei der Deinstallation von Rescue and Recovery 3.0 gelöscht.

Kennwörter und Verschlüsselungstexte von Rescue and Recovery

Sie können für den Schutz des Arbeitsbereichs von Rescue and Recovery Kennwörter oder Verschlüsselungstexte verwenden und dadurch kritische Daten vor unberechtigtem Zugriff schützen. Sie können den Arbeitsbereich von Rescue and Recovery schützen, indem Sie über den Konfigurationsassistenten von Client Security Sicherheitseinstellungen festlegen oder indem Sie über Client Security Ihre Anmeldeeinstellungen ändern. Über Client Security können Sie auch Optionen zur Kennwortwiederherstellung innerhalb des Arbeitsbereichs von Rescue and Recovery erstellen.

Anmerkungen:

1. Diese Funktion ist nur verfügbar, wenn Client Security 6.0 installiert ist. Wenn Sie diese Funktion verwenden möchten, führen Sie den Konfigurationsassistenten von Client Security 6.0 aus, und geben Sie an, dass Sie bei der Anmeldung am Computer entweder ein Kennwort oder einen Verschlüsselungstext verwenden möchten.
2. Sowohl auf den Konfigurationsassistenten von Client Security 6.0 als auch auf Client Security 6.0 kann nur von der Windows-Umgebung aus zugegriffen werden. Wenn Sie sich für die Verwendung von Rescue and Recovery ohne Client Security entscheiden, wird der Arbeitsbereich von Rescue and Recovery nicht durch ein Kennwort oder einen Verschlüsselungstext geschützt.
3. Über Client Security können Sie Optionen zur Kennwortwiederherstellung innerhalb des Arbeitsbereichs von Rescue and Recovery erstellen.

Verwenden Sie die folgenden Methoden, um den Arbeitsbereich von Rescue and Recovery durch ein Kennwort oder einen Verschlüsselungstext zu schützen.

Methode 1: Wenn Sie den Konfigurationsassistenten von Client Security nicht ausführen, gehen Sie wie folgt vor, um den Arbeitsbereich von Rescue and Recovery mit einem Kennwort oder einem Verschlüsselungstext zu schützen:

1. Klicken Sie auf dem Windows-Desktop auf **Start**, **Alle Programme**, **ThinkVantage** und anschließend doppelt auf **Client Security**.
2. Wenn das Fenster für Client Security geöffnet wird, klicken Sie auf den Menüpunkt **Erweitert**.
3. Klicken Sie auf das Symbol **Sicherheits- und Sicherungseinstellungen festlegen**. Daraufhin wird der Konfigurationsassistent von Client Security geöffnet.
4. Legen Sie Ihre Sicherheitseinstellungen fest. Wählen Sie bei Aufforderung eine der folgenden Optionen aus:
   - Wenn Sie den Arbeitsbereich von Rescue and Recovery mit dem Windows-Anmeldekennwort schützen möchten, aktivieren Sie das Markierungsfeld **Windows-Kennwort für den Zugriff auf den Arbeitsbereich von Rescue and Recovery verwenden**.
   - Wenn Sie den Arbeitsbereich von Rescue and Recovery mit dem Anmeldeverschlüsselungstext von Client Security schützen möchten, aktivieren Sie das Markierungsfeld **CSS-Verschlüsselungstext für den Zugriff auf den Arbeitsbereich von Rescue and Recovery verwenden**.
5. Führen Sie die erforderlichen Schritte im Konfigurationsassistenten von Client Security aus, und klicken Sie anschließend auf **Fertig stellen**. Weitere Informationen erhalten Sie im Konfigurationsassistenten von Client Security, indem Sie auf **Hilfe** klicken.

Methode 2: Wenn Sie den Konfigurationsassistenten von Client Security ausführen, gehen Sie wie folgt vor, um den Arbeitsbereich von Rescue and Recovery mit einem Kennwort oder einem Verschlüsselungstext zu schützen:

1. Klicken Sie auf dem Windows-Desktop auf **Start**, **Alle Programme**, **ThinkVantage** und anschließend doppelt auf **Client Security**.
2. Wenn das Fenster für Client Security geöffnet wird, klicken Sie auf den Menüpunkt **Erweitert**.
3. Klicken Sie auf **Anmeldeeinstellungen ändern**.
4. Befolgen Sie die angezeigten Anweisungen. Ausführliche Informationen erhalten Sie in Client Security, indem Sie auf **Hilfe** klicken.

Sicherungseinstellungen mit dem Konfigurationsassistenten von Client Security festlegen

Der Konfigurationsassistent von Client Security bietet Konfigurationsoptionen, mit denen Sie eine Reihe von Sicherheitsfunktionen festlegen können, wie z. B. die Aktivierung des integrierten Security Chips, die Auswahl, wie Sie sich in der Windows-Umgebung authentifizieren möchten, die Verwendung von Rescue and Recovery zum Sichern Ihrer sensiblen Daten oder die Möglichkeit der Authentifizierung über Fingerabdrücke.

Gehen Sie wie folgt vor, um den Konfigurationsassistenten von Client Security zu verwenden:

1. Klicken Sie auf dem Windows-Desktop auf **Start**, **Alle Programme**, **ThinkVantage** und anschließend doppelt auf **Client Security**.
2. Wenn das Fenster für Client Security geöffnet wird, klicken Sie auf den Menüpunkt **Erweitert**.
3. Wenn das Fenster für Client Security geöffnet wird, klicken Sie auf **Sicherheits- und Sicherungseinstellungen festlegen**. Daraufhin wird der Konfigurationsassistent von Client Security geöffnet.
4. Legen Sie Ihre Sicherheitseinstellungen fest.
5. Führen Sie die erforderlichen Schritte im Konfigurationsassistenten von Client Security aus, und klicken Sie anschließend auf **Fertig stellen**. Ausführliche Informationen erhalten Sie im Konfigurationsassistenten von Client Security, indem Sie auf **Hilfe** klicken.

Weitere Informationen zu Client Security

Ausführliche Informationen zu Client Security und den zugehörigen Funktionen finden Sie im Benutzerhandbuch zu Client Security im Internet unter der Adresse:

`http://www.ibm.com/pc/support/site.wss/`

Wenn Sie Client Security bereits installiert haben, finden Sie ausführlichere Informationen im Benutzerhandbuch, indem Sie wie folgt vorgehen:

1. Klicken Sie auf dem Windows-Desktop auf **Start**.
2. Wählen Sie **Alle Programme** aus.
3. Wählen Sie **ThinkVantage** aus.
4. Klicken Sie auf **Client Security**.
5. Klicken Sie in der Menüleiste von Client Security auf **Hilfe**.
6. Klicken Sie auf die Option für das Benutzerhandbuch.

Capitolo 4. Italiano

L'applicazione CSS (Client Security Solution) è una suite di strumenti ThinkVantage™ Technology designati per proteggere l'accesso ai dati sensibili e al sistema operativo del computer. L'applicazione CSS (Client Security Solution) integra la protezione dell'hardware del proprio chip integrato con la protezione fornita dal software di protezione. Mediante l'associazione dell'hardware dedicato con la protezione del software, l'applicazione CSS (Client Security Solution) migliora le funzioni di sicurezza integrate nel sistema operativo del computer.

A chi è rivolta questa guida

La pubblicazione *ThinkVantage Client Security Solution -Guida per l'utente* è intesa i singoli utenti e per gli utenti che operano all'interno di un ambiente aziendale. Questa guida fornisce le informazioni sulle seguenti aree:

- Componenti di CSS (Client Security Solution)
- Considerazioni sull'installazione di CSS (Client Security Solution)
- Funzioni di CSS (Client Security Solution)

Questa guida integra il sistema di aiuto di CSS (Client Security Solution), che fornisce le istruzioni dettagliate su come eseguire le attività specifiche all'interno del programma.

Informazioni aggiuntive

Se l'utente è un amministratore del sistema, un ingegnere, un amministratore di rete che cerca di implementare CSS (Client Security Solution) in un'impresa di grandi dimensioni, è possibile ottenere le informazioni dettagliate consultando la pubblicazione *ThinkVantage Rescue and Recovery™ and Client Security Solution Deployment Guide* situata presso il seguente sito Web:

`http://www.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-54502`

Componenti di CSS (Client Security Solution)

L'applicazione CSS (Client Security Solution) è designata per i computer forniti con un Security Chip integrato, che consente di fornire ulteriori livelli di sicurezza ai dati e ai processi del computer. Tuttavia, il software CSS (Client Security Solution) può essere configurato per migliorare la sicurezza dei computer che non sono forniti con un Security Chip.

CSS (Client Security Solution) viene suddiviso nei seguenti componenti hardware e software.

- **Security Chip integrato**

  L'applicazione CSS (Client Security Solution) è designata per i computer forniti con un Security Chip integrato. Un Security Chip integrato è una tecnologia hardware di codifica integrata che fornisce un livello aggiuntivo di sicurezza al computer. Security Chip consente la codifica e il trasferimento dei processi di autenticazione dal software vulnerabile all'ambiente protetto dell'hardware dedicato. La sicurezza aumentata fornita è tangibile.
- **Installazione guidata di Client Security**

  L'installazione guidata di Client Security consente di assistere l'utente durante il processo di configurazione delle opzioni di sicurezza. La procedura guidata consente di abilitare Security Chip integrato, selezionare un'autenticazione e il metodo di accesso, creare le domande per il ripristino della password, stabilire l'autenticazione delle impronte digitali (facoltativo) e configurare ulteriori componenti di CSS (Client Security Solution).

- **Password Manager**

  Client Security Password Manager consente di gestire in maniera sicura le applicazioni sensibili e facili da dimenticare e le informazioni di accesso sul sito Web, quali gli ID utente, le password e le altre informazioni personali. Client Security Password Manager memorizza tutte le informazioni mediante Security Chip integrato in modo tale che l'accesso alle applicazioni e ai siti Web resti completamente protetto.
- **PrivateDisk**

  PrivateDisk imposta un'unità disco fisso virtuale codificata che codifica automaticamente i dati memorizzati nella ″sicurezza elettronica″. Utilizzare l'unità virtuale per codificare e memorizzare i dati critici. I dati sono codificati automaticamente quando sono memorizzati nel volume PrivateDisk.
- **Applicazione CSS (Client Security Solution)**

  L'applicazione CSS (Client Security Solution) fornisce una singola interfaccia che consente di effettuare le funzioni di sicurezza avanzate e di base, quali l'abilitazione di Security Chip integrato, la modifica di passphrase o l'utilizzo del software delle impronte digitali. Per un elenco delle funzioni di CSS (Client Security Solution) complete, consultare "Funzioni di CSS (Client Security Solution)" a pagina 4-3
- **Software delle impronte digitali ThinkVantage**

  Il software delle impronte digitali ThinkVantage consente agli utenti di stabilire l'autenticazione delle impronte digitali. Questa funzione di sicurezza conveniente è disponibile su opzioni e modelli di ThinkPad e ThinkCentre scelti.

Prima di installare CSS (Client Security Solution)

Prima di installare l'applicazione CSS (Client Security Solution), è importante che i seguenti prerequisiti siano soddisfatti:

- Windows XP o Windows 2000 con Service Pack 3. Se si installa questo programma su un'unità disco fisso con capacità superiore a 137 GB, Service Pack 1 viene richiesto per Windows XP.
- Internet Explorer 5.5 (o successive).
- 128 MB di memoria di cui non è possibile designare più di 8 MB come memoria condivisa nell'installazione video nel BIOS.
- 800 MB di spazio su disco disponibile.

Se si dispone di una versione precedente di CSS (Client Security Solution), Client Security Software o Rescue and Recovery, consultare "Utilizzo di Client Security Solution con Rescue and Recovery" a pagina 4-5 per le istruzioni specifiche.

Impostazione di CSS (Client Security Solution)

L'applicazione CSS (Client Security Solution) è disponibile sul sito Web `http://www.pc.ibm.com/thinkvantage`. Il download, l'installazione e la configurazione di CSS (Client Security Solution) possono essere eseguite in pochi minuti.

Download e installazione di CSS (Client Security Solution)

Completare la seguente installazione per scaricare e installare il programma CSS (Client Security Solution):

1. Avviare il computer e chiudere qualsiasi programma aperto.
2. Andare al sito Web `http://www.pc.ibm.com/thinkvantage`.
3. Fare clic sul collegamento **Support and downloads** nella sezione Resources.
4. Scorrere la sezione Embedded Security Subsystem e Client Security Solution e fare clic su **Software download**.
5. Seguire le istruzioni visualizzate.
6. Eseguire il file eseguibile di installazione e seguire le istruzioni visualizzate. Sarà fornita l'opzione per installare i componenti Password Manager e PrivateDisk di CSS (Client Security Solution).
7. Una volta apportate le selezioni, sarà richiesto il riavvio del computer.
8. Al riavvio del computer, viene visualizzata l'installazione guidata di Client Security. Se l'installazione guidata non viene avviata, consultare "Avvio dell'installazione guidata di Client Security"
9. Completare l'installazione guidata di Client Security per completare il processo di configurazione.

Avvio dell'installazione guidata di Client Security

Completare la seguente procedura per configurare il programma Client Security Solution utilizzando l'installazione guidata di Client Security:

1. Dal desktop di Windows, fare clic su **Start**, **Tutti i programmi**, selezionare **ThinkVantage** e quindi fare doppio clic su **Client Security Solution**.
2. Quando viene avviato Client Security Solution, fare clic sulla voce di menu **Avanzate**.
3. Quando viene avviato Client Security Solution, fare clic su **Imposta preferenze di sicurezza e backup**. Viene avviata l'installazione guidata di Client Security.
4. Completare l'installazione guidata di Client Security Solution e quindi fare clic su **Fine**. Per le informazioni dettagliate, fare clic su **?** all'interno dell'installazione guidata di Client Security.

Utilizzo di CSS (Client Security Solution)

Completare la seguente procedura per accedere all'applicazione CSS (Client Security Solution):

1. Dal desktop di Windows, fare clic su **Start**.
2. Selezionare **Tutti i programmi**.
3. Selezionare **ThinkVantage**.
4. Fare clic su **Client Security Solution**.

Funzioni di CSS (Client Security Solution)

Le seguenti informazioni descrivono in maniera dettagliata le varie attività che possono essere fornite utilizzando l'applicazione CSS (Client Security Solution).

Nota: Se alcuni strumenti menzionati di seguito non sono disponibili,è possibile che non sia installato il software appropriato, il computer non supporta l'applicazione o l'applicazione richiede l'accesso del responsabile o dell'amministratore.

Funzioni di base

Le seguenti informazioni descrivono in maniera dettagliata le attività di base che possono essere fornite utilizzando l'applicazione CSS (Client Security Solution).

Modifica di una passphrase: Lo strumento di modifica di passphrase consente di stabilire una nuova passphrase di Client Security. Le passphrase devono aderire ai requisiti della passphrase di Client Security.

Configurazione del ripristino della password: Lo strumento per la configurazione del ripristino di password consente di stabilire un supporto per ripristinare una password di Windows dimenticata o una passphrase di Client Security, a seconda della metodologia di autenticazione in uso.

Gestione delle informazioni di accesso: L'applicazione Password Manager consente di utilizzare Client Security Solution per gestire le informazioni di accesso sensibili e facili da dimenticare, quali gli ID utente, le password e le altre informazioni personali. L'applicazione Password Manager memorizza tutte le informazioni mediante Security Chip integrato in modo tale che i criteri di protezione di autenticazione dell'utente controllano l'accesso alle applicazioni sicure e ai siti Web. Ciò significa che piuttosto che dover ricordare e fornire una pletora si singole password-- tutte soggette a diverse regole e date di scadenza-- è necessario ricordare solo una passphrase o, quando il software delle impronte digitali viene installato, fornire le impronte digitali.

Utilizzo del software delle impronte digitali: Il lettore per le impronte digitali integrato consente di registrare e associare le impronte digitali con una password di accensione, password del disco fisso ed una password di Windows in modo tale che l'autenticazione delle impronte digitali può sostituire le password e consentire un accesso utente semplice e sicuro. Una tastiera del lettore per le impronte digitali è disponibile su computer scelti e può essere acquistata come opzione. Questa opzione è supportata solo su computer scelti ThinkCentre e ThinkPad.

Protezione dei dati: Lo strumento PrivateDisk genera un'unità disco fisso virtuale codificata, che codifica automaticamente i dati e li memorizza all'interno della ″sicurezza elettronica″.

Funzioni avanzate

Le seguenti informazioni descrivono in maniera dettagliata le attività avanzate che possono essere fornite utilizzando l'applicazione CSS (Client Security Solution).

Nota: È necessario disporre dei diritti dell'amministratore per effettuare le seguenti operazioni.

Controllo delle impostazioni di sicurezza: Lo strumento Security Advisor consente di visualizzare un riepilogo delle impostazioni di sicurezza impostate sul computer. Consultare queste impostazioni per visualizzare lo stato di sicurezza corrente o per migliorare la sicurezza del sistema. Alcune sezioni di sicurezza incluse sono le password hardware, password degli utenti di Windows, i criteri di protezione della password di Windows, screen saver protetti e la condivisione di file.

Nota: Lo strumento di Security Advisor fornisce solo un riepilogo delle impostazioni di sicurezza e i consigli per migliorare la sicurezza del sistema. Solo alcuni aspetti di sicurezza sono indirizzati, quali l'utilizzo e la manutenzione di programmi antivirus e firewall. Molte impostazioni richiedono l'accesso del responsabile o dell'amministratore.

Trasferimento di certificati digitali: Il trasferimento guidato dei certificati di Client Security assiste l'utente durante il processo di trasferimento delle chiavi private associate ai certificati da CSP (cryptographic service provider) della Microsoft basato su software al CSP di CSS (Client Security Solution) basato sull'hardware. In seguito al trasferimento, le operazioni che utilizzano i certificati sono più sicure poiché le chiavi private sono protette da Security Chip integrato.

Definizione di un meccanismo di reimpostazione della password hardware: Questo strumento crea un ambiente protetto che viene eseguito in maniera indipendente da Windows e consente di reimpostare le password dell'unità disco fisso e di accensione dimenticate. L'identità è stabilita rispondendo ad una serie di domande create. È preferibile creare questo ambiente protetto, prima che sia dimenticata una password. Non è possibile reimpostare una password hardware dimenticata fino a quando questo ambiente protetto non viene creato sull'unità disco fisso e in seguito alla registrazione. Questo strumento è disponibile solo su computer ThinkCentre e ThinkPad scelti.

Nota: È preferibile impostare una password dell'amministratore o del responsabile prima di utilizzare questo strumento. Se non è stata impostata una password del responsabile o dell'amministratore, l'ambiente non sarà sicuro. Una volta completata questa procedura, la password di accensione e quella dell'unità disco fisso corrisponderanno. Questa procedura è designata per completare l'attività di creazione dell'ambiente protetto e per reimpostare le password dimenticate in seguito alla creazione dell'ambiente protetto.

Attivazione di Security Chip integrato: Questo strumento avvia una modifica di impostazione del BIOS utilizzata per attivare o disattivare Security Chip integrato. È necessario riavviare il computer per rendere effettiva questa modifica.

Modifica delle impostazioni di accesso: Questo strumento visualizza le impostazioni di accesso correnti e consente ad un amministratore di modificare l'accesso degli utenti al sistema operativo Windows e a ThinkVantage Rescue and Recovery workspace.

Eliminazione del contatore protetto: Questo strumento reimposta il contatore protetto di autenticazione che controlla quanti tentativi di autenticazione errati sono stati trasferiti a Security Chip integrato. Dopo un determinato numero di tentativi non riusciti, il chip si blocca per un intervallo di tempo. L'intervallo di tempo del blocco aumenta con i continui tentativi non riusciti.

Impostazione delle preferenze di sicurezza e di backup: L'installazione guidata di Client Security consente di configurare una varietà di strumenti per il software di sicurezza. Questa procedura guidata fornisce le opzioni di configurazione che consentono di impostare una varietà di funzioni di sicurezza, quali l'abilitazione di Security Chip integrato di Client Security, la selezione di autenticazione sull'ambiente Windows, la scelta di utilizzare Rescue and Recovery per eseguire il backup dei dati sensibili o la scelta di utilizzare l'autenticazione delle impronte digitali.

Utilizzo di Client Security Solution con Rescue and Recovery

Il programma Rescue and Recovery e l'applicazione CSS (Client Security Solution) sono tecnologie ThinkVantage sviluppate. Ossia, sono designate per operare insieme o separatamente, a seconda delle esigenze. Le seguenti informazioni sono intese per designare la strategia per utilizzare questi programmi e per evidenziare come questi programmi migliorano gli altri.

Sono presenti importanti considerazioni da intraprendere nell'account quando si installa il programma Rescue and Recovery, l'applicazione Client Security Solution o entrambi. Le seguenti tabelle forniscono le informazioni per determinare la corretta procedura per la configurazione desiderata:

Tabella 1-1. La seguente tabella fornisce le informazioni per modificare la configurazione di Rescue and Recovery e Client Security. Client Security Solution standalone significa che il pacchetto di installazione è stato acquistato dal Web o dal CD.

Il software installato è...	**E si desidera...**	**Seguire questo processo**	**Commenti**
Client Security Software 5.4x	Client Security Software 5.4x e Rescue and Recovery 3.0	1. Installare il programma Rescue and Recovery 3.0. 2. Alla richiesta, indicare che si desidera conservare l'applicazione Client Security Software 5.4x installata.	I backup non possono essere protetti utilizzando l'applicazione Client Security Software 5.4x e qualsiasi utilizzo delle funzioni di Client Security Software dal programma Rescue and Recovery 3.0 sarà eseguito mediante una versione emulata di Client Security Software. La funzione della password principale viene aggiunta alle funzioni di sicurezza. Di solito, una password principale viene utilizzata in un ambiente aziendale. Per ulteriori informazioni, consultare "Informazioni aggiuntive" a pagina 4-1
Client Security Software 5.4x	Pacchetto di installazione Client Security Solution 6.0 Standalone	1. Disinstallare l'applicazione Client Security Software 5.4x. 2. Installare l'applicazione Client Security Solution 6.0 (Standalone).	• È necessario decodificare qualsiasi file codificato ed esportare le informazioni di Password Manager prima della disinstallazione. Diversamente, queste informazioni andranno perdute. • È necessario disinstallare il software IBM® File and Folder Encryption prima di installare l'applicazione Client Security Solution.

Tabella 1-1. La seguente tabella fornisce le informazioni per modificare la configurazione di Rescue and Recovery e Client Security. Client Security Solution standalone significa che il pacchetto di installazione è stato acquistato dal Web o dal CD. (Continua)

Il software installato è...	**E si desidera...**	**Seguire questo processo**	**Commenti**
Client Security Software 5.4x	Client Security Solution 6.0 e Rescue and Recovery 3.0	1. Disinstallare l'applicazione Client Security Software 5.4x. 2. Installare il programma Rescue and Recovery 3.0. (Verificare che il componente Client Security Solution 6.0 sia stato selezionato.)	• L'installazione di Rescue and Recovery 3.0 in Client Security Software 5.4x senza disinstallare prima Client Security Software risulta solo in Rescue and Recovery. • Prima di disinstallare l'applicazione Client Security Software 5.4x, è necessario decodificare i file codificati ed esportare le informazioni di Password Manager prima della disinstallazione. Diversamente, queste informazioni andranno perdute. • È necessario disinstallare il software IBM File and Folder Encryption prima di installare l'applicazione Client Security Solution 6.0.
Rescue and Recovery 3.0	Client Security Software 5.4x e Rescue and Recovery 3.0	1. Disinstallare il programma Rescue and Recovery 3.0. 2. Installare l'applicazione Client Security Software 5.4x. 3. Installare il programma Rescue and Recovery 3.0. 4. Alla richiesta, indicare che si desidera conservare l'applicazione Client Security Software 5.4x installata.	• L'applicazione Client Security Software 5.4x non può essere installata sul programma Rescue and Recovery 3.0. • I backup locali sono eliminati quando viene disinstallato il programma Rescue and Recovery 3.0.

Tabella 1-1. La seguente tabella fornisce le informazioni per modificare la configurazione di Rescue and Recovery e Client Security. Client Security Solution standalone significa che il pacchetto di installazione è stato acquistato dal Web o dal CD. (Continua)

Il software installato è...	E si desidera...	Seguire questo processo	Commenti
Rescue and Recovery 3.0	Pacchetto di installazione Client Security Solution 6.0 Standalone	1. Disinstallare il programma Rescue and Recovery 3.0. 2. Installare l'applicazione Client Security Solution 6.0 (Standalone).	• Disinstallazione Rescue and Recovery elimina i file dell'utente e le impostazioni di registro di Client Security Solution. • I backup Rescue and Recovery protetti da Client Security Solution non sono più accessibili. • I backup locali sono eliminati durante la disinstallazione di Rescue and Recovery 3.0. • Client Security Solution 6.0 (Standalone) non può essere installato su Rescue and Recovery 3.0.
Rescue and Recovery 3.0	Rescue and Recovery 3.0 e Client Security Solution 6.0	1. Selezionare l'opzione **Modifica** dall'Installazione applicazioni. 2. Completare l'operazione di modifica aggiungendo l'applicazione Client Security Solution e qualsiasi componente secondario desiderato.	• I backup locali sono eliminati quando viene aggiunta l'applicazione Client Security Solution. • Una volta aggiunta l'applicazione Client Security Solution, creare un nuovo backup di base. • I file di dati e le impostazioni di Client Security Solution sono eliminati. • L'applicazione Client Security Solution 6.0 (Standalone) non può essere installata sul programma Rescue and Recovery 3.0.
Pacchetto di installazione Client Security Solution 6.0 Standalone	Client Security Software 5.4x	1. Disinstallare l'applicazione Client Security Solution 6.0 (Standalone). 2. Installare l'applicazione Client Security Software 5.4x.	• L'eliminazione delle impostazioni e dei file di dati di Client Security Solution 6.0 nel prompt non influenza le operazioni di Client Security Software 5.4x.

Tabella 1-1. La seguente tabella fornisce le informazioni per modificare la configurazione di Rescue and Recovery e Client Security. Client Security Solution standalone significa che il pacchetto di installazione è stato acquistato dal Web o dal CD. (Continua)

Il software installato è...	**E si desidera...**	**Seguire questo processo**	**Commenti**
Pacchetto di installazione Client Security Solution 6.0 Standalone	Rescue and Recovery 3.0	1. Disinstallare l'applicazione Client Security Solution 6.0. 2. Installare il programma Rescue and Recovery 3.0. 3. Durante l'installazione, scegliere di installare solo il programma Rescue and Recovery.	Durante la disinstallazione dell'applicazione Client Security Solution 6.0, è necessario eliminare le impostazioni ed i file di Security Solution 6.0. L'installazione di Rescue and Recovery 3.0 termina con un errore durante la rimozione nel prompt.
Client Security Solution 6.0 Standalone	Rescue and Recovery 3.0 e Client Security Solution 6.0	1. Installare il programma Rescue and Recovery 3.0. 2. Selezionare qualsiasi componente secondario dell'applicazione Client Security Solution 6.0 che si desidera installare.	• Le impostazioni ed i file di dati di Client Security Solution 6.0 sono preservati. • Per scegliere di proteggere i backup utilizzando l'applicazione Client Security Solution 6.0, utilizzare il programma Rescue and Recovery.
Rescue and Recovery 3.0 e Client Security Solution 6.0	Client Security Software 5.4x	1. Disinstallare l'applicazione Rescue and Recovery - Client Security Solution. 2. Installare l'applicazione Client Security Software 5.4x.	• L'applicazione Client Security Software 5.4x non può essere installata sull'applicazione Client Security Solution 6.0. • L'eliminazione delle impostazioni e dei file di dati nel prompt non influenza le operazioni di Client Security Software 5.4x. • Mediante la disinstallazione del programma Rescue and Recovery 3.0, l'applicazione Client Security Solution 6.0 viene disinstallata automaticamente.

Tabella 1-1. La seguente tabella fornisce le informazioni per modificare la configurazione di Rescue and Recovery e Client Security. Client Security Solution standalone significa che il pacchetto di installazione è stato acquistato dal Web o dal CD. (Continua)

Il software installato è...	E si desidera...	Seguire questo processo	Commenti
Rescue and Recovery 3.0 e Client Security Solution 6.0	Rescue and Recovery 3.0	1. Selezionare **Modifica** dall'Installazione applicazioni. 2. Rimuovere l'applicazione Client Security Solution 6.0.	• I backup locali sono eliminati quando viene rimossa l'applicazione Client Security Solution 6.0. • La disinstallazione dell'applicazione Client Security Solution 6.0 risulta nella mancanza di Password Manager o PrivateDisk. • I backup di Rescue and Recovery 3.0 protetti con l'applicazione Client Security Solution 6.0 non sono più accessibili. Creare un nuovo backup.
Rescue and Recovery 3.0 e Client Security Solution 6.0	Client Security Solution 6.0	1. Disinstallare il programma Rescue and Recovery 3.0. 2. Alla richiesta, scegliere di conservare le impostazioni correnti di Client Security Solution 6.0 solo se si desidera conservare la configurazione di sicurezza corrente. 3. Installare l'applicazione Client Security Solution 6.0 (Standalone).	1. I backup di Rescue and Recovery 3.0 protetti con l'applicazione Client Security Solution 6.0 non sono più accessibili. 2. I backup locali sono eliminati quando è disinstallata l'applicazione Rescue and Recovery 3.0.

Passphrase e password di Rescue and Recovery

È possibile utilizzare le password o passphrase da poter utilizzare per proteggere Rescue and Recovery workspace, quindi per proteggere i dati critici dall'accesso non autorizzato. È possibile specificare di proteggere Rescue and Recovery workspace utilizzando l'installazione guidata di Client Security per impostare le preferenze di sicurezza o modificando le impostazioni di accesso mediante l'applicazione Client Security Solution. L'applicazione Client Security Solution consente anche di stabilire le opzioni per il ripristino di password all'interno di Rescue and Recovery workspace.

Note:

1. Questa funzione è disponibile solo se il programma Client Security Solution 6.0 viene installato. Per utilizzare questa funzione, è necessario completare l'installazione guidata di Client Security 6.0 e specificare l'utilizzo di una password o passphrase per accedere al computer.
2. La procedura guidata di Client Security Setup 6.0 e l'applicazione Client Security Solution 6.0 sono accessibili solo in ambiente Windows. Se si sceglie

di utilizzare Rescue and Recovery senza Client Security Solution, Rescue and Recovery workspace non sarà protetto da una password o passphrase.

3. L'applicazione Client Security Solution consente di stabilire le opzioni per il ripristino di password all'interno di Rescue and Recovery workspace.

Utilizzare i seguenti metodi per proteggere Rescue and Recovery workspace utilizzando una password o passphrase.

Metodo 1: se non è stata completata l'installazione guidata di Client Security, procedere nel modo seguente per proteggere Rescue and Recovery workspace con una password o passphrase:

1. Dal desktop di Windows, fare clic su **Start**, **Tutti i programmi**, selezionare **ThinkVantage** e quindi fare doppio clic su **Client Security Solution**.
2. Quando viene avviato Client Security Solution, fare clic sulla voce di menu **Avanzate**.
3. Fare clic sull'icona **Imposta preferenze di sicurezza e di backup**. Viene visualizzata l'installazione guidata di Client Security.
4. Impostare le preferenze di sicurezza. Alla richiesta, scegliere una delle seguenti operazioni:
   - Se si desidera proteggere Rescue and Recovery workspace utilizzando la password di accesso di Windows, contrassegnare la casella **Utilizza password di Windows per accedere a Rescue and Recovery workspace**.
   - Se si desidera proteggere Rescue and Recovery workspace utilizzando la passphrase di accesso di Client Security Solution, contrassegnare la casella **Utilizza passphrase di Client Security Solution per accedere a Rescue and Recovery workspace**.
5. Completare l'installazione guidata di Client Security Solution, quindi fare clic su **Fine**. Per ulteriori informazioni, fare clic su **?** all'interno dell'installazione guidata di Client Security.

Metodo 2: se è stata completata l'installazione guidata di Client Security, procedere nel modo seguente per proteggere Rescue and Recovery workspace con una password o passphrase:

1. Dal desktop di Windows, fare clic su **Start**, **Tutti i programmi**, selezionare **ThinkVantage** e quindi fare doppio clic su **Client Security Solution**.
2. Quando viene avviato Client Security Solution, fare clic sulla voce di menu **Avanzate**.
3. Fare clic su **Cambia impostazioni di accesso**.
4. Seguire le istruzioni visualizzate. Per le informazioni dettagliate, fare clic su **?** all'interno dell'applicazione Client Security Solution.

Impostazione delle preferenze di backup utilizzando l'installazione guidata di Client Security

L'installazione guidata di Client Security Solution fornisce le opzioni di configurazione che consentono di impostare una varietà di funzioni di sicurezza, quali l'abilitazione di Security Chip integrato, la selezione di autenticazione sull'ambiente Windows, la scelta di utilizzare Rescue and Recovery per eseguire il backup dei dati sensibili o la scelta di utilizzare l'autenticazione delle impronte digitali.

Completare la seguente procedura per utilizzare l'installazione guidata di Client Security:

1. Dal desktop di Windows, fare clic su **Start**, **Tutti i programmi**, selezionare **ThinkVantage** e quindi fare doppio clic su **Client Security Solution**.
2. Quando viene avviato Client Security Solution, fare clic sulla voce di menu **Avanzate**.
3. Quando viene avviato Client Security Solution, fare clic su **Imposta preferenze di sicurezza e backup**. Viene visualizzata l'installazione guidata di Client Security.
4. Impostare le preferenze di sicurezza.
5. Completare l'installazione guidata di Client Security Solution, quindi fare clic su **Fine**. Per le informazioni dettagliate, fare clic su **?** all'interno dell'installazione guidata di Client Security.

Ulteriori informazioni su Client Security Solution

Per le informazioni dettagliate sull'applicazione Client Security Solution e le relative funzioni, consultare *Client Security Solution User Guide* sul Web all'indirizzo:

`http://www.ibm.com/pc/support/site.wss/`

Se l'applicazione Client Security Solution è stata già installata, è possibile consultare le informazioni dettagliate della guida per l'utente completando la seguente procedura:

1. Dal desktop di Windows, fare clic su **Start**.
2. Selezionare **Tutti i programmi**.
3. Selezionare **ThinkVantage**.
4. Fare clic su **Client Security Solution**.
5. Dalla barra di menu di Client Security Solution, fare clic su **?**.
6. Fare clic su **Guida per l'utente**.

Capítulo 5. Español

La aplicación Client Security Solution es una suite de herramientas de ThinkVantage™ Technology diseñada para ayudarle a proteger el acceso al sistema operativo y a los datos importantes del sistema. Client Security Solution integra la protección de hardware de su chip incorporado con la protección que ofrece su software seguro. Combinando software dedicado con su protección de software, Client Security Solution mejora ampliamente las características de seguridad incorporadas en el sistema operativo del sistema.

A quién va dirigida esta guía

El manual *ThinkVantage Client Security Solution Guía del usuario* está diseñado para usuarios finales individuales y para usuarios finales que trabajen en un entorno comercial. Esta guía proporciona información sobre las áreas siguientes:

- Componentes de Client Security Solution
- Consideraciones sobre la instalación de Client Security Solution
- Características de Client Security Solution

Esta guía complementa el sistema de ayuda de Client Security Solution, que proporciona instrucciones paso a paso acerca de cómo realizar tareas específicas dentro del programa.

Información adicional

Si es un administrador de sistemas, un ingeniero de sistemas, un administrador de red o un ingeniero de clientes que está buscando como implantar Client Security Solution en un gran empresa, puede obtener información detallada leyendo el manual *ThinkVantage Rescue and Recovery™ and Client Security Solution Deployment Guide* ubicado en el siguiente sitio Web:

`http://www.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-54502`

Componentes de Client Security Solution

Client Security Solution está diseñado para sistemas que vienen equipados con un chip de seguridad incorporado, que le ayuda a proporcionar niveles adicionales de seguridad a los datos y procesos del sistema. Sin embargo, el software de Client Security Solution se puede ahora configurar para mejorar la seguridad de sistemas que no están equipados con un chip de seguridad.

Client Security Solution se divide en los siguientes componentes de hardware y software.

- **Chip de seguridad incorporado**

  Client Security Solution está diseñado para sistemas que vienen equipados con un chip de seguridad incorporado. Un chip de seguridad incorporado es tecnología incorporada de hardware de cifrado que proporciona un nivel adicional de seguridad al sistema. El chip de seguridad permite que los procesos de autentificación y cifrado se transfieran de software vulnerable al entorno seguro de hardware dedicado. El aumento de seguridad que esto proporciona es tangible.
- **Asistente de instalación de Client Security**

Las ayudas del Asistente de instalación de Client Security le guían por el proceso de configuración de las opciones de seguridad. El asistente le ayuda a habilitar el chip de seguridad incorporado, a seleccionar un método de inicio de sesión y de autentificación, a crear preguntas para la recuperación de contraseña, a establecer la autentificación de huellas dactilares (opcional) y a configurar los componentes de Client Security Solution.

- **Gestor de contraseñas**

  El Gestor de contraseñas de Client Security le permite gestionar de forma segura y cómoda la información importante y que se puede olvidar fácilmente de inicio de sesión de aplicaciones y sitios Web, como por ejemplo ID de usuario, contraseñas y otra información personal. El Gestor de contraseñas de Client Security almacena toda la información mediante el chip de seguridad incorporado de forma que el acceso a las aplicaciones y a los sitios Web sigue siendo totalmente seguro.
- **PrivateDisk**

  PrivateDisk configura una unidad de disco virtual cifrado que cifra automáticamente los datos que se almacenan dentro de los límites seguros de esta ″caja fuerte electrónica″. Utilice su propia unidad virtual para cifrar y almacenar todos los datos críticos. Los datos se cifran automáticamente cuando se almacenan en cualquier volumen PrivateDisk.
- **Aplicación Client Security Solution**

  La aplicación Client Security Solution proporciona una única interfaz que permite a los usuarios realizar funciones básicas y avanzadas de seguridad, como por ejemplo habilitar el chip de seguridad incorporado, cambiar una frase de paso o utilizar el software de huellas dactilares. Para obtener una lista de todas las características de Client Security Solution, consulte “Características de Client Security Solution” en la página 5-3
- **Software de huellas dactilares de ThinkVantage**

  El software de huellas dactilares de ThinkVantage permite a los usuarios establecer la autentificación de huellas dactilares. Esta cómoda característica está disponible en modelos y opciones de ThinkPad y ThinkCentre seleccionados.

Antes de instalar Client Security Solution

Antes de instalar la aplicación Client Security Solution, es importante que se cumplan los requisitos previos siguientes:

- Windows XP o Windows 2000 con Service Pack 3. Si está instalando este programa en un disco duro que tiene una capacidad mayor de 137 GB, Service Pack 1 es necesario para Windows XP.
- Internet Explorer 5.5 (o superior).
- 128 MB de memoria de los que no más de 8 MB se pueden designar como memoria compartida bajo la configuración de vídeo en el BIOS.
- 800 MB de espacio libre de disco.

Si tiene una versión anterior de Client Security Solution, Client Security Software o Rescue and Recovery, consulte “Utilización de Client Security Solution con Rescue and Recovery” en la página 5-6 para obtener instrucciones específicas.

Configuración de Client Security Solution

La aplicación Client Security Solution está disponible en el sitio Web `http://www.pc.ibm.com/thinkvantage`. Se puede realizar la descarga, instalación y configuración de Client Security Solution en cuestión de minutos.

Descarga e instalación de Client Security Solution

Complete el siguiente proceso de instalación para descargar e instalar el programa Client Security Solution:

1. Inicie el sistema y cierre todos los programas abiertos.
2. Vaya al sitio Web `http://www.pc.ibm.com/thinkvantage`.
3. Pulse el enlace **Support and downloads** (Soporte y descargas) en la sección Resources (Recursos).
4. Desplácese hacia abajo a la sección Embedded Security Subsystem and Client Security Solution y pulse **Software download** (Descarga de software).
5. Siga las instrucciones de la pantalla.
6. Ejecute el archivo ejecutable de instalación y siga las instrucciones de la pantalla. Se le dará la opción de instalar los componentes Gestor de contraseñas y PrivateDisk de Client Security Solution.
7. Después de haber realizado las selecciones, se le solicitará que reinicie el sistema.
8. Cuando se reinicie el sistema, se abrirá el Asistente de instalación de Client Security. Si el asistente de instalación no se abre, consulte "Cómo abrir el Asistente de instalación de Client Security"
9. Complete el Asistente de instalación de Client Security para completar el proceso de configuración.

Cómo abrir el Asistente de instalación de Client Security

Complete el siguiente procedimiento para configurar el programa Client Security Solution utilizando el Asistente de instalación de Client Security:

1. En el escritorio de Windows, pulse **Inicio**, **Todos los programas**, seleccione **ThinkVantage** y, a continuación, efectúe una doble pulsación en **Client Security Solution**.
2. Cuando se abra la ventana Client Security Solution, pulse el elemento de menú **Avanzadas**.
3. Cuando se abra la ventana Client Security Solution, pulse **Establecer preferencias de seguridad y copia de seguridad**. Se abrirá la ventana Asistente de instalación de Client Security.
4. Complete los pasos del Asistente de instalación de Client Security Solution y a continuación pulse **Finalizar**. Para obtener información detallada, pulse **Ayuda** en el Asistente de instalación de Client Security.

Utilización de Client Security Solution

Complete el siguiente procedimiento para acceder a la aplicación Client Security Solution:

1. En el escritorio de Windows, pulse **Inicio**.
2. Seleccione **Todos los programas**.
3. Seleccione **ThinkVantage**.
4. Pulse **Client Security Solution**.

Características de Client Security Solution

La siguiente información detalla las diferentes tareas que se pueden realizar utilizando la aplicación Client Security Solution.

Nota: Si algunas de las herramientas mencionadas no está disponible para usted, es posible que se deba a que no tenga el software adecuado instalado, a que el sistema no soporte la aplicación o a que la aplicación requiera acceso de administrador o de supervisor.

Características básicas

La siguiente información detalla las tareas básicas que se pueden realizar utilizando la aplicación Client Security Solution.

Cómo cambiar una frase de paso: La herramienta Cambiar frase de paso le permite establecer una nueva frase de paso de Client Security. Las frases de paso deben satisfacer los requisitos de frase de paso de Client Security.

Configuración de la recuperación de contraseña: La herramienta Configurar recuperación de contraseña le permite establecer una forma de recuperar una contraseña de Windows o una frase de paso de Client Security que haya olvidado, en función de la metodología de autentificación que utilice.

Gestión de la información de inicio de sesión: La aplicación Gestión de contraseñas le permite utilizar Client Security Solution para gestionar la información importante y que se puede olvidar fácilmente de inicio de sesión, como por ejemplo ID de usuario, contraseñas y otra información personal. La aplicación Gestor de contraseñas almacena toda la información mediante el chip de seguridad incorporado de forma que los controles de política de autentificación de usuario acceden a las aplicaciones y a los sitios Web seguros. Esto significa que en lugar de tener que recordar numerosas contraseñas individuales-- todas sujetas a diferentes normas y fechas de caducidad-- sólo debe recordar una frase de paso o, cuando esté instalado el software de huellas dactilares, proporcionar la huella dactilar.

Utilización del software de huellas dactilares: El lector de huellas dactilares integrado le permite registrar y asociar su huella dactilar con la contraseña de inicio de sesión, la contraseña de disco duro o la contraseña de Windows, de forma que la autentificación de huellas dactilares puede sustituir las contraseñas y permitir un acceso de usuario sencillo y seguro. Un teclado con lector de huellas dactilares está disponible en los modelos seleccionados y se puede adquirir como opción. Esta opción está soportada sólo en sistemas ThinkCentre y ThinkPad.

Protección de los datos: La herramienta PrivateDisk genera una unidad de disco virtual cifrado, que cifra automáticamente los datos que se almacenan dentro de los límites seguros de esta ″caja fuerte electrónica″.

Características avanzadas

La siguiente información detalla las tareas avanzadas que se pueden realizar utilizando la aplicación Client Security Solution.

Nota: Debe tener privilegios de administrador para realizar las siguientes operaciones.

Supervisión de los valores de seguridad: La herramienta Security Advisor le permite visualizar un resumen de los valores de seguridad actualmente establecidos en el sistema. Revise estos valores para visualizar el estado de seguridad actual o para mejorar la seguridad del sistema. Algunos de los temas de seguridad incluidos son contraseñas de hardware, contraseñas de usuarios de Windows, política de contraseña de Windows, protector de pantalla protegido y compartimiento de archivos.

Nota: La herramienta Security Advisor sólo proporciona un resumen de los valores de seguridad y sugerencias para ayudarle a mejorar la seguridad del sistema. No se tratan todos los aspectos de la seguridad, como por ejemplo la utilización y el mantenimiento de programas antivirus y cortafuegos. Muchos de los valores requieren acceso de supervisor o administrador.

Transferencia de certificados digitales: El Asistente de transferencia de certificados de Client Security le guía por el proceso de transferir las claves privadas asociadas con los certificados del proveedor del servicio de cifrado (CSP) de Microsoft basado en software al CSP de Client Security Solution basado en hardware. Después de la transferencia, las operaciones que utilizan los certificados son más seguras porque las claves privadas están protegidas por el chip de seguridad incorporado.

Establecimiento de un mecanismo de restablecimiento de contraseña de hardware: Esta herramienta crea un entorno seguro que se ejecuta independientemente de Windows y que le ayuda a restablecer contraseñas de inicio de sesión y de disco duro olvidadas. La identidad del usuario se establece respondiendo a una serie de preguntas que el usuario ha creado. Es recomendable crear este entorno seguro lo antes posible, antes de que se olvide una contraseña. No podrá restablecer una contraseña de hardware olvidada hasta que se haya creado este entorno seguro en el disco duro y se haya registrado. Esta herramienta está disponible sólo en sistemas ThinkCentre y ThinkPad seleccionados.

Nota: Es recomendable establecer una contraseña de administrador o supervisor antes de utilizar esta herramienta. Si no ha establecido una contraseña de administrador o de supervisor, el entorno no será lo más seguro posible. Cuando complete este procedimiento, la contraseña de inicio de sesión y la contraseña de disco duro coincidirán. Este procedimiento está diseñado para ayudarle a completar la tarea de creación del entorno seguro y para ayudarle a restablecer las contraseñas olvidadas después de haber creado el entorno seguro.

Activación del chip de seguridad incorporado: Esta herramienta inicializa un cambio del valor del BIOS que se utiliza para activar o desactivar el chip de seguridad incorporado. Debe reiniciar el sistema para que este cambio sea efectivo.

Cómo cambiar los valores de inicio des sesión: Esta herramienta visualiza los valores actuales de inicio de sesión y permite a un administrador cambiar la forma en la que los usuarios inician sesión en el sistema operativo Windows y en el espacio de trabajo de ThinkVantage Rescue and Recovery.

Cómo borrar el contador de fallos seguros: Esta herramienta restablece el contador de fallos seguros que supervisa el número de intentos de autentificación incorrectos que han pasado al chip de seguridad incorporado. Después de cierto número de intentos fallidos, el chip se bloquea durante un período de tiempo. El período de bloqueo aumenta con los intentos fallidos continuados.

Establecimiento de preferencias de seguridad y copia de seguridad: El Asistente de instalación de Client Security le permite configurar una serie de herramientas de software de seguridad. Este asistente proporciona opciones de configuración que le permiten establecer una serie de características de seguridad, como por ejemplo habilitar el chip de seguridad incorporado de Client Security, seleccionar cómo desea autentificarse en el entorno de Windows, seleccionar utilizar Rescue and Recovery para realizar copia de seguridad de los datos importantes o elegir utilizar la autentificación de huellas dactilares.

Utilización de Client Security Solution con Rescue and Recovery

Tanto el programa Rescue and Recovery como la aplicación Client Security Solution son Tecnologías ThinkVantage que se han desarrollado teniendo en cuenta al usuario. Es decir, están diseñadas para funcionar separadamente o conjuntamente, en función de las necesidades del usuario. La siguiente información está destinada a ayudarle a diseñar su estrategia para utilizar estos programas, y para resaltar cómo estos programas se mejoran mutuamente.

Hay consideraciones importantes que se deben tener en cuenta al instalar el programa Rescue and Recovery, la aplicación Client Security Solution o ambas. Las tablas siguientes proporcionan información para ayudarle a determinar el procedimiento correcto para la configuración que desee:

Tabla 1-1. La tabla siguiente proporciona información para ayudarle a cambiar la configuración de Rescue and Recovery y Client Security. Client Security Solution Standalone significa que el paquete de instalación se ha adquirido de la Web o en CD.

El software instalado es...	Y desea...	Siga este proceso	Comentarios
Client Security Software 5.4x	Client Security Software 5.4x y Rescue and Recovery 3.0	1. Instale el programa Rescue and Recovery 3.0. 2. Cuando se le solicite, indique que desea mantener instalada la aplicación Client Security Software 5.4x.	Las copias de seguridad no se pueden proteger utilizando la aplicación Client Security Software 5.4x, y cualquier utilización de Client Security Software por parte del programa Rescue and Recovery 3.0 se realizará utilizando una versión emulada de Client Security Software. La característica de contraseña maestra se añade a las características de seguridad. Se utiliza normalmente una contraseña maestra en un entorno de empresa. Para obtener más información, consulte “Información adicional” en la página 5-1
Client Security Software 5.4x	Paquete de instalación de Client Security Solution 6.0 Standalone	1. Desinstale la aplicación Client Security Software 5.4x. 2. Instale la aplicación Client Security Solution 6.0 (Standalone).	• Debe descifrar los archivos cifrados y exportar la información del Gestor de contraseñas antes de desinstalar. De lo contrario, esta información se perderá. • Debe desinstalar el software de Cifrado de archivos y carpetas de IBM® antes de instalar la aplicación Client Security Solution.

Tabla 1-1. La tabla siguiente proporciona información para ayudarle a cambiar la configuración de Rescue and Recovery y Client Security. Client Security Solution Standalone significa que el paquete de instalación se ha adquirido de la Web o en CD. (continuación)

El software instalado es...	Y desea...	Siga este proceso	Comentarios
Client Security Software 5.4x	Client Security Solution 6.0 y Rescue and Recovery 3.0	1. Desinstale la aplicación Client Security Software 5.4x. 2. Instale el programa Rescue and Recovery 3.0. (Asegúrese de que esté instalado el componente Client Security Solution 6.0.)	• Si instala Rescue and Recovery 3.0 encima de Client Security Software 5.4x sin desinstalar en primer lugar Client Security Software, dará como resultado sólo Rescue and Recovery. • Antes de desinstalar la aplicación Client Security Software 5.4x, debe descifrar los archivos cifrados y exportar la información del Gestor de contraseñas antes de desinstalar. De lo contrario, esta información se perderá. • Debe desinstalar el software de Cifrado de archivos y carpetas de IBM antes de instalar la aplicación Client Security Solution 6.0.
Rescue and Recovery 3.0	Client Security Software 5.4x y Rescue and Recovery 3.0	1. Desinstale el programa Rescue and Recovery 3.0. 2. Instale la aplicación Client Security Software 5.4x. 3. Instale el programa Rescue and Recovery 3.0. 4. Cuando se le solicite, indique que desea mantener instalada la aplicación Client Security Software 5.4x.	• La aplicación Client Security Software 5.4x no se puede instalar encima del programa Rescue and Recovery 3.0. • Las copias de seguridad locales se suprimen al desinstalar el programa Rescue and Recovery 3.0.

Tabla 1-1. La tabla siguiente proporciona información para ayudarle a cambiar la configuración de Rescue and Recovery y Client Security. Client Security Solution Standalone significa que el paquete de instalación se ha adquirido de la Web o en CD. (continuación)

El software instalado es...	Y desea...	Siga este proceso	Comentarios
Rescue and Recovery 3.0	Paquete de instalación de Client Security Solution 6.0 Standalone	1. Desinstale el programa Rescue and Recovery 3.0. 2. Instale la aplicación Client Security Solution 6.0 (Standalone).	• Desinstalación Rescue and Recovery suprimirá los archivos de usuario y los valores de registro de Client Security Solution. • Las copias de seguridad de Rescue and Recovery protegidas por Client Security Solution dejarán de ser accesibles. • Las copias de seguridad locales se suprimirán al desinstalar Rescue and Recovery 3.0. • Client Security Solution 6.0 (Standalone) no se puede instalar encima de Rescue and Recovery 3.0.
Rescue and Recovery 3.0	Rescue and Recovery 3.0 y Client Security Solution 6.0	1. Seleccione la opción **Cambiar** de Agregar o quitar programas. 2. Complete la operación de modificación añadiendo la aplicación Client Security Solution y los subcomponentes que desee.	• Las copias de seguridad locales se suprimen al añadir la aplicación Client Security Solution. • Después de añadir la aplicación Client Security Solution, cree una nueva copia de seguridad base lo antes posible. • Se suprimen los valores y los archivos de datos de Client Security Solution. • La aplicación Client Security Solution 6.0 (Standalone) no se puede instalar encima del programa Rescue and Recovery 3.0.
Paquete de instalación de Client Security Solution 6.0 Standalone	Client Security Software 5.4x	1. Desinstale la aplicación Client Security Solution 6.0 (Standalone). 2. Instale la aplicación Client Security Software 5.4x.	• Si suprime los archivos de datos y los valores de Client Security Solution 6.0 cuando se le solicite, esto no afectará a las operaciones de Client Security Software 5.4x.

Tabla 1-1. La tabla siguiente proporciona información para ayudarle a cambiar la configuración de Rescue and Recovery y Client Security. Client Security Solution Standalone significa que el paquete de instalación se ha adquirido de la Web o en CD. (continuación)

El software instalado es...	Y desea...	Siga este proceso	Comentarios
Paquete de instalación de Client Security Solution 6.0 Standalone	Rescue and Recovery 3.0	1. Desinstale la aplicación Client Security Solution 6.0. 2. Instale el programa Rescue and Recovery 3.0. 3. Durante la instalación, seleccione instalar sólo el programa Rescue and Recovery.	Al desinstalar la aplicación Client Security Solution 6.0, debe suprimir los archivos y los valores de Security Solution 6.0. Si no los elimina cuando se le solicite, se terminará la instalación de Rescue and Recovery 3.0.
Client Security Solution 6.0 Standalone	Rescue and Recovery 3.0 y Client Security Solution 6.0	1. Instale el programa Rescue and Recovery 3.0. 2. Seleccione los subcomponentes de la aplicación Client Security Solution 6.0 que desee instalar.	• Se conservarán los valores y los archivos de datos de Client Security Solution 6.0. • Para seleccionar proteger las copias de seguridad utilizando la aplicación Client Security Solution 6.0, utilice el programa Rescue and Recovery.
Rescue and Recovery 3.0 y Client Security Solution 6.0	Client Security Software 5.4x	1. Desinstale la aplicación Rescue and Recovery - Client Security Solution. 2. Instale la aplicación Client Security Software 5.4x.	• La aplicación Client Security Software 5.4x no se puede instalar encima de la aplicación Client Security Solution 6.0. • Si suprime los archivos de datos y los valores cuando se le solicite, esto no afectará a las operaciones de Client Security Software 5.4x. • Desinstalando el programa Rescue and Recovery 3.0, la aplicación Client Security Solution 6.0 se desinstala automáticamente.

Tabla 1-1. La tabla siguiente proporciona información para ayudarle a cambiar la configuración de Rescue and Recovery y Client Security. Client Security Solution Standalone significa que el paquete de instalación se ha adquirido de la Web o en CD. (continuación)

El software instalado es...	Y desea...	Siga este proceso	Comentarios
Rescue and Recovery 3.0 y Client Security Solution 6.0	Rescue and Recovery 3.0	1. Seleccione **Cambiar** de Agregar o quitar programas. 2. Extraiga la aplicación Client Security Solution 6.0.	• Las copias de seguridad locales se suprimen al añadir la aplicación Client Security Solution 6.0. • La desinstalación de la aplicación Client Security Solution 6.0, dará como resultado que no se tenga el Gestor de contraseñas o PrivateDisk. • Las copias de seguridad de Rescue and Recovery 3.0 protegidas con la aplicación Client Security Solution 6.0 dejarán de ser accesibles. Cree una nueva copia de seguridad lo antes posible.
Rescue and Recovery 3.0 y Client Security Solution 6.0	Client Security Solution 6.0	1. Desinstale el programa Rescue and Recovery 3.0. 2. Cuando se le solicite, seleccione conservar los valores de Client Security Solution 6.0 sólo si desea conservar la configuración actual de seguridad. 3. Instale la aplicación Client Security Solution 6.0 (Standalone).	1. Las copias de seguridad de Rescue and Recovery 3.0 protegidas con la aplicación Client Security Solution 6.0 dejarán de ser accesibles. 2. Las copias de seguridad locales se suprimen al desinstalar la aplicación Rescue and Recovery 3.0.

Contraseñas y frases de paso de Rescue and Recovery

Puede utilizar contraseñas o puede utilizar frases de paso para proteger el espacio de trabajo de Rescue and Recovery, protegiendo de este modo los datos críticos frente a un acceso no autorizado. Puede especificar proteger el espacio de trabajo de Rescue and Recovery utilizando el Asistente de instalación de Client Security para establecer las preferencias de seguridad o cambiando los valores de inicio de sesión utilizando la aplicación Client Security Solution. La aplicación Client Security Solution también le permite establecer las opciones de recuperación de contraseña dentro del espacio de trabajo de Rescue and Recovery.

Notas:

1. Esta característica sólo está disponible si está instalado el programa Client Security Solution 6.0. Para utilizar esta característica, debe haber completado el Asistente de instalación de Client Security 6.0 y haber especificado que desea utilizar una contraseña o frase de paso para iniciar sesión en el sistema.
2. Tanto el Asistente de instalación de Client Security 6.0 como la aplicación Client Security Solution 6.0 son accesibles sólo en el entorno de Windows. Si

selecciona utilizar Rescue and Recovery sin Client Security Solution, el espacio de trabajo Rescue and Recovery no estará protegido mediante una contraseña o frase de paso.

3. La aplicación Client Security Solution le permite establecer las opciones de recuperación de contraseña dentro del espacio de trabajo Rescue and Recovery.

Utilice los métodos siguientes para proteger el espacio de trabajo de Rescue and Recovery utilizando una contraseña o frase de paso.

Método 1: si no ha completado el Asistente de instalación de Client Security, efectúe lo siguiente para proteger el espacio de trabajo de Rescue and Recovery con una contraseña o frase de paso:

1. En el escritorio de Windows, pulse **Inicio**, **Todos los programas**, seleccione **ThinkVantage** y, a continuación, efectúe una doble pulsación en **Client Security Solution**.
2. Cuando se abra la ventana Client Security Solution, pulse el elemento de menú **Avanzadas**.
3. Pulse el icono **Establecer preferencias de seguridad y copia de seguridad**. Se abrirá el Asistente de instalación de Client Security.
4. Establezca las preferencias de seguridad. Cuando se le solicite, seleccione una de las opciones siguientes:
   - Si desea proteger el espacio de trabajo de Rescue and Recovery utilizando la contraseña de inicio de sesión de Windows, marque el recuadro de selección **Utilizar contraseña de Windows para acceder al espacio de trabajo de Rescue and Recovery**.
   - Si desea proteger el espacio de trabajo de Rescue and Recovery utilizando la frase de paso de inicio de sesión de Client Security Solution, marque el recuadro de selección **Utilizar la frase de paso de Client Security Solution para acceder al espacio de trabajo de Rescue and Recovery**.
5. Complete el Asistente de instalación de Client Security Solution y, a continuación, pulse **Finalizar**. Para obtener más información, pulse **Ayuda** en el Asistente de instalación de Client Security.

Método 2: si ha completado el Asistente de instalación de Client Security, efectúe lo siguiente para proteger el espacio de trabajo de Rescue and Recovery con una contraseña o frase de paso:

1. En el escritorio de Windows, pulse **Inicio**, **Todos los programas**, seleccione **ThinkVantage** y, a continuación, efectúe una doble pulsación en **Client Security Solution**.
2. Cuando se abra la ventana Client Security Solution, pulse el elemento de menú **Avanzadas**.
3. Pulse **Cambiar valores de inicio de sesión**.
4. Siga las instrucciones de la pantalla. Para obtener información detallada, pulse **Ayuda** en la aplicación Client Security Solution.

Configuración de las preferencias de copia de seguridad utilizando el Asistente de instalación de Client Security

El Asistente de instalación de Client Security Solution proporciona opciones de configuración que le permiten establecer una variedad de características de seguridad, como por ejemplo habilitar el chip de seguridad incorporado, seleccionar cómo desea autentificarse en el entorno de Windows, seleccionar utilizar Rescue and Recovery para realizar copias de seguridad de los datos importantes o elegir utilizar la autentificación de huellas dactilares.

Complete el procedimiento siguiente para utilizar el Asistente de instalación de Client Security:

1. En el escritorio de Windows, pulse **Inicio**, **Todos los programas**, seleccione **ThinkVantage** y, a continuación, efectúe una doble pulsación en **Client Security Solution**.
2. Cuando se abra la ventana Client Security Solution, pulse el elemento de menú **Avanzadas**.
3. Cuando se abra la ventana Client Security Solution, pulse **Establecer preferencias de seguridad y copia de seguridad**. Se abrirá el Asistente de instalación de Client Security.
4. Establezca las preferencias de seguridad.
5. Complete el Asistente de instalación de Client Security Solution y, a continuación, pulse **Finalizar**. Para obtener información detallada, pulse **Ayuda** en el Asistente de instalación de Client Security.

Más información acerca de Client Security Solution

Para obtener información detallada acerca de la aplicación Client Security Solution y sus características, consulte el manual *Client Security Solution Guía del usuario* en el sitio Web en la dirección:

```
http://www.ibm.com/pc/support/site.wss/
```

Si ya tiene instalada la aplicación Client Security Solution, puede leer información más detallada en el manual Guía del usuario completando el procedimiento siguiente:

1. En el escritorio de Windows, pulse **Inicio**.
2. Seleccione **Todos los programas**.
3. Seleccione **ThinkVantage**.
4. Pulse **Client Security Solution**.
5. En la barra de menús de Client Security Solution, pulse **Ayuda**.
6. Pulse **Guía del usuario**.

Kapitel 6. Dansk

Programmet Client Security Solution består af en række ThinkVantage Technology-værktøjer, som skal hjælpe med at beskytte adgangen til computersystemet og følsomme data. Client Security Solution-programmet integrerer hardwarebeskyttelsen i den indbyggede chip med den beskyttelse, der ligger i programmets sikre software. Ved at kombinere den dedikerede hardware med Client Security Solution-programmets softwarebeskyttelse styrkes de sikkerhedsfaciliteter, der er bygget ind i computerens styresystem, betydeligt.

Hvem henvender vejledningen sig til?

Brugervejledningen til *ThinkVantage Client Security Solution* er beregnet til privatpersoner og personer, der arbejder for en virksomhed. Vejledningen indeholder oplysninger inden for følgende områder:

- Client Security Solution-komponenter
- Overvejelser i forbindelse med installation af Client Security Solution
- Faciliteter i Client Security Solution

Vejledningen er et supplement til Client Security Solution-hjælpen, der giver en trinvis vejledning i, hvordan bestemte opgaver skal udføres i programmet.

Flere oplysninger

Hvis du er administrator, systemtekniker, netværksadministrator eller CE'er og forsøger at implementere Client Security Solution-programmet på tværs af en stor virksomhed, kan du få flere oplysninger ved at læse *ThinkVantage Rescue and Recovery and Client Security Solution Deployment Guide*, der er placeret på følgende websted:

`http://www.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-54502`

Client Security Solution-komponenter

Client Security Solution er beregnet til computere, der bliver leveret med en indbygget sikkerhedschip, som øger sikkerheden i forbindelse med computerdata og -processer. Client Security Solution-programmet kan nu konfigureres, så det også øger sikkerheden i computere, som ikke er leveret med en sikkerhedschip.

Client Security Solution er opdelt i følgende hardware- og softwarekomponenter:

- **Indbygget sikkerhedschip**

  Client Security Solution er beregnet til computere, der leveres med en indbygget sikkerhedschip. En indbygget sikkerhedschip er indbygget hardwareteknologi til kryptering. Det giver computeren et ekstra sikkerhedslag. Sikkerhedschippen gør det muligt at overføre krypterings- og godkendelsesprocessen fra sårbar software til det sikre miljø i den dedikerede hardware. Det giver en betydeligt øget sikkerhed.
- **Guiden Client Security Setup**

  Guiden Client Security Setup hjælper dig med at konfigurere sikkerhedsfaciliteterne. Guiden beskriver, hvordan du aktiverer den indbyggede sikkerhedschip, vælger en godkendelses- og logonmetode, opretter spørgsmål til brug i forbindelse med retablering af kodeord, etablerer fingeraftryksgodkendelse (valgfri) og konfigurerer yderligere Client Security Solution-komponenter.

- **Password Manager**

  Med Client Security Password Manager kan du administrere alle dine følsomme logonoplysninger til programmer websteder, f.eks. bruger-id'er, kodeord og andre personlige oplysninger. Client Security Password Manager gemmer alle oplysninger via den indbyggede sikkerhedschip, så adgang til dine programmer og websteder forbliver fuldstændig sikker.
- **PrivateDisk**

  PrivateDisk konfigurerer en krypteret virtuel disk, som automatisk krypterer de data, du gemmer på diskdrevets sikre område. Brug dit eget virtuelle drev til at kryptere og gemme alle dine særligt vigtige data. Data krypteres automatisk, når de gemmes på et PrivateDisk-afsnit.
- **Programmet Client Security Solution**

  Programmet Client Security Solution indeholder én grænseflade, som gør det muligt for brugerne at udføre grundlæggende og udvidede sikkerhedsfunktioner, f.eks. aktivere den indbyggede sikkerhedschip, skifte en kodesætning eller bruge fingeraftryksprogrammer. "Faciliteter i Client Security Solution" på side 6-3 indeholder en fuldstændig oversigt over faciliteterne i Client Security Solution.
- **ThinkVantage-fingeraftryksprogram**

  Med ThinkVantage-fingeraftryksprogrammet kan brugerne etablere fingeraftryksgodkendelse. Denne praktiske sikkerhedsfacilitet kan benyttes på udvalgte ThinkPad- og ThinkCentre-modeller og på udvalgt ekstraudstyr.

Før du installerer Client Security Solution

Før du installerer programmet Client Security Solution, er det vigtigt, at følgende forudsætninger opfyldes:

- Windows XP eller Windows 2000 med servicepakke 3. Hvis du installerer dette program på en harddisk, der er større end 137 GB, skal du bruge servicepakke 1 til Windows XP.
- Internet Explorer 5.5 (eller nyere)
- 128 MB hukommelse, hvor der ikke kan tildeles mere end 8 MB som fælles hukommelse under videokonfigurationen i BIOS.
- 800 MB ledig diskplads.

Hvis du har en ældre version af Client Security Solution, Client Security Software eller Rescue and Recovery, skal du læse "Brug af Client Security Solution sammen med Rescue and Recovery-programmet" på side 6-5, som indeholder særlige oplysninger.

Konfiguration af Client Security Solution

Programmet Client Security Solution er tilgængeligt på webstedet `http://www.pc.ibm.com/thinkvantage`. Det tager kun et par minutter at hente, installere og konfigurere Client Security Solution.

Overførsel og installation af Client Security Solution

Gør følgende for at hente og installere programmet Client Security Solution:

1. Start computeren, og luk alle åbne programmer.
2. Skift til webstedet `http://www.pc.ibm.com/thinkvantage`.
3. Klik på linket **Support and downloads** i afsnittet Resources.
4. Blad ned til afsnittet Embedded Security Subsystem and Client Security Solution, og klik på **Software download**.

5. Følg vejledningen på skærmen.
6. Udfør installationsfilen, og følg vejledningen på skærmen. Du kan vælge at installere Password Manager- og PrivateDisk-komponenterne i Client Security Solution.
7. Når du har valgt, bliver du bedt om at genstarte computeren.
8. Når computeren genstarter, åbnes guiden Client Security Setup. Læs afsnittet "Åbning af guiden Client Security Setup", hvis guiden ikke åbnes.
9. Gennemgå guiden Client Security Setup for at færdiggøre konfigurationen.

Åbning af guiden Client Security Setup

Gennemgå følgende procedure for at konfigurere programmet Client Security Solution ved hjælp af guiden Client Security Setup:

1. Klik på **Start** på Windows-skrivebordet, klik på **Alle programmer**, vælg **ThinkVantage**, og dobbeltklik på **Client Security Solution**.
2. Klik på menupunktet **Udvidet** i vinduet Client Security Solution.
3. Klik på **Angiv indstillinger til sikkerhed og sikkerhedskopiering** i vinduet Client Security Solution. Guiden Client Security Setup åbnes.
4. Gennemgå trinene i guiden Client Security Solution Setup, og klik på **Udfør**. Klik på **Hjælp** i guiden Client Security Setup for at få flere oplysninger.

Brug af Client Security Solution

Gør følgende for at få adgang til programmet Client Security Solution:

1. Klik på **Start** på Windows-skrivebordet.
2. Vælg **Alle programmer**.
3. Vælg **ThinkVantage**.
4. Klik på **Client Security Solution**.

Faciliteter i Client Security Solution

Nedenfor beskrives de forskellige opgaver, som kan udføres ved hjælp af programmet Client Security Solution.

Bemærk: Hvis der er nogle af værktøjerne nedenfor, du ikke har adgang til, kan det skyldes, at du ikke har det korrekte program installeret, at computeren ikke understøtter programmet, eller at programmet kræver administratoradgang.

Grundlæggende faciliteter

Nedenfor beskrives de grundlæggende opgaver, som kan udføres ved hjælp af programmet Client Security Solution.

Skift kodesætning: Med værktøjet Skift kodesætning kan du oprette en ny Client Security-kodesætning. Kodesætningerne skal opfylde kravene til Client Security-kodesætninger.

Konfigurér retablering af kodeord: Med værktøjet Konfigurér retablering af kodeord kan du oprette en metode til at retablere en glemt Windows-adgangskode eller en Client Security-kodesætning, afhængig af den godkendelsesmetode, du bruger.

Administrér logonoplysninger: Med programmet Password Manager kan du bruge Client Security Solution til at administrere dine følsomme logonoplysninger, f.eks. bruger-id'er, kodeord og andre personlige oplysninger. Programmet Password Manager gemmer alle oplysninger via den indbyggede sikkerhedschip, så din brugergodkendelsespolitik styrer adgang til dine sikre programmer og websteder. Det betyder, at i stedet for at du skal huske og indtaste mange forskellige kodeord, som alle er underlagt forskellige regler og udløbsdatoer, så skal du kun huske én kodesætning, eller hvis du bruger fingeraftrykslæseren, skal du bruge dit fingeraftryk.

Brug fingeraftryksprogram: Med den indbyggede fingeraftrykslæser kan du registrere og tilknytte dit fingeraftryk til dit startkodeord, harddiskkodeord og din Windows-adgangskode, så fingeaftryksgodkendelse kan erstatte kodeord og levere en mere simpel og sikker brugeradgang. Et tastatur med en fingeraftrykslæser leveres med udvalgte computere og kan købes som ekstraudstyr. Denne facilitet kan kun anvendes på udvalgte ThinkCentre- og ThinkPad-computere.

Beskyt data: Værktøjet PrivateDisk genererer et krypteret virtuelt diskdrev, som automatisk krypterer de data, du gemmer på diskdrevets sikre område.

Udvidede funktioner

Nedenfor beskrives de udvidede opgaver, som kan udføres ved hjælp af programmet Client Security Solution.

Bemærk: Du skal have administratorrettigheder for at kunne udføre nedenstående funktioner.

Overvåg sikkerhedsindstillinger: Med værktøjet Security Advisor kan du få vist en oversigt over de sikkerhedsindstillinger, som er angivet på computeren. Gennemgå indstillingerne for at få vist den aktuelle sikkerhedsstatus eller øge systemsikkerheden. Emnerne omfatter hardwarekodeord, Windows-brugeradgangskoder, Windows-adgangskodepolitik, beskyttede pauseskærme og fildeling.

Bemærk: Værktøjet Security Advisor viser kun en oversigt over sikkerhedsindstillingerne og forslag til, hvordan du kan forbedre systemets sikkerhed. Ikke alle sikkerhedsrisici berøres, f.eks. brug og vedligeholdelse af antivirus- og firewall-programmer. Mange af indstillingerne kræver administratoradgang.

Overfør digitale certifikater: Guiden Client Security Certificate Transfer hjælper dig med at overføre de private nøgler, der er tilknyttet dine certifikater, fra den softwarebaserede Microsoft CSP (Cryptographic Service Provider) til den hardwarebaserede Client Security Solution CSP. Når overførslen er afsluttet, er de funktioner, som bruger certifikaterne, mere sikre, fordi de private nøgler er beskyttet af den indbyggede sikkerhedschip.

Etablér mekanisme til nulstilling af hardwarekodeord: Dette værktøj opretter et sikkert miljø, som udføres uafhængigt af Windows, og du kan bruge det til at nulstille glemte start- og harddiskkodeord. Du bekræfter din identitet ved at besvare en række spørgsmål, du har oprettet. Det er en god idé at oprette dette sikre miljø så hurtigt som muligt, før du glemmer et kodeord. Du kan ikke nulstille glemte hardwarekodeord, før dette sikre miljø er oprettet på harddisken, og du har oprettet dig som bruger. Dette værktøj kan kun anvendes på udvalgte ThinkCentre- og ThinkPad-computere.

Bemærk: Det er en god idé at angive et administratorkodeord, før du begynder at bruge værktøjet. Hvis du ikke angiver et administratorkodeord, er miljøet ikke så sikkert som det ellers vil være. Når du har udført denne procedure, er start- og harddiskkodeordet det samme. Denne procedure hjælper dig med at oprette det sikre miljø og nulstille glemte kodeord, når det sikre miljø er oprettet.

Aktivér den indbyggede sikkerhedschip: Dette værktøj foretager en ændring af BIOS-indstillingen, der bruges til at aktivere eller deaktivere den indbyggede sikkerhedschip. Du skal genstarte computeren, før ændringer træder i kraft.

Revidér logonindstillinger: Dette værktøj viser de aktuelle logonindstillinger. Administratoren kan også bruge funktionen til at ændre, hvordan brugerne logger på Windows-styresystemet og ThinkVantage Rescue and Recovery-arbejdsområdet.

Clearing the fail safe counter: Dette værktøj nulstiller den tæller, der overvåger, hvor mange forkerte forsøg på godkendelse, der er videregivet til den indbyggede sikkerhedschip. Efter et vist antal ikke-gennemførte forsøg, låser chippen sig selv i en periode. Lockout-perioden forlænges i takt med antallet af ikke-gennemførte forsøg.

Angiv indstillinger til sikkerhed og sikkerhedskopiering: Med Guiden Client Security Setup kan du konfigurere mange forskellige sikkerhedsprogrammer. Denne guide indeholder konfigurationsvalg, som du kan bruge til at angive mange forskellige sikkerhedsfaciliteter, f.eks. aktivering af den indbyggede sikkerhedschip i Client Security, angivelse af, hvordan du vil godkende i Windows, hvordan du vil bruge Rescue and Recovery til at tage sikkerhedskopier af dine følsomme data, eller om du vil bruge fingeraftryksgodkendelse.

Brug af Client Security Solution sammen med Rescue and Recovery-programmet

Rescue and Recovery og Client Security Solution er begge ThinkVantage-teknologier, der er udviklet med brugeren for øje. Det vil sige, de kan bruges hver for sig eller sammen, alt efter hvad du har brug for. Oplysningerne nedenfor skal hjælpe dig med at udvikle en strategi for brug af programmerne, og du får at vide, hvordan programmerne supplerer hinanden.

Der er visse ting, du skal overveje, når du installerer Rescue and Recovery-programmet, Client Security Solution-programmet eller begge programmer sammen. Tabellen nedenfor indeholder oplysninger, der kan hjælpe dig med at fastslå, hvilken procedure du skal bruge for at opnå den ønskede konfiguration:

Tabel 6-1. Tabellen nedenfor indeholder oplysninger, der kan hjælpe dig med at ændre konfigurationen af Rescue and Recovery- og Client Security-programmet. Standalone Client Security Solution betyder, at installationspakken er anskaffet fra internettet eller fra en cd.

Installeret software:	**Du vil:**	**Gør følgende:**	**Kommentarer**
Client Security Software 5.4x	Client Security Software 5.4x og Rescue and Recovery 3.0	1. Installér programmet Rescue and Recovery 3.0. 2. Når du bliver bedt om det, skal du angive, at du stadig vil have programmet Client Security Software 5.4x installeret.	Du kan ikke beskytte sikkerhedskopier ved hjælp af programmet Client Security Software 5.4x, og programmet Rescue and Recovery 3.0 bruger eventuelle faciliteter i Client Security Software ved hjælp af en emuleret version af Client Security Software. Masterkodeordsfaciliteten føjes til sikkerhedsfaciliteterne. Masterkodeord benyttes typisk i virksomhedssammenhæng. Der er flere oplysninger i “Flere oplysninger” på side 6-1
Client Security Software 5.4x	Client Security Solution 6.0 Standalone-installationspakke	1. Fjern programmet Client Security Software 5.4x. 2. Installér programmet Client Security Solution 6.0 (Standalone).	• Du skal dekryptere eventuelle krypterede filer og eksportere eventuelle Password Manager-oplysninger, før du fjerner programmet. Hvis du ikke gør det, går oplysningerne tabt. • Du skal fjerne IBM File and Folder Encryption-softwaren, inden du installerer programmet Client Security Solution.

Tabel 6-1. Tabellen nedenfor indeholder oplysninger, der kan hjælpe dig med at ændre konfigurationen af Rescue and Recovery- og Client Security-programmet. Standalone Client Security Solution betyder, at installationspakken er anskaffet fra internettet eller fra en cd. (fortsat)

Installeret software:	**Du vil:**	**Gør følgende:**	**Kommentarer**
Client Security Software 5.4x	Client Security Solution 6.0 og Rescue and Recovery 3.0	1. Fjern programmet Client Security Software 5.4x. 2. Installér programmet Rescue and Recovery 3.0. Kontrollér, at du har valgt komponenten Client Security Solution 6.0.	• Hvis du installerer Rescue and Recovery 3.0 oven i Client Security Software 5.4x uden først at have fjernet Client Security Software, har du kun Rescue and Recovery tilbage. • Før du fjerner programmet Client Security Software 5.4x, skal du have dekrypteret eventuelle krypterede filer og eksporteret eventuelle Password Manager-oplysninger. Hvis du ikke gør det, går oplysningerne tabt. • Du skal fjerne IBM File and Folder Encryption-softwaren, inden du installerer programmet Client Security Solution 6.0.
Rescue and Recovery 3.0	Client Security Software 5.4x og Rescue and Recovery 3.0	1. Fjern programmet Rescue and Recovery 3.0. 2. Installér programmet Client Security Software 5.4x. 3. Installér programmet Rescue and Recovery 3.0. 4. Når du bliver bedt om det, skal du angive, at du stadig vil have programmet Client Security Software 5.4x installeret.	• Du kan ikke installere Client Security Software 5.4x-programmet oven i programmet Rescue and Recovery 3.0. • Lokale sikkerhedskopier slettes, når du fjerner programmet Rescue and Recovery 3.0.

Tabel 6-1. Tabellen nedenfor indeholder oplysninger, der kan hjælpe dig med at ændre konfigurationen af Rescue and Recovery- og Client Security-programmet. Standalone Client Security Solution betyder, at installationspakken er anskaffet fra internettet eller fra en cd. (fortsat)

Installeret software:	**Du vil:**	**Gør følgende:**	**Kommentarer**
Rescue and Recovery 3.0	Client Security Solution 6.0 Standalone-installationspakke	1. Fjern programmet Rescue and Recovery 3.0. 2. Installér programmet Client Security Solution 6.0 (Standalone).	• Hvis du fjerner Rescue and Recovery, slettes brugerfiler og indstillinger for Client Security Solution-registreringsdatabasen. • De Rescue and Recovery-sikkerhedskopier, der beskyttes af Client Security Solution, er ikke længere tilgængelige. • Lokale sikkerhedskopier slettes, når du fjerner programmet Rescue and Recovery 3.0. • Client Security Solution 6.0 (Standalone) kan ikke installeres oven i Rescue and Recovery 3.0.
Rescue and Recovery 3.0	Rescue and Recovery 3.0 og Client Security Solution 6.0	1. Vælg **Rediger** under Tilføj/fjern programmer. 2. Gennemfør ændringen ved at tilføje programmet Client Security Solution og eventuelle underkomponenter.	• Lokale sikkerhedskopier slettes, når du tilføjer programmet Client Security Solution. • Når du har tilføjet programmet Client Security Solution, skal du hurtigst muligt oprette en ny, grundlæggende sikkerhedskopi. • Indstillinger og datafiler i Client Security Solution slettes. • Programmet Client Security Solution 6.0 (Standalone) kan ikke installeres oven i programmet Rescue and Recovery 3.0.
Client Security Solution 6.0 Standalone-installationspakke	Client Security Software 5.4x	1. Fjern programmet Client Security Solution 6.0 (Standalone). 2. Installér programmet Client Security Software 5.4x.	• Funktionerne i Client Security Software 5.4x påvirkes ikke af, at du vælger at slette datafiler og indstillinger i Client Security Solution 6.0.

Tabel 6-1. Tabellen nedenfor indeholder oplysninger, der kan hjælpe dig med at ændre konfigurationen af Rescue and Recovery- og Client Security-programmet. Standalone Client Security Solution betyder, at installationspakken er anskaffet fra internettet eller fra en cd. (fortsat)

Installeret software:	**Du vil:**	**Gør følgende:**	**Kommentarer**
Client Security Solution 6.0 Standalone-installationspakke	Rescue and Recovery 3.0	1. Fjern programmet Client Security Solution 6.0. 2. Installér programmet Rescue and Recovery 3.0. 3. Under installation skal du vælge kun at installere programmet Rescue and Recovery.	Når du fjerner programmet Client Security Solution 6.0, skal du også slette Security Solution 6.0-filer og -indstillinger. Hvis du ikke fjerner disse, når du bliver bedt om det, afsluttes installationen af Rescue and Recovery 3.0.
Client Security Solution 6.0 Standalone	Rescue and Recovery 3.0 og Client Security Solution 6.0	1. Installér programmet Rescue and Recovery 3.0. 2. Vælg de underkomponenter i Client Security Solution 6.0, som du vil installere.	• Datafiler og indstillinger i Client Security Solution 6.0 bliver bevaret. • Brug programmet Rescue and Recovery, hvis du vil beskytte sikkerhedskopier ved hjælp af programmet Client Security Solution 6.0.
Rescue and Recovery 3.0 og Client Security Solution 6.0	Client Security Software 5.4x	1. Fjern programmet Rescue and Recovery - Client Security Solution. 2. Installér programmet Client Security Software 5.4x.	• Programmet Client Security Software 5.4x kan ikke installeres oven i programmet Client Security Solution 6.0. • Funktionerne i Client Security Software 5.4x påvirkes ikke af, at du vælger at slette datafiler og indstillinger, når du bliver spurgt om du vil slette dem. • Når du fjerner programmet Rescue and Recovery 3.0, fjerner du også automatisk programmet Client Security Solution 6.0.

Tabel 6-1. Tabellen nedenfor indeholder oplysninger, der kan hjælpe dig med at ændre konfigurationen af Rescue and Recovery- og Client Security-programmet. Standalone Client Security Solution betyder, at installationspakken er anskaffet fra internettet eller fra en cd. (fortsat)

Installeret software:	Du vil:	Gør følgende:	Kommentarer
Rescue and Recovery 3.0 og Client Security Solution 6.0	Rescue and Recovery 3.0	1. Vælg **Rediger** under Tilføj/fjern programmer. 2. Fjern programmet Client Security Solution 6.0.	• Lokale sikkerhedskopier slettes, når programmet Client Security Solution 6.0 fjernes. • Når du fjerner programmet Client Security Solution 6.0, har du heller ikke længere Password Manager eller PrivateDisk. • De Rescue and Recovery 3.0-sikkerhedskopier, som er beskyttet med programmet Client Security Solution 6.0, er ikke længere tilgængelige. Opret en ny sikkerhedskopi så hurtigt som muligt.
Rescue and Recovery 3.0 og Client Security Solution 6.0	Client Security Solution 6.0	1. Fjern programmet Rescue and Recovery 3.0. 2. Når du bliver spurgt, skal du kun vælge at beholde de aktive Client Security Solution 6.0-indstillinger, hvis du vil bevare den aktuelle sikkerhedskonfiguration. 3. Installér programmet Client Security Solution 6.0 (Standalone).	1. De Rescue and Recovery 3.0-sikkerhedskopier, der er beskyttet af Client Security Solution 6.0, er ikke længere tilgængelige. 2. Lokale sikkerhedskopier slettes, når du fjerner programmet Rescue and Recovery 3.0.

Rescue and Recovery-kodeord og -kodesætninger

Du kan bruge kodeord eller kodesætninger til at beskytte Rescue and Recovery-arbejdsområdet, hvorved du beskytter centrale data mod uautoriseret adgang. Du kan angive, at du vil beskytte Rescue and Recovery-arbejdsområdet ved at bruge guiden Client Security Setup til at angive sikkerhedsindstillinger eller programmet Client Security Solution til at ændre logonindstillingerne. Med programmet Client Security Solution kan du angive muligheder for retablering af kodeord i Rescue and Recovery-arbejdsområdet.

Bemærkninger:

1. Denne facilitet er kun tilgængelig, hvis programmet Client Security Solution er installeret. Hvis du vil bruge denne facilitet, skal du have afsluttet guiden Client Security 6.0 Setup og angivet, at du vil bruge et kodeord eller en kodesætning for at kunne logge på computeren.
2. Guiden Client Security Setup 6.0 og programmet Client Security Solution 6.0 er kun tilgængelige under Windows. Hvis du vælger at bruge Rescue and Reco-

very uden Client Security Solution, bliver Rescue and Recovery-arbejdsområdet ikke beskyttet af et kodeord eller en kodesætning.

3. Med programmet Client Security Solution kan du angive muligheder for retablering af kodeord i Rescue and Recovery-arbejdsområdet.

Brug følgende metoder for at beskytte Rescue and Recovery-området med et kodeord eller en kodesætning.

Metode 1: Hvis du ikke har gennemført guiden Client Security Setup, skal du gøre følgende for at beskytte Rescue and Recovery-arbejdsområdet med et kodeord eller en kodesætning:

1. Klik på **Start** på Windows-skrivebordet, klik på **Alle programmer**, vælg **ThinkVantage**, og dobbeltklik på **Client Security Solution**.
2. Klik på menupunktet **Udvidet** i vinduet Client Security Solution.
3. Klik på ikonen **Angiv indstillinger til sikkerhed og sikkerhedskopiering**. Guiden Client Security Setup åbnes.
4. Angiv sikkerhedsindstillingerne. Gør herefter et af følgende:
   - Hvis du vil beskytte Rescue and Recovery-arbejdsområdet vha. din Windows-logonadgangskode, skal du markere afkrydsningsfeltet **Brug Windows-kodeordet til at beskytte adgang til Rescue and Recovery-arbejdsområdet**.
   - Hvis du vil beskytte Rescue and Recovery-arbejdsområdet vha. din Client Security Solution-logonkodesætning, skal du markere afkrydsningsfeltet **Brug Client Security Solution-kodesætningen til at beskytte adgang til Rescue and Recovery-området**.
5. Gennemfør guiden Client Security Solution Setup, og klik på **Udfør**. Klik på **Hjælp** i guiden Client Security Setup for at få flere oplysninger.

Metode 2: Hvis du har gennemført guiden Client Security Setup, skal du gøre følgende for at beskytte Rescue and Recovery-arbejdsområdet med et kodeord eller en kodesætning:

1. Klik på **Start** på Windows-skrivebordet, klik på **Alle programmer**, vælg **ThinkVantage**, og dobbeltklik på **Client Security Solution**.
2. Klik på menupunktet **Udvidet** i vinduet Client Security Solution.
3. Klik på **Revidér logonindstillinger**.
4. Følg vejledningen på skærmen. Klik på **Hjælp** i programmet Client Security Solution for at få flere oplysninger.

Angivelse af indstillinger for sikkerhedskopiering ved hjælp af guiden Client Security Setup

Guiden Client Security Solution Setup indeholder konfigurationsvalg, som du kan bruge til at angive mange forskellige sikkerhedsfaciliteter, f.eks. aktivering af den indbyggede sikkerhedschip, angivelse af, hvordan du vil godkende i Windows, hvordan du vil bruge Rescue and Recovery til at tage sikkerhedskopier af dine følsomme data, eller om du vil bruge fingeraftryksgodkendelse.

Gør følgende for at bruge guiden Client Security Setup:

1. Klik på **Start** på Windows-skrivebordet, klik på **Alle programmer**, vælg **ThinkVantage**, og dobbeltklik på **Client Security Solution**.
2. Klik på menupunktet **Udvidet** i vinduet Client Security Solution.
3. Klik på **Angiv indstillinger til sikkerhed og sikkerhedskopiering** i vinduet Client Security Solution. Guiden Client Security Setup åbnes.

4. Angiv sikkerhedsindstillingerne.
5. Gennemfør guiden Client Security Solution Setup, og klik på **Udfør**. Klik på **Hjælp** i guiden Client Security Setup for at få flere oplysninger.

Flere oplysninger om Client Security Solution

Brugervejledning til Client Security Solution på internettet indeholder flere oplysninger om programmet Client Security Solution og dets faciliteter:

`http://www.ibm.com/pc/support/site.wss/`

Hvis du allerede har installeret programmet Client Security Solution, kan du få adgang til brugervejledningen, der indeholder flere oplysninger, ved at gøre følgende:

1. Klik på **Start** på Windows-skrivebordet.
2. Vælg **Alle programmer**.
3. Vælg **ThinkVantage**.
4. Klik på **Client Security Solution**.
5. Klik på **Hjælp** på menulinjen i Client Security Solution.
6. Klik på **User's Guide**.

Hoofdstuk 7. Nederlands

Client Security Solution is een suite van ThinkVantage™ Technology-hulpprogramma's die zijn ontworpen om toegang tot het besturingssysteem en de persoonlijke gegevens op uw computer te beveiligen. Client Security Solution integreert de hardwarebeveiliging van de ingebedde chip en de beveiligingsmogelijkheden van de software. Door de vast toegewezen hardware te combineren met de softwarebeveiliging, vormt Client Security Solution een krachtige verbetering van het beveiligingssysteem van het besturingssysteem.

Voor wie is deze handleiding bestemd

De *ThinkVantage Client Security Solution-gebruikershandleiding* is bedoeld voor zelfstandige eindgebruikers en eindgebruikers in een bedrijfsomgeving. Deze handleiding biedt informatie over de volgende onderwerpen:

- Client Security Solution-componenten
- Client Security Solution-installatie
- Client Security Solution-functies

Deze handleiding is een aanvulling op het Client Security Solution-helpsysteem, waarin u stap voor stap instructies krijgt over het uitvoeren van specifieke taken.

Aanvullende informatie

Als u systeembeheerder, systeemtechnicus, netwerkbeheerder of klanttechnicus bent en Client Security Solution in een grote onderneming wilt implementeren, kunt u gedetailleerde informatie lezen in *ThinkVantage Rescue and Recovery™ en Client Security Solution Gids voor ingebruikname* op de volgende website:

`http://www.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-54502`

Client Security Solution-componenten

Client Security Solution is ontworpen voor computers die zijn uitgerust met een ingebedde beveiligings-chip, die diverse beveiligingsniveaus toevoegt voor computergegevens en -processen. De Client Security Solution-software kan nu echter ook worden geconfigureerd om de beveiliging te verbeteren van computers die geen beveiligings-chip hebben.

Client Security Solution is onderverdeeld in de volgende hardware- en software-componenten.

- **Ingebedde beveiligings-chip**

  Client Security Solution is ontworpen voor computers die zijn uitgerust met een ingebedde beveiligings-chip. Een ingebedde beveiligings-chip is ingebouwde cryptografische hardware die een extra niveau toevoegt aan de beveiliging van de computer. Dankzij de beveiligings-chip kunt u coderings- en verificatie-processen overbrengen van kwetsbare software naar de veilige omgeving van vast toegewezen hardware. Het verhoogde niveau van beveiliging is direct te merken.
- **Client Security Setup Wizard**

  De Client Security Setup Wizard leidt u door de configuratieprocessen van de beveiliging. Met behulp van de wizard kunt u de ingebedde beveiligings-chip inschakelen, de verificatie- en aanmeldingsmethode selecteren, vragen instellen voor het geval van vergeten wachtwoorden, vingerafdrukverificatie instellen (optioneel) en verdere Client Security Solution-componenten configureren.

- **Wachtwoordbeheer**

  Met Client Security-wachtwoordbeheer kunt u veilig en handig de persoonlijke aanmeldingsinformatie voor toepassingen en websites beheren. Dit betreft bijvoorbeeld gebruikers-ID's, wachtwoorden en andere persoonlijke informatie. Client Security-wachtwoordbeheer slaat alle informatie op via de ingebedde beveiligings-chip, zodat de toegang tot toepassingen en websites volledig beveiligd is.
- **PrivateDisk**

  PrivateDisk stelt een gecodeerd virtueel schijfstation in dat automatisch alle gegevens codeert die u opslaat in de veilige omgeving van de ″elektronische kluis″. Met uw eigen virtuele schijfstation codeert u alle belangrijke gegevens voordat u ze opslaat. De gegevens worden automatisch gecodeerd als ze worden opgeslagen in een PrivateDisk-volume.
- **Client Security Solution-toepassing**

  De Client Security Solution-toepassing biedt een enkelvoudige interface waarmee gebruikers eenvoudige of geavanceerde taken kunnen uitvoeren, zoals het inschakelen van de ingebedde beveiligings-chip, het wijzigen van het wachtwoord en het gebruiken van vingerafdruksoftware. Voor een complete lijst met Client Security Solution-functies raadpleegt u “Client Security Solution-functies” op pagina 7-3
- **ThinkVantage-vingerafdruksoftware**

  Met ThinkVantage-vingerafdruksoftware kunnen gebruikers verificatie van vingerafdrukken instellen. Deze handige beveiligingsmogelijkheid is beschikbaar op geavanceerde ThinkPad- en ThinkCentre-modellen en -opties.

Voordat u Client Security Solution installeert

Voordat u de toepassing Client Security Solution installeert, moet u zeker weten dat aan de volgende vereisten is voldaan:

- Windows XP of Windows 2000 met Service Pack 3. Als u dit programma installeert op een vaste schijf met een capaciteit van meer dan 137 GB, is Service Pack 1 vereist voor Windows XP.
- Internet Explorer 5.5 (of hoger).
- 128 MB geheugen, waarvan niet meer dan 8 MB als gedeeld geheugen kan worden toegewezen onder de beeldinstelling in het BIOS.
- 800 MB vrije schijfruimte.

Als u een vorige versie van Client Security Solution, Client Security Software of Rescue and Recovery hebt, raadpleegt u “Client Security Solution gebruiken met Rescue and Recovery” op pagina 7-5 voor specifieke instructies.

Client Security Solution instellen

De Client Security Solution-toepassing is beschikbaar op de website `http://www.pc.ibm.com/thinkvantage`. Het ophalen, installeren en configureren van Client Security Solution kost niet meer dan een paar minuten.

Client Security Solution ophalen en installeren

Voer het volgende proces uit om het programma Client Security Solution op te halen en te installeren:

1. Start de computer en sluit alle geopende programma’s.
2. Ga naar de website `http://www.pc.ibm.com/thinkvantage`.
3. Klik op **Support and downloads** in de sectie Resources.
4. Blader naar de sectie Embedded Security Subsystem and Client Security Solution en klik op **Software download**.
5. Volg de aanwijzingen op het scherm.
6. Start het uitvoerbare installatiebestand en volg de instructies op het scherm. U krijgt de keuze om de Client Security Solution-componenten Password Manager en PrivateDisk te installeren.
7. Nadat u uw keuze hebt gemaakt, wordt u gevraagd de computer opnieuw te starten.
8. Als dit is gebeurd, wordt Client Security Setup Wizard geopend. Als de installatiewizard niet wordt geopend, raadpleegt u “Client Security Setup Wizard openen”
9. Doorloop alle stappen van Client Security Setup Wizard om het configuratieproces te voltooien.

Client Security Setup Wizard openen

Voer de volgende procedure uit om Client Security Solution te configureren met behulp van Client Security Setup Wizard:

1. Klik op het Windows-bureaublad op **Start** en **Programma’s**, selecteer **ThinkVantage** en dubbelklik op **Client Security Solution**.
2. Klik in het Client Security Solution-venster op de menuoptie **Advanced.**
3. Klik in het Client Security Solution-venster op **Set security and backup preferences**. De Client Security Setup Wizard wordt nu geopend.
4. Doorloop de stappen in de Client Security Solution Setup Wizard en klik vervolgens op **Finish**. Voor gedetailleerde informatie klikt u op **Help** in de Client Security Setup Wizard.

Client Security Solution gebruiken

Voer de volgende procedure uit om toegang te krijgen tot Client Security Solution:

1. Klik op het Windows-bureaublad op de knop **Start**.
2. Kies **Programma’s**.
3. Kies **ThinkVantage**.
4. Klik op **Client Security Solution**.

Client Security Solution-functies

De volgende informatie betreft de verschillende taken die u met Client Security Solution kunt uitvoeren.

Opmerking: Als bepaalde vermelde hulpprogramma’s niet beschikbaar zijn, kan dit komen doordat u niet de juiste software hebt geïnstalleerd, uw computer de toepassing niet ondersteunt of de toepassing alleen toegankelijk is voor beheerders of supervisors.

Basisfuncties

De volgende informatie betreft de basistaken die u met Client Security Solution kunt uitvoeren.

Het wachtwoord wijzigen: Met het hulpprogramma Change passphrase kunt u een nieuw wachtwoord voor Client Security instellen. Wachtwoorden moeten voldoen aan de Client Security-wachtwoordvereisten.

Wachtwoordherstel configureren: Met het hulpprogramma Configure password recovery kunt u een vergeten Windows- of Client Security-wachtwoord herstellen, afhankelijk van de verificatiemethode die u gebruikt.

Aanmeldingsinformatie beheren: Dankzij de toepassing Password Manager kunt u Client Security Solution gebruiken om persoonlijke of eenvoudig te vergeten aanmeldingsinformatie te beheren, zoals gebruikers-ID's, wachtwoorden en andere persoonlijke informatie. Password Manager slaat alle informatie op via de ingebedde beveiligings-chip, zodat uw verificatiebeleid de toegang regelt tot beveiligde toepassingen en websites. In plaats van het onthouden of leveren van een grote hoeveelheid wachtwoorden (die alle andere regels en vervaldatums kennen) hoeft u slechts één wachtwoord te onthouden. Als u vingerafdruksoftware hebt geïnstalleerd, is zelfs een vingerafdruk voldoende.

Vingerafdruksoftware gebruiken: Met de geïntegreerde vingerafdruklezer kunt u zich aanmelden met uw vingerafdruk voor het aanzetten van de computer en toegang tot Windows en de vaste schijf. De vingerafdruk neemt de plaats van het wachtwoord in en biedt een eenvoudige en veilige gebruikerstoegang. Er is een toetsenbord met vingerafdruklezer beschikbaar voor bepaalde computers en deze kan als optie worden aangeschaft. Deze optie wordt alleen ondersteund door bepaalde ThinkCentre- en ThinkPad-computers.

Gegevens beschermen: Het hulpprogramma PrivateDisk genereert een gecodeerd virtueel schijfstation dat automatisch alle gegevens codeert die u opslaat in de veilige omgeving van de ″elektronische kluis″.

Geavanceerde mogelijkheden

De volgende informatie betreft de geavanceerde taken die u met Client Security Solution kunt uitvoeren.

Opmerking: U moet beschikken over een toegangsmachtiging als beheerder om de volgende taken te kunnen verrichten.

De beveiligingsinstellingen bewaken: Met het hulpprogramma Security Advisor kunt u een samenvatting bekijken van de beveiligingsinstellingen op de computer. U kunt de huidige beveiligingsstatus bekijken of de systeembeveiliging verbeteren. Enkele verdere beveiligingsonderwerpen zijn hardwarewachtwoorden, Windows-gebruikerswachtwoorden, Windows-wachtwoordenbeleid, beveiligde screensavers en bestandsdeling.

Opmerking: Het hulpprogramma Security Advisor biedt alleen een samenvatting en suggesties om de veiligheid van het systeem te verbeteren. Op bepaalde aspecten van de beveiliging wordt niet ingegaan, zoals het gebruik van antivirus-programma's en firewalls. Voor veel instellingen is de status van beheerder of supervisor vereist.

Digitale certificaten overdragen: Met de Client Security Certificate Transfer Wizard brengt u de persoonlijke sleutels van certificaten over van de software-gebaseerde cryptografische serviceprovider (CSP) van Microsoft naar de hardware-gebaseerde CSP van Client Security Solution. Na de overdracht zijn alle acties die de certificaten gebruiken veiliger, omdat de persoonlijke sleutels zijn beveiligd door de ingebedde beveiligings-chip.

Een mechanisme voor het herstel van hardwarewachtwoorden in gebruik nemen: Dit hulpprogramma maakt een beveiligde omgeving die onafhankelijk van Windows actief is en u helpt bij het opnieuw instellen van vergeten systeemwachtwoorden of wachtwoorden voor de vaste schijf. De identiteit wordt vastgesteld aan de hand van een aantal vragen. Het is verstandig om zo snel mogelijk een beveiligde omgeving te maken, voordat iemand een wachtwoord vergeet. U kunt een vergeten wachtwoord pas herstellen als deze veilige omgeving op de vaste schijf is gemaakt en u de registratie hebt uitgevoerd. Het hulpprogramma is alleen beschikbaar op bepaalde ThinkCentre- en ThinkPad-computers.

Opmerking: Het is verstandig een beheerders- of supervisorwachtwoord in te stellen voordat u dit hulpprogramma gebruikt. Als u geen beheerders- of supervisorwachtwoord hebt ingesteld, is uw omgeving niet optimaal beveiligd. Als u deze procedure voltooit, zijn het systeemwachtwoord en het wachtwoord voor de vaste schijf gelijk. De procedure is bedoeld om u te helpen bij het maken van een veilige omgeving en hierna vergeten wachtwoorden te herstellen.

De ingebedde beveiligings-chip activeren: Dit hulpprogramma voert een wijziging in de BIOS-instellingen uit, zodat de ingebedde beveiligings-chip in- of uitgeschakeld kan worden. U moet de computer opnieuw starten voordat deze wijziging van kracht wordt.

De aanmeldingsinstellingen wijzigen: Dit hulpprogramma geeft de huidige aanmeldingsinstellingen weer en stelt een beheerder in staat de wijze van aanmelding bij Windows en het werkgebied ThinkVantage Rescue and Recovery te wijzigen.

De teller van onjuiste aanmeldingen op nul zetten: Dit hulpprogramma zet de verificatieteller op nul. Deze houdt bij hoeveel onjuiste verificatiepogingen naar de ingebedde beveiligings-chip zijn gestuurd. Na een vastgesteld aantal mislukte pogingen wordt de chip voor een bepaalde tijd geblokkeerd. De blokkadeperiode wordt langer naarmate er meer mislukte pogingen worden gedaan.

Voorkeuren voor beveiliging en backups instellen: Met de Client Security Setup Wizard kunt u een verscheidenheid aan hulpprogramma’s voor beveiligingssoftware configureren. De wizard biedt configuratiemogelijkheden voor beveiligingsopties, zoals het inschakelen van de ingebedde beveiligings-chip, het kiezen van de Windows-verificatieomgeving, het kiezen van Rescue and Recovery voor backups van vertrouwelijke gegevens of het gebruiken van een vingerafdruk als verificatie.

Client Security Solution gebruiken met Rescue and Recovery

Het programma Rescue and Recovery en de toepassing Client Security Solution zijn ThinkVantage-technologieën die zijn ontwikkeld om aan uw behoeften te voldoen. Dat betekent dat ze zijn ontworpen om afzonderlijk of samen gebruikt te kunnen worden, afhankelijk van wat u nodig hebt. De volgende informatie is bedoeld om te bepalen hoe u deze programma’s wilt gebruiken en hoe de programma’s elkaar aanvullen.

Er zijn belangrijke zaken om rekening mee te houden als u Rescue and Recovery, Client Security Solution of beide installeert. In de volgende tabellen vindt u informatie waarmee u de juiste procedure voor de gewenste configuratie kunt bepalen:

Tabel 1-1. In de volgende tabel vindt u informatie over het wijzigen van de configuratie van Rescue and Recovery en Client Security. Client Security Solution-standalone betekent dat de installatie afkomstig is van het web of een CD.

Geïnstalleerde software is...	**En u wilt...**	**Dit proces volgen**	**Commentaar**
Client Security Software 5.4x	Client Security Software 5.4x en Rescue and Recovery 3.0	1. Rescue and Recovery 3.0 installeren. 2. Geef als het wordt gevraagd aan dat u de installatie van Client Security Software 5.4x wilt behouden.	Backups kunnen niet worden beveiligd met Client Security Software 5.4x. Het gebruik van Client Security Software-functies door Rescue and Recovery 3.0 wordt uitgevoerd door een geëmuleerde versie van Client Security Software. De masterwachtwoord-functie wordt aan de beveiligingsmogelijkheden toegevoegd. Een master-wachtwoord wordt normaal in een bedrijfsomgeving gebruikt. Voor verdere informatie raadpleegt u “Aanvullende informatie” op pagina 7-1
Client Security Software 5.4x	Client Security Solution 6.0 Standalone-installatiepakket	1. Verwijder de installatie van Client Security Software 5.4x. 2. Installeer Client Security Solution 6.0 (standalone).	• U moet gecodeerde bestanden decoderen en eventueel aanwezige wachtwoordbeheer-informatie exporteren voordat u de installatie verwijdert. Hiermee voorkomt u dat de informatie verloren gaat. • U moet IBM® File and Folder Encryption verwijderen voordat u Client Security Solution installeert.

Tabel 1-1. In de volgende tabel vindt u informatie over het wijzigen van de configuratie van Rescue and Recovery en Client Security. Client Security Solution-standalone betekent dat de installatie afkomstig is van het web of een CD. (vervolg)

Geïnstalleerde software is...	**En u wilt...**	**Dit proces volgen**	**Commentaar**
Client Security Software 5.4x	Client Security Solution 6.0 en Rescue and Recovery 3.0	1. Verwijder de installatie van Client Security Software 5.4x 2. Installeer Rescue and Recovery 3.0. (Zorg dat de component Client Security Solution 6.0 is geselecteerd.)	• Als u Rescue and Recovery 3.0 over Client Security Software 5.4x installeert zonder eerst de installatie van Client Security Software te verwijderen, beschikt u alleen over Rescue and Recovery. • Voordat u de installatie van Client Security Software 5.4x verwijdert, moet u gecodeerde bestanden decoderen en eventueel aanwezige wachtwoordbeheer-informatie exporteren. Hiermee voorkomt u dat de informatie verloren gaat. • U moet IBM® File and Folder Encryption verwijderen voordat u Client Security Solution 6.0 installeert.
Rescue and Recovery 3.0	Client Security Software 5.4x en Rescue and Recovery 3.0	1. Verwijder de installatie van Rescue and Recovery 3.0. 2. Installeer Client Security Software 5.4x. 3. Installeer Rescue and Recovery 3.0. 4. Geef als het wordt gevraagd aan dat u de installatie van Client Security Software 5.4x wilt behouden.	• Client Security Software 5.4x kan niet worden geïnstalleerd over Rescue and Recovery 3.0. • Bij het verwijderen van de installatie van Rescue and Recovery 3.0 worden lokale backups gewist.

Tabel 1-1. In de volgende tabel vindt u informatie over het wijzigen van de configuratie van Rescue and Recovery en Client Security. Client Security Solution-standalone betekent dat de installatie afkomstig is van het web of een CD. (vervolg)

Geïnstalleerde software is...	En u wilt...	Dit proces volgen	Commentaar
Rescue and Recovery 3.0	Client Security Solution 6.0 Standalone-installatiepakket	1. Verwijder de installatie van Rescue and Recovery 3.0. 2. Installeer Client Security Solution 6.0 (standalone).	• Installatie verwijderen Rescue and Recovery wist de gebruikersbestanden en de registerinstellingen van Client Security Solution. • Rescue and Recovery-backups die zijn beveiligd met Client Security Solution, zijn niet meer toegankelijk. • Bij het verwijderen van de installatie van Rescue and Recovery 3.0 worden lokale backups gewist. • Client Security Solution 6.0 (standalone) kan niet worden geïnstalleerd over Rescue and Recovery 3.0.
Rescue and Recovery 3.0	Rescue and Recovery 3.0 en Client Security Solution 6.0	1. Selecteer de optie **Wijzigen** onder Programma’s toevoegen of verwijderen. 2. Voer de wijzigingen uit door Client Security Solution en eventuele subcomponenten toe te voegen.	• Bij het toevoegen van Client Security Solution worden lokale backups verwijderd. • Na het toevoegen van Client Security Solution maakt u zo snel mogelijk een nieuwe basisbackup. • De Client Security Solution-instellingen en -gegevensbestanden worden gewist. • Client Security Solution 6.0 (standalone) kan niet worden geïnstalleerd over Rescue and Recovery 3.0.
Client Security Solution 6.0 Standalone-installatiepakket	Client Security Software 5.4x	1. Verwijder de installatie van Client Security Solution 6.0 (standalone). 2. Installeer Client Security Software 5.4x.	• Het wissen van de gegevensbestanden en instellingen van Client Security Solution 6.0 is niet van invloed op Client Security Software 5.4x-bewerkingen.

Tabel 1-1. In de volgende tabel vindt u informatie over het wijzigen van de configuratie van Rescue and Recovery en Client Security. Client Security Solution-standalone betekent dat de installatie afkomstig is van het web of een CD. (vervolg)

Geïnstalleerde software is...	En u wilt...	Dit proces volgen	Commentaar
Client Security Solution 6.0 Standalone-installatiepakket	Rescue and Recovery 3.0	1. Verwijder de installatie van Client Security Solution 6.0 2. Installeer Rescue and Recovery 3.0. 3. Installeer tijdens het installatieproces alleen Rescue and Recovery.	Wanneer u de installatie van Client Security Solution 6.0 verwijdert, moet u ook de Security Solution 6.0-bestanden en -instellingen verwijderen. Als u dit niet doet als het u wordt gevraagd, wordt het installatieproces van Rescue and Recovery 3.0 beëindigd.
Client Security Solution 6.0 Standalone	Rescue and Recovery 3.0 en Client Security Solution 6.0	1. Installeer Rescue and Recovery 3.0. 2. Selecteer de subcomponenten van Client Security Solution 6.0 die u wilt installeren.	• Gegevensbestanden en instellingen van Client Security Solution 6.0 blijven behouden. • Wanneer u backups wilt beveiligen die zijn gemaakt met Client Security Solution 6.0, gebruikt u Rescue and Recovery.
Rescue and Recovery 3.0 en Client Security Solution 6.0	Client Security Software 5.4x	1. Verwijder de installatie van Rescue and Recovery - Client Security Solution. 2. Installeer Client Security Software 5.4x.	• Client Security Software 5.4x kan niet worden geïnstalleerd over Client Security Solution 6.0. • Het wissen van de gegevensbestanden en instellingen is niet van invloed op Client Security Software 5.4x-bewerkingen. • Als u de installatie van Rescue and Recovery 3.0 verwijdert, wordt automatisch ook de installatie van Client Security Solution 6.0 verwijderd.

Tabel 1-1. In de volgende tabel vindt u informatie over het wijzigen van de configuratie van Rescue and Recovery en Client Security. Client Security Solution-standalone betekent dat de installatie afkomstig is van het web of een CD. (vervolg)

Geïnstalleerde software is...	**En u wilt...**	**Dit proces volgen**	**Commentaar**
Rescue and Recovery 3.0 en Client Security Solution 6.0	Rescue and Recovery 3.0	1. Selecteer **Wijzigen** onder Programma's toevoegen of verwijderen. 2. Verwijder de installatie van Client Security Solution 6.0	• Bij het verwijderen van Client Security Solution worden lokale backups ook verwijderd. • Wanneer Client Security Solution 6.0 verwijdert, hebt u geen beschikking meer over Password Manager en PrivateDisk. • De backups van Rescue and Recovery 3.0 die zijn beschermd met Client Security Solution 6.0, zijn niet meer toegankelijk. Maak zo snel mogelijk een nieuwe backup.
Rescue and Recovery 3.0 en Client Security Solution 6.0	Client Security Solution 6.0	1. Verwijder de installatie van Rescue and Recovery 3.0. 2. Bewaar de huidige Client Security Solution 6.0-instellingen alleen als u de huidige beveiligingsconfiguratie wilt behouden. 3. Installeer Client Security Solution 6.0 (standalone).	1. De backups van Rescue and Recovery 3.0 die zijn beschermd met Client Security Solution 6.0, zijn niet meer toegankelijk. 2. Bij het verwijderen van de installatie van Rescue and Recovery 3.0 worden lokale backups gewist.

Wachtwoorden van Rescue and Recovery

U kunt wachtwoorden gebruiken om het werkgebied van Rescue and Recovery te beveiligen. Op deze manier zijn vertrouwelijke gegevens beveiligd tegen ongemachtigde toegang. U kunt het werkgebied van Rescue and Recovery beveiligen door beveiligingsvoorkeuren in te stellen met de Client Security Setup Wizard of door de aanmeldingsinstellingen te wijzigen met Client Security Solution. Met Client Security Solution kunt u ook opties voor het herstel van wachtwoorden definiëren in het werkgebied van Rescue and Recovery.

Opmerkingen:

1. Deze mogelijkheid is alleen aanwezig als Client Security Solution 6.0 is geïnstalleerd. Om deze functie te kunnen gebruiken, moet u de stappen van de Client Security 6.0 Setup Wizard hebben doorlopen en opgegeven dat u een wachtwoord wilt gebruiken om u bij de computer aan te melden.
2. De Client Security Setup 6.0 Wizard en Client Security Solution 6.0 zijn beide alleen in de Windows-omgeving toegankelijk. Als u Rescue and Recovery zonder Client Security Solution wilt gebruiken, is het werkgebied van Rescue and Recovery niet beveiligd met een wachtwoord.
3. Met Client Security Solution kunt u opties voor het herstel van wachtwoorden definiëren in het werkgebied van Rescue and Recovery.

U gebruikt de volgende methoden om het werkgebied van Rescue and Recovery te beveiligen met een wachtwoord.

Methode 1: Als u niet alle stappen van de Client Security Setup Wizard hebt doorlopen, doet u het volgende om het werkgebied van Rescue and Recovery te beveiligen met een wachtwoord:

1. Klik op het Windows-bureaublad op **Start** en **Programma's**, selecteer **ThinkVantage** en dubbelklik op **Client Security Solution**.
2. Klik in het Client Security Solution-venster op de menuoptie **Advanced.**
3. Klik op het pictogram **Set security and backup preferences**. De Client Security Setup Wizard wordt nu geopend.
4. Stel de beveiligingsvoorkeuren in. Kies een van de volgende opties als erom wordt gevraagd:
   - Als u het werkgebied van Rescue and Recovery wilt beveiligen met uw Windows-aanmeldingswachtwoord, selecteert u het selectievakje **Use Windows password to gain access to the Rescue and Recovery workspace** .
   - Als u het werkgebied van Rescue and Recovery wilt beveiligen met uw Client Security Solution-aanmeldingswachtwoord, selecteert u het selectievakje **Use the Client Security Solution passphrase to gain access to the Rescue and Recovery workspace** .
5. Doorloop de stappen in de Client Security Solution Setup Wizard en klik vervolgens op **Finish**. Voor gedetailleerde informatie klikt u op **Help** in de Client Security Setup Wizard.

Methode 2: Als u alle stappen van de Client Security Setup Wizard hebt doorlopen, doet u het volgende om het werkgebied van Rescue and Recovery te beveiligen met een wachtwoord:

1. Klik op het Windows-bureaublad op **Start** en **Programma's**, selecteer **ThinkVantage** en dubbelklik op **Client Security Solution**.
2. Klik in het Client Security Solution-venster op de menuoptie **Advanced.**
3. Klik op **Change logon settings**.
4. Volg de aanwijzingen op het scherm. Voor gedetailleerde informatie klikt u op **Help** in Client Security Solution.

Backupvoorkeuren instellen met de Client Security Setup Wizard

De Client Security Solution Setup Wizard biedt configuratiemogelijkheden voor beveiligingsopties, zoals het inschakelen van de ingebedde beveiligings-chip, het kiezen van de Windows-verificatieomgeving, het kiezen van Rescue and Recovery voor backups van vertrouwelijke gegevens of het gebruiken van een vingerafdruk als verificatie.

Voer de volgende procedure uit om de Client Security Setup Wizard te kunnen gebruiken:

1. Klik op het Windows-bureaublad op **Start** en **Programma's**, selecteer **ThinkVantage** en dubbelklik op **Client Security Solution**.
2. Klik in het Client Security Solution-venster op de menuoptie **Advanced**.
3. Klik in het Client Security Solution-venster op **Set security and backup preferences**. De Client Security Setup Wizard wordt nu geopend.
4. Stel de beveiligingsvoorkeuren in.

5. Doorloop de stappen in de Client Security Solution Setup Wizard en klik vervolgens op **Finish**. Voor gedetailleerde informatie klikt u op **Help** in de Client Security Setup Wizard.

Meer informatie over Client Security Solution

Voor verdere informatie over Client Security Solution en alle functies raadpleegt u *Client Security Solution User Guide* op het webadres:

```
http://www.ibm.com/pc/support/site.wss/
```

Als u Client Security Solution als hebt geïnstalleerd, kunt u verdere informatie in de Gebruikershandleiding vinden volgens de volgende procedure:

1. Klik op het Windows-bureaublad op de knop **Start**.
2. Kies **Programma's**.
3. Kies **ThinkVantage**.
4. Klik op **Client Security Solution**.
5. Klik op de menubalk in Client Security Solution op de optie **Help**.
6. Klik op **User's Guide**.

Luku 8. Suomi

Client Security Solution -sovellus hyödyntää ThinkVantage-tekniikkaa, joka on kehitetty auttamaan käyttäjää tietokoneen käyttöjärjestelmän ja tärkeiden tietojen suojauksessa. Client Security Solution -sovelluksessa sisäisen turvapiirin laitteistoperustainen suojaus yhdistyy sen suojausohjelman suojaukseen.Yhdistetyn laitteisto- ja ohjelmistosuojauksen johdosta Client Security Solution -sovellus parantaa tehokkaasti tietokoneen käyttöjärjestelmän sisäisiä suojausominaisuuksia.

Tämän julkaisun käyttäjät

ThinkVantage Client Security Solution User's Guide -julkaisu on tarkoitettu yksittäisille peruskäyttäjille ja yritysympäristössä työskenteleville käyttäjille. Tämä opas sisältää tietoja

- Client Security Solution -sovelluksen osista
- Client Security Solution -sovelluksen asennuksesta
- Client Security Solution -sovelluksen ominaisuuksista.

Tämä opas täydentää Client Security Solution -ohjetoimintoa, jossa on vaiheittaisia ohjeita siitä, miten tiettyjä tehtäviä toteutetaan ohjelmassa.

Lisätietoja

Jos olet järjestelmän pääkäyttäjä, järjestelmäteknikko, verkon pääkäyttäjä tai huoltoteknikko ja haluat ottaa käyttöön Client Security Solution -sovelluksen suuressa yrityksessä, saat lisätietoja *ThinkVantage Rescue and Recovery and Client Security Solution Deployment Guide* -oppaasta, joka on saatavana WWW-osoitteessa

`http://www.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-54502`

Client Security Solution -sovelluksen osat

Client Security Solution -sovellus on suunniteltu sellaisia tietokoneita varten, jotka on varustettu tietokoneen tiedoille ja prosesseille lisäsuojaa antavalla sisäisellä turvapiirillä. Client Security Solution -ohjelman kokoonpanon voi kuitenkin nykyisin määrittää niin, että se takaa myös sellaisten tietokoneiden suojauksen, joissa ei ole turvapiiriä.

Client Security Solution -sovellus on jaettu seuraaviin laitteistoihin ja ohjelmiston osiin:

- **Sisäinen turvapiiri**

  Client Security Solution -sovellus on suunniteltu sellaisia tietokoneita varten, jotka on varustettu sisäisellä turvapiirillä.Sisäinen turvapiiri on laitteiston sisäinen salaustekniikka, joka parantaa tietokoneen suojausta entisestään. Turvapiiri mahdollistaa salaus- ja todennusprosessien siirron vahingoittuneesta ohjelmasta laitteiston suojattuun ympäristöön. Näin parantuneesta suojauksesta saadaan myös rahallista hyötyä.
- **Client Security Setup Wizard -toiminto**

  Ohjattu Client Security Setup Wizard -toiminto opastaa suojausvaihtoehtojen määrityksessä. Ohjattu toiminto auttaa sisäisen turvapiirin käyttöönotossa, todennuksen ja sisäänkirjausmenetelmän valinnassa, salasanan elvytyskysymysten luonnissa, sormenjälkitodennuksen muodostuksessa (valinnainen) ja Client Security Solution -sovelluksen lisäosien kokoonpanon määrityksessä.

- **Password Manager -ohjelma**

  Client Security Password Manager -ohjelma auttaa tärkeiden ja helposti unohtuvien sovellus-tietojen ja WWW-sivustojen sisäänkirjaustietojen, kuten käyttäjätunnusten, salasanojen ja muiden henkilökohtaisten tietojen, turvallisessa ja helpossa hallinnassa. Client Security Password Manager -ohjelma tallentaa kaikki tiedot sisäisen turvapiirin kautta, jotta pääsy sovelluksiin ja WWW-sivustoihin säilyisi varmasti suojattuna.
- **PrivateDisk-ohjelma**

  PrivateDisk-ohjelma luo salatun näennäislevyaseman, joka salaa automaattisesti kaikki tiedot, jotka tallennetaan suojassa tässä ″sähköisessä kassakaapissa″. Tärkeiden tietojen salauksessa ja tallenuksessa voi käyttää omaa näennäislevyasemaa. Järjestelmä salaa tiedot automaattisesti, kun ne on tallennettu johonkin PrivateDisk-taltioon.
- **Client Security Solution -sovellus**

  Client Security Solution -sovelluksen ansiosta käyttäjät voivat yhden liittymän avulla toteuttaa perus- ja lisäsuojaustoimintoja, esimerkiksi ottaa käyttöön sisäisen turvapiirin, vaihtaa salalauseen tai käyttää sormenjälkiohjelmaa. Ohjeet Client Security Solution -toiminnoista ovat kohdassa ”Client Security Solution -ominaisuudet” sivulla 1-3
- **ThinkVantage-sormenjälkiohjelma**

  ThinkVantage-sormenjälkiohjelman avulla voi muodostaa sormenjälkitodennuksen. Tämä kätevä suojaustoiminto on saatavana tietyissä ThinkPad- ja ThinkCentre-malleissa ja -vaihtoehdoissa.

Ennen Client Security Solution -sovelluksen asennusta

Varmista, että seuraavat edellytykset täyttyvät, ennen kuin asennat Client Security Solution -sovelluksen:

- Tietokoneessa on Windows XP- tai Windows 2000 -käyttöjärjestelmä ja Service Pack 3. Jos asennat tämän ohjelman kiintolevyyn, jonka kapasiteetti on yli 137 gigatavua, Windows XP -käyttöjärjestelmässä on oltava Service Pack 1.
- Asennettuna on Internet Explorer 5.5 (tai uudempi).
- Tietokoneessa on 128 megatavua muistia, josta enintään 8 megatavua voidaan määrittää yhteiseksi muistiksi BIOSin näyttöasetuksissa.
- Vapaata levytilaa on 800 megatavua.

Jos käytössä on jokin aiempi Client Security Solution-, Client Security Software- tai Rescue and Recovery -versio, katso erityisohjeita kohdasta ”Client Security Solution -ohjelman käyttö yhdessä Rescue and Recovery -ohjelman kanssa” sivulla 1-5.

Client Security Solution -sovelluksen asennus

Client Security Solution -sovellus on saatavana WWW-sivustosta `http://www.pc.ibm.com/thinkvantage`. Client Security Solution -sovelluksen nouto, asennus ja kokoonpanon määritys kestää vain muutamia minuutteja.

Client Security Solution -sovelluksen nouto ja asennus

Voit noutaa ja asentaa Client Security Solution -ohjelman seuraavasti:

1. Käynnistä tietokone ja lopeta toiminnassa olevat ohjelmat.

2. Siirry WWW-osoitteeseen `http://www.pc.ibm.com/thinkvantage`.
3. Napsauta **Support and downloads** -linkkiä Resources-osassa.
4. Selaa luetteloa Embedded Security Subsystem and Client Security Solution -osan kohtaan ja napsauta kohtaa **Software download**.
5. Noudata kuvaruutuun tulevia ohjeita.
6. Aja asennuksen ohjelmatiedosto ja noudata kuvaruutuun tulevia ohjeita. Voit valita, haluatko asentaa Client Security Solution -ohjelman Password Manager- ja PrivateDisk-osia.
7. Kun olet tehnyt valintasi, sinua kehotetaan käynnistämään tietokone uudelleen.
8. Kun tietokone on käynnistynyt uudelleen, ohjattu Client Security Setup Wizard -toiminto tulee kuvaruutuun. Jos ohjattu asennustoiminto ei ala, katso lisätietoja kohdasta Ohjatun ”Ohjatun Client Security Setup Wizard -toiminnon aloitus” sivulla 1-3 -toiminnon aloitus
9. Aja Client Security Setup Wizard -toiminto loppuun, jotta kokoonpanon määritys onnistuisi.

Ohjatun Client Security Setup Wizard -toiminnon aloitus

Voit määrittää ohjatun Client Security Solution -toiminnon kokoonpanon ohjatun Client Security Setup Wizard -toiminnon avulla seuraavasti:

1. Napsauta Windowsin **Käynnistä**-painiketta, napsauta **Kaikki ohjelmat** -vaihtoehtoa, valitse **ThinkVantage**-vaihtoehto ja kaksoisnapsauta sitten **Client Security Solution** -vaihtoehtoa.
2. Kun Client Security Solution -sovelluksen ikkuna tulee kuvaruutuun, napsauta **Lisäasetukset** -valikkovaihtoehtoa.
3. Kun Client Security Solution -sovelluksen ikkuna tulee kuvaruutuun, napsauta **Suojaus- ja varmistuskopioasetusten määritys** -vaihtoehtoa. Ohjattu Client Security Setup Wizard -toiminto alkaa.
4. Tee loppuun ohjatun Client Security Solution Setup Wizard -toiminnon vaiheet ja napsauta sitten **Lopetus**-painiketta. Lisätietoja saat napsauttamalla ohjatun Client Security Setup Wizard -toiminnon vaihtoehtoa **Ohje**.

Client Security Solution -sovelluksen käyttö

Voit ottaa Client Security Solution -sovelluksen käyttöön seuraavasti:

1. Napsauta Windowsin **Käynnistä**-painiketta.
2. Valitse **Kaikki ohjelmat** -vaihtoehto.
3. Valitse **ThinkVantage**-vaihtoehto.
4. Napsauta **Client Security Solution** -vaihtoehtoa.

Client Security Solution -ominaisuudet

Seuraavassa on yksityiskohtaisia tietoja tehtävistä, jotka voi toteuttaa Client Security Solution -sovelluksen avulla.

Huomautus: Jos et pysty käyttämään kaikkia alla mainittuja työkaluja, tietokoneeseen ei ehkä ole asennettu tarvittavaa ohjelmaa, tietokone ei tue kyseistä sovellusta tai sovelluksen käyttö vaatii pääkäyttäjän oikeudet.

Perusominaisuudet

Seuraavassa on tietoa perustehtävistä, jotka voi toteuttaa Client Security Solution -sovelluksen avulla.

Salalauseen vaihto: Salalauseen vaihto -työkalun avulla voi muodostaa uuden Client Security -salalauseen. Salalauseiden on vastattava Client Security -salalausevaatimuksia.

Salasanan elvytyskokoonpanon määritys: Salasanan elvytyskokoonpanon määritys -työkalun avulla voi elvyttää unohtuneen Windows-salasanan tai Client Security -salalauseen käytössä olevan todennusmenetelmän mukaisesti.

Sisäänkirjaustietojen hallinta: Password Manager -sovellus auttaa tärkeiden ja helposti unohtuvien sisäänkirjaustietojen, kuten käyttäjätunnusten, salasanojen ja muiden henkilökohtaisten tietojen, hallinnassa Client Security Solution -sovelluksen avulla. Password Manager -sovellus tallentaa kaikki tiedot sisäisen turvapiirin kautta, jolloin käyttäjän todennuskäytäntö valvoo suojattujen sovellusten ja WWW-sivustojen käyttöä. Tämä tarkoittaa sitä, että käyttäjän ei tarvitse muistaa monia yksittäisiä salasanoja (joilla kaikilla on eri säännöt ja vanhenemispäivät) vaan hänen on muistettava vain yksi salalause. Jos tietokoneeseen on asennettu sormenjälkiohjelma, käyttäjän on vain annettava sormenjälkensä.

Sormenjälkiohjelman käyttö: Sisäisen sormenjälkitunnistimen avulla käyttäjä voi rekisteröidä ja yhdistää sormenjälkensä käynnistyssalasanaan, kiintolevyn salasanaan ja Windows-salasanaan, niin että sormenjälkitodennus korvaa salasanoja ja mahdollistaa yksinkertaisen ja turvallisen pääsyn tietokoneeseen. Sormenjälkitunnistimen sisältävä näppäimistö on saatavana tiettyihin tietokoneisiin, ja sen voi ostaa lisävarusteena. Tämä vaihtoehto on käytettävissä vain tietyissä ThinkCentre- ja ThinkPad-tietokoneissa.

Tietojen suojaus: PrivateDisk-työkalu luo salatun näennäislevyaseman, joka salaa automaattisesti kaikki tiedot, jotka tallennetaan suojassa tässä ″sähköisessä kassakaapissa″.

Lisätoiminnot

Seuraavassa on tietoa lisätehtävistä, jotka voi toteuttaa Client Security Solution -sovelluksen avulla.

Huomautus: Sinulla on oltava pääkäyttäjän oikeudet, jotta voit toteuttaa seuraavat toiminnot.

Suojausasetusten valvonta: Security Advisor -työkalun avulla voi tarkastella yhteenvetoa senhetkisistä suojausasetuksista. Voit tarkastella joko nykyisen suojauksen tilan asetuksia tai lisätä järjestelmäsuojausta. Joitakin suojaukseen liittyviä aiheita ovat muun muassa laitteistosalasanat, Windows-käyttäjien salasanat, Windows-salasanakäytännöt, suojattu näytönsäästäjä ja tiedostojen yhteiskäyttö.

Huomautus: Security Advisor -työkalu tarjoaa vain yhteenvedon suojausasetuksista ja järjestelmäsuojauksen parannusehdotuksia. Työkalussa ei käsitellä kaikkia suojauksen osa-alueita, esimerkiksi virustentorjunta- ja palomuuriohjelmien käyttöä ja ylläpitoa. Monet asetuksista vaativat pääkäyttäjän oikeuksia.

Digitaalisten varmenteiden siirto: Client Security Certificate Transfer Wizard -ohjelma opastaa varmenteisiin liittyvien yksityisten avaimien siirrossa Microsoftin ohjelmistoperustaisista salausratkaisuista (CSP) laitteistoperustaisiin Client Security Solution (CSP) -salausratkaisuihin. Siirron jälkeen varmenteita käyttävät toiminnot ovat entistä paremmin suojattuja, koska sisäinen turvapiiri suojaa yksityisiä avaimia.

Laitteistosalasanan vaihtomekanismin muodostus: Tämän työkalun avulla voi luoda suojatun ympäristön, joka toimii itsenäisesti Windows-käyttöjärjestelmästä riippumatta. Työkalun avulla voi vaihtaa unohtuneet käynnistyssalasanat ja kiintolevysalasanat. Käyttäjäprofiili muodostuu vastauksista käyttäjän itsensä luomaan kysymyssarjaan. Tämä suojattu ympäristö on hyvä luoda mahdollisimman pian, ennen kuin salasana unohtuu. Unohtunutta salasanaa ei voi vaihtaa, ennen kuin suojattu ympäristö on luotu kiintoasemaan ja käyttäjä on rekisteröitynyt järjestelmään. Tämä työkalu on käytettävissä vain tietyissä ThinkCentre- ja ThinkPad-tietokoneissa.

Huomautus: On suositeltavaa määrittää pääkäyttäjän salasana ennen tämän työkalun käyttöä. Jos pääkäyttäjän salasanaa ei ole määritetty, käyttöympäristö ei ole niin suojattu kuin olisi mahdollista. Kun tämä on tehty, käynnistyssalasana ja kiintolevyn salasana vastaavat toisiaan. Tämä laitteistosalasanan vaihtoprosessi on suunniteltu auttamaan suojatun ympäristön luonnissa ja unohtuneiden salasanojen vaihdossa, kun suojattu ympäristö on jo luotu.

Sisäisen turvapiirin aktivointi: Tämän työkalun avulla voi muuttaa BIOS-asetuksia, joita käytetään sisäisen turvapiirin aktivoinnissa ja käytöstä poistossa. Tietokone on käynnistettävä uudelleen, jotta muutokset tulisivat voimaan.

Sisäänkirjausasetusten vaihto: Tällä työkalulla saa näkyviin nykyiset sisäänkirjausasetukset ja pääkäyttäjä voi vaihtaa Windows-käyttöjärjestelmän sekä ThinkVantage- ja Rescue and Recovery -työtilan sisäänkirjaustiedot.

Todennusten turvalaskurin tyhjennys: Tämä työkalu nollaa epäonnistuneiden todennusten laskurin, joka valvoo, kuinka monta sisäiseen turvapiiriin kohdistuvaa virheellistä todennusyritystä on tapahtunut.Kun tietty määrä yrityksiä on epäonnistunut, turvapiiri lukitsee itsensä tietyksi ajaksi. Lukitusaika on sitä pitempi, mitä enemmän epäonnistuneita yrityksiä tehdään.

Suojaus- ja varmistuskopioasetusten määritys: Ohjatun Client Security Setup Wizard -toiminnon avulla kokoonpanoon voi määrittää useita suojausohjelmia. Tässä ohjatussa toiminnossa on kokoonpanovaihtoehtoja, joiden avulla voi määrittää useita eri suojausominaisuuksia,esimerkiksi sisäisen Client Security -turvapiirin käyttöönoton, Windows-todennuksen valinnan, Rescue and Recovery -ohjelman valinnan tärkeiden tietojen varmistuskopioimiseksi tai sormenjälkitodennuksen käytön valinnan.

Client Security Solution -ohjelman käyttö yhdessä Rescue and Recovery -ohjelman kanssa

Sekä Rescue and Recovery -ohjelma että Client Security Solution -sovellus perustuvat ThinkVantage-tekniikkaan, ja ne on kehitetty käyttäjiä ajatellen. Ne on suunniteltu toimimaan joko yhdessä tai erikseen toisiaan täydentäen käyttäjän tarpeiden mukaan. Seuraavat ohjeet auttavat käyttäjää näiden ohjelmien käytön suunnittelussa. Ohjeista käy myös ilmi, kuinka ohjelmat täydentävät toisiaan.

Asennettaessa Rescue and Recovery -ohjelmaa ja Client Security Solution -sovellusta, joko yhdessä tai erikseen, on kiinnitettävä huomiota tiettyihin asioihin. Seuraavissa taulukoissa olevat tiedot auttavat oikean asennustavan valinnassa haluttua kokoonpanoa varten:

Taulukko 8-1. Seuraavassa taulukossa on tietoja Rescue and Recovery- ja Client Security -ohjelmien kokoonpanon muuttamisesta. Client Security Solution Standalone tarkoittaa, että asennus on tehty WWW-sivustosta tai CD-tietolevystä.

Asennettu ohjelma	Asennettava ohjelma	Toimet	Huomautuksia
Client Security Software 5.4x	Client Security Software 5.4x ja Rescue and Recovery 3.0	1. Asenna Rescue and Recovery 3.0 -ohjelma. 2. Vastaa pyydettäessä, että haluat säilyttää asennetun Client Security Software 5.4x -sovelluksen.	Varmistuskopioita ei voi suojata käyttämällä Client Security Software 5.4x -sovellusta. Kaikki Rescue and Recovery 3.0 -ohjelman käyttämät Client Security Software -toiminnot tehdään emuloidun Client Security Software -ohjelmaversion avulla. Pääkäyttäjän salasanatoiminto lisätään suojausominaisuuksiin. Pääkäyttäjän salasanaa käytetään tavallisesti yrityksissä. Lisätietoja on kohdassa ”Lisätietoja” sivulla 8-1
Client Security Software 5.4x	Client Security Solution 6.0 Standalone -asennuspaketti	1. Poista Client Security Software 5.4x -sovelluksen asennus. 2. Asenna Client Security Solution 6.0 (Standalone) -sovellus.	• Sinun on purettava salaus kaikista salatuista tiedostoista ja vietävä salasanan hallintatiedot ennen sovelluksen poistoa. Muutoin tiedot häviävät. • Sinun on poistettava IBM File and Folder Encryption -salausohjelma, ennen kuin asennat Client Security Solution -sovelluksen.

Taulukko 8-1. Seuraavassa taulukossa on tietoja Rescue and Recovery- ja Client Security -ohjelmien kokoonpanon muuttamisesta. Client Security Solution Standalone tarkoittaa, että asennus on tehty WWW-sivustosta tai CD-tietolevystä. (jatkoa)

Asennettu ohjelma	Asennettava ohjelma	Toimet	Huomautuksia
Client Security Software 5.4x	Client Security Solution 6.0 ja Rescue and Recovery 3.0	1. Poista Client Security Software 5.4x -sovelluksen asennus. 2. Asenna Rescue and Recovery 3.0 -ohjelma. (Varmista, että Client Security Solution 6.0 -osa on valittuna.)	• Jos Rescue and Recovery 3.0 -ohjelma asennetaan Client Security Software 5.4x -sovelluksen päälle poistamatta Client Security Software -ohjelmaa ensin, tuloksena on vain Rescue and Recovery -ohjelman asennus. • Ennen kuin poistat Client Security Software 5.4x -sovelluksen, sinun on purettava salaus kaikista salatuista tiedostoista ja vietävä salasanan hallintatiedot ennen sovelluksen poistoa. Muutoin tiedot häviävät. • Sinun on poistettava IBM File and Folder Encryption -salausohjelma, ennen kuin asennat Client Security Solution 6.0 -sovelluksen.
Rescue and Recovery 3.0	Client Security Software 5.4x ja Rescue and Recovery 3.0	1. Poista Rescue and Recovery 3.0 -ohjelman asennus. 2. Asenna Client Security Software 5.4x -sovellus. 3. Asenna Rescue and Recovery 3.0 -ohjelma. 4. Vastaa pyydettäessä, että haluat säilyttää asennetun Client Security Software 5.4x -sovelluksen.	• Client Security Software 5.4x -sovellusta ei voi asentaa Rescue and Recovery 3.0 -ohjelman päälle. • Paikalliset varmistuskopiot poistetaan, kun Rescue and Recovery 3.0 -ohjelman asennus on poistettu.

Taulukko 8-1. Seuraavassa taulukossa on tietoja Rescue and Recovery- ja Client Security -ohjelmien kokoonpanon muuttamisesta. Client Security Solution Standalone tarkoittaa, että asennus on tehty WWW-sivustosta tai CD-tietolevystä. (jatkoa)

Asennettu ohjelma	Asennettava ohjelma	Toimet	Huomautuksia
Rescue and Recovery 3.0	Client Security Solution 6.0 Standalone -asennuspaketti	1. Poista Rescue and Recovery 3.0 -ohjelman asennus. 2. Asenna Client Security Solution 6.0 (Standalone) -sovellus.	• Rescue and Recovery -ohjelman poisto poistaa käyttäjätiedostot ja Client Security Solution -rekisteriasetukset. • Client Security Solution -sovelluksen suojaamat Rescue and Recovery -varmistuskopiot eivät ole enää käytettävissä. • Paikalliset varmistuskopiot poistetaan, kun Rescue and Recovery 3.0 -ohjelman asennus on poistettu. • Client Security Solution 6.0 (Standalone) -sovellusta ei voi asentaa Rescue and Recovery 3.0 -ohjelman päälle.
Rescue and Recovery 3.0	Rescue and Recovery 3.0 ja Client Security Solution 6.0	1. Valitse **Muokkaus**-vaihtoehto kohdasta Sovelluksen lisäys tai poisto. 2. Toteuta muutos lisäämällä Client Security Solution -sovellus ja muut halutut aliosat.	• Paikalliset varmistuskopiot poistetaan, kun Client Security Solution -sovellus on lisätty. • Luo Client Security Solution -sovelluksen lisäyksen jälkeen uusi perusvarmistuskopio mahdollisimman pian. • Client Security Solution -asetukset ja datatiedostot poistetaan. • Client Security Solution 6.0 (Standalone) -sovellusta ei voi asentaa Rescue and Recovery 3.0 -ohjelman päälle.
Client Security Solution 6.0 Standalone -asennuspaketti	Client Security Software 5.4x	1. Poista Client Security Solution 6.0 (Standalone) -sovelluksen asennus. 2. Asenna Client Security Software 5.4x -sovellus.	• Client Security Solution 6.0 -datatiedostojen ja -asetusten poisto pyydettäessä ei vaikuta Client Security Software 5.4x -sovelluksen toimintoihin.

Taulukko 8-1. Seuraavassa taulukossa on tietoja Rescue and Recovery- ja Client Security -ohjelmien kokoonpanon muuttamisesta. Client Security Solution Standalone tarkoittaa, että asennus on tehty WWW-sivustosta tai CD-tietolevystä. (jatkoa)

Asennettu ohjelma	Asennettava ohjelma	Toimet	Huomautuksia
Client Security Solution 6.0 Standalone -asennuspaketti	Rescue and Recovery 3.0	1. Poista Client Security Solution 6.0 -sovelluksen asennus. 2. Asenna Rescue and Recovery 3.0 -ohjelma. 3. Valitse asennuksen aikana vain Rescue and Recovery -ohjelman asennus.	Kun poistat Client Security Solution 6.0 -sovelluksen asennusta, saat kehotuksen poistaa Security Solution 6.0 -tiedostot ja -asetukset. Jos epäonnistut näiden tiedostojen ja asetusten poistossa, Rescue and Recovery 3.0 -ohjelman asennus päättyy.
Client Security Solution 6.0 Standalone	Rescue and Recovery 3.0 ja Client Security Solution 6.0	1. Asenna Rescue and Recovery 3.0 -ohjelma. 2. Valitse Client Security Solution 6.0 -sovelluksen kaikki aliosat, jotka haluat asentaa.	• Client Security Solution 6.0 -datatiedostot ja -asetukset säilyvät. • Voit käyttää Rescue and Recovery -ohjelmaa Client Security Solution 6.0 -sovelluksen avulla tapahtuvan varmistuskopioinnin suojauksessa.
Rescue and Recovery 3.0 ja Client Security Solution 6.0	Client Security Software 5.4x	1. Poista Rescue and Recovery - Client Security Solution -sovellus. 2. Asenna Client Security Software 5.4x -sovellus.	• Client Security Software 5.4x -sovellusta ei voi asentaa Client Security Solution 6.0 -sovelluksen päälle. • Datatiedostojen ja asetusten poisto pyydettäessä ei vaikuta Client Security Software 5.4x -sovelluksen toimintoihin. • Rescue and Recovery 3.0 -ohjelman asennuksen poisto poistaa automaattisesti Client Security Solution 6.0 -sovelluksen asennuksen.

Taulukko 8-1. Seuraavassa taulukossa on tietoja Rescue and Recovery- ja Client Security -ohjelmien kokoonpanon muuttamisesta. Client Security Solution Standalone tarkoittaa, että asennus on tehty WWW-sivustosta tai CD-tietolevystä. (jatkoa)

Asennettu ohjelma	Asennettava ohjelma	Toimet	Huomautuksia
Rescue and Recovery 3.0 ja Client Security Solution 6.0	Rescue and Recovery 3.0	1. Valitse **Muokkaus**-vaihtoehto kohdasta Sovelluksen lisäys tai poisto. 2. Poista Client Security Solution 6.0 -sovellus.	• Paikalliset varmistuskopiot poistetaan, kun Client Security Solution 6.0 -sovellus on poistettu. • Client Security Solution 6.0 -sovelluksen poiston jälkeen käytettävänä ei ole Password Manager- tai PrivateDisk-ohjelmaa. • Client Security Solution 6.0 -sovelluksen avulla suojatut Rescue and Recovery 3.0 -varmistuskopiot eivät ole enää käytettävissä. Luo uusi varmistuskopio mahdollisimman pian.
Rescue and Recovery 3.0 ja Client Security Solution 6.0	Client Security Solution 6.0	1. Poista Rescue and Recovery 3.0 -ohjelman asennus. 2. Säilytä pyydettäessä nykyiset Client Security Solution 6.0 -asetukset vain, jos haluat säilyttää nykyiset suojausmääritykset. 3. Asenna Client Security Solution 6.0 (Standalone) -sovellus.	1. Client Security Solution 6.0 -sovelluksen avulla suojatut Rescue and Recovery 3.0 -varmistuskopiot eivät ole enää käytettävissä. 2. Paikalliset varmistuskopiot poistetaan, kun Rescue and Recovery 3.0 -ohjelman asennus on poistettu.

Rescue and Recovery -salasanat ja -salalauseet

Salasanoja tai salalauseita voi käyttää Rescue and Recovery -työtilan suojauksessa estämään tärkeiden tietojen luvaton käyttö. Rescue and Recovery -työtilan voi suojata määrittämällä ohjatun Client Security Setup -toiminnon avulla suojausasetukset tai vaihtamalla sisäänkirjausasetukset Client Security Solution -sovelluksen avulla. Client Security Solution -sovelluksen avulla voi myös muodostaa salasanan elvytysvaihtoehtoja Rescue and Recovery -työtilassa.

Huomautuksia:

1. Tämä toiminto on käytössä vain, jos Client Security Solution 6.0 -ohjelma on asennettuna tietokoneeseen. Jotta voisit käyttää tätä toimintoa, sinun on täytynyt toteuttaa ohjattu Client Security 6.0 Setup -toiminto ja määrittää, haluatko käyttää salasanaa vai salalausetta tietokoneeseen sisäänkirjautumisen yhteydessä.
2. Ohjattu Client Security Setup 6.0 -toiminto ja Client Security Solution 6.0 -sovellus ovat käytettävissä vain Windows-ympäristössä. Jos haluat käyttää Rescue and Recovery -ohjelmaa ilman Client Security Solution -sovellusta, Rescue and Recovery -työtilaa ei voi suojata salasanalla tai salalauseella.

3. Client Security Solution -sovelluksen avulla voi muodostaa salasanan elvytysvaihtoehtoja Rescue and Recovery -työtilassa.

Voit suojata Rescue and Recovery -työtilan salasanan tai salalauseen avulla seuraavin menetelmin.

Menetelmä 1: Jos et ole toteuttanut ohjattua Client Security Setup Wizard -toimintoa, voit suojata Rescue and Recovery -työtilan joko salasanalla tai salalauseella seuraavasti:

1. Napsauta Windowsin **Käynnistä**-painiketta, napsauta **Kaikki ohjelmat** -vaihtoehtoa, valitse **ThinkVantage**-vaihtoehto ja kaksoisnapsauta sitten **Client Security Solution** -vaihtoehtoa.
2. Kun Client Security Solution -sovelluksen ikkuna tulee kuvaruutuun, napsauta **Lisäasetukset** -valikkovaihtoehtoa.
3. Napsauta **Suojaus- ja varmistuskopiointiasetusten määritys** -kuvaketta. Ohjattu Client Security Setup Wizard -toiminto alkaa.
4. Määritä suojausasetukset. Tee pyydettäessä jompikumpi seuraavista toimista:
   - Jos haluat suojata Rescue and Recovery -työtilan Windowsin sisäänkirjaussalasanan avulla, valitse **Windows-salasanan käyttö Rescue and Recovery -työtilan käyttöönotossa** -valintaruutu.
   - Jos haluat suojata Rescue and Recovery -työtilan Client Security Solution -sisäänkirjaussalalauseen avulla, valitse **Client Security Solution -salalauseen käyttö Rescue and Recovery -työtilan käyttöönotossa** -valintaruutu.
5. Tee loppuun ohjatun Client Security Solution Setup Wizard -toiminnon vaiheet ja napsauta sitten**Lopetus**-painiketta. Lisätietoja saat napsauttamalla ohjatun Client Security Setup Wizard -toiminnon **Ohje**-vaihtoehtoa.

Menetelmä 2: Jos olet toteuttanut ohjatun Client Security Setup Wizard -toiminnon, voit suojata Rescue and Recovery -työtilan joko salasanalla tai salalauseella seuraavasti:

1. Napsauta Windowsin **Käynnistä**-painiketta, napsauta **Kaikki ohjelmat** -vaihtoehtoa, valitse **ThinkVantage**-vaihtoehto ja kaksoisnapsauta sitten **Client Security Solution** -vaihtoehtoa.
2. Kun Client Security Solution -sovelluksen ikkuna tulee kuvaruutuun, napsauta **Lisäasetukset** -valikkovaihtoehtoa.
3. Napsauta **Sisäänkirjausasetusten vaihto** -vaihtoehtoa.
4. Noudata kuvaruutuun tulevia ohjeita. Lisätietoja saat napsauttamalla Client Security Solution -sovelluksen **Ohje**-vaihtoehtoa.

Varmistuskopioasetusten määritys ohjatun Client Security Setup Wizard -toiminnon avulla

Ohjatussa Client Security Solution Setup Wizard -toiminnossa on kokoonpanovaihtoehtoja, joiden avulla voi määrittää useita eri suojausominaisuuksia, esimerkiksi sisäisen turvapiirin käyttöönoton, Windows-ympäristön todennuksen valinnan, Rescue and Recovery -ohjelman valinnan tärkeiden tietojen varmistuskopioimiseksi tai sormenjälkitodennuksen käytön valinnan.

Voit ottaa ohjatun Client Security Setup -toiminnon käyttöön seuraavasti:

1. Napsauta Windowsin **Käynnistä**-painiketta, napsauta **Kaikki ohjelmat** -vaihtoehtoa, valitse **ThinkVantage**-vaihtoehto ja kaksoisnapsauta sitten **Client Security Solution** -vaihtoehtoa.
2. Kun Client Security Solution -sovelluksen ikkuna tulee kuvaruutuun, napsauta **Lisäasetukset** -valikkovaihtoehtoa.
3. Kun Client Security Solution -sovelluksen ikkuna tulee kuvaruutuun, napsauta **Suojaus- ja varmistuskopioasetusten määritys** -vaihtoehtoa. Ohjattu Client Security Setup Wizard -toiminto alkaa.
4. Määritä suojausasetukset.
5. Tee ohjattu Client Security Solution Setup Wizard -toiminto loppuun ja napsauta sitten**Lopetus**-painiketta. Lisätietoja saat napsauttamalla ohjatun Client Security Setup Wizard -toiminnon **Ohje**-vaihtoehtoa.

Lisätietoja Client Security Solution -sovelluksesta

Lisätietoja Client Security Solution -sovelluksesta ja sen ominaisuuksista saat julkaisusta *Client Security Solution User Guide*, joka on saatavana WWW-osoitteessa

`http://www.ibm.com/pc/support/site.wss/`

Jos olet jo asentanut Client Security Solution -sovelluksen, voit lukea lisätietoja käyttöoppaasta seuraavasti:

1. Napsauta Windowsin **Käynnistä**-painiketta.
2. Valitse **Kaikki ohjelmat** -vaihtoehto.
3. Valitse **ThinkVantage**-vaihtoehto.
4. Napsauta **Client Security Solution** -vaihtoehtoa.
5. Valitse Client Security Solution -sovelluksen valikkorivin **Ohje**-vaihtoehtoa.
6. Napsauta **User’s Guide** -vaihtoehtoa.

Kapittel 9. Norsk

Applikasjonen Client Security Solution er en pakke med ThinkVantage-teknologiverktøy som beskytter tilgangen til operativsystemet og sensitive data. Client Security Solution integrerer maskinvarebeskyttelse i den innebygde brikken med beskyttelsen som den sikre programvaren gir. Ved å kombinere reservert programvare med programvarebeskyttelse, økes beskyttelsen betraktelig i sikkerhetsfunksjonene som er innebygd i operativsystemet i datamaskinen.

Hvem håndboken er beregnet på

Brukerhåndbok for ThinkVantage Client Security Solution er beregnet på enkeltsluttbrukere og sluttbrukere i en bedrift. Håndboken inneholder informasjon om følgende emner:

- Client Security Solution-komponenter
- Informasjon om installasjon av Client Security Solution
- Client Security Solution-funksjoner

Denne håndboken er et tillegg til hjelpesystemet for Client Security Solution, som inneholder trinnvise instruksjoner om hvordan bestemte oppgaver skal utføres i programmet.

Tilleggsinformasjon

Hvis du som systemansvarlig, systemtekniker, systemansvarlig eller kundetekniker implementerer Client Security Solution i store bedrifter, finner du mer detaljert informasjon i *distribusjonshåndbøkene (Deployment Guide) for ThinkVantage Rescue and Recovery™ og Client Security Solution* på nettstedet nedenfor:

`http://www.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-54502`

Client Security Solution-komponenter

Client Security Solution er beregnet på datamaskiner med en innebygd sikkerhetsbrikke, som øker sikkerheten for data og prosesser på maskinen. Nå kan imidlertid programvaren for Client Security Solution konfigureres slik at sikkerheten forbedres på maskiner uten slike sikkerhetsbrikker.

Client Security Solution er delt inn i følgende maskinvare- og programvarekomponenter.

- **Innebygd sikkerhetsbrikke**

  Client Security Solution er beregnet på datamaskiner med en innebygd sikkerhetsbrikke. En innebygd sikkerhetsbrikke er en innebygd kryptografisk maskinvareteknologi som øker sikkerheten på maskinen ytterligere. Sikkerhetsbrikken gjør det mulig å overføre kryptering og autentiseringsprosesser fra en sårbar programvare til et sikkert miljø med reservert godkjenning. Det oppnås en markant forbedring i sikkerheten.

- **Installeringsveiviser for Client Security**

  Installeringsveiviseren for Client Security veileder deg gjennom prosessen med å konfigurere sikkerhetsinnstillingene dine. Ved hjelp av veiviseren kan du aktivere den innebygde sikkerhetsbrikken, velge autentiserings- og påloggingsmetode, lage spørsmål for gjenoppretting av passord, opprette autentisering med fingeravtrykk (valgfritt) og konfigurere flere Client Security Solution-komponenter.

- **Password Manager**

  Med Client Security Password Manager kan du administrere sensitiv påloggingsinformasjon til applikasjoner og nettsteder, for eksempel bruker-IDer, passord og annen personlig informasjon som det er lett å glemme. Client Security Password Manager lagrer all informasjon ved hjelp av den innebygde sikkerhetsbrikken slik at du er sikret sikker tilgang til applikasjonene og nettstedene.
- **PrivateDisk**

  PrivateDisk konfigurerer en kryptert virtuell stasjon som automatisk krypterer data du lagrer innenfor det sikre området til denne ″elektroniske safen″. Bruk din egen virtuelle stasjon når du krypterer og lagrer all de kritiske dataene dine. Data krypteres automatisk når de lagres i et PrivateDisk-volum.
- **Client Security Solution-applikasjonen**

  Applikasjonen Client Security Solution inneholder ett grensesnitt som lar brukere utføre grunnleggende og avanserte sikkerhetsfunksjoner. Du kan for eksempel aktivere den innebygde sikkerhetsbrikken, endre en passordfrase eller bruke fingeravtrykkprogram. Du finner en oversikt over alle funksjonene i Client Security Solution, under "Client Security Solution-funksjoner" på side 9-3
- **ThinkVantage-fingeravtrykkprogramvare**

  Med ThinkVantage-fingeravtrykkprogramvaren kan brukere opprette autentisering ved hjelp av fingeravtrykk. Denne nyttige sikkerhetsfunksjonen er tilgjengelig på utvalgte ThinkPad- og ThinkCentre-modeller og -tilleggsutstyr.

Før du installerer Client Security Solution

Før du kan installere Client Security Solution, må følgende krav oppfylles:

- Windows XP eller Windows 2000 med Service Pack 3. Hvis du installerer dette programmet på en harddisk som har en kapasitet som er større enn 137 GB, må du ha Service Pack 1 for Windows XP.
- Internet Explorer 5.5 (eller senere)
- 128 MB minne, der ikke mer enn 8 MB kan være definert som delt minne under skjermkonfigureringen i BIOS.
- 800 MB ledig plass på harddisken.

Hvis du har en tidligere versjon av Client Security Solution, Client Security Software eller Rescue and Recovery, finner du nærmere opplysninger under "Bruke Client Security Solution med Rescue and Recovery" på side 9-5.

Konfigurere Client Security Solution

Client Security Solution-applikasjonen er tilgjengelig på nettstedet `http://www.pc.ibm.com/thinkvantage`. Du kan laste ned, installere og konfigurere Client Security Solution i løpet av noen minutter.

Laste ned og installere Client Security Solution

Fullfør følgende installeringsprosess hvis du vil laste ned og installere Client Security Solution-programmet:

1. Start datamaskinen og lukk eventuelle åpne programmer.
2. Gå til nettstedet `http://www.pc.ibm.com/thinkvantage`.
3. Klikk på koblingen **Support and downloads** i ressursdelen.
4. Rull nedover siden til du kommer til Embedded Security Subsystem and Client Security Solution, og klikk på **Software download**.

5. Følg instruksjonene på skjermen.
6. Kjør den kjørbare installasjonsfilen og følg instruksjonene på skjermen. Du kan enten installere Password Manager- eller PrivateDisk-komponenter for Client Security Solution.
7. Når du har angitt valgene dine, blir du bedt om å starte maskinen på nytt.
8. Når datamaskinen startes på nytt, startes installeringsveiviseren for Client Security. Hvis veiviseren ikke startes, leser du informasjonen under "Åpne installeringsveiviseren for Client Security".
9. Fullfør installeringsveiviseren for Client Security for å fullføre konfigureringsprosessen.

Åpne installeringsveiviseren for Client Security

Slik konfigurerer du Client Security Solution ved hjelp av installeringsveiviseren for Client Security:

1. Fra Windows-skrivebordet klikker du på **Start**, **Alle programmer**, velger **ThinkVantage** og dobbeltklikker på **Client Security Solution**.
2. Når Client Security Solution-vinduet åpnes, klikker du på **Avansert**.
3. Når Client Security Solution-vinduet åpnes, klikker du på **Definer sikkerhets- og sikkerhetskopieringsinnstillinger**. Installeringsveiviseren for Client Security blir åpnet.
4. Fullfør trinnene i installeringsveiviseren for Client Security Solution, og klikk på **Fullfør**. Klikk på **Hjelp** i installeringsveiviseren for Client Security hvis du vil ha mer detaljert informasjon.

Bruke Client Security Solution

Slik får du tilgang til Client Security Solution:

1. Fra Windows-skrivebordet klikker du på **Start**.
2. Velg **Alle programmer**.
3. Velg **ThinkVantage**.
4. Klikk på **Client Security Solution**.

Client Security Solution-funksjoner

Nedenfor finner du informasjon om de forskjellige oppgavene du kan utføre ved hjelp av Client Security Solution.

Merk: Hvis du ikke har tilgang til enkelte av verktøyene som beskrives nedenfor, kan dette skyldes at det ikke er installert riktig programvare, at datamaskinen ikke støtter applikasjonen, eller at applikasjonen krever tilgang som administrator eller systemansvarlig.

Grunnfunksjoner

Nedenfor finner du informasjon om de grunnleggende oppgavene du kan utføre ved hjelp av Client Security Solution.

Endre passordfrase: Med verktøyet for endring av passordfrase kan du opprette en ny passordfrase for Client Security. Passordfraser må oppfylle kravene til passordfraser for Client Security.

Konfigurere gjenoppretting av passord: Med verktøyet for konfigurering av passordgjenoppretting kan du opprette en metode for å gjenopprette et glemt Windows-passord eller en glemt Client Security-passordfrase, avhengig av hvilken autentiseringsmetode du bruker.

Administrere påloggingsinformasjon: Med applikasjonen Password Manager kan du bruke Client Security Solution til å administrere sensitiv påloggingsinformasjon som lett kan glemmes, for eksempel bruker-IDer, passord og annen personlig informasjon. Password Manager lagrer all informasjon ved hjelp av den innebygde sikkerhetsbrikken slik at brukerautentiseringspolicyen regulerer tilgangen til de sikre applikasjonene og nettstedene. I stedet for å måtte huske og oppgi en rekke passord som har forskjellige regler og utløpsdatoer, trenger du bare å huske en enkelt passordfrase eller, hvis fingeravtrykkprogramvare er installert, vise fingeravtrykket ditt.

Bruke programvare for fingeravtrykk: Med den integrerte fingeravtrykkavleseren kan du registrere og knytte fingeravtrykket ditt til oppstartingspassordet, harddiskpassordet og Windows-passordet ditt, slik at fingeravtrykkautentisering kan erstatte passordene og gi deg enkel og sikker tilgang. Et tastatur med fingeravtrykkleser er bare tilgjengelig for utvalgte datamaskiner og kan kjøpes som tilleggsutstyr. Dette utstyret støttes bare på utvalgte ThinkCentre- og ThinkPad-maskiner.

Beskytte data: Verktøyet PrivateDisk genererer en kryptert virtuell stasjon som automatisk krypterer data du lagrer innenfor det sikre området til denne ″elektroniske safen″.

Avanserte funksjoner

Nedenfor finner du informasjon om de avanserte oppgavene du kan utføre ved hjelp av Client Security Solution.

Merk: Du må ha administratorrettigheter for å utføre operasjonene nedenfor.

Overvåke sikkerhetsinnstillinger: Med Security Advisor-verktøyet kan du vise en oversikt over de gjeldende sikkerhetsinnstillingene på datamaskinen. Se gjennom innstillingene for å vise den gjeldende sikkerhetsstatusen eller øke systemsikkerheten. Enkelte sikkerhetsinnstillinger omfatter blant annet maskinvarepassord, Windows-brukerpassord, Windows-passordpolicy, skjermbeskytter og fildeling.

Merk: Security Advisor-verktøyet gir deg bare en oversikt over sikkerhetsinnstillingene og forslag som kan forbedre sikkerheten på maskinen. Ikke alle aspekter av sikkerheten er dekket, for eksempel bruk og vedlikehold av antivirus- og brannmurprogrammer. Mange av innstillingene krever at du har tilgang som administrator eller systemansvarlig.

Overføre digitale sertifikater: Veiviseren for sertifikatoverføring for Client Security leder deg gjennom prosessen med å overføre de private nøklene som er knyttet til sertifikatene dine, fra programvarebaserte Microsoft Cryptographic Service Provider (CSP) til maskinvarebaserte Client Security Solution CSP. Etter overføringen er operasjoner som bruker sertifikatene, mer sikre fordi de private nøklene er beskyttet av den innebygde sikkerhetsbrikken.

Opprette en metode for tilbakestilling av et maskinpassord: Dette verktøyet oppretter et sikkert miljø som kjøres uavhengig av Windows, og hjelper deg med å tilbakestille glemte oppstartings- og harddiskpassord. Din identitet blir kontrollert ved at du svarer på et sett med spørsmål som du selv oppretter. Du bør så snart som mulig opprette dette sikre miljøet, før du glemmer passordene. Før du kan tilbakestille et glemt maskinvarepassord, må du opprette det sikre miljøet på harddisken og registrere deg. Dette verktøyet er bare tilgjengelig på utvalgte ThinkCentre- og ThinkPad-maskiner.

Merk: Du bør definere et administratorpassord eller et passord for systemansvarlig før du bruker dette verktøyet. Hvis du ikke har definert et administratorpassord eller passord for systemansvarlig, er ikke sikkerheten i miljøet optimal. Når du har fullført denne fremgangsmåten, vil oppstartingspassordet og harddiskpassordet være det samme. Med denne fremgangsmåten fullfører du oppgaven med å opprette et sikkert miljø, og du kan tilbakestille glemte passord etter at det sikre miljøet er opprettet.

Aktivere den innebygde sikkerhetsbrikken: Med aktiveringsverktøyet kan du starte en endring av en BIOS-innstilling som blir brukt til å aktivere eller deaktivere den innebygde sikkerhetsbrikken. Du må starte maskinen på nytt for å aktivere endringen.

Endre påloggingsinnstillinger: Med verktøyet for endring av påloggingsinnstillinger vises de gjeldende påloggingsinnstillingene, og med dette verktøyet kan en administrator endre måten brukere logger seg på Windows-operativsystemet og ThinkVantage Rescue and Recovery-arbeidsområdet.

Fjerne feilbeskyttet teller: Det finnes et verktøyet som tilbakestiller telleren for mislykket autentisering. Denne telleren overvåker hvor mange mislykkede autentiseringsforsøk som er sendt til den innebygde sikkerhetsbrikken. Etter et bestemt antall mislykkede forsøk, låses brikken for en periode. Jo flere mislykkede forsøk, jo lenger blir utestengingsperioden.

Definere sikkerhets- og sikkerhetskopieringsinnstillinger: Med installeringsveiviseren for Client Security kan du konfigurere en rekke sikkerhetsverktøy. Denne veiviseren inneholder konfigureringsalternativer som gjør det mulig å definere en rekke sikkerhetsfunksjoner. Du kan for eksempel aktivere den innebygde Client Security-sikkerhetsbrikken, velge autentiseringsmetode for Windows-miljøet, velge å bruke Rescue and Recovery til å sikkerhetskopiere sensitive data, eller velge å bruke fingeravtrykkautentisering.

Bruke Client Security Solution med Rescue and Recovery

Både Rescue and Recovery og Client Security Solution bygger på ThinkVantage-teknologi og er utviklet med tanke på brukerne. Dette betyr at de både fungerer separat og sammen, avhengig av brukernes behov. Nedenfor finner du informasjon om hvordan du bør planlegge bruken av disse programmene, og hvordan de utfyller hverandre.

Du må ta stilling til noen viktige spørsmål når du skal installere Rescue and Recovery, Client Security Solution eller begge. De følgende tabellene inneholder informasjon som er nyttig når du skal finne ut hvilken fremgangsmåte som er best for konfigurasjonen din.

Tabell 9-1. Du finner informasjon i tabellen nedenfor som er nyttig når du skal endre konfigurering av Rescue and Recovery og Client Security. Client Security Solution Standalone betyr at installeringspakken er hentet fra nettet eller CD.

Installert programvare...	Du ønsker...	Gjør slik	Kommentarer
Client Security Software 5.4x	Client Security Software 5.4x og Rescue and Recovery 3.0	1. Installer Rescue and Recovery 3.0. 2. Når du får spørsmål om det, angir du at du vil beholde den installerte applikasjonen Client Security Software 5.4x.	Sikkerhetskopier kan ikke beskyttes med Client Security Software 5.4x, og hvis Rescue and Recovery 3.0 bruker Client Security Software-funksjoner, brukes en emulert versjon av Client Security Software. Hovedpassordet blir tilføyd i sikkerhetsfunksjonene. Et hovedpassord blir vanligvis brukt i bedrifter. Du finner mer informasjon under "Tilleggsinformasjon" på side 9-1
Client Security Software 5.4x	Installeringspakke for Client Security Solution 6.0 Standalone	1. Avinstaller Client Security Software 5.4x. 2. Installer Client Security Solution 6.0 (Standalone).	• Dekrypter eventuelle krypterte filer og eksporter Password Manager-informasjon før du avinstallerer. Ellers går denne informasjonen tapt. • Du må avinstallere programvaren IBM File and Folder Encryption før du installerer Client Security Solution-applikasjonen.
Client Security Software 5.4x	Client Security Solution 6.0 og Rescue and Recovery 3.0	1. Avinstaller Client Security Software 5.4x. 2. Installer Rescue and Recovery 3.0. (Kontroller at Client Security Solution 6.0-komponenten er valgt.)	• Hvis du installerer Rescue and Recovery 3.0 over Client Security Software 5.4x uten først å avinstallere Client Security Software, blir resultatet bare Rescue and Recovery. • Før du avinstallerer Client Security Software 5.4x, må du dekryptere eventuelle krypterte filer og eksportere Password Manager-informasjon før du avinstallerer. Ellers går denne informasjonen tapt. • Du må avinstallere programvaren IBM File and Folder Encryption før du installerer Client Security Solution 6.0.

Tabell 9-1. Du finner informasjon i tabellen nedenfor som er nyttig når du skal endre konfigurering av Rescue and Recovery og Client Security. Client Security Solution Standalone betyr at installeringspakken er hentet fra nettet eller CD. (fortsettelse)

Installert programvare...	Du ønsker...	Gjør slik	Kommentarer
Rescue and Recovery 3.0	Client Security Software 5.4x og Rescue and Recovery 3.0	1. Avinstaller Rescue and Recovery 3.0. 2. Installer Client Security Software 5.4x. 3. Installer Rescue and Recovery 3.0. 4. Når du får spørsmål om det, angir du at du vil beholde den installerte applikasjonen Client Security Software 5.4x.	• Client Security Software 5.4x kan ikke installeres over Rescue and Recovery 3.0. • Lokale sikkerhetskopier vil bli slettet når du avinstallerer Rescue and Recovery 3.0.
Rescue and Recovery 3.0	Installeringspakke for Client Security Solution 6.0 Standalone	1. Avinstaller Rescue and Recovery 3.0. 2. Installer Client Security Solution 6.0 (Standalone).	• Hvis du avinstallerer Rescue and Recovery, blir brukerfiler og registerinnstillinger for Client Security Solution slettet. • Rescue and Recovery-sikkerhetskopier som er beskyttet av Client Security Solution, vil ikke lenger være tilgjengelig. • Lokale sikkerhetskopier vil bli slettet når du avinstallerer Rescue and Recovery 3.0. • Client Security Solution 6.0 (Standalone) kan ikke installeres over Rescue and Recovery 3.0.
Rescue and Recovery 3.0	Rescue and Recovery 3.0 og Client Security Solution 6.0	1. Velg alternativet **Endre** i Legg til/fjern programmer. 2. Fullfør endringen ved å tilføye Client Security Solution og ønskede delkomponenter.	• Lokale sikkerhetskopier blir slettet når Client Security Solution tilføyes. • Når du har lagt til Client Security Solution, oppretter du en ny hovedsikkerhetskopi så snart som mulig. • Innstillinger og datafiler for Client Security Solution blir slettet. • Client Security Solution 6.0 (Standalone) kan ikke installeres over Rescue and Recovery 3.0.

Tabell 9-1. Du finner informasjon i tabellen nedenfor som er nyttig når du skal endre konfigurering av Rescue and Recovery og Client Security. Client Security Solution Standalone betyr at installeringspakken er hentet fra nettet eller CD. (fortsettelse)

Installert programvare...	Du ønsker...	Gjør slik	Kommentarer
Installeringspakke for Client Security Solution 6.0 Standalone	Client Security Software 5.4x	1. Avinstaller Client Security Solution 6.0 (Standalone). 2. Installer Client Security Software 5.4x.	• Hvis du sletter datafiler og innstillinger for Client Security Solution 6.0, har dette ingen innvirkning på operasjoner i Client Security Software 5.4x.
Installeringspakke for Client Security Solution 6.0 Standalone	Rescue and Recovery 3.0	1. Avinstaller Client Security Solution 6.0. 2. Installer Rescue and Recovery 3.0. 3. Velg bare Rescue and Recovery under installeringen.	Hvis du avinstallerer Client Security Solution 6.0, må du slette filene og innstillingene for Security Solution 6.0. Hvis du ikke gjør dette, avsluttes installeringen av Rescue and Recovery 3.0.
Client Security Solution 6.0 Standalone	Rescue and Recovery 3.0 og Client Security Solution 6.0	1. Installer Rescue and Recovery 3.0. 2. Angi hvilke delkomponenter for Client Security Solution 6.0 du vil installere.	• Datafilene og innstillingene for Client Security Solution 6.0 blir bevart. • Hvis du vil beskytte sikkerhetskopier ved hjelp av Client Security Solution 6.0, bruker du Rescue and Recovery.
Rescue and Recovery 3.0 og Client Security Solution 6.0	Client Security Software 5.4x	1. Avinstaller Rescue and Recovery - Client Security Solution. 2. Installer Client Security Software 5.4x.	• Client Security Software 5.4x kan ikke installeres over Client Security Solution 6.0. • Operasjoner i Client Security Software 5.4x påvirkes ikke selv om du sletter datafiler og innstillinger. • Hvis du avinstallerer Rescue and Recovery 3.0, avinstalleres automatisk Client Security Solution 6.0.

Tabell 9-1. Du finner informasjon i tabellen nedenfor som er nyttig når du skal endre konfigurering av Rescue and Recovery og Client Security. Client Security Solution Standalone betyr at installeringspakken er hentet fra nettet eller CD. (fortsettelse)

Installert programvare...	Du ønsker...	Gjør slik	Kommentarer
Rescue and Recovery 3.0 og Client Security Solution 6.0	Rescue and Recovery 3.0	1. Velg **Endre** i Legg til/fjern programmer. 2. Fjern Client Security Solution 6.0.	• Lokale sikkerhetskopier blir slettet når Client Security Solution 6.0 fjernes. • Hvis du avinstallerer Client Security Solution 6.0, fjernes også Password Manager eller PrivateDisk. • Sikkerhetskopier for Rescue and Recovery 3.0 som beskyttes med Client Security Solution 6.0, vil ikke lenger være tilgjengelige. Opprett en ny sikkerhetskopi så snart som mulig.
Rescue and Recovery 3.0 og Client Security Solution 6.0	Client Security Solution 6.0	1. Avinstaller Rescue and Recovery 3.0. 2. Behold de gjeldende innstillingene for Client Security Solution 6.0 bare hvis du vil beholde gjeldende sikkerhetskonfigurering. 3. Installer Client Security Solution 6.0 (Standalone).	1. Sikkerhetskopier for Rescue and Recovery 3.0 som beskyttes med Client Security Solution 6.0, vil ikke lenger være tilgjengelige. 2. Lokale sikkerhetskopier vil bli slettet når du avinstallerer Rescue and Recovery 3.0.

Passord og passordfraser for Rescue and Recovery

Du kan beskytte Rescue and Recovery-arbeidsområdet med passord og passordfraser og dermed beskytte kritiske data mot uautorisert tilgang. Du kan beskytte Rescue and Recovery-arbeidsområdet ved å angi sikkerhetsinnstillinger ved hjelp av installeringsveiviseren for Client Security, eller ved å endre påloggingsinnstillingene ved hjelp av Client Security Solution. Med Client Security Solution kan du også opprette alternativer for gjenoppretting av passord i Rescue and Recovery-arbeidsområdet.

Merk:

1. Denne funksjonen er tilgjengelig bare hvis Client Security Solution 6.0 er installert. Hvis du vil bruke denne funksjonen, må du fullføre installeringsveiviseren for Client Security 6.0 og oppgi om du vil bruke et passord eller en passordfrase når du logger deg på datamaskinen.
2. I Windows-miljøet har du både tilgang til installeringsveiviseren for Client Security 6.0 og Client Security Solution 6.0. Hvis du bruker Rescue and Recovery uten Client Security Solution, blir ikke Rescue and Recovery-arbeidsområdet beskyttet med passord eller passordfrase.
3. Med Client Security Solution kan du også opprette alternativer for gjenoppretting av passord i Rescue and Recovery-arbeidsområdet.

Du kan bruke metodene nedenfor hvis du vil beskytte Rescue and Recovery-arbeidsområdet med et passord eller en passordfrase.

Metode 1: Hvis du ikke har fullført installeringsveiviseren for Client Security, beskytter du Rescue and Recovery-arbeidsområdet med et passord eller en passordfrase på følgende måte:

1. Fra Windows-skrivebordet klikker du på **Start**, **Alle programmer**, velger **ThinkVantage** og dobbeltklikker på **Client Security Solution**.
2. Når Client Security Solution-vinduet åpnes, klikker du på **Avansert**.
3. Klikk på ikonet **Definer sikkerhets- og sikkerhetskopieringsinnstillinger**. Installeringsveiviseren for Client Security blir åpnet.
4. Angi sikkerhetsinnstillingene. Velg et av disse alternativene når du får spørsmål om det:
   - Hvis du vil beskytte Rescue and Recovery-arbeidsområdet med Windows-påloggingspassordet, merker du av for **Bruk Windows-passordet til å få tilgang til Rescue and Recovery-arbeidsområdet**.
   - Hvis du vil beskytte Rescue and Recovery-arbeidsområdet med Client Security Solution-påloggingspassordfrasen, merker du av for **Bruk Client Security Solution-passordfrasen til å få tilgang til Rescue and Recovery-arbeidsområdet**.
5. Fullfør installeringsveiviseren for Client Security, og klikk på **Fullfør**. Klikk på **Hjelp** i installeringsveiviseren for Client Security hvis du vil ha mer informasjon.

Metode 2: Hvis du ikke har fullført installeringsveiviseren for Client Security, beskytter du Rescue and Recovery-arbeidsområdet med et passord eller en passordfrase på følgende måte:

1. Fra Windows-skrivebordet klikker du på **Start**, **Alle programmer**, velger **ThinkVantage** og dobbeltklikker på **Client Security Solution**.
2. Når Client Security Solution-vinduet åpnes, klikker du på **Avansert**.
3. Klikk på **Endre påloggingsinnstillinger**.
4. Følg instruksjonene på skjermen. Klikk på **Hjelp** i Client Security Solution hvis du vil ha mer informasjon.

Definere sikkerhetskopieringsinnstillinger ved hjelp av installeringsveiviseren for Client Security

Installeringsveiviseren for Client Security Solution inneholder konfigureringsalternativer som gjør det mulig å definere en rekke sikkerhetsfunksjoner. Du kan for eksempel aktivere den innebygde sikkerhetsbrikken, velge autentiseringsmetode for Windows-miljøet, velge å bruke Rescue and Recovery til å sikkerhetskopiere sensitive data, eller velge å bruke fingeravtrykkautentisering.

Slik bruker du installeringsveiviseren for Client Security:

1. Fra Windows-skrivebordet klikker du på **Start**, **Alle programmer**, velger **ThinkVantage** og dobbeltklikker på **Client Security Solution**.
2. Når Client Security Solution-vinduet åpnes, klikker du på **Avansert**.
3. Når Client Security Solution-vinduet åpnes, klikker du på **Definer sikkerhets- og sikkerhetskopieringsinnstillinger**. Installeringsveiviseren for Client Security blir åpnet.
4. Angi sikkerhetsinnstillingene.

5. Fullfør installeringsveiviseren for Client Security Solution, og klikk på **Fullfør**. Klikk på **Hjelp** i installeringsveiviseren for Client Security hvis du vil ha mer detaljert informasjon.

Mer informasjon om Client Security Solution

Du finner mer detaljert informasjon om Client Security Solution og funksjonene i denne applikasjonen, i *brukerhåndboken for Client Security Solution* på følgende nettadresse:

`http://www.ibm.com/pc/support/site.wss/`

Hvis du allerede har installert Client Security Solution, finner du mer detaljert informasjon i brukerhåndboken ved å gjøre følgende:

1. Fra Windows-skrivebordet klikker du på **Start**.
2. Velg **Alle programmer**.
3. Velg **ThinkVantage**.
4. Klikk på **Client Security Solution**.
5. Klikk på **Hjelp** på menylinjen i Client Security Solution.
6. Klikk på **Brukerhåndbok**.

Kapitel 10. Svenska

Client Security Solution är en uppsättning ThinkVantage-verktyg som hjälper dig att skydda datorns operativsystem och känsliga data mot obehöriga användare. Client Security Solution består av en integrerad säkerhetskrets som skyddar datorns maskinvara och av säkerhetsprogramvara. Genom att Client Security Solution kombinerar särskild maskinvara med programvaruskydd ger lösningen en kraftig förstärkning av de säkerhetsfunktioner som är inbyggda i datorns operativsystem.

Vem bör läsa den här handboken

Användarhandboken till ThinkVantage Client Security Solution är avsedd för både för dem som använder sin dator fristående och för dem som arbetar i en nätverksmiljö. Handboken ger information om följande områden:

- Komponenterna i Client Security Solution
- Råd inför installationen av Client Security Solution
- Funktioner i Client Security Solution

Handboken kompletterar Client Security Solutions hjälpsystem, där det finns steg-för-steg-anvisningar om hur du utför olika uppgifter i programmet.

Mer information

Om du är systemadministratör, systemtekniker eller nätverksadministratör och tänker installera Client Security Solution i ett större företag kan du få detaljerad information genom att läsa *ThinkVantage Rescue and Recovery™ and Client Security Solution Deployment Guide* som du kan hämta på webbadressen:

`http://www.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-54502`

Komponenterna i Client Security Solution

Client Security Solution är utformades för datorer med en integrerad säkerhetskrets, som ger ett förstärkt skydd av datorns data och processer. Numera kan dock Client Security Solution konfigureras för att förbättra säkerheten även på datorer som saknar säkerhetskrets.

Client Security Solution består av följande maskin- och programkomponenter:

- **Integrerad säkerhetskrets**

  Client Security Solution är gjord för datorer som har en integrerad säkerhetskrets. Den integrerade säkerhetskretsen innehåller krypteringsfunktioner som ökar skyddet av datorn. Säkerhetskretsen gör det möjligt att flytta krypterings- och autentiseringsfunktioner från sårbar programvara till den skyddade miljö som särskild maskinvara ger. Därigenom ökas säkerheten betydligt.
- **Konfigureringsguiden Client Security**

  Client Security-guiden hjälper dig att konfigurera säkerhetsalternativen. I guiden kan du aktivera den integrerade säkerhetskretsen, välja autentiserings- och inloggningsmetod, skapa frågor för återställning av lösenord, ställa in autentisering med hjälp av fingeravtryck (valfritt) och konfigurera fler Client Security Solution-komponenter.
- **Password Manager**

  Med hjälp av Client Security Password Manager kan du bekvämt och säkert hantera känslig information (som är lätt att glömma bort) för inloggning till program och webbplatser, t.ex. användar-IDn, lösenord och annan personlig information. Client Security Password Manager lagrar all information i den integrerade säkerhetskretsen så att informationen som ger dig tillgång till program och webbplatser är helt skyddad.

- **PrivateDisk**

  PrivateDisk definierar en krypterad virtuell hårddisk som automatiskt krypterar data som du lagrar i detta ″elektroniska kassaskåp″. Med hjälp av din virtuella enhet kan du kryptera och lagra alla viktiga data du har. Data krypteras automatiskt när de lagras i en PrivateDisk-volym.

- **Programmet Client Security Solution**

  Programmet Client Security Solution har ett gränssnitt där användarna kan utföra både enkla och avancerade säkerhetsfunktioner, exempelvis aktivera den integrerade säkerhetskretsen, byta sin lösenmening eller använda programvara för fingeravtryck. En lista över alla funktionerna i Client Security Solution finns i ”Funktioner i Client Security Solution” på sidan 10-3

- **ThinkVantage-fingeravtrycksprogram**

  Med hjälp av ThinkVantage-fingeravtrycksprogrammet kan användare identifiera sig genom ett fingeravtryck. Denna bekväma säkerhetsfunktion finns på vissa ThinkPad- och ThinkCentre-modeller och finns även att köpa som tillbehör.

Innan du installerar Client Security Solution

Innan du installerar Client Security Solution bör du kontrollera att följande systemkrav är uppfyllda:

- Windows XP eller Windows 2000 med Service Pack 3. Om du installerar programmet på en hårddisk med större kapacitet än 137 GB, behöver du installera Service Pack 1 för Windows XP.
- Internet Explorer 5.5 (eller högre).
- 128 MB minne varav högst 8 MB för vara tilldelat som delat minne under Video setup i BIOS-inställningarna.
- 800 MB ledigt utrymme på hårddisken.

Om du har en tidigare version av Client Security Solution, Client Security Software eller Rescue and Recovery läser du de särskilda anvisningarna i ”Använda Client Security Solution med Rescue and Recovery” på sidan 10-5.

Installera Client Security Solution

Du kan hämta Client Security Solution på webbplatsen `http://www.pc.ibm.com/thinkvantage`. Det tar bara ett par minuter att hämta, installera och konfigurera Client Security Solution.

Hämta och installera Client Security Solution

Så här hämtar och installerar du Client Security Solution:

1. Starta datorn och stäng alla öppna program.
2. Gå till webbplatsen `http://www.pc.ibm.com/thinkvantage`.
3. Klicka på länken **Support and downloads** i avsnittet Resources.
4. Bläddra fram till avsnittet Embedded Security Subsystem and Client Security Solution och klicka på **Software download**.
5. Följ anvisningarna på skärmen.

6. Kör installationsfilen (.exe) och följ anvisningarna på skärmen. Du får möjlighet att välja om du vill installera komponenterna Password Manager och PrivateDisk i Client Security Solution.
7. När du har gjort dina val blir du ombedd att starta om datorn.
8. När datorn startat om öppnas konfigureringsguiden för Client Security. Om konfigureringsguiden inte öppnas läser du ”Öppna konfigureringsguiden för Client Security”
9. Genomför konfigureringsstegen i Client Security-guiden.

Öppna konfigureringsguiden för Client Security

Så här gör du inställningar för programmet Client Security Solution med hjälp av konfigureringsguiden:

1. På skrivbordet i Windows klickar du på **Start**, **Alla program** och **ThinkVantage**. Dubbelklicka sedan på **Client Security Solution**.
2. När fönstret Client Security Solution öppnas klickar du på menyalternativet **Avancerat**.
3. När fönstret Client Security Solution öppnas klickar du på **Inställningar för säkerhet och säkerhetskopiering**. Konfigureringsguiden för Client Security öppnas.
4. Genomför stegen i konfigureringsguiden för Client Security Solution och klicka sedan på **Slutför**. Klicka på **Hjälp** i konfigureringsguiden om du vill ha mer detaljerad information.

Använda Client Security Solution

Så här startar du programmet Client Security Solution:

1. Från skrivbordet i Windows klickar du på **Start**.
2. Välj **Alla program**.
3. Välj **ThinkVantage**.
4. Klicka på **Client Security Solution**.

Funktioner i Client Security Solution

I det följande avsnittet beskrivs de olika uppgifter som du kan utföra med programmet Client Security Solution.

Anm: Om några av de verktyg som nämns nedan inte är tillgängliga för dig kan det bero på att du inte har rätt programvara installerad, att din datorn inte är kompatibel med programmet eller på att programmet kräver administratörsbehörighet.

Grundfunktioner

I det följande beskrivs de grundläggande uppgifter som du kan utföra med programmet Client Security Solution.

Byt lösenmening: Med funktionen Byt lösenmening kan du ange en ny Client Security-lösenmening. Lösenmeningar måste uppfylla kraven för Client Security-lösenmeningar.

Konfigurera återställning av lösenord: Med funktionen Konfigurera återställning av lösenord kan du förbereda återställning av ett bortglömt Windows-lösenord eller en Client Security-lösenmening, beroende på vilken autentiseringsmetod du använder.

Hantera inloggningsinformation: Med programmet Password Manager kan du hantera känslig inloggningsinformation (som är lätt att glömma bort), t.ex. användar-IDn, lösenord och annan personlig information. Password Manager lagrar all information i den integrerade säkerhetskretsen så att autentiseringsregler styr åtkomsten till dina säkra program och webbplatser. I stället för att behöva komma ihåg och ange ett stort antal olika lösenord - vart och ett omgärdat av olika regler och med olika förfallodatum - behöver du bara komma ihåg en lösenmening, eller ge ett fingeravtryck om du använder fingeravtrycksprogram.

Använda fingeravtrycksprogram: Med den inbyggda fingeravtrycksläsaren kan du registrera ditt fingeravtryck och koppla det till dina lösenord för start av datorn, hårddisken och Windows. Sedan kan du använda ditt fingeravtryck i stället för lösenordet, vilket är en enklare och säkrare metod för behörighetskontroll. Tangentbord med fingeravtrycksläsare finns för vissa datormodeller och kan dessutom köpas som tillbehör. Funktionen kan användas enbart på vissa ThinkCentre- och ThinkPad-datorer.

Skydda data: Verktyget PrivateDisk skapar en krypterad virtuell disk, där alla data som du lagrar krypteras automatiskt. Disken fungerar som ett ″elektroniskt kassaskåp″.

Avancerade funktioner

I det följande beskrivs avancerade uppgifter som du kan utföra med programmet Client Security Solution.

Anm: Du måste ha administratörsbehörigheter för att utföra följande åtgärder.

Övervaka säkerhetsinställningar: Med hjälp av verktyget Säkerhetsrådgivaren kan du visa en översikt över datorns aktuella säkerhetsinställningar. Granska inställningarna och bedöm om du vill förbättra systemsäkerheten. Exempel på säkerhetsinställningar är lösenord för maskinvara, Windows användarlösenord, Windows lösenordsprinciper, skyddad skärmsläckare och fildelning.

Anm: Säkerhetsrådgivaren ger bara en översikt över säkerhetsinställningarna och förslag på förbättringar av säkerheten. Vissa säkerhetsaspekter tas inte upp, t.ex. användning samt underhåll av antivirus- och brandväggsprogram. Många av inställningarna kräver administratörsbehörighet.

Överföra digitala certifikat: Client Security-guiden Certifikatöverföring vägleder dig genom hela processen för att överföra de privata nycklarna för dina certifikat, från programbaserade Microsoft Cryptographic Service Provider (CSP) till maskinbaserade Client Security Solution CSP. Efter överföringen är åtgärder som använder certifikat säkrare tack vare att de privata nycklarna skyddas av den integrerade säkerhetskretsen.

Ställa in funktionen för återställning av lösenord för maskinvara: Med hjälp av det här verktyget kan du skapa en skyddad miljö som kan köras oberoende av Windows och där du kan återställa bortglömda lösenord för start av datorn och för hårddisken. Du bevisar din identitet genom att svara på en rad frågor som du själv skapat. Du bör skapa en skyddad miljö så snart som möjligt innan ett lösenord blir bortglömt. Du kan inte återställa glömda lösenord för hårddisken förrän den här skyddade miljön har skapats på hårddisken och du har registrerat dig där. Verktyget hanteras bara av vissa ThinkCentre- och ThinkPad-datorer.

Anm: Du bör skapa ett administratörslösenord innan du genomför den här åtgärden. Om du saknar administratörslösenord är inte miljön så säker som den kan vara. När du är klar med åtgärden kommer ditt lösenord för start av datorn och för hårddisken att vara detsamma. Proceduren är utformad så att du ska kunna skapa en säker miljö och återställa lösenord du glömt efter det att du skapat miljön.

Aktivera den integrerade säkerhetskretsen: Verktyget ändrar BIOS-inställningarna genom att aktivera eller avaktivera den integrerade säkerhetskretsen. Du måste starta om datorn för att ändringen ska börja gälla.

Ändra inloggningsinställningar: Verktyget visar dina nuvarande inloggningsinställningar och om du är administratör kan du också ändra hur användarna loggar in till operativsystemet Windows och till ThinkVantage Rescue and Recovery-arbetsutrymmet.

Rensa räknaren för inloggningsförsök: Verktyget återställer räknaren som håller reda på hur många misslyckade inloggningsförsök som skickats vidare till den integrerade säkerhetskretsen. Efter ett visst antal misslyckade försök låser sig kretsen för en viss tidsperiod. Utlåsningsperioden blir längre för varje ytterligare misslyckat försök att logga in.

Göra inställningar för säkerhet och säkerhetskopiering: Med konfigureringsguiden för Client Security kan du göra inställningar för en rad olika säkerhetsverktyg. Med guidens konfigureringsalternativ kan du ange en mängd säkerhetsfunktioner, t.ex. aktivering av den integrerade säkerhetskretsen, du kan välja hur autentiseringen ska göras i Windows-miljön, välja Rescue and Recovery för att säkerhetskopiera känsliga data och aktivera autentisering med fingeravtryck.

Använda Client Security Solution med Rescue and Recovery

Både Rescue and Recovery och Client Security Solution är ThinkVantage-tekniker som har utvecklats med dig i åtanke. De är gjorda så att de kan användas separat eller tillsammans, beroende på vilka behov du har. Följande information är avsedd att hjälpa dig att utforma en strategi för hur du bäst använder programmen och förklara hur programmen förstärker varandra.

Det finns viktiga aspekter som du kan behöva ta hänsyn till när du installerar Rescue and Recovery eller Client Security Solution, eller båda programmen samtidigt. I följande tabell får du information som hjälper dig att hitta rätt metod för önskad konfiguration:

Tabell 10-1. I tabellen finns information som hjälper dig att ändra din konfiguration av Rescue and Recovery och Client Security. Med fristående Client Security Solution avses det installationspaket som kan hämtas från webben eller installeras från CD-skiva.

Den installerade programvaran är...	**och du vill...**	**Följ den här proceduren**	**Kommentarer**
Client Security Software 5.4x	Client Security Software 5.4x och Rescue and Recovery 3.0	1. Installera programmet Rescue and Recovery 3.0. 2. När du blir tillfrågad anger du att du vill behålla den installerade programvaran Client Security Software 5.4x.	Säkerhetskopior kan inte skyddas med hjälp av Client Security Software 5.4x och all användning av funktioner i Client Security Software i programmet Rescue and Recovery 3.0 sker med en emulerad version av Client Security Software. Funktionen för huvudlösenord läggs till bland säkerhetsfunktionerna. Huvudlösenord används ofta i företagsmiljöer. Mer information finns i ”Mer information” på sidan 10-1
Client Security Software 5.4x	Fristående installationspaket med Client Security Solution 6.0	1. Avinstallera Client Security Software 5.4x. 2. Installera Client Security Solution 6.0 (fristående).	• Du måste dekryptera alla krypterade filer och exportera all information från Password Manager innan du avinstallerar programmet. I annat fall går den informationen förlorad. • Du måste avinstallera IBM-programmet File and Folder Encryption innan du installerar programmet Client Security Solution.

Tabell 10-1. I tabellen finns information som hjälper dig att ändra din konfiguration av Rescue and Recovery och Client Security. Med fristående Client Security Solution avses det installationspaket som kan hämtas från webben eller installeras från CD-skiva. (forts)

Den installerade programvaran är...	och du vill...	Följ den här proceduren	Kommentarer
Client Security Software 5.4x	Client Security Solution 6.0 och Rescue and Recovery 3.0	1. Avinstallera Client Security Software 5.4x. 2. Installera programmet Rescue and Recovery 3.0. (Se till att komponenten Client Security Solution 6.0 är vald.)	• Om du installerar Rescue and Recovery 3.0 ovanpå Client Security Software 5.4x utan att först avinstallera Client Security Software kommer du att kunna använda enbart Rescue and Recovery. • Innan du avinstallerar Client Security Software 5.4x, måste du dekryptera filer och exportera Password Manager-informationen. I annat fall går den informationen förlorad. • Du måste avinstallera IBM-programmet File and Folder Encryption innan du installerar Client Security Solution 6.0.
Rescue and Recovery 3.0	Client Security Software 5.4x och Rescue and Recovery 3.0	1. Avinstallera programmet Rescue and Recovery 3.0. 2. Installera programmet Client Security Software 5.4x. 3. Installera programmet Rescue and Recovery 3.0. 4. När du blir tillfrågad anger du att du vill behålla den installerade programvaran Client Security Software 5.4x.	• Client Security Software 5.4x kan inte installeras ovanpå Rescue and Recovery 3.0. • Lokala säkerhetskopior tas bort när du avinstallerar Rescue and Recovery 3.0.

Tabell 10-1. I tabellen finns information som hjälper dig att ändra din konfiguration av Rescue and Recovery och Client Security. Med fristående Client Security Solution avses det installationspaket som kan hämtas från webben eller installeras från CD-skiva. (forts)

Den installerade programvaran är...	och du vill...	Följ den här proceduren	Kommentarer
Rescue and Recovery 3.0	Client Security Solution 6.0, installationspaket för fristående installation	1. Avinstallera programmet Rescue and Recovery 3.0. 2. Installera Client Security Solution 6.0 (fristående).	• Avinstallera Rescue and Recovery raderar alla användarfiler och registerinställningar för Client Security Solution. • Rescue and Recovery-säkerhetskopior som skyddas av Client Security Solution kommer inte längre att vara tillgängliga. • Lokala säkerhetskopior tas bort när du avinstallerar Rescue and Recovery 3.0. • Client Security Solution 6.0 (fristående) kan inte installeras ovanpå Rescue and Recovery 3.0.
Rescue and Recovery 3.0	Rescue and Recovery 3.0 och Client Security Solution 6.0	1. Välj alternativet **Ändra** i funktionen Lägg till eller ta bort program i Kontrollpanelen. 2. Ändra programmet genom att lägga till programmet Client Security Solution och önskade delkomponenter.	• Lokala säkerhetskopior tas bort när du lägger till programmet Client Security Solution. • När du har lagt till programmet Client Security Solution skapar du en ny bassäkerhetskopia så snart som möjligt. • Inställningarna och datafilerna för Client Security Solution tas bort. • Client Security Solution 6.0 (fristående) kan inte installeras ovanpå programmet Rescue and Recovery 3.0.
Fristående installationspaket med Client Security Solution 6.0	Client Security Software 5.4x	1. Avinstallera Client Security Solution 6.0 (fristående). 2. Installera programmet Client Security Software 5.4x.	• Om du väljer att ta bort datafiler och inställningar för Client Security Solution 6.0 påverkar inte detta åtgärder som du utför med Client Security Software 5.4x.

Tabell 10-1. I tabellen finns information som hjälper dig att ändra din konfiguration av Rescue and Recovery och Client Security. Med fristående Client Security Solution avses det installationspaket som kan hämtas från webben eller installeras från CD-skiva. (forts)

Den installerade programvaran är...	**och du vill...**	**Följ den här proceduren**	**Kommentarer**
Fristående installationspaket med Client Security Solution 6.0	Rescue and Recovery 3.0	1. Avinstallera Client Security Solution 6.0. 2. Installera programmet Rescue and Recovery 3.0. 3. Under installationen väljer du att installera enbart programmet Rescue and Recovery.	När du avinstallerar Client Security Solution 6.0 måste du radera filer och inställningar för Security Solution 6.0. Om du inte gör det när du får ett meddelande avbryts installationen av Rescue and Recovery 3.0.
Fristående Client Security Solution 6.0	Rescue and Recovery 3.0 och Client Security Solution 6.0	1. Installera programmet Rescue and Recovery 3.0. 2. Välj valfria delkomponenter i programmet Client Security Solution 6.0 som du vill installera.	• Datafiler och inställningar för Client Security Solution 6.0 bevaras. • Om du vill skydda säkerhetskopior med hjälp av programmet Client Security Solution 6.0 använder du programmet Rescue and Recovery.
Rescue and Recovery 3.0 och Client Security Solution 6.0	Client Security Software 5.4x	1. Avinstallera Rescue and Recovery - Client Security Solution. 2. Installera programmet Client Security Software 5.4x.	• Client Security Software 5.4x kan inte installeras ovanpå Client Security Solution 6.0. • Du kan välja att ta bort datafiler och inställningar när du blir tillfrågad om du vill göra det, utan att det påverkar funktionerna i Client Security Software 5.4x. • Genom att avinstallera programmet Rescue and Recovery 3.0 avinstallerar du automatiskt Client Security Solution 6.0.

Tabell 10-1. I tabellen finns information som hjälper dig att ändra din konfiguration av Rescue and Recovery och Client Security. Med fristående Client Security Solution avses det installationspaket som kan hämtas från webben eller installeras från CD-skiva. (forts)

Den installerade programvaran är...	och du vill...	Följ den här proceduren	Kommentarer
Rescue and Recovery 3.0 och Client Security Solution 6.0	Rescue and Recovery 3.0	1. Välj alternativet **Ändra** i funktionen Lägg till eller ta bort program i Kontrollpanelen. 2. Ta bort programmet Client Security Solution 6.0.	• Lokala säkerhetskopior tas bort när du tar bort programmet Client Security Solution 6.0. • Om du avinstallerar Client Security Solution 6.0 har du inte längre tillgång till Password Manager eller PrivateDisk. • Säkerhetskopior i Rescue and Recovery 3.0 som skyddas av Client Security Solution 6.0 är inte längre tillgängliga. Skapa därför en säkerhetskopia så snart som möjligt.
Rescue and Recovery 3.0 och Client Security Solution 6.0	Client Security Solution 6.0	1. Avinstallera programmet Rescue and Recovery 3.0. 2. När du blir tillfrågad väljer du att behålla dina aktuella inställningar för Client Security Solution 6.0 endast om du vill fortsätta att använda din nuvarande säkerhetskonfiguration. 3. Installera Client Security Solution 6.0 (fristående).	1. Säkerhetskopior som skyddas av Rescue and Recovery 3.0 med Client Security Solution 6.0 är inte längre tillgängliga. 2. Lokala säkerhetskopior tas bort när du avinstallerar Rescue and Recovery 3.0.

Lösenord och lösenmeningar för Rescue and Recovery

Du kan skydda Rescue and Recovery-arbetsutrymmet med lösenord eller lösenmeningar och på så sätt förhindra att obehöriga kommer åt kritiska data. Du kan konfigurera skyddet av Rescue and Recovery-arbetsutrymmet i konfigureringsguiden Client Security Solution eller genom att ändra inloggningsinställningarna med programmet Client Security Solution. Med Client Security Solution kan du också välja alternativ för återställning av lösenord i Rescue and Recovery-arbetsmiljön.

Anmärkningar:

1. Funktionen är tillgänglig endast om programmet Client Security Solution är installerat. Om du vill använda funktionen måste du ha slutfört guiden för att ställa in Client Security 6.0 och ha angett att du vill använda lösenord eller lösenmening för att logga på datorn.
2. Konfigureringsguiden för Client Security Solution och programmet Client Security Solution kan bara användas i Windows-miljö. Om du väljer att använda

Rescue and Recovery utan Client Security Solution, kommer Rescue and Recovery-arbetsutrymmet inte att vara skyddat av något lösenord eller någon lösenmening.

3. Med Client Security Solution kan du välja alternativ för återställning av lösenord i Rescue and Recovery-arbetsmiljön.

Med följande metoder skyddar du Rescue and Recovery-arbetsutrymmet via lösenord eller lösenmening.

Metod 1: Om du har slutfört konfigureringsguiden för Client Security gör du följande för att skydda Rescue and Recovery-arbetsutrymmet med ett lösenord eller en lösenmening.

1. På skrivbordet i Windows klickar du på **Start**, **Alla program**, **ThinkVantage** och dubbelklickar sedan på **Client Security Solution**.
2. När fönstret Client Security Solution öppnas klickar du på menyalternativet **Avancerat**.
3. Klicka på ikonen **Inställningar för säkerhet och säkerhetskopiering**. Konfigureringsguiden för Client Security öppnas.
4. Gör dina säkerhetsinställningar. När du blir tillfrågad väljer du något av följande:
   - Om du vill skydda Rescue and Recovery-arbetsutrymmet med hjälp av ditt lösenord för inloggning till Windows markerar du kryssrutan **Använd Windows-lösenordet för att komma åt Rescue and Recovery-arbetsutrymmet**.
   - Om du vill skydda Rescue and Recovery-arbetsutrymmet med din lösenmening för inloggning till Client Security Solution markerar du kryssrutan **Använd Client Security Solution-lösenmeningen för att komma åt Rescue and Recovery-arbetsutrymmet**.
5. Genomför stegen i konfigureringsguiden Client Security Solution och klicka sedan på **Slutför**. Om du vill ha mer information klickar du på **Hjälp** i konfigureringsguiden för Client Security.

Metod 2: Om du har genomfört inställningarna i konfigueringsguiden för Client Security gör du så här för att skydda Rescue and Recovery-arbetsutrymmet med ett lösenord eller en lösenmening:

1. På skrivbordet i Windows klickar du på **Start**, **Alla program**, **ThinkVantage** och dubbelklickar sedan på **Client Security Solution**.
2. När fönstret Client Security Solution öppnas klickar du på menyalternativet **Avancerat**.
3. Klicka på **Ändra inloggningsinställningar**.
4. Följ anvisningarna på skärmen. Klicka på **Hjälp** i Client Security Solution om du vill ha mer detaljerad information.

Inställningar för säkerhetskopiering i konfigureringsguiden för Client Security

Med guidens konfigureringsalternativ kan du ange en mängd säkerhetsfunktioner, t.ex. aktivering av den integrerade säkerhetskretsen, du kan välja hur autentiseringen ska göras i Windows-miljön, välja Rescue and Recovery för att säkerhetskopiera känsliga data och aktivera autentisering med fingeravtryck.

Genomför följande steg i konfigueringsguiden för Client Security:

1. På skrivbordet i Windows klickar du på **Start**, **Alla program**, **ThinkVantage** och dubbelklickar sedan på **Client Security Solution**.

2. När fönstret Client Security Solution öppnas klickar du på menyalternativet **Avancerat**.
3. När fönstret Client Security Solution öppnas klickar du på **Göra inställningar för säkerhet och säkerhetskopiering**. Konfigureringsguiden för Client Security öppnas.
4. Gör dina säkerhetsinställningar.
5. Genomför stegen i konfigureringsguiden Client Security Solution och klicka sedan på **Slutför**. Klicka på **Hjälp** i konfigureringsguiden för Client Security om du vill ha mer detaljerad information.

Mer information om Client Security Solution

Du hittar mer information om programmet Client Security Solution och dess funktioner i *Användarhandbok för Client Security Solution* som du kan hämta på webbadressen:

`http://www.ibm.com/pc/support/site.wss/`

Om du redan har installerat programmet Client Security Solution kan du läsa mer detaljerad information i handboken, som du öppnar på följande sätt:

1. Från skrivbordet i Windows klickar du på **Start**.
2. Välj **Alla program**.
3. Välj **ThinkVantage**.
4. Klicka på **Client Security Solution**.
5. Klicka på **Hjälp** i menyraden i Client Security Solution.
6. Klicka på **Användarhandbok**.

Capítulo 11. Português do Brasil

O aplicativo Client Security Solution é um conjunto de ferramentas ThinkVantage™ Technology projetadas para ajudar a proteger o acesso ao sistema operacional de seu computador e a seus dados sensíveis. O Client Security Solution integra a proteção de hardware de seu chip incorporado à proteção proporcionada por seu software seguro. Combinando hardware dedicado com sua proteção de software, o Client Security Solution aprimora de forma poderosa os recursos de segurança internos do sistema operacional de seu computador.

Quem Deve Ler este Guia

O *Guia do Usuário do ThinkVantage Client Security Solution* é direcionado a usuários finais individuais e usuários finais que estejam trabalhando em um ambiente de negócios. Este guia fornece informações sobre as seguintes áreas:

- Componentes do Client Security Solution
- Considerações sobre a instalação do Client Security Solution
- Recursos do Client Security Solution

Este guia suplementa o sistema de ajuda do Client Security Solution, que fornece instruções passo a passo sobre como executar tarefas específicas no programa.

Informações Adicionais

Se você for um administrador de sistema, engenheiro de sistema, administrador de rede ou engenheiro cliente que busca implementar o Client Security Solution em uma grande empresa, é possível obter informações detalhadas lendo o *Guia de Implementação do ThinkVantage Rescue and Recovery™ e do Client Security Solution* localizado no Web site a seguir:

`http://www.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-54502`

Componentes do Client Security Solution

O Client Security Solution foi projetado para computadores que são fornecidos equipados com um chip de segurança incorporado, que ajuda a fornecer níveis adicionais de segurança aos dados e processos de seu computador. No entanto, o software Client Security Solution agora pode ser configurado para aprimorar a segurança dos computadores que não estão equipados com um chip de segurança.

O Client Security Solution é dividido nos seguintes componentes de hardware e software.

- **Chip de Segurança Incorporado**

  O Client Security Solution foi projetado para computadores que são fornecidos equipados com um chip de segurança incorporado. Um chip de segurança incorporado é uma tecnologia de hardware criptográfico interno que fornece um nível extra de segurança a seu computador. O chip de segurança permite que os processos de criptografia e autenticação sejam transferidos de software vulnerável para o ambiente seguro de hardware dedicado. A maior segurança fornecida é tangível.
- **Client Security Setup Wizard**

O Assistente de Configuração do Client Security ajuda a guiá-lo pelo processo de configuração de suas opções de segurança. O assistente ajuda a ativar o chip de segurança incorporado, selecionar um método de autenticação e login, criar perguntas de recuperação de senha, estabelecer autenticação por impressão digital (opcional) e configurar componentes adicionais do Client Security Solution.

- **Password Manager**

  O Password Manager do Client Security permite gerenciar de forma segura e conveniente as informações de login sigilosas e de fácil esquecimento de aplicativos e Web sites, como IDs de usuários, senhas e outras informações pessoais. O Password Manager do Client Security armazena todas as informações através do chip de segurança incorporado, de forma que o acesso a seus aplicativos e Web sites permaneça totalmente seguro.
- **PrivateDisk**

  O PrivateDisk configura uma unidade de disco virtual criptografada que criptografa automaticamente quaisquer dados armazenados nos limites seguros deste ″cofre eletrônico″. Utilize sua própria unidade virtual para criptografar e armazenar todos os dados críticos. Os dados são automaticamente criptografados quando armazenados em qualquer volume do PrivateDisk.
- **Aplicativo Client Security Solution**

  O aplicativo Client Security Solution fornece uma única interface que permite que usuários executem funções básicas e avançadas de segurança, como ativar o chip de segurança incorporado, alterar a passphrase ou utilizar software de impressão digital. Para obter uma lista completa de recursos do Client Security Solution, consulte “Recursos do Client Security Solution” na página 11-3
- **Software de Impressão Digital ThinkVantage**

  O software de impressão digital ThinkVantage permite que usuários estabeleçam autenticação por impressão digital. Esse recurso de segurança conveniente está disponível em modelos e opcionais selecionados do ThinkPad e do ThinkCentre.

Antes de Instalar o Client Security Solution

Antes de instalar o aplicativo Client Security Solution, é importante que os seguintes pré-requisitos sejam atendidos:

- Windows XP ou Windows 2000 com Service Pack 3. Se estiver instalando esse programa em um disco rígido que tenha uma capacidade de mais de 137 GB, o Service Pack 1 é requerido para o Windows XP.
- Internet Explorer 5.5 (ou superior).
- 128 MB de memória dos quais mais de 8 MB podem ser designados como memória compartilhada sob a configuração de vídeo em BIOS.
- 800 MB de espaço em disco livre.

Se você tiver uma versão anterior do Client Security Solution, o Client Security Software ou o Rescue and Recovery, consulte “Utilizando o Client Security Solution com o Rescue and Recovery” na página 11-6 para obter instruções específicas.

Configurando o Client Security Solution

O aplicativo Client Security Solution está disponível no Web site `http://www.pc.ibm.com/thinkvantage` . O download, a instalação e a configuração do Client Security Solution podem ser feitos em questão de minutos.

Fazendo Download e Instalando o Client Security Solution

Execute o seguinte processo de instalação para fazer download e instalar o programa Client Security Solution:

1. Inicie seu computador e feche quaisquer programas abertos.
2. Vá para o Web site `http://www.pc.ibm.com/thinkvantage`.
3. Clique no link **Suporte e Downloads** na seção Recursos.
4. Role para baixo até a seção Embedded Security Subsystem e Client Security Solution e clique em **Download de Software**.
5. Siga as instruções na tela.
6. Execute o arquivo executável de instalação e siga as instruções da tela. Você terá a opção de instalar os componentes Password Manager e PrivateDisk do Client Security Solution.
7. Após fazer suas seleções, será solicitado que você reinicie seu computador.
8. Quando o computador é reiniciado, o Assistente de Configuração do Client Security será aberto. Se o assistente de configuração não abrir, consulte "Abrindo o Assistente de Configuração do Client Security"
9. Conclua o Assistente de Configuração do Client Security para concluir o processo de configuração.

Abrindo o Assistente de Configuração do Client Security

Execute os procedimentos a seguir para configurar o programa Client Security Solution utilizando o Assistente de Configuração do Client Security:

1. No desktop do Windows, clique em **Iniciar**, clique em **Todos os Programas**, selecione **ThinkVantage** e, em seguida, dê um clique duplo em **Client Security Solution**.
2. Quando a janela Client Security Solution for aberta, clique no item de menu **Avançado**.
3. Quando a janela Client Security Solution for aberta, clique em **Configurar Preferências de Segurança e Backup**. O Assistente de Configuração do Client Security será aberto.
4. Conclua as etapas do Assistente de Configuração do Client Security e, em seguida, clique em **Concluir**. Para obter informações detalhadas, clique em **Ajuda** no Assistente de Configuração do Client Security.

Utilizando o Client Security Solution

Execute o procedimento a seguir para acessar o aplicativo Client Security Solution:

1. No desktop do Windows, clique em **Iniciar**.
2. Selecione **Todos os Programas**.
3. Selecione **ThinkVantage**.
4. Clique em **Client Security Solution**.

Recursos do Client Security Solution

As informações a seguir detalham as várias tarefas que podem ser realizadas através do aplicativo Client Security Solution.

Nota: Se algumas das ferramentas mencionadas abaixo não estiverem disponíveis para você, pode ser que não tenha o software apropriado instalado, seu computador não suporta o aplicativo ou o aplicativo requer acesso de administrador ou supervisor.

Recursos Básicos

As informações a seguir detalham tarefas básicas que podem ser realizadas através do aplicativo Client Security Solution.

Alterando uma Passphrase: A ferramenta Alterar Passphrase permite estabelecer uma nova passphrase para o Client Security. Passphrases devem estar de acordo com os requisitos de passphrase do Client Security.

Configurando a Recuperação de Senha: A ferramenta Configurar Recuperação de Senha permite estabelecer uma maneira para recuperar uma senha esquecida do Windows ou uma passphrase do Client Security, dependendo da metodologia de autenticação utilizada.

Gerenciando Informações de Logon: O aplicativo Password Manager permite utilizar o Client Security Solution para gerenciar suas informações sigilosas e de fácil esquecimento de login, como IDs de usuários, senhas e outras informações pessoais. O aplicativo Password Manager armazena todas as informações através do chip de segurança incorporado de forma que sua política de autenticação de usuários controle o acesso aos aplicativos e Web sites seguros. Isso significa que em vez de precisar lembrar e fornecer uma grande quantidade de senhas individuais -- todas sujeitas a diferentes regras e datas de expiração -- será necessário lembrar de somente uma passphrase ou, quando o software de impressão digital estiver instalado, fornecer sua impressão digital.

Utilizando Software de Impressão Digital: O leitor de impressão digital integrado permite cadastrar e associar sua impressão digital à sua senha de ativação, senha de disco rígido e senha do Windows, de forma que a autenticação por impressão digital possa substituir senhas e ativar acesso do usuário simples e seguro. Um teclado com leitor de impressão digital está disponível com computadores selecionados e pode ser adquirido como um opcional. Esse opcional é suportado somente em computadores ThinkCentre e ThinkPad selecionados.

Protegendo Dados: A ferramenta PrivateDisk gera uma unidade de disco virtual criptografada, que criptografa automaticamente quaisquer dados armazenados nos limites seguros deste ″cofre eletrônico″.

Recursos Avançados

As informações a seguir detalham tarefas avançadas que podem ser realizadas através do aplicativo Client Security Solution.

Nota: Você deve ter direitos de administrador para executar as operações a seguir.

Monitorando Configurações de Segurança: A ferramenta Security Advisor permite visualizar um resumo das configurações de segurança atualmente configuradas em seu computador. Revise essas configurações para visualizar o status de segurança atual ou para aprimorar a segurança do sistema. Alguns dos tópicos de segurança incluídos são senhas de hardware, senhas de usuários do Windows, política de senhas do Windows, protetor de tela protegida e compartilhamento de arquivos.

Nota: A ferramenta Security Advisor fornece somente um resumo de configurações de segurança e sugestões para ajudar a aprimorar a segurança de seu sistema. Nem todos os aspectos de segurança são abordados, como por exemplo, o uso e a manutenção de programas de antivírus e de firewall. Muitas das configurações requerem acesso de supervisor ou administrador.

Transferindo Certificados Digitais: O Assistente de Transferência de Certificados do Client Security o guia pelo processo de transferência das chaves privadas associadas a seus certificados do Microsoft CSP (Cryptographic Service Provider) baseado em software para o Client Security Solution CSP baseado em hardware. Após a transferência, as operações que utilizam certificados são mais seguras, pois as chaves privadas são protegidas pelo chip de segurança incorporado.

Estabelecendo um Mecanismo de Reconfiguração da Senha de Hardware: Essa ferramenta cria um ambiente seguro que é executado independentemente do Windows e ajuda a reconfigurar senhas de ativação e de unidade de disco rígido esquecidas. Sua identidade é estabelecida pela resposta de um conjunto de perguntas criadas. É interessante criar esse ambiente seguro assim que possível, antes que uma senha seja esquecida. Não é possível reconfigurar uma senha de hardware esquecida até que esse ambiente seguro seja criado na unidade de disco rígido e após ter-se cadastrado. Essa ferramenta está disponível apenas na seleção de computadores ThinkCentre e ThinkPad.

Nota: É uma boa idéia configurar uma senha de administrador ou supervisor antes de utilizar essa ferramenta. Se você não tiver uma senha do administrador ou supervisor definida, seu ambiente não será tão seguro quanto possível. Quando você concluir esse procedimento, suas senhas de inicialização e da unidade de disco rígido irão corresponder. Esse procedimento é projetado para ajudá-lo na conclusão da tarefa de criação do ambiente seguro e para ajudá-lo na reconfiguração de senhas esquecidas, após a criação do ambiente seguro.

Ativando o Chip de Segurança Incorporado: Essa ferramenta inicia uma alteração de configuração do BIOS utilizada para ativar ou desativar o chip de segurança incorporado. Você deve reiniciar o computador para que essa alteração tenha efeito.

Alterando as Configurações de Logon: Essa ferramenta exibe as configurações de logon atuais e permite que o administrador altere como usuários efetuam logon no sistema operacional Windows e no espaço de trabalho ThinkVantage Rescue and Recovery.

Limpando o Contador de Proteção contra Falha: Essa ferramenta reconfigura o contador de falha de autenticação que monitora quantas tentativas de autenticação incorretas foram transmitidas ao chip de segurança incorporado. Após um determinado número de tentativas que falharam, o chip é travado por um período de tempo. O período de bloqueio aumenta com novas tentativas que falham.

Configurando Preferências de Segurança e Backup: O Assistente de Configuração do Client Security permite configurar várias ferramentas de software de segurança. Esse assistente fornece opções de configuração que permitem configurar vários recursos de segurança, como a ativação do chip de segurança incorporado do Client Security, a seleção de como deseja autenticar no ambiente Windows, a opção de utilizar o Rescue and Recovery para fazer backup de seus dados sensíveis ou a opção de utilizar autenticação por impressão digital.

Utilizando o Client Security Solution com o Rescue and Recovery

O programa Rescue and Recovery e o aplicativo Client Security Solution são ThinkVantage Technologies que foram desenvolvidas pensando em você. Ou seja, foram projetadas para funcionar separadamente ou juntas, dependendo de suas necessidades. As informações a seguir têm a intenção de ajudá-lo a projetar sua estratégia para utilizar esses programas e para destacar como esses programas aprimoram um ao outro.

Há considerações importantes a serem consideradas ao instalar o programa Rescue and Recovery, o aplicativo Client Security Solution ou ambos juntos. As tabelas a seguir fornecem informações para ajudar a determinar o procedimento correto para sua configuração desejada:

Tabela 1-1. A tabela a seguir fornece informações para ajudar a alterar a configuração do Rescue and Recovery e do Client Security. O Client Security Solution independente significa que o pacote de instalação foi adquirido na Web ou em CD.

O software instalado é o...	E você deseja o...	Siga este processo	Comentários
Client Security Software 5.4x	Client Security Software 5.4x e Rescue and Recovery 3.0	1. Instale o programa Rescue and Recovery 3.0. 2. Quando solicitado, indique que deseja manter o aplicativo Client Security Software 5.4x instalado.	Os backups não podem ser protegidos utilizando o aplicativo Client Security Software 5.4x, e qualquer utilização dos recursos do Client Security Software pelo programa Rescue and Recovery 3.0 será realizada utilizando uma versão emulada do Client Security Software. O recurso de senha principal é incluído em seus recursos de segurança. Uma senha principal é geralmente utilizada em um ambiente corporativo. Para obter informações adicionais, consulte “Informações Adicionais” na página 11-1
Client Security Software 5.4x	Pacote de instalação Independente do Client Security Solution 6.0	1. Desinstale o aplicativo Client Security Software 5.4x. 2. Instale o aplicativo Client Security Solution 6.0 (Independente).	• Você deve decriptografar arquivos e exportar qualquer informação do Password Manager antes da desinstalação. Caso contrário, essas informações serão perdidas. • Você deve desinstalar o software IBM® File and Folder Encryption antes de instalar o aplicativo Client Security Solution.

Tabela 1-1. A tabela a seguir fornece informações para ajudar a alterar a configuração do Rescue and Recovery e do Client Security. O Client Security Solution independente significa que o pacote de instalação foi adquirido na Web ou em CD. (continuação)

O software instalado é o...	E você deseja o...	Siga este processo	Comentários
Client Security Software 5.4x	Client Security Solution 6.0 e Rescue and Recovery 3.0	1. Desinstale o aplicativo Client Security Software 5.4x. 2. Instale o programa Rescue and Recovery 3.0. (Certifique-se de que o componente Client Security Solution 6.0 esteja selecionado.)	• Instalar o Rescue and Recovery 3.0 sobre o Client Security Software 5.4x sem antes desinstalar o Client Security Software resultará somente no Rescue and Recovery. • Antes de desinstalar o aplicativo Client Security Software 5.4x, você deve decriptografar quaisquer arquivos criptografados e exportar quaisquer informações do Password Manager antes da desinstalação. Caso contrário, essas informações serão perdidas. • Você deve desinstalar o software IBM File and Folder Encryption antes de instalar o aplicativo Client Security Solution 6.0.
Rescue and Recovery 3.0	Client Security Software 5.4x e Rescue and Recovery 3.0	1. Desinstale o programa Rescue and Recovery 3.0. 2. Instale o aplicativo Client Security Software 5.4x. 3. Instale o programa Rescue and Recovery 3.0. 4. Quando solicitado, indique que deseja manter o aplicativo Client Security Software 5.4x instalado.	• O aplicativo Client Security Software 5.4x não pode ser instalado sobre o programa Rescue and Recovery 3.0. • Backups locais são excluídos quando o programa Rescue and Recovery 3.0 é desinstalado.

Tabela 1-1. A tabela a seguir fornece informações para ajudar a alterar a configuração do Rescue and Recovery e do Client Security. O Client Security Solution independente significa que o pacote de instalação foi adquirido na Web ou em CD. (continuação)

O software instalado é o...	E você deseja o...	Siga este processo	Comentários
Rescue and Recovery 3.0	Pacote de instalação Independente do Client Security Solution 6.0	1. Desinstale o programa Rescue and Recovery 3.0. 2. Instale o aplicativo Client Security Solution 6.0 (Independente).	• Desinstalar o Rescue and Recovery excluirá os arquivos de usuário e as configurações de registro do Client Security Solution. • Os backups do Rescue and Recovery protegidos pelo Client Security Solution não estarão mais disponíveis. • Os backups locais são excluídos na desinstalação do Rescue and Recovery 3.0. • O Client Security Solution 6.0 (Independente) não pode ser instalado sobre o Rescue and Recovery 3.0.
Rescue and Recovery 3.0	Rescue and Recovery 3.0 e Client Security Solution 6.0	1. Selecione a opção **Modificar** em Adicionar ou remover programas. 2. Conclua a operação de modificação incluindo o aplicativo Client Security Solution e quaisquer subcomponentes desejados.	• Backups locais são excluídos quando o aplicativo Client Security Solution é incluído. • Após incluir o aplicativo Client Security Solution, crie um novo backup base assim que possível. • As configurações e os arquivos de dados do Client Security Solution são excluídos. • O aplicativo Client Security Solution 6.0 (Independente) não pode ser instalado sobre o programa Rescue and Recovery 3.0.
Pacote de instalação Independente do Client Security Solution 6.0	Client Security Software 5.4x	1. Desinstale o aplicativo Client Security Solution 6.0 (Independente). 2. Instale o aplicativo Client Security Software 5.4x.	• Excluir os arquivos de dados e as configurações do Client Security Solution 6.0 no prompt não afetará as operações do Client Security Software 5.4x.

Tabela 1-1. A tabela a seguir fornece informações para ajudar a alterar a configuração do Rescue and Recovery e do Client Security. O Client Security Solution independente significa que o pacote de instalação foi adquirido na Web ou em CD. (continuação)

O software instalado é o...	E você deseja o...	Siga este processo	Comentários
Pacote de instalação Independente do Client Security Solution 6.0	Rescue and Recovery 3.0	1. Desinstale o aplicativo Client Security Solution 6.0. 2. Instale o programa Rescue and Recovery 3.0. 3. Durante a instalação, opte por instalar somente o programa Rescue and Recovery.	Ao desinstalar o aplicativo Client Security Solution 6.0, você deve excluir os arquivos e as configurações do Security Solution 6.0. A não remoção dos mesmos no prompt encerrará a instalação do Rescue and Recovery 3.0.
Client Security Solution 6.0 Independente	Rescue and Recovery 3.0 e Client Security Solution 6.0	1. Instale o programa Rescue and Recovery 3.0. 2. Selecione os subcomponentes do aplicativo Client Security Solution 6.0 que deseja instalar.	• Os arquivos de dados e as configurações do Client Security Solution 6.0 são preservadas. • Para optar pela proteção de backups utilizando o aplicativo Client Security Solution 6.0, utilize o programa Rescue and Recovery.
Rescue and Recovery 3.0 e Client Security Solution 6.0	Client Security Software 5.4x	1. Desinstale o aplicativo Rescue and Recovery - Client Security Solution. 2. Instale o aplicativo Client Security Software 5.4x.	• O aplicativo Client Security Software 5.4x não pode ser instalado sobre o aplicativo Client Security Solution 6.0. • Excluir os arquivos de dados e as configurações no prompt não afetará as operações do Client Security Software 5.4x. • Desinstalando o programa Rescue and Recovery 3.0, o aplicativo Client Security Solution 6.0 é desinstalado automaticamente.

Tabela 1-1. A tabela a seguir fornece informações para ajudar a alterar a configuração do Rescue and Recovery e do Client Security. O Client Security Solution independente significa que o pacote de instalação foi adquirido na Web ou em CD. (continuação)

O software instalado é o...	E você deseja o...	Siga este processo	Comentários
Rescue and Recovery 3.0 e Client Security Solution 6.0	Rescue and Recovery 3.0	1. Selecione **Modificar** em Adicionar ou remover programas. 2. Remova o aplicativo Client Security Solution 6.0.	• Backups locais são excluídos quando o aplicativo Client Security Solution 6.0 é removido. • A desinstalação do aplicativo Client Security Solution 6.0 resultará em não ter o Password Manager ou o PrivateDisk. • Os backups do Rescue and Recovery 3.0 protegidos pelo aplicativo Client Security Solution 6.0 não estão mais acessíveis. Crie um novo backup assim que possível.
Rescue and Recovery 3.0 e Client Security Solution 6.0	Client Security Solution 6.0	1. Desinstale o programa Rescue and Recovery 3.0. 2. Quando solicitado, opte por manter as configurações atuais do Client Security Solution 6.0 somente se quiser manter a configuração da segurança atual. 3. Instale o aplicativo Client Security Solution 6.0 (Independente).	1. Os backups do Rescue and Recovery 3.0 protegidos pelo Client Security Solution 6.0 não estão mais acessíveis. 2. Backups locais são excluídos quando o aplicativo Rescue and Recovery 3.0 é desinstalado.

Senhas e Passphrases do Rescue and Recovery

É possível utilizar senhas ou passphrases para proteger o espaço de trabalho Rescue and Recovery, protegendo, assim, dados críticos contra acesso não autorizado. É possível especificar a proteção do espaço de trabalho Rescue and Recovery utilizando o assistente de Configuração do Client Security para configurar as preferências de segurança ou alterando suas configurações de logon através do aplicativo Client Security Solution. O aplicativo Client Security Solution também permite que você estabeleça as opções de recuperação de senha no espaço de trabalho Rescue and Recovery.

Notas:

1. Esse recurso estará disponível somente se o programa Client Security Solution 6.0 for instalado. Para utilizar esse recurso, você deve ter concluído o assistente de Configuração do Client Security 6.0 e ter especificado que deseja utilizar uma senha ou passphrase para efetuar logon em seu computador.
2. O assistente de Configuração do Client Security 6.0 e o aplicativo Client Security Solution 6.0 estão acessíveis somente no ambiente Windows. Se optar

por utilizar o Rescue and Recovery sem o Client Security Solution, então, o espaço de trabalho Rescue and Recovery não será protegido por uma senha ou passphrase.

3. O aplicativo Client Security Solution permite que você estabeleça as opções de recuperação de senha no espaço de trabalho Rescue and Recovery.

Utilize os métodos a seguir para proteger o espaço de trabalho do Rescue and Recovery utilizando uma senha ou passphrase.

Método 1: Se não tiver concluído o Assistente de Configuração do Client Security, faça o seguinte para proteger o espaço de trabalho Rescue and Recovery com uma senha ou passphrase:

1. No desktop do Windows, clique em **Iniciar**, clique em **Todos os Programas**, selecione **ThinkVantage** e, em seguida, dê um clique duplo em **Client Security Solution**.
2. Quando a janela Client Security Solution for aberta, clique no item de menu **Avançado**.
3. Clique no ícone **Configurar Preferências de Segurança e Backup**. O Assistente de Configuração do Client Security é aberto.
4. Configure suas preferências de segurança. Quando solicitado, escolha uma das seguintes opções:
   - Se quiser proteger o espaço de trabalho Rescue and Recovery utilizando a senha de logon do Windows, selecione a caixa de opções **Utilizar Senha do Windows para Obter Acesso ao Espaço de Trabalho Rescue and Recovery**.
   - Se quiser proteger o espaço de trabalho Rescue and Recovery utilizando a passphrase de logon do Client Security Solution, selecione a caixa de opções **Utilizar a Passphrase do Client Security Solution para Obter Acesso ao Espaço de Trabalho Rescue and Recovery**.
5. Conclua o assistente de Configuração do Client Security Solution, em seguida, clique em **Concluir**. Para obter informações adicionais, clique em **Ajuda** no Assistente de Configuração do Client Security.

Método 2: Se tiver concluído o Assistente de Configuração do Client Security, faça o seguinte para proteger o espaço de trabalho Rescue and Recovery com uma senha ou passphrase:

1. No desktop do Windows, clique em **Iniciar**, clique em **Todos os Programas**, selecione **ThinkVantage** e, em seguida, dê um clique duplo em **Client Security Solution**.
2. Quando a janela Client Security Solution for aberta, clique no item de menu **Avançado**.
3. Clique em **Alterar Configurações de Logon**.
4. Siga as instruções na tela. Para obter informações detalhadas, clique em **Ajuda** no aplicativo Client Security Solution.

Configurando Preferências de Backup Utilizando o Assistente de Configuração do Client Security

O Assistente de Configuração do Cliente Security Solution fornece opções de configuração que permitem configurar vários recursos de segurança, como a ativação do chip de segurança incorporado, a seleção de como deseja autenticar no ambiente Windows, a opção de utilizar o Rescue and Recovery para fazer backup de seus dados sensíveis ou a opção de utilizar autenticação por impressão digital.

Execute o procedimento a seguir para utilizar o assistente de Configuração do Client Security:

1. No desktop do Windows, clique em **Iniciar**, clique em **Todos os Programas**, selecione **ThinkVantage** e, em seguida, dê um clique duplo em **Client Security Solution**.
2. Quando a janela Client Security Solution for aberta, clique no item de menu **Avançado**.
3. Quando a janela Client Security Solution for aberta, clique em **Configurar Preferências de Segurança e Backup**. O Assistente de Configuração do Client Security é aberto.
4. Configure suas preferências de segurança.
5. Conclua o assistente de Configuração do Client Security Solution, em seguida, clique em **Concluir**. Para obter informações detalhadas, clique em **Ajuda** no Assistente de Configuração do Client Security.

Informações Adicionais sobre o Client Security Solution

Para obter informações adicionais sobre o aplicativo Client Security Solution e seus recursos, consulte o *Guia do Usuário do Client Security Solution* na Web no endereço:

`http://www.ibm.com/pc/support/site.wss/`

Se o aplicativo Client Security Solution já estiver instalado, é possível ler informações mais detalhadas do Guia do usuário, concluindo o seguinte procedimento:

1. No desktop do Windows, clique em **Iniciar**.
2. Selecione **Todos os Programas**.
3. Selecione **ThinkVantage**.
4. Clique em **Client Security Solution**.
5. Na barra de menus do Client Security Solution, clique em **Ajuda**.
6. Clique em **Guia do Usuário**.

Capítulo 12. Português

A aplicação Client Security Solution é um conjunto de ferramentas de tecnologia ThinkVantage™ concebidas para proteger o acesso ao sistema operativo do computador e a dados importantes. O Client Security Solution integra a protecção de equipamento do microcircuito incorporado com a protecção proporcionada pelo respectivo software seguro. Ao combinar o equipamento dedicado com a protecção de software, o Client Security Solution melhora consideravelmente as funções de segurança integradas no sistema operativo do computador.

Quem deverá ler este manual

O *Manual do Utilizador do ThinkVantage Client Security Solution* destina-se a utilizadores finais individuais e utilizadores finais que trabalhem num ambiente comercial. Este manual fornece informações sobre as seguintes áreas:

- Os componentes do Client Security Solution
- As considerações de instalação do Client Security Solution
- As funções do Client Security Solution

Este manual serve de suplemento ao sistema de ajuda do Client Security Solution, que fornece instruções passo-a-passo sobre como executar determinadas tarefas no programa.

Informações adicionais

Se for um administrador do sistema, um engenheiro do sistema, um administrador da rede ou um técnico que esteja a tentar implementar o Client Security Solution numa grande empresa, poderá obter informações detalhadas através do *Manual de Implementação do ThinkVantage Rescue and Recovery™ e do Client Security Solution* localizado no seguinte sítio da Web:

`http://www.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-54502`

Componentes do Client Security Solution

O Client Security Solution foi concebido para computadores equipados com um microcircuito de segurança incorporado, que ajuda a fornecer níveis adicionais de segurança aos dados e processos do computador. Contudo, o software Client Security Solution pode agora ser configurado de modo a melhorar a segurança dos computadores que não estão equipados com um microcircuito de segurança.

O Client Security Solution está dividido nos seguintes componentes de equipamento e software.

- **Microcircuito de segurança incorporado**

  O Client Security Solution foi concebido para computadores equipados com um microcircuito de segurança incorporado. Um microcircuito de segurança incorporado é uma tecnologia de equipamento criptográfico incorporado que fornece um nível adicional de segurança ao computador. O microcircuito de segurança permite que os processos de codificação e autenticação sejam transferidos de um software vulnerável para o ambiente protegido do equipamento dedicado. O aumento da segurança fornecida é evidente.
- **Assistente de configuração do Client Security**

O assistente de configuração do Client Security fornece instruções ao utilizador através do processo de configuração das opções de segurança. O assistente ajuda-o a activar o microcircuito de segurança incorporado, a seleccionar um método de autenticação e de início de sessão, a criar perguntas de recuperação de palavras-passe, a estabelecer uma autenticação por leitura de impressões digitais (opcional) e a configurar componentes adicionais do Client Security Solution.

- **Password Manager**

  O Client Security Password Manager permite gerir de forma cómoda e com segurança as informações importantes e fáceis de esquecer relativas ao início de sessão em aplicações ou sítios da Web, tais como IDs de utilizador, palavras-passe e outras informações pessoais. O Client Security Password Manager armazena todas as informações através do microcircuito de segurança incorporado, de modo a que o acesso às aplicações e aos sítios da Web permaneça totalmente seguro.
- **PrivateDisk**

  O PrivateDisk define uma unidade de disco virtual codificada que codifica automaticamente todos os dados armazenados nos limites seguros deste ″cofre electrónico″. Utilize a sua própria unidade virtual para codificar e armazenar todos os dados importantes. Os dados são automaticamente codificados ao serem armazenados em qualquer volume PrivateDisk.
- **Aplicação Client Security Solution**

  A aplicação Client Security Solution fornece uma interface única que permite aos utilizadores executarem funções de segurança básicas e avançadas, tais como activar o microcircuito de segurança incorporado, alterar uma frase-passe ou utilizar software de leitura de impressões digitais. Para obter uma lista de funções completas do Client Security Solution, consulte o tópico "Funções do Client Security Solution" na página 12-4
- **Software de leitura de impressões digitais ThinkVantage**

  O software de leitura de impressões digitais ThinkVantage permite que os utilizadores efectuem a autenticação através da leitura de impressões digitais. Esta cómoda função de segurança está disponível em modelos e opções ThinkPad e ThinkCentre seleccionados.

Antes de instalar o Client Security Solution

Antes de instalar a aplicação Client Security Solution, é importante cumprir os seguintes pré-requisitos:

- Windows XP ou Windows 2000 com o Service Pack 3. Se instalar este programa num disco rígido com uma capacidade igual ou superior a 137 GB, será necessário ter instalado o Service Pack 1 para o Windows XP.
- Internet Explorer 5.5 (ou superior).
- 128 MB de memória, dos quais não é possível designar mais do que 8 MB como memória partilhada na configuração de vídeo do BIOS.
- 800 MB de espaço disponível em disco.

Se possuir uma versão anterior do Client Security Solution, Client Security Software ou Rescue and Recovery, consulte o tópico "Utilizar o Client Security Solution com o Rescue and Recovery" na página 12-6 para obter instruções específicas.

Definir o Client Security Solution

A aplicação Client Security Solution está disponível no sítio da Web `http://www.pc.ibm.com/thinkvantage`. A transferência, instalação e configuração do Client Security Solution pode ser executada numa questão de minutos.

Transferir e instalar o Client Security Solution

Execute o seguinte processo de instalação para transferir e instalar o programa Client Security Solution:

1. Inicie o computador e feche todos os programas abertos.
2. Aceda ao sítio da Web `http://www.pc.ibm.com/thinkvantage`.
3. Faça clique na ligação **Support and downloads** na secção Resources.
4. Avance para a secção Embedded Security Subsystem and Client Security Solution e faça clique em **Software download**.
5. Siga as instruções apresentadas no ecrã.
6. Execute o ficheiro executável de instalação e siga as instruções apresentadas no ecrã. Será apresentada a opção de instalar os componentes do Password Manager e do PrivateDisk do Client Security Solution.
7. Depois de ter efectuado as selecções, receberá um pedido para reiniciar o computador.
8. Quando o computador reiniciar, será aberto o assistente de configuração do Client Security. Se o assistente de configuração não abrir, consulte o tópico "Abrir o assistente de configuração do Client Security"
9. Conclua o assistente de configuração do Client Security de modo a concluir o processo de configuração.

Abrir o assistente de configuração do Client Security

Conclua o seguinte procedimento de modo a configurar o programa Client Security Solution através do assistente de configuração do Client Security:

1. A partir do ambiente de trabalho do Windows, faça clique em **Iniciar**, faça clique em **Todos os programas**, seleccione **ThinkVantage** e depois faça duplo clique em **Client Security Solution**.
2. Quando a janela Client Security Solution abrir, faça clique no item de menu **Avançadas**.
3. Quando a janela Client Security Solution abrir, faça clique em **Definir preferências de segurança e cópia de segurança**. Será aberto o assistente de configuração do Client Security.
4. Conclua os passos do assistente de configuração do Client Security Solution e, em seguida, faça clique em **Terminar**. Para obter informações detalhadas, faça clique em **Ajuda** dentro do assistente de configuração do Client Security.

Utilizar o Client Security Solution

Conclua o seguinte procedimento para aceder à aplicação Client Security Solution:

1. A partir do ambiente de trabalho do Windows, faça clique em **Iniciar**.
2. Seleccione **Todos os programas**.
3. Seleccione **ThinkVantage**.
4. Faça clique em **Client Security Solution**.

Funções do Client Security Solution

As informações seguintes especificam as várias tarefas que podem ser executadas a partir da aplicação Client Security Solution.

Nota: Algumas das ferramentas mencionadas abaixo poderão não estar disponíveis se não tiver instalado o software adequado, o computador não suportar a aplicação ou se a aplicação exigir um acesso de administrador ou supervisor.

Funções básicas

As informações seguintes especificam as tarefas básicas que podem ser executadas a partir da aplicação Client Security Solution.

Alterar uma frase-passe: A ferramenta Alterar frase-passe permite estabelecer uma nova frase-passe do Client Security. As frases-passe devem cumprir os requisitos de frase-passe do Client Security.

Configurar a recuperação de palavras-passe: A ferramenta Configurar a recuperação da palavra-passe permite estabelecer uma forma de recuperar uma palavra-passe do Windows ou uma frase-passe do Client Security que tenha sido esquecida, dependendo da metodologia de autenticação utilizada.

Gerir as informações de início de sessão: A aplicação Password Manager permite utilizar o Client Security Solution para gerir informações importantes e de fácil esquecimento, tais como IDs de utilizador, palavras-passe e outras informações pessoais. A aplicação Password Manager armazena todas as informações através do microcircuito de segurança incorporado, de modo a que a política de autenticação de utilizador controle o acesso às aplicações protegidas e aos sítios da Web. Isto significa que, ao invés de ter de memorizar e fornecer uma enorme quantidade de palavras-passe individuais -- todas sujeitas a regras e prazos de validade diferentes -- terá apenas de memorizar uma palavra-passe ou, se tiver instalado um software de leitura de impressões digitais, fornecer a sua impressão digital.

Utilizar software de leitura de impressões digitais: O leitor de impressões digitais incorporado permite registar e associar a sua impressão digital à palavra-passe de ligação, à palavra-passe de disco rígido e à palavra-passe do Windows, de forma a que a autenticação por leitura de impressões digitais possa substituir as palavras-passe e permitir um acesso do utilizador simples e seguro. Está disponível um teclado com leitor de impressões digitais em computadores seleccionados, que pode ser adquirido como opção. Esta opção é apenas suportada em computadores ThinkCentre e ThinkPad seleccionados.

Proteger dados: A ferramenta PrivateDisk cria uma unidade de disco virtual codificada que codifica automaticamente todos os dados armazenados nos limites seguros deste ″cofre electrónico″.

Funções avançadas

As informações seguintes especificam as tarefas avançadas que podem ser executadas a partir da aplicação Client Security Solution.

Nota: Terá de possuir direitos de administrador para executar as seguintes operações.

Supervisionar as definições de segurança: A ferramenta Security Advisor permite ver um resumo das definições de segurança actualmente definidas para o computador. Reveja estas definições de modo a ver o actual estado de segurança ou a melhorar a segurança do sistema. Alguns tópicos de segurança incluídos são palavras-passe do equipamento, palavras-passe de utilizadores do Windows, protecções de ecrã protegidas e partilha de ficheiros.

Nota: A ferramenta Security Advisor apenas fornece um resumo das definições de segurança e sugestões de ajuda para melhorar a segurança do sistema. Nem todos os aspectos de segurança são abrangidos, tais como a utilização e manutenção de programas de antivírus e firewall. Muitas definições requerem um acesso de supervisor ou administrador.

Transferir certificados digitais: O assistente de transferência de certificados do Client Security ajuda-o no processo de transferência de chaves privadas associadas com os certificados, a partir do fornecedor de serviços criptográficos (CSP) da Microsoft baseado em software para o CSP do Client Security Solution baseado em equipamento. Após a transferência, as operações que utilizem os certificados estarão mais protegidas devido às chaves privadas protegidas pelo microcircuito de segurança incorporado.

Estabelecer um mecanismo de reposição de palavras-passe de equipamento: Esta ferramenta cria um ambiente protegido que é executado independentemente do Windows e ajuda a repor palavras-passe de ligação e unidade de disco rígido que tenham sido esquecidas. A identidade do utilizador é estabelecida ao responder a um conjunto de perguntas que criou previamente. É aconselhável criar este ambiente protegido o mais depressa possível, para evitar qualquer esquecimento de palavras-passe. Não é possível repor uma palavra-passe de equipamento antes da criação deste ambiente de segurança no disco rígido e do registo. Esta ferramenta está apenas disponível em computadores seleccionados ThinkCentre e ThinkPad.

Nota: É aconselhável definir uma palavra-passe de administrador ou supervisor antes de utilizar esta ferramenta. Se não tiver definido uma palavra-passe de administrador ou supervisor, o ambiente não será abrangido pela protecção máxima. Quando concluir este procedimento, as palavras-passe de ligação e de unidade de disco rígido serão iguais. Este procedimento foi concebido para ajudar a concluir a tarefa de criação do ambiente protegido e repor as palavras-passe que tenham sido esquecidas após a sua criação.

Activar o microcircuito de segurança incorporado: Esta tarefa dá início a uma alteração de definições do BIOS que é utilizada para activar ou desactivar o microcircuito de segurança incorporado. Terá de reiniciar o computador para que esta alteração tenha efeito.

Alterar as definições de início de sessão: Esta ferramenta apresenta as definições de início de sessão actuais e permite que um administrador altere a forma como os utilizadores iniciam sessão no sistema operativo Windows e na área de trabalho ThinkVantage Rescue and Recovery.

Limpar o contador "fail safe": Esta ferramenta repõe o contador de falhas de autenticação que supervisiona o número de tentativas incorrectas de autenticação que foram transferidas para o microcircuito de segurança incorporado. Após um determinado número de tentativas falhadas, o microcircuito é bloqueado por um período de tempo. O período de bloqueio aumenta com sucessivas tentativas falhadas.

Definir preferências de segurança e de cópia de segurança: O assistente de configuração do Client Security permite configurar uma variedade de ferramentas de software de segurança. Este assistente fornece opções de configuração que permitem definir uma variedade de funções de segurança, tais como activar o microcircuito de segurança incorporado, seleccionar como prefere efectuar a autenticação no ambiente do Windows, utilizar o Rescue and Recovery para fazer uma cópia de segurança de dados importantes ou utilizar a autenticação por leitura de impressões digitais.

Utilizar o Client Security Solution com o Rescue and Recovery

O programa Rescue and Recovery e a aplicação Client Security Solution são tecnologias ThinkVantage desenvolvidas especialmente para o cliente. Isto é, foram concebidas para funcionar separadamente ou em conjunto, dependendo das suas necessidades. As informações seguintes pretendem ajudar a estabelecer uma estratégia para a utilização destes programas e a realçar a forma como estes programas se optimizam mutuamente.

Existem considerações importantes a ter em conta aquando da instalação do programa Rescue and Recovery, da aplicação Client Security Solution ou de ambos. A tabela seguinte fornece informações para o ajudar a determinar o procedimento correcto para a configuração desejada:

Tabela 1-1. A tabela seguinte fornece informações para ajudar a alterar a configuração do Rescue and Recovery e do Client Security. A definição Client Security Solution autónomo (Standalone) significa que o pacote de instalação foi adquirido pela Web ou a partir de um CD.

O software instalado é...	E pretende instalar o...	Siga este processo	Comentários
Client Security Software 5.4x	Client Security Software 5.4x e Rescue and Recovery 3.0	1. Instalar o programa Rescue and Recovery 3.0 2. Quando for solicitado, indique que pretende manter instalada a aplicação Client Security Software 5.4x.	As cópias de segurança não podem ser protegidas através da aplicação Client Security Software 5.4x e qualquer utilização das funções do Client Security Software por parte do programa Rescue and Recovery 3.0 será efectuado utilizando uma versão emulada do Client Security Software. A função de palavra-passe principal é adicionada às funções de segurança. Uma palavra-passe principal é habitualmente utilizada num ambiente de empresa. Para obter mais informações, consulte o tópico “Informações adicionais” na página 12-1

Tabela 1-1. A tabela seguinte fornece informações para ajudar a alterar a configuração do Rescue and Recovery e do Client Security. A definição Client Security Solution autónomo (Standalone) significa que o pacote de instalação foi adquirido pela Web ou a partir de um CD. (continuação)

O software instalado é...	E pretende instalar o...	Siga este processo	Comentários
Client Security Software 5.4x	Pacote de instalação Client Security Solution 6.0 Standalone	1. Anular a instalação da aplicação Client Security Software 5.4x. 2. Instalar a aplicação Client Security Solution 6.0 (Standalone).	• Terá de descodificar todos os ficheiros codificados e exportar todas as informações do Password Manager antes de anular a instalação. De outro modo, esta informação será perdida. • Terá de anular a instalação do software IBM® File and Folder Encryption antes de instalar a aplicação Client Security Solution.
Client Security Software 5.4x	Client Security Solution 6.0 e Rescue and Recovery 3.0	1. Anular a instalação da aplicação Client Security Software 5.4x. 2. Instalar o programa Rescue and Recovery 3.0. (Certifique-se de que o componente Client Security Solution 6.0 está seleccionado.)	• Se instalar o Rescue and Recovery 3.0 sobre o Client Security Software 5.4x sem primeiro anular a instalação do Client Security Software irá apenas resultar na instalação do primeiro. • Antes de anular a instalação da aplicação Client Security Software 5.4x, terá de descodificar todos os ficheiros codificados e exportar todas as informações do Password Manager. De outro modo, estas informações serão perdidas. • Terá de anular a instalação do software IBM File and Folder Encryption antes de instalar a aplicação Client Security 6.0 Solution.

Tabela 1-1. A tabela seguinte fornece informações para ajudar a alterar a configuração do Rescue and Recovery e do Client Security. A definição Client Security Solution autónomo (Standalone) significa que o pacote de instalação foi adquirido pela Web ou a partir de um CD. (continuação)

O software instalado é...	E pretende instalar o...	Siga este processo	Comentários
Rescue and Recovery 3.0	Client Security Software 5.4x e Rescue and Recovery 3.0	1. Anular a instalação do programa Rescue and Recovery 3.0. 2. Instalar a aplicação Client Security Software 5.4x. 3. Instalar o programa Rescue and Recovery 3.0. 4. Quando solicitado, indique que pretende manter instalada a aplicação Client Security Software 5.4x.	• A aplicação Client Security Software 5.4x não pode ser instalada sobre o programa Rescue and Recovery 3.0. • As cópias de segurança locais são eliminadas ao anular a instalação do programa Rescue and Recovery 3.0.
Rescue and Recovery 3.0	Pacote de instalação Client Security Solution 6.0 Standalone	1. Anular a instalação do programa Rescue and Recovery 3.0. 2. Instalar a aplicação Client Security Solution 6.0 (Standalone).	• Anular a instalação do Rescue and Recovery irá eliminar os ficheiros de utilizador e as definições de registo do Client Security Solution. • As cópias de segurança do Rescue and Recovery protegidas através do Client Security Solution deixarão de estar acessíveis. • As cópias de segurança locais são eliminadas ao anular a instalação do Rescue and Recovery 3.0. • O Client Security Solution 6.0 (Standalone) não pode ser instalado sobre o Rescue and Recovery 3.0.

Tabela 1-1. A tabela seguinte fornece informações para ajudar a alterar a configuração do Rescue and Recovery e do Client Security. A definição Client Security Solution autónomo (Standalone) significa que o pacote de instalação foi adquirido pela Web ou a partir de um CD. (continuação)

O software instalado é...	E pretende instalar o...	Siga este processo	Comentários
Rescue and Recovery 3.0	Rescue and Recovery 3.0 e Client Security Solution 6.0	1. Seleccione a opção **Modificar** a partir de Adicionar/Remover programas. 2. Conclua a operação de modificação ao adicionar a aplicação Client Security Solution e outros sub-components pretendidos.	• As cópias de segurança locais são eliminadas quando a aplicação Client Security Solution é adicionada. • Depois de adicionar a aplicação Client Security Solution, crie uma nova cópia de segurança de base logo que possível. • As definições do Client Security Solution e os ficheiros de dados são eliminados. • A aplicação Client Security Solution 6.0 (Standalone) não pode ser instalada sobre o programa Rescue and Recovery 3.0.
Pacote de instalação Client Security Solution 6.0 Standalone	Client Security Software 5.4x	1. Anular a instalação da aplicação Client Security Solution 6.0 (Standalone). 2. Instalar a aplicação Client Security Software 5.4x.	• Eliminar os ficheiros de dados e as definições do Client Security Solution 6.0 quando for solicitado não afecta as operações do Client Security Software 5.4x.
Pacote de instalação Client Security Solution 6.0 Standalone	Rescue and Recovery 3.0	1. Anular a instalação da aplicação Client Security Solution 6.0. 2. Instalar o programa Rescue and Recovery 3.0. 3. Durante a instalação, seleccione apenas o programa Rescue and Recovery.	Quando anular a instalação da aplicação Client Security Solution 6.0, terá de eliminar os ficheiros e definições do Security Solution 6.0. Se estes não forem eliminados quando a eliminação for solicitada, a instalação do Rescue and Recovery 3.0 terminará.
Client Security Solution 6.0 Standalone	Rescue and Recovery 3.0 e Client Security Solution 6.0	1. Instalar o programa Rescue and Recovery 3.0. 2. Seleccione todos os sub-componentes da aplicação Client Security Solution 6.0 que pretenda instalar.	• Os ficheiros de dados e as definições do Client Security Solution 6.0 são mantidos. • Para proteger as cópias de segurança através da aplicação Client Security Solution 6.0, utilize o programa Rescue and Recovery.

Tabela 1-1. A tabela seguinte fornece informações para ajudar a alterar a configuração do Rescue and Recovery e do Client Security. A definição Client Security Solution autónomo (Standalone) significa que o pacote de instalação foi adquirido pela Web ou a partir de um CD. (continuação)

O software instalado é...	E pretende instalar o...	Siga este processo	Comentários
Rescue and Recovery 3.0 e Client Security Solution 6.0	Client Security Software 5.4x	1. Anular a instalação da aplicação Rescue and Recovery - Client Security Solution. 2. Instalar a aplicação Client Security Software 5.4x.	• A aplicação Client Security Software 5.4x não pode ser instalada sobre a aplicação Client Security Solution 6.0. • Eliminar os ficheiros de dados e as definições quando a eliminação for solicitada não afecta as operações do Client Security Software 5.4x. • Ao anular a instalação do programa Rescue and Recovery 3.0, anulará automaticamente a aplicação Client Security Solution 6.0.
Rescue and Recovery 3.0 e Client Security Solution 6.0	Rescue and Recovery 3.0	1. Seleccione **Modificar** a partir de Adicionar/Remover programas. 2. Elimine a aplicação Client Security Solution 6.0.	• As cópias de segurança locais são eliminadas quando a aplicação Client Security Solution 6.0 é eliminada. • Ao anular a instalação da aplicação Client Security Solution 6.0, deixará de poder utilizar o Password Manager ou o PrivateDisk. • As cópias de segurança do Rescue and Recovery 3.0 protegidas através da aplicação Client Security Solution 6.0 deixaram de estar acessíveis. Crie uma nova cópia de segurança logo que possível.
Rescue and Recovery 3.0 e Client Security Solution 6.0	Client Security Solution 6.0	1. Anular a instalação do programa Rescue and Recovery 3.0. 2. Quando solicitado, opte por manter as definições actuais do Client Security Solution 6.0 apenas se pretender manter a configuração de segurança actual. 3. Instalar a aplicação Client Security Solution 6.0 (Standalone).	1. As cópias de segurança do Rescue and Recovery 3.0 protegidas através do Client Security Solution 6.0 deixaram de estar acessíveis. 2. As cópias de segurança locais são eliminadas ao anular a instalação da aplicação Rescue and Recovery 3.0.

Palavras-passe e frases-passe do Rescue and Recovery

Poderá utilizar palavras-passe ou frases-passe para proteger a área de trabalho do Rescue and Recovery, evitando desta forma que dados importantes sejam acedidos sem autorização. Poderá especificar a protecção da área de trabalho do Rescue and Recovery, utilizando o assistente de configuração de Segurança de cliente para definir preferências de segurança ou alterando as definições de início de sessão através da aplicação Client Security Solution. A aplicação Client Security Solution também permite estabelecer opções de recuperação de palavras-passe dentro da área de trabalho do Rescue and Recovery.

Notas:

1. Esta função só está disponível se o programa Client Security Solution 6.0 estiver instalado. Para utilizar esta função, terá de concluir o assistente de configuração do Client Security 6.0 e especificar se pretende utilizar uma palavra-passe ou uma frase-passe para iniciar sessão no computador.
2. O assistente de configuração do Client Security 6.0 e a aplicação Client Security Solution 6.0 estão apenas acessíveis no ambiente Windows. Se utilizar o Rescue and Recovery sem o Client Security Solution, a área de trabalho do Rescue and Recovery não estará protegida por uma palavra-passe ou frase-passe.
3. A aplicação Client Security Solution permite estabelecer opções de recuperação de palavras-passe dentro da área de trabalho do Rescue and Recovery.

Utilize os métodos seguintes para proteger a área de trabalho do Rescue and Recovery utilizando uma palavra-passe ou frase-passe.

Método 1: Se não tiver concluído o assistente de configuração do Client Security, execute os passos seguintes para proteger a área de trabalho do Rescue and Recovery com uma palavra-passe ou uma frase-passe:

1. A partir do ambiente de trabalho do Windows, faça clique em **Iniciar**, faça clique em **Todos os programas**, seleccione **ThinkVantage** e depois faça duplo clique em **Client Security Solution**.
2. Quando a janela Client Security Solution abrir, faça clique no item do menu **Avançadas**.
3. Faça clique no ícone **Definir preferências de segurança e cópia de segurança**. Será aberto o assistente de configuração do Client Security.
4. Defina as preferências de segurança. Quando solicitado, seleccione uma das seguintes opções:
   - Se pretende proteger a área de trabalho do Rescue and Recovery utilizando uma palavra-passe de início de sessão do Windows, active o selector de confirmação **Utilizar a palavra-passe do Windows para obter acesso à área de trabalho do Rescue and Recovery**.
   - Se pretende proteger a área de trabalho do Rescue and Recovery utilizando uma frase-passe de início de sessão do Client Security Solution, marque o selector de confirmação **Utilizar a frase-passe do Client Security Solution para obter acesso à área de trabalho do Rescue and Recovery**.
5. Conclua o assistente de configuração do Client Security Solution e, em seguida, faça clique em **Terminar**. Para obter mais informações, faça clique em **Ajuda** dentro do assistente de configuração do Client Security.

Método 2: Se tiver concluído o assistente de configuração do Client Security, execute os passos seguintes para proteger a área de trabalho do Rescue and Recovery com uma palavra-passe ou uma frase-passe:

1. No ambiente de trabalho do Windows, faça clique em **Iniciar**, faça clique em **Todos os programas**, seleccione **ThinkVantage** e depois faça duplo clique em **Client Security Solution**.
2. Quando a janela Client Security Solution abrir, faça clique no item do menu **Avançadas**.
3. Faça clique em **Alterar definições de início de sessão**.
4. Siga as instruções apresentadas no ecrã. Para obter informações detalhadas, faça clique em **Ajuda** dentro da aplicação Client Security Solution.

Definir preferências de cópias de segurança utilizando o assistente de configuração do Client Security

O assistente de configuração do Client Security Solution fornece opções de configuração que permitem definir uma variedade de funções de segurança, tais como activar o microcircuito de segurança incorporado, seleccionar como prefere autenticar no ambiente Windows, utilizar o Rescue and Recovery para fazer uma cópia de segurança de dados importantes ou utilizar a autenticação por leitura de impressões digitais.

Conclua o seguinte procedimento para utilizar o assistente de configuração do Client Security:

1. A partir do ambiente de trabalho do Windows, faça clique em **Start**, faça clique em **Todos os programas**, seleccione **ThinkVantage** e depois faça duplo clique em **Client Security Solution**.
2. Quando a janela Client Security Solution abrir, faça clique no item do menu **Avançadas**.
3. Quando a janela Client Security Solution abrir, faça clique em **Definir preferências de segurança e cópia de segurança**. Será aberto o assistente de configuração do Client Security.
4. Defina as preferências de segurança.
5. Conclua o assistente de configuração do Client Security Solution e, em seguida, faça clique em **Terminar**. Para obter informações detalhadas, faça clique em **Ajudar** dentro do assistente de configuração do Client Security.

Informações adicionais sobre o Client Security Solution

Para obter informações detalhadas sobre a aplicação Client Security Solution e as respectivas funções, consulte o *Manual de utilizador do Client Security Solution* na Web em:

```
http://www.ibm.com/pc/support/site.wss/
```

Se já tiver a aplicação Client Security Solution instalada, poderá aceder a informações mais detalhadas a partir do Manual do Utilizador se executar o seguinte procedimento:

1. A partir do ambiente de trabalho do Windows, faça clique em **Iniciar**.
2. Seleccione **Todos os programas**.
3. Seleccione **ThinkVantage**.
4. Faça clique em **Client Security Solution**.
5. A partir da barra de acções do Client Security Solution, faça clique em **Ajuda**.
6. Faça clique em **Manual do utilizador**.

第 13 章 Japanese

Client Security Solution アプリケーションは、ご使用のコンピューター・オペレーティング・システムおよび重要データに対するアクセスの保護に役立つよう設計された、ThinkVantage™ テクノロジー・ツールです。 Client Security Solution は、エンベデッド・セキュリティー・チップによるハードウェア保護と、機密保護機能のあるソフトウェアによって提供される保護を統合します。Client Security Solution は、専用のハードウェアをソフトウェア保護と結合させることにより、コンピューターのオペレーティング・システムに組み込まれているセキュリティー機能を大幅に強化します。

本書の対象読者

「*ThinkVantage Client Security Solution ユーザーズ・ガイド*」は、個人のエンド・ユーザー、およびビジネス環境で作業を行うエンド・ユーザーを対象としています。本書では、以下の領域に関する情報を記載します。

- Client Security Solution のコンポーネント
- Client Security Solution のインストールの注意点
- Client Security Solution の機能

本書は、Client Security Solution のヘルプ・システムを補足するものです。ヘルプ・システムは、Client Security Solution の中の特定のタスクを実行する方法について、ステップバイステップで説明します。

追加情報

大規模組織全体で Client Security Solution を実施しようとしているシステム管理者、システム・エンジニア、ネットワーク管理者、または技術員は、下記の Web サイトにある「*ThinkVantage Rescue and Recovery™ − Client Security Solution デプロイメント・ガイド*」を読むことにより、詳細な情報を得ることができます。

`http://www-6.ibm.com/jp/pc/migration/rr/`

Client Security Solution のコンポーネント

Client Security Solution は、エンベデッド・セキュリティー・チップが装備されているコンピューターを対象に設計されています。エンベデッド・セキュリティー・チップは、ご使用のコンピューター、データ、およびプロセスに対し、追加のセキュリティー・レベルを提供するのに役立ちます。更に、Client Security Solution ソフトウェアは、セキュリティー・チップを装備していないコンピューターのセキュリティーを強化するために構成することが可能です。

Client Security Solution は、以下のハードウェア・コンポーネントとソフトウェア・コンポーネントに分かれます。

- **エンベデッド・セキュリティー・チップ**

  Client Security Solution は、エンベデッド・セキュリティー・チップが装備されているコンピューターを対象に設計されています。エンベデッド・セキュリティ

ー・チップは、ご使用のコンピューターに特別なセキュリティー・レベルを提供する組み込み暗号ハードウェア・テクノロジーです。セキュリティー・チップにより、暗号化および認証プロセスを、ぜい弱なソフトウェアから、専用ハードウェアによる機密保護機能のある環境に移し変えることができます。これによりセキュリティーが強化されます。

- **Client Security セットアップ・ウィザード**

  Client Security セットアップ・ウィザードは、セキュリティー・オプションを構成するプロセス全体にわたるガイドとして役立ちます。このウィザードにより、エンベデッド・セキュリティー・チップを使用可能にして、認証およびログインの方法を選択し、パスワードのリカバリーを行うための質問を作成し、指紋認証を設定し (オプション)、追加の Client Security Solution コンポーネントを構成することができます。

- **Password Manager**

  Client Security Password Manager では、重要で忘れやすい、アプリケーションおよび Web サイトへログインする情報であるユーザー ID、パスワード、その他の個人情報などを、確実かつ簡単に管理できます。 Client Security Password Manager は、すべての情報をエンベデッド・セキュリティー・チップによって保管します。これにより、ユーザーのアプリケーションおよび Web サイトへのアクセスを安全におこなうことが可能です

- **PrivateDisk**

  PrivateDisk は、暗号化された仮想ディスク・ドライブをセットアップします。この仮想暗号化ディスクは、「電子的に安全」であるこの保護領域の中に保管するすべてのデータを、自動的に暗号化します。ユーザーのすべての重要データを暗号化し保管するには、ユーザー自身の仮想暗号化ディスクを使用します。データは、 PrivateDisk の仮想暗号化ディスクに保管される時に自動的に暗号化されます。

- **Client Security Solution アプリケーション**

  Client Security Solution アプリケーションは、エンベデッド・セキュリティー・チップを使用可能にしたり、パスフレーズを変更したり、指紋ソフトウェアを使用するなどの、基本的なセキュリティー機能および拡張セキュリティー機能をユーザーが実行できる、単一のインターフェースを提供します。Client Security Solution の機能の完全なリストについては、 13-4 ページの『Client Security Solution の機能』を参照してください。

- **ThinkVantage 指紋ソフトウェア**

  ThinkVantage 指紋ソフトウェアにより、指紋認証を設定することができます。この便利なセキュリティー機能は、ThinkPad モデルとオプション、および ThinkCentre モデルとオプションの選択時に、使用することができます。

Client Security Solution をインストールする前に

Client Security Solution アプリケーションをインストールする前に、以下の前提条件を満たすことが重要です。

- Windows XP または Windows 2000 (Service Pack 3 またはそれ以降)。137 GB より大きな容量のハード・ディスクに Client Security Solution アプリケーションをインストールする場合、Windows XP では Service Pack 1 またはそれ以降が必要です。
- Internet Explorer 5.5 (またはそれ以降)。
- メモリー 128 MB で、このうち BIOS 内のビデオ・セットアップで共用メモリーとして指定できるのは 8 MB 以内。
- 800 MB 以上の空きディスク・スペース。

Client Security Solution、Client Security Software、または Rescue and Recovery のいずれかの旧バージョンがある場合には、 13-6 ページの『Client Security Solution を Rescue and Recovery とともに使用する』で個別の説明を参照してください。

Client Security Solution のセットアップ

Client Security Solution アプリケーションは、 `http://www-6.ibm.com/jp/pc/think/thinkvantagetech.shtml` で使用可能です。 Client Security Solution のダウンロード、インストール、および構成は、数分かかります。

Client Security Solution のダウンロードとインストール

以下のインストール・プロセスを完了することにより、Client Security Solution プログラムをダウンロードしてインストールします。

1. ご使用のコンピューターを始動し、開いているプログラムがあれば閉じます。
2. `http://www-6.ibm.com/jp/pc/think/thinkvantagetech.shtml` に進みます。
3. ThinkVantage の Security アイコンをクリックし、「リンク」セクションの「**ダウンロード**」リンクをクリックします。
4. 「ダウンロード」セクションまでスクロールダウンして、「**ダウンロード**」をクリックします。
5. 画面の指示に従ってください。
6. インストール実行可能ファイルを実行して、画面の指示に従ってください。
   Client Security Solution の Password Manager コンポーネントおよび PrivateDisk コンポーネントをインストールするオプションが表示されます。
7. 選択を行った後、コンピューターを再始動するためのプロンプトが出されます。
8. コンピューターが再始動すると、Client Security セットアップ・ウィザードが開きます。セットアップ・ウィザードが開かない場合は、『Client Security セットアップ・ウィザードを開く』 を参照してください。
9. Client Security セットアップ・ウィザードを完了して、構成プロセスを終了します。

Client Security セットアップ・ウィザードを開く

Client Security セットアップ・ウィザードを使用して Client Security Solution プログラムを構成するには、以下の手順を完了します。

1. Windows デスクトップから「**スタート**」をクリックし、「**すべてのプログラム**」をクリックし、「**ThinkVantage**」を選択して「**Client Security Tools**」をダブルクリックします。
2. 「Client Security Solution」ウィンドウが開いたら、「**拡張**」メニュー項目をクリックします。
3. 「Client Security Solution」ウィンドウが開いたら、「**セキュリティーおよびバックアップの項目の設定**」をクリックします。 Client Security セットアップ・ウィザードが開きます。
4. Client Security セットアップ・ウィザードのステップを完了してから、「**終了**」をクリックします。詳細については、Client Security セットアップ・ウィザードで「**ヘルプ**」をクリックしてください。

Client Security Solution の使用法

Client Security Solution アプリケーションにアクセスするには、以下の手順を完了します。

1. Windows デスクトップから「**スタート**」をクリックします。
2. 「**すべてのプログラム**」を選択します。
3. 「**ThinkVantage**」を選択します。
4. 「**Client Security Tools**」を選択します。

Client Security Solution の機能

以下に、Client Security Solution アプリケーションを使用して行うことができるさまざまなタスクについて、詳細に説明します。

注: 下記で言及するツールの一部が使用できない場合、その原因として、正規のソフトウェアがインストールされていない、ご使用のコンピューターでそのアプリケーションがサポートされない、そのアプリケーションが管理者アクセスまたはスーパーバイザー・アクセスを必要とする、などが考えられます。

基本機能

以下に、Client Security Solution アプリケーションを使用して行うことができる基本的なタスクについて、詳細に説明します。

パスフレーズの変更: パスフレーズの変更ツールにより、新しい Client Security パスフレーズを設定することができます。パスフレーズは、Client Security パスフレーズのルールに従う必要があります。

パスワード/パスフレーズ復元の構成: パスワード/パスフレーズ復元の構成ツールにより、忘れてしまった Windows パスワードや Client Security パスフレーズを、ご使用の認証方法に合わせて復元する手段を設定することができます。

ログオン情報の管理: Password Manager アプリケーションにより、Client Security Solution を使用して、ユーザー ID、パスワード、その他の個人情報など、重要で、忘れがちなログイン情報を管理することができます。 Password Manager アプリケーションでは、重要なアプリケーションおよび Web サイトへのアクセスをユーザー認証ポリシーが制御するよう、すべての情報をエンベデッド・セキュリティー・チップを使用して保管します。これにより、(それぞれ個別の規則に従い、別々の有

効期日を持つ) 個々のパスワードを数多く覚えて指定する必要がなくなり、1 つのパスフレーズだけ覚えるか、またはソフトウェアのインストール時に指紋を提供するだけで済みます。

指紋ソフトウェアの使用法: 統合指紋読み取り装置により、指紋を登録し、パワーオン・パスワード、ハード・ディスク・パスワード、および Windows パスワードと関連付けることができます。これにより、パスワードを指紋認証に置き換えることができ、簡単で安全なユーザー・アクセスが可能になります。指紋読み取り装置キーボードは、コンピューターと一緒に選択でき、オプションで購入することができます。このオプションは、ThinkCentre コンピューターおよび ThinkPad コンピューターを選択した場合にのみサポートされます。

データの保護: PrivateDisk ツールは、暗号化された仮想暗号化ディスクを生成します。この仮想暗号化ディスクは、「電子的に安全」であるこの保護領域の中に保管するすべてのデータを、自動的に暗号化します。

拡張機能

以下に、Client Security Solution アプリケーションを使用して行うことができる拡張タスクについて、詳細に説明します。

注: 以下の操作を行うには、管理者権限が必要です。

セキュリティー設定のモニター: Security Advisor ツールにより、ご使用のコンピューターに現在設定されているセキュリティー設定の要約を表示することができます。現行の状況を表示したり、あるいはご使用のシステムのセキュリティーを拡張するために、これらの設定を検討します。ここに含まれるセキュリティー・トピックは、ハードウェア・パスワード、Windows ユーザー・パスワード、Windows パスワード・ポリシー、保護スクリーン・セーバー、およびファイル共有です。

注: Security Advisor ツールは、セキュリティー設定の要約と、ご使用のシステムのセキュリティーを拡張する助けとなる提案のみを提供します。アンチウィルス・プログラムやファイアウォール・プログラムの使用など、セキュリティーのすべての局面を扱うわけではありません。多くの設定は、スーパーバイザー・アクセスまたは管理者アクセスを必要とします。

ディジタル証明書の転送: Client Security 証明書転送ウィザードは、ソフトウェア・ベースの Microsoft 暗号サービス・プロバイダー (CSP) による証明書に関連する秘密鍵を、ハードウェア・ベースの Client Security Solution CSP に転送するプロセスをガイドします。転送した後は、エンベデッド・セキュリティー・チップによって秘密鍵が保護されるため、証明書を使用する操作の安全性がさらに高くなります。

ハードウェア・パスワードのリセットを行う仕組み: このツールは、Windows とは独立して稼働する保護環境を作成し、忘れてしまったパワーオン・パスワードおよびハード・ディスク・パスワードをリセットする援助を行います。ユーザーの識別は、ユーザーが作成する質問のセットに回答することにより、確立されます。パスワードを忘れてしまう前にできるだけ早く、この保護環境を作成することをお勧めします。この保護環境をハード・ディスク上に作成して登録を行うまでは、忘れてしまったハードウェア・パスワードをリセットすることはできません。このツール

は、ハードウェア・パスワードのリセットをサポートしている ThinkCentre コンピューターおよび ThinkPad コンピューターをご使用の場合にのみ使用可能です。

注: このツールを使用する前に、BIOS 管理者パスワードまたはスーパーバイザー・パスワードを設定することをお勧めします。BIOS 管理者パスワードかスーパーバイザー・パスワードが設定されていない環境では、最大限の保護は行われません。この手順を完了すると、パワーオン・パスワードとハード・ディスク・パスワードが一致することになります。この手順により、セキュア環境の作成、およびセキュア環境が作成された後に忘れてしまったパスワードをリセットできるようになります。

エンベデッド・セキュリティー・チップの使用可能化: このツールは、エンベデッド・セキュリティー・チップを使用可能または使用不可能にするために使用される、BIOS の設定変更を行います。この変更内容を有効にするには、コンピューターの再起動が必要です。

ログオン方法の変更: このツールは、現行のログオン方法を表示し、ユーザーの Windows オペレーティング・システムおよび ThinkVantage Rescue and Recovery ワークスペースにログオンする方法を、管理者が変更できるようにします。

ロックアウトの解除: このツールは、正しくない認証の試みがエンベデッド・セキュリティー・チップに渡された認証失敗回数のリセットを行います。認証失敗がある回数続いた後に、エンベデッド・セキュリティー・チップは一定期間、自身をロックします。このロックアウト期間は、失敗した試みが続けば続くほど長くなります。

Client Security セットアップ・ウィザードの起動: Client Security セットアップ・ウィザードにより、さまざまなセキュリティー・ソフトウェア・ツールを構成することができます。このウィザードは、エンベデッド・セキュリティー・チップを使用可能にしたり、Windows 環境への認証を行う方法を選択したり、重要なデータをバックアップするために Rescue and Recovery を使用することを選択したり、あるいは指紋認証を使用することを選択するなどの、さまざまなセキュリティー機能を設定できる構成オプションを提供します。

Client Security Solution を Rescue and Recovery とともに使用する

Rescue and Recovery プログラムと Client Security Solution アプリケーションはともに、ユーザーの使用目的を考慮し開発された ThinkVantage テクノロジーです。つまりこれらは、ユーザーの要求に応じて別々でも一緒でも動作するように、設計されています。以下の情報は、これらのプログラムの使用に関するユーザーのセキュリティー・ポリシーを設計する手助けとなること、そしてこれらのプログラムが互いに強化しあう方法に焦点を当てています。

Rescue and Recovery プログラムまたは Client Security Solution アプリケーションをインストールする時、あるいはその両方を一緒にインストールする時、重要な考慮事項があります。以下の表は、ユーザーが意図する構成に合った正しい手順を判断するのに有益な情報を提供します。

表 13-1. 以下の表では、Rescue and Recovery および Client Security の構成を変更するのに役立つ情報を提供します。Client Security Solution スタンドアロンとは、Web または CD から入手したインストール・パッケージを意味します。

インストール済み ソフトウェア	使用したいソフトウェア	行うプロセス	コメント
Client Security Software 5.4x	Client Security Software 5.4x および Rescue and Recovery 3.0	1. Rescue and Recovery 3.0 プログラムをインストールする。 2. インストールの途中で Client Security Software 5.4x アプリケーションがインストールされていることを示す画面が表示されるので、インストールしたままにしておくために「**続行**」をクリックする。	Client Security Software 5.4x アプリケーションを使用してバックアップを保護することはできません。Rescue and Recovery 3.0 プログラムによる Client Security Software の使用は、Client Security Software のエミュレーション・バージョンを使用して行われることになります。 マスター・パスワード機能が、ご使用のセキュリティー機能に追加されます。マスター・パスワードは、通常、エンタープライズ環境で使用されます。詳しくは、 13-1 ページの『追加情報』を参照してください。
Client Security Software 5.4x	Client Security Solution 6.0 スタンドアロン・インストール・パッケージ	1. Client Security Software 5.4x アプリケーションをアンインストールする。 2. Client Security Solution 6.0 (スタンドアロン) アプリケーションをインストールする。	• アンインストールする前に、暗号化されたファイルがあれば復号化し、Password Manager 情報があればエクスポートしておく必要があります。行わない場合、これらの情報が失われることになります。 • Client Security Solution アプリケーションをインストールする前に、File and Folder Encryption ソフトウェアを アンインストールする必要があります。

表 13-1. 以下の表では、Rescue and Recovery および Client Security の構成を変更するのに役立つ情報を提供します。Client Security Solution スタンドアロンとは、Web または CD から入手したインストール・パッケージを意味します。 (続き)

インストール済みソフトウェア	使用したいソフトウェア	行うプロセス	コメント
Client Security Software 5.4x	Client Security Solution 6.0 および Rescue and Recovery 3.0	1. Client Security Software 5.4x アプリケーションをアンインストールする。 2. Rescue and Recovery 3.0 プログラムをインストールする。(Client Security Solution 6.0 コンポーネントが選択されていることを確認してください。)	• 最初に Client Security Software をアンインストールしないで Rescue and Recovery 3.0 を Client Security Software 5.4x 上にインストールすると、Rescue and Recovery のみになります。 • Client Security Software 5.4x アプリケーションをアンインストールする前に、暗号化されたファイルがあれば復号化し、Password Manager 情報があればエクスポートしておく必要があります。行わない場合、これらの情報が失われることになります。 • Client Security Solution 6.0 アプリケーションをインストールする前に、File and Folder Encryption ソフトウェアをアンインストールする必要があります。
Rescue and Recovery 3.0	Client Security Software 5.4x および Rescue and Recovery 3.0	1. Rescue and Recovery 3.0 プログラムをアンインストールする。 2. Client Security Software 5.4x アプリケーションをインストールする。 3. Rescue and Recovery 3.0 プログラムをインストールする。 4. インストールの途中で Client Security Software 5.4x アプリケーションがインストールされていることを示す画面が表示されるので、インストールしたままにしておくために「**続行**」をクリックする。	• Client Security Software 5.4x アプリケーションは、Rescue and Recovery 3.0 プログラム上にインストールすることはできません。 • ローカル・バックアップは、Rescue and Recovery 3.0 プログラムのアンインストール時に削除されます。

表 13-1. 以下の表では、Rescue and Recovery および Client Security の構成を変更するのに役立つ情報を提供します。Client Security Solution スタンドアロンとは、Web または CD から入手したインストール・パッケージを意味します。 (続き)

インストール済み ソフトウェア	使用したいソフトウェア	行うプロセス	コメント
Rescue and Recovery 3.0	Client Security Solution 6.0 スタンドアロン・インストール・パッケージ	1. Rescue and Recovery 3.0 プログラムをアンインストールする。 2. Client Security Solution 6.0 (スタンドアロン) アプリケーションをインストールする。	• Rescue and Recovery をアンインストールすると、ユーザー・ファイルおよび Client Security Solution レジストリー設定が削除されます。 • Client Security Solution によって保護される Rescue and Recovery バックアップには、もうアクセスできなくなります。 • ローカル・バックアップは、Rescue and Recovery 3.0 のアンインストール時に削除されます。 • Client Security Solution 6.0 (スタンドアロン) は、Rescue and Recovery 3.0 上にインストールすることはできません。
Rescue and Recovery 3.0	Rescue and Recovery 3.0 および Client Security Solution 6.0	1. 「プログラムの追加/削除」から「**変更**」オプションを選択する。 2. Client Security Solution アプリケーションおよび必要なサブコンポーネントを追加することにより、変更操作を完了する。	• ローカル・バックアップは、Client Security Solution アプリケーションの追加時に削除されます。 • Client Security Solution アプリケーションの追加後、できるだけ早く新しい基本バックアップを作成してください。 • Client Security Solution 設定およびデータ・ファイルは削除されます。 • Client Security Solution 6.0 (スタンドアロン) アプリケーションは、Rescue and Recovery 3.0 プログラム上にインストールすることはできません。

表 13-1. 以下の表では、Rescue and Recovery および Client Security の構成を変更するのに役立つ情報を提供します。Client Security Solution スタンドアロンとは、Web または CD から入手したインストール・パッケージを意味します。 (続き)

インストール済み ソフトウェア	使用したいソフトウェア	行うプロセス	コメント
Client Security Solution 6.0 スタンドアロン・インストール・パッケージ	Client Security Software 5.4x	1. Client Security Solution 6.0 (スタンドアロン) アプリケーションをアンインストールする。 2. Client Security Software 5.4x アプリケーションをインストールする。	• プロンプトで Client Security Solution 6.0 データ・ファイルおよび設定を削除しても、Client Security Software 5.4x の操作には影響しません。
Client Security Solution 6.0 スタンドアロン・インストール・パッケージ	Rescue and Recovery 3.0	1. Client Security Solution 6.0 アプリケーションをアンインストールする。 2. Rescue and Recovery 3.0 プログラムをインストールする。	Client Security Solution 6.0 アプリケーションのアンインストール時に、Security Solution 6.0 ファイルおよび設定を削除する必要があります。プロンプトでこれらを削除できなかった場合、Rescue and Recovery 3.0 のインストールは終了します。
Client Security Solution 6.0 スタンドアロン	Rescue and Recovery 3.0 および Client Security Solution 6.0	1. Rescue and Recovery 3.0 プログラムをインストールする。 2. インストールしたい Client Security Solution 6.0 アプリケーションのサブコンポーネントがあれば、選択する。	• Client Security Solution 6.0 データ・ファイルおよび設定は保持されます。 • Client Security Solution 6.0 アプリケーションを使用してバックアップを保護することを選択するには、Rescue and Recovery プログラムを使用します。

表 13-1. 以下の表では、Rescue and Recovery および Client Security の構成を変更するのに役立つ情報を提供します。Client Security Solution スタンドアロンとは、Web または CD から入手したインストール・パッケージを意味します。 (続き)

インストール済み ソフトウェア	使用したいソフトウェア	行うプロセス	コメント
Rescue and Recovery 3.0 および Client Security Solution 6.0	Client Security Software 5.4x	1. Rescue and Recovery - Client Security Solution アプリケーションをアンインストールする。 2. Client Security Software 5.4x アプリケーションをインストールする。	• Client Security Software 5.4x アプリケーションは、Client Security Solution 6.0 アプリケーション上にインストールすることはできません。 • プロンプトでデータ・ファイルおよび設定を削除しても、Client Security Software 5.4x の操作には影響しません。 • Rescue and Recovery 3.0 プログラムをアンインストールすることにより、Client Security Solution 6.0 アプリケーションは自動的にアンインストールされます。
Rescue and Recovery 3.0 および Client Security Solution 6.0	Rescue and Recovery 3.0	1. 「プログラムの追加/削除」から「**変更**」を選択する。 2. Client Security Solution 6.0 アプリケーションを削除する。	• ローカル・バックアップは、Client Security Solution 6.0 アプリケーションの削除時に削除されます。 • Client Security Solution 6.0 アプリケーションをアンインストールすると、Password Manager および PrivateDisk が失われます。 • Client Security Solution 6.0 アプリケーションで保護される Rescue and Recovery 3.0 バックアップには、もうアクセスできません。できるだけ早く、新しいバックアップを作成してください。

表 13-1. 以下の表では、Rescue and Recovery および Client Security の構成を変更するのに役立つ情報を提供します。Client Security Solution スタンドアロンとは、Web または CD から入手したインストール・パッケージを意味します。 (続き)

インストール済みソフトウェア	使用したいソフトウェア	行うプロセス	コメント
Rescue and Recovery 3.0 および Client Security Solution 6.0	Client Security Solution 6.0	1. Rescue and Recovery 3.0 プログラムをアンインストールする。 2. プロンプトが出されたら、現行のセキュリティー構成を保持したい場合にのみ、現行の Client Security Solution 6.0 設定を保持することを選択する。 3. Client Security Solution 6.0 (スタンドアロン) アプリケーションをインストールする。	1. Client Security Solution 6.0 で保護される Rescue and Recovery 3.0 バックアップには、もうアクセスできません。 2. ローカル・バックアップは、Rescue and Recovery 3.0 アプリケーションのアンインストール時に削除されます。

Rescue and Recovery パスワードおよびパスフレーズ

パスワードあるいはパスフレーズを使用して、Rescue and Recovery ワークスペースを保護することができ、これによって重要なデータを許可されていないアクセスから保護します。Client Security セットアップ・ウィザードを使用してセキュリティーを設定するか、あるいは Client Security Solution アプリケーションを使用してログオン方法を変更することにより、Rescue and Recovery ワークスペースを保護するよう指定することができます。Client Security Solution アプリケーションでも、Rescue and Recovery ワークスペースの中のパスワードのリカバリー・オプションを設定することができます。

注:

1. この機能は、Client Security Solution 6.0 プログラムがインストールされている場合にのみ、使用できます。この機能を使用するには、Client Security 6.0 セットアップ・ウィザードを完了し、コンピューターへのログオンにパスワードまたはパスフレーズのいずれかを使用することを指定しておく必要があります。
2. Client Security セットアップ・ウィザードや Client Security Solution 6.0 アプリケーションは、Windows 環境でのみ、アクセスすることができます。Client Security Solution を使用せずに Rescue and Recovery を選択する場合、Rescue and Recovery ワークスペースは、パスワードやパスフレーズでは保護されません。
3. Client Security Solution アプリケーションで、Rescue and Recovery ワークスペースの中のパスワードのリカバリー・オプションを設定できます。

パスワードまたはパスフレーズを使用して Rescue and Recovery ワークスペースを保護するには、以下の方法を使用します。

方法 1: Client Security セットアップ・ウィザードをまだ完了していない場合は、パスワードまたはパスフレーズのいずれかで Rescue and Recovery ワークスペースを保護するために、次の操作を行います。

1. Windows デスクトップから「**スタート**」をクリックし、「**すべてのプログラム**」をクリックし、「**ThinkVantage**」を選択して「**Client Security Tools**」をダブルクリックします。
2. 「Client Security Solution」ウィンドウが開いたら、「**拡張**」メニュー項目をクリックします。
3. 「**セキュリティーおよびバックアップの項目の設定**」アイコンをクリックします。 Client Security セットアップ・ウィザードが開きます。
4. セキュリティー設定を行います。プロンプトが出されたら、次のいずれかを選択します。
   - Windows ログオン・パスワードを使用して Rescue and Recovery ワークスペースを保護したい場合は、「**Windows パスワードを使用して、Rescue and Recovery ワークスペースへのアクセスを保護する**」チェック・ボックスにマークを付けます。
   - Client Security Solution ログオン・パスフレーズを使用して Rescue and Recovery ワークスペースを保護したい場合は、「**Client Security パスフレーズを使用して、Rescue and Recovery ワークスペースへのアクセスを保護する**」チェック・ボックスにマークを付けます。
5. Client Security Solution セットアップ・ウィザードを完了してから、「**終了**」をクリックします。詳細については、Client Security セットアップ・ウィザードで「**ヘルプ**」をクリックしてください。

方法 2 Client Security セットアップ・ウィザードが完了している場合は、パスワードまたはパスフレーズで Rescue and Recovery ワークスペースを保護するために、次の操作を行います。

1. Windows デスクトップから「**スタート**」をクリックし、「**すべてのプログラム**」をクリックし、「**ThinkVantage**」を選択して「**Client Security Tools**」をダブルクリックします。
2. 「Client Security Solution」ウィンドウが開いたら、「**拡張**」メニュー項目をクリックします。
3. 「**ログオン方法の変更**」をクリックします。
4. 画面の指示に従ってください。詳細については、Client Security Solution アプリケーション内の「**ヘルプ** 」をクリックしてください。

Client Security セットアップ・ウィザードを使用してバックアップ設定を行う

Client Security Solution セットアップ・ウィザードは、エンベデッド・セキュリティー・チップを使用可能にしたり、Windows 環境への認証を行う方法を選択、Rescue and Recovery を使用して重要データをバックアップすることの選択、指紋認証を使用することの選択などの、さまざまなセキュリティー機能を使用可能にする構成オプションを提供します。

Client Security Setup ウィザードを使用するには、以下の手順を完了します。

1. Windows デスクトップから「**スタート**」をクリックし、「**すべてのプログラム**」をクリックし、「**ThinkVantage**」を選択して「**Client Security Tools**」をダブルクリックします。
2. 「Client Security Solution」ウィンドウが開いたら、「**拡張**」メニュー項目をクリックします。
3. 「Client Security Solution」ウィンドウが開いたら、「**セキュリティーおよびバックアップの項目の設定**」をクリックします。 Client Security セットアップ・ウィザードが開きます。
4. セキュリティー設定を行います。
5. Client Security セットアップ・ウィザードを完了してから、「**終了**」をクリックします。詳細については、Client Security セットアップ・ウィザードで「**ヘルプ**」をクリックしてください。

Client Security Solution の詳細情報

Client Security Solution アプリケーションおよびその機能に関する詳細な情報は、以下の Web で「*Client Security Solution ユーザーズ・ガイド*」を参照してください。

`http://www-6.ibm.com/jp/pc/security/css/security.shtml`

すでに Client Security Solution アプリケーションがインストール済みであれば、以下の手順を完了することにより、「ユーザーズ・ガイド」でさらに詳しい情報を読むことができます。

1. Windows デスクトップから「**スタート**」をクリックします。
2. 「**すべてのプログラム**」を選択します。
3. 「**ThinkVantage**」を選択します。
4. 「**Client Security Tools**」を選択します。
5. Client Security Solution メニュー・バーから、「**ヘルプ**」をクリックします。
6. 「**ユーザーズ・ガイド**」をクリックします。

제 14 장 Korean

Client Security Solution 응용프로그램은 컴퓨터 운영 체제 및 중요 데이터에 대한 액세스를 보호하기 위해 설계된 ThinkVantage™ Technology의 도구 세트입니다. Client Security Solution은 해당 임베디드 칩의 하드웨어 보호와 해당 보안 소프트웨어에 의해 제공되는 보호를 통합합니다. 하드웨어와 소프트웨어를 보호하는 Client Security Solution은 컴퓨터의 운영 체제에 포함된 보안 기능을 강력하게 향상시켜 줍니다.

이 책의 독자

*ThinkVantage Client Security Solution User's Guide*는 개인 일반 사용자와 비즈니스 환경에서 일하는 일반 사용자를 위한 것입니다. 이 책에서는 다음과 같은 정보를 제공합니다.

- Client Security Solution 구성 요소
- Client Security Solution 설치 고려 사항
- Client Security Solution 기능

이 책은 프로그램 내에서 특정 작업의 수행 방법에 대한 단계별 지시사항을 제공하는 Client Security Solution 도움말 시스템을 보충합니다.

추가 정보

대기업에서 Client Security Solution을 구현하려는 시스템 관리자, 시스템 엔지니어, 네트워크 관리자 또는 고객 엔지니어인 경우 다음 웹 사이트에 있는 *ThinkVantage Rescue and Recovery™ and Client Security Solution Deployment Guide*를 참고하여 세부 정보를 얻을 수 있습니다.

http://www.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-54502

Client Security Solution 구성 요소

Client Security Solution은 컴퓨터 데이터 및 프로세스에 추가 보안 레벨을 제공해주는 임베디드 Security Chip이 내장된 컴퓨터를 위해 설계되었습니다. 그러나 이제 Client Security Solution 소프트웨어는 Security Chip이 갖춰져 있지 않은 컴퓨터의 보안을 향상시키기 위해서도 구성할 수 있습니다.

Client Security Solution은 다음과 같은 하드웨어 및 소프트웨어 구성 요소로 나뉩니다.

- **임베디드 Security Chip**

Client Security Solution은 임베디드 Security Chip이 내장된 컴퓨터를 위해 설계되었습니다. 임베디드 Security Chip은 컴퓨터에 추가 보안 레벨을 제공하는 내장 암호식 하드웨어 기술입니다. Security Chip은 취약한 소프트웨어 보안 환경에서 하드웨어의 보안 환경으로 암호화 및 인증 프로세스의 전송을 가능하게 합니다. 이로 인해 보안이 확실하게 향상됩니다.

- **Client Security Setup Wizard**

  Client Security Setup Wizard는 보안 옵션 구성 프로세스를 안내해줍니다. 이 마법사는 임베디드 Security Chip의 사용, 인증 및 로그인 방법의 선택, 암호 복구 질문의 작성, 지문 인증 설정(선택적) 및 Client Security Solution 추가 구성 요소의 구성을 도와줍니다.

- **Password Manager**

  Client Security Password Manager는 사용자 ID, 암호 및 기타 개인 정보와 같은 중요하고 잊기 쉬운 응용프로그램 및 웹 사이트 로그인 정보를 안전하고 편리하게 관리할 수 있게 해줍니다. Client Security Password Manager는 모든 정보를 임베디드 Security Chip를 통해 저장함으로써 응용프로그램 및 웹 사이트에 대한 액세스 보안을 철저하게 유지합니다.

- **PrivateDisk**

  PrivateDisk는 이 "전자 금고"의 안전한 영역에 저장하는 모든 데이터를 자동으로 암호화하는 암호화 가상 디스크 드라이브를 설정합니다. 자체 가상 드라이브를 사용하여 중요한 모든 데이터를 암호화하고 저장합니다. 데이터는 PrivateDisk 볼륨에 저장될 때 자동으로 암호화됩니다.

- **Client Security Solution 응용프로그램**

  Client Security Solution 응용프로그램은 임베디드 Security Chip 사용, 암호구 변경 또는 지문 인식 소프트웨어 사용과 같은 기본 및 고급 보안 기능을 사용자가 수행할 수 있는 단일 인터페이스를 제공합니다. Client Security Solution 기능의 전체 목록은 14-4 페이지의 『Client Security Solution 기능』을 참고하십시오.

- **ThinkVantage 지문 인식 소프트웨어**

  ThinkVantage 지문 인식 소프트웨어는 사용자가 지문 인증을 설정할 수 있게 해줍니다. 이 편리한 보안 기능은 일부 ThinkPad 및 ThinkCentre 모델에서 사용 가능합니다.

Client Security Solution을 설치하기 전에

Client Security Solution 응용프로그램을 설치하기 전에 다음 전제조건을 충족시켜야 합니다.

- Windows XP 또는 Windows 2000(Service Pack 3 포함). 137GB를 초과하는 용량을 가진 하드 디스크에서 이 프로그램을 설치하는 경우 Service Pack 1이 Windows XP에 필요합니다.
- Internet Explorer 5.5 이상
- 128MB 메모리(이 중 최소한 8MB는 BIOS의 비디오 설정에서 공유 메모리로 지정됨)
- 800MB의 디스크 여유 공간

이전 버전의 Client Security Solution, Client Security Software 또는 Rescue and Recovery가 있는 경우 해당 지시사항에 대해서는 14-6 페이지의 『Rescue and Recovery와 함께 Client Security Solution 사용』을 참고하십시오.

Client Security Solution 설정

Client Security Solution 응용프로그램은 `http://www.pc.ibm.com/thinkvantage` 웹 사이트에서 얻을 수 있습니다. Client Security Solution의 다운로드, 설치 및 구성은 수 분 내에 수행할 수 있습니다.

Client Security Solution 다운로드 및 설치

다음 설치 프로세스를 완료하여 Client Security Solution 프로그램을 다운로드하고 설치하십시오.

1. 컴퓨터를 시작하고 열려 있는 프로그램을 닫으십시오.
2. `http://www.pc.ibm.com/thinkvantage` 웹 사이트로 이동하십시오.
3. Resources 섹션에서 **Support and downloads** 링크를 클릭하십시오.
4. Embedded Security Subsystem and Client Security Solution 섹션의 **Software download**를 클릭하십시오.
5. 화면의 지시사항을 따르십시오.
6. 설치 실행 파일을 실행하고 화면의 지시사항을 따르십시오. Client Security Solution의 Password Manager 및 PrivateDisk 구성 요소를 설치하는 옵션이 제공됩니다.
7. 사용자가 선택하면 컴퓨터 재시작을 알리는 메시지가 프롬프트됩니다.
8. 컴퓨터가 다시 시작되면 Client Security Setup Wizard가 열립니다. 이 마법사가 열리지 않으면 『Client Security Setup Wizard 열기』를 참고하십시오.
9. Client Security Setup Wizard를 완료하여 구성 프로세스를 완료하십시오.

Client Security Setup Wizard 열기

다음 절차를 완료하여 Client Security Setup Wizard를 사용하여 Client Security Solution 프로그램을 구성하십시오.

1. Windows 바탕 화면에서 **시작**을 클릭하고 **모든 프로그램**을 클릭하고 **ThinkVantage**를 선택한 후 **Client Security Solution**을 더블 클릭하십시오.
2. Client Security Solution 창이 열리면 **고급** 메뉴 항목을 클릭하십시오.
3. Client Security Solution 창이 열리면 **보안 및 백업 환경 설정**을 클릭하십시오. Client Security Setup Wizard가 열립니다.
4. Client Security Solution Setup Wizard 단계를 완료한 후 **완료**를 클릭하십시오. 자세한 정보는 Client Security Setup Wizard 내의 **도움말**을 클릭하십시오.

Client Security Solution 사용

다음 절차를 완료하여 Client Security Solution 응용프로그램에 액세스하십시오.

1. Windows 바탕 화면에서 **시작**을 클릭하십시오.
2. **모든 프로그램**을 선택하십시오.
3. **ThinkVantage**를 선택하십시오.
4. **Client Security Solution**을 클릭하십시오.

Client Security Solution 기능

다음 정보는 Client Security Solution 응용프로그램을 사용하여 수행할 수 있는 여러 가지 작업에 대해 설명합니다.

주: 아래에 언급된 일부 도구를 사용할 수 없는 경우 적절한 소프트웨어가 설치되어 있지 않거나 컴퓨터가 응용프로그램을 지원하지 않거나 응용프로그램에 관리자 액세스 권한이 필요한 것일 수 있습니다.

기본 기능

다음 정보는 Client Security Solution 응용프로그램을 사용하여 수행할 수 있는 기본 작업에 대해 설명합니다.

암호구 변경: 암호구 변경 도구로 새 Client Security 암호구를 설정할 수 있습니다. 암호구는 Client Security 암호구 요구사항을 반드시 따라야 합니다.

암호 복구 구성: 암호 복구 구성 도구는 사용하는 인증 방식에 따라 잊어버린 Windows 암호 또는 Client Security 암호구를 복구하는 방법을 설정할 수 있게 합니다.

로그온 정보 관리: Password Manager 응용프로그램은 Client Security Solution을 사용하여 사용자 ID, 암호 및 기타 개인 정보와 같은 중요하고 잊기 쉬운 로그인 정보를 관리할 수 있게 합니다. Password Manager 응용프로그램은 모든 정보를 임베디드 Security Chip를 통해 저장함으로써 사용자 인증 정책이 보안 응용프로그램 및 웹 사이트에 대한 액세스를 제어할 수 있게 해줍니다. 이는 다수의 각 암호(규칙 및 만기일

이 다른)를 기억하고 제공할 필요없이 오직 한 암호구만 기억하거나 지문 인식 소프트웨어가 설치된 경우 지문을 제공한다는 것을 의미합니다.

지문 인식 소프트웨어 사용: 통합 지문 인식 장치는 지문을 시동 암호, 하드 디스크 암호 및 Windows 암호에 등록하고 연관시킴으로써 지문 인증이 암호를 대체하여 간단하고 안전한 사용자 액세스를 가능하게 해줍니다. 지문 인식 장치 키보드는 일부 컴퓨터 모델에만 제공되며 옵션으로 구매할 수 있습니다. 이 옵션은 일부 ThinkCentre 및 ThinkPad 컴퓨터 모델만 지원합니다.

데이터 보호: PrivateDisk 도구는 이 ″전자 금고″의 안전한 영역에 저장되는 모든 데이터를 자동으로 암호화하는 암호화 가상 디스크 드라이브를 생성합니다.

고급 기능

다음 정보는 Client Security Solution 응용프로그램을 사용하여 수행할 수 있는 고급 작업에 대해 설명합니다.

주: 다음 작업을 수행하려면 관리자 권한이 반드시 있어야 합니다.

보안 설정 모니터링: Security Advisor 도구는 현재 컴퓨터에 설정된 보안 설정의 요약 정보를 볼 수 있게 합니다. 이러한 설정을 검토하여 현재 보안 상태를 점검하거나 시스템 보안을 향상시킬 수 있습니다. 포함되는 몇 가지 보안 항목으로는 하드웨어 암호, Windows 사용자 암호, Windows 암호 정책, 보안 화면 보호기 및 파일 공유 등이 있습니다.

주: Security Advisor 도구는 보안 설정 및 제안사항의 요약 정보만 제공하여 시스템 보안 향상에 도움을 줍니다. 안티바이러스 및 방화벽 프로그램의 사용 및 유지보수와 같은 모든 보안 측면을 다루지는 않습니다. 이러한 대부분의 설정에는 관리자 액세스 권한이 요구됩니다.

디지털 인증서 전송: Client Security Certificate Transfer Wizard는 인증서와 연관된 개인용 키를 소프트웨어 기반 Microsoft CSP(Cryptographic Service Provider)에서 하드웨어 기반 Client Security Solution CSP로 전송하는 프로세스를 안내해줍니다. 전송 후에 인증서를 사용하는 작업은 개인용 키가 임베디드 Security Chip에 의해 보호되므로 보다 안전해집니다.

하드웨어 암호 재설정 메커니즘 설정: 이 도구는 Windows와 독립적으로 실행되며 잊어버린 시동 및 하드 디스크 드라이브 암호의 재설정을 도와주는 보안 환경을 만듭니다. 직접 작성한 질문 세트에 응답함으로써 사용자의 신분이 인증됩니다. 이 보안 환경은 암호를 잊어버리기 전에 가능한 빨리 작성하는 것이 좋습니다. 이 보안 환경은 하드 드라이브에 만들고 등록한 후에야 잊어버린 하드웨어 암호를 재설정할 수 있습니다. 이 도구는 일부 ThinkCentre 및 ThinkPad 컴퓨터 모델에서만 사용 가능합니다.

주: 이 도구를 사용하기 전에 관리자 암호를 설정하는 것이 좋습니다. 관리자 암호를 설정하지 않으면 환경을 최대한 안전하게 할 수 없습니다. 이 절차를 완료하면 시동 암호와 하드 디스크 드라이브 암호가 일치하게 됩니다. 이 절차는 보안 환경 생성 작업을 완료하고 보안 환경 생성 후 잊어버린 암호의 재설정을 도와주기 위해 설계되었습니다.

임베디드 Security Chip 활성화: 이 도구는 임베디드 Security Chip를 활성화하거나 비활성화하는 데 사용되는 BIOS 설정 변경을 시작합니다. 이 변경사항을 적용하려면 컴퓨터를 다시 시작해야 합니다.

로그온 설정 변경: 이 도구는 현재 로그온 설정을 표시하고 관리자가 사용자들의 Windows 운영 체제 및 ThinkVantage Rescue and Recovery 작업 공간 로그온 방식을 변경할 수 있게 합니다.

인증 실패 카운터 지우기: 이 도구는 임베디드 Security Chip에 전달된 올바르지 않은 인증 시도 횟수를 모니터하는 인증 실패 카운터를 재설정합니다. 일정한 실패 시도 횟수에 도달하면 칩이 한동안 자체적으로 잠깁니다. 잠금 기간은 실패 시도 횟수가 누적될수록 증가합니다.

보안 및 백업 환경 설정: Client Security Setup Wizard는 여러 가지 보안 소프트웨어 도구를 구성할 수 있게 합니다. 이 마법사는 Client Security 임베디드 Security Chip 사용, 원하는 Windows 환경 인증 방식 선택, 중요 데이터 백업을 위한 Rescue and Recovery 사용의 선택 또는 지문 인증 사용 선택과 같은 다양한 보안 기능을 설정할 수 있는 구성 옵션을 제공합니다.

Rescue and Recovery와 함께 Client Security Solution 사용

Rescue and Recovery 프로그램 및 Client Security Solution 응용프로그램은 모두 사용자를 염두에 두고 개발된 ThinkVantage Technologies입니다. 즉 사용자 요구사항에 따라 함께 또는 따로 작동하도록 설계되었습니다. 다음 정보는 이러한 프로그램들의 사용 전략을 세울 수 있게 도와주고 이러한 프로그램의 상호 증진 방법에 대해 설명합니다.

Rescue and Recovery 프로그램, Client Security Solution 응용프로그램 또는 둘다를 설치할 때 고려할 중요한 사항이 있습니다. 다음 표는 원하는 구성을 위해 올바른 절차를 결정하도록 도와주는 정보를 제공합니다.

표 14-1. 다음 표는 Rescue and Recovery 및 Client Security 구성 변경을 도와주는 정보를 제공합니다. Client Security Solution 독립형은 설치 패키지를 웹이나 CD에서 가져왔음을 의미합니다.

설치된 소프트웨어	원하는 사항	따라야 할 프로세스	설명
Client Security Software 5.4x	Client Security Software 5.4x 및 Rescue and Recovery 3.0	1. Rescue and Recovery 3.0 프로그램을 설치하십시오. 2. 프롬프트되면 Client Security Software 5.4x 응용프로그램 설치를 유지하도록 지정하십시오.	Client Security Software 5.4x 응용프로그램을 사용한 백업은 보호될 수 없으며 Rescue and Recovery 3.0 프로그램은 에뮬레이트 버전의 Client Security Software를 사용하여 Client Security Software 기능을 사용하게 됩니다. 마스터 암호 기능이 보안 기능에 추가됩니다. 마스터 암호는 보통 기업 환경에서 사용됩니다. 자세한 정보는 14-1 페이지의 『추가 정보』를 참고하십시오.
Client Security Software 5.4x	Client Security Solution 6.0 독립형 설치 패키지	1. Client Security Software 5.4x 응용프로그램을 제거하십시오. 2. Client Security Solution 6.0(독립형) 응용프로그램을 설치하십시오.	• 제거하기 전에 암호화 파일을 해독하고 Password Manager 정보를 내보내야 합니다. 그렇지 않으면 해당 정보를 잃게 됩니다. • Client Security Solution 응용프로그램을 설치하기 전에 IBM® File and Folder Encryption 소프트웨어를 제거해야 합니다.
Client Security Software 5.4x	Client Security Solution 6.0 및 Rescue and Recovery 3.0	1. Client Security Software 5.4x 응용프로그램을 제거하십시오. 2. Rescue and Recovery 3.0 프로그램을 설치하십시오. (Client Security Solution 6.0 구성 요소가 선택되었는지 확인하십시오.)	• 먼저 Client Security Software를 제거하지 않고 Client Security Software 5.4x 위에 Rescue and Recovery 3.0을 설치하면 Rescue and Recovery만 남게 됩니다. • Client Security Software 5.4x 응용프로그램을 제거하기 전에 암호화 파일을 해독하고 Password Manager 정보를 내보내야 합니다. 그렇지 않으면 해당 정보를 잃게 됩니다. • Client Security Solution 6.0 응용프로그램을 설치하기 전에 IBM File and Folder Encryption 소프트웨어를 제거해야 합니다.

표 14-1. 다음 표는 Rescue and Recovery 및 Client Security 구성 변경을 도와주는 정보를 제공합니다. Client Security Solution 독립형은 설치 패키지를 웹이나 CD에서 가져왔음을 의미합니다. (계속)

설치된 소프트웨어	원하는 사항	따라야 할 프로세스	설명
Rescue and Recovery 3.0	Client Security Software 5.4x 및 Rescue and Recovery 3.0	1. Rescue and Recovery 3.0 프로그램을 제거하십시오. 2. Client Security Software 5.4x 응용프로그램을 설치하십시오. 3. Rescue and Recovery 3.0 프로그램을 설치하십시오. 4. 프롬프트되면 Client Security Software 5.4x 응용프로그램 설치를 유지하도록 지정하십시오.	• Client Security Software 5.4x 응용프로그램은 Rescue and Recovery 3.0 프로그램 위에 설치할 수 없습니다. • Rescue and Recovery 3.0 프로그램을 제거하면 로컬 백업이 삭제됩니다.
Rescue and Recovery 3.0	Client Security Solution 6.0 독립형 설치 패키지	1. Rescue and Recovery 3.0 프로그램을 제거하십시오. 2. Client Security Solution 6.0(독립형) 응용프로그램을 설치하십시오.	• Rescue and Recovery를 제거하면 사용자 파일과 Client Security Solution 레지스트리 설정이 삭제됩니다. • Client Security Solution에서 보호되는 Rescue and Recovery 백업은 더 이상 액세스할 수 없습니다. • Rescue and Recovery 3.0을 제거하면 로컬 백업이 삭제됩니다. • Client Security Solution 6.0(독립형)은 Rescue and Recovery 3.0 위에 설치할 수 없습니다.

표 14-1. 다음 표는 Rescue and Recovery 및 Client Security 구성 변경을 도와주는 정보를 제공합니다. Client Security Solution 독립형은 설치 패키지를 웹이나 CD에서 가져왔음을 의미합니다. (계속)

설치된 소프트웨어	원하는 사항	따라야 할 프로세스	설명
Rescue and Recovery 3.0	Rescue and Recovery 3.0 및 Client Security Solution 6.0	1. 프로그램 추가/제거에서 **수정** 옵션을 선택하십시오. 2. Client Security Solution 응용프로그램과 원하는 하위 구성 요소를 추가하여 수정 작업을 완료하십시오.	• Client Security Solution 응용프로그램이 추가되면 로컬 백업이 삭제됩니다. • Client Security Solution 응용프로그램을 추가한 후 가능한 빨리 새 기본 백업을 작성하십시오. • Client Security Solution 설정 및 데이터 파일이 삭제됩니다. • Client Security Solution 6.0(독립형) 응용프로그램은 Rescue and Recovery 3.0 프로그램 위에 설치할 수 없습니다.
Client Security Solution 6.0 독립형 설치 패키지	Client Security Software 5.4x	1. Client Security Solution 6.0(독립형) 응용프로그램을 제거하십시오. 2. Client Security Software 5.4x 응용프로그램을 설치하십시오.	• 프롬프트되었을 때 Client Security Solution 6.0 데이터 파일과 설정을 삭제해도 Client Security Software 5.4x 작업에는 영향을 주지 않습니다.
Client Security Solution 6.0 독립형 설치 패키지	Rescue and Recovery 3.0	1. Client Security Solution 6.0 응용프로그램을 제거하십시오. 2. Rescue and Recovery 3.0 프로그램을 설치하십시오. 3. 설치 중에 Rescue and Recovery 프로그램 설치만 선택하십시오.	Client Security Solution 6.0 응용프로그램을 제거할 때 Security Solution 6.0 파일과 설정도 삭제해야 합니다. 프롬프트되었을 때 이들을 제거하지 않으면 Rescue and Recovery 3.0 설치가 종료됩니다.
Client Security Solution 6.0 독립형	Rescue and Recovery 3.0 및 Client Security Solution 6.0	1. Rescue and Recovery 3.0 프로그램을 설치하십시오. 2. 설치할 Client Security Solution 6.0 응용프로그램의 하위 구성 요소를 선택하십시오.	• Client Security Solution 6.0 데이터 파일과 설정이 보존됩니다. • Client Security Solution 6.0 응용프로그램을 사용한 백업을 보호하려면 Rescue and Recovery 프로그램을 사용하십시오.

표 14-1. 다음 표는 Rescue and Recovery 및 Client Security 구성 변경을 도와주는 정보를 제공합니다. Client Security Solution 독립형은 설치 패키지를 웹이나 CD에서 가져왔음을 의미합니다. (계속)

설치된 소프트웨어	원하는 사항	따라야 할 프로세스	설명
Rescue and Recovery 3.0 및 Client Security Solution 6.0	Client Security Software 5.4x	1. Rescue and Recovery - Client Security Solution 응용프로그램을 제거하십시오. 2. Client Security Software 5.4x 응용프로그램을 설치하십시오.	• Client Security Software 5.4x 응용프로그램은 Client Security Solution 6.0 응용프로그램 위에 설치할 수 없습니다. • 프롬프트되었을 때 데이터 파일과 설정을 삭제해도 Client Security Software 5.4x 작업에는 영향을 주지 않습니다. • Rescue and Recovery 3.0 프로그램을 제거하면 Client Security Solution 6.0 응용프로그램도 자동으로 제거됩니다.
Rescue and Recovery 3.0 및 Client Security Solution 6.0	Rescue and Recovery 3.0	1. 프로그램 추가/제거에서 **수정**을 선택하십시오. 2. Client Security Solution 6.0 응용프로그램을 제거하십시오.	• Client Security Solution 6.0 응용프로그램이 제거되면 로컬 백업이 삭제됩니다. • Client Security Solution 6.0 응용프로그램을 제거하면 Password Manager 또는 PrivateDisk도 제거됩니다. • Client Security Solution 6.0 응용프로그램으로 보호되는 Rescue and Recovery 3.0 백업에 더 이상 액세스할 수 없습니다. 가능한 빨리 새 백업을 작성하십시오.
Rescue and Recovery 3.0 및 Client Security Solution 6.0	Client Security Solution 6.0	1. Rescue and Recovery 3.0 프로그램을 제거하십시오. 2. 현재 보안 구성을 유지하려는 경우에만 프롬프트되었을 때 현재 Client Security Solution 6.0 설정 유지를 선택하십시오. 3. Client Security Solution 6.0(독립형) 응용프로그램을 설치하십시오.	1. Client Security Solution 6.0으로 보호되는 Rescue and Recovery 3.0 백업에 더 이상 액세스할 수 없습니다. 2. Rescue and Recovery 3.0 응용프로그램을 제거하면 로컬 백업이 삭제됩니다.

Rescue and Recovery 암호 및 암호구

암호나 암호구를 사용하여 Rescue and Recovery 작업 공간을 보호함으로써 권한이 부여되지 않은 액세스로부터 중요 데이터를 보호할 수 있습니다. Client Security Setup wizard로 보안 환경을 설정하거나 Client Security Solution 응용프로그램으로 로그온 설정을 변경하여 Rescue and Recovery 작업 공간을 보호하도록 지정할 수 있습니다. Client Security Solution 응용프로그램은 Rescue and Recovery 작업 공간 내에서도 암호 복구 옵션을 설정할 수 있게 합니다.

주:

1. 이 기능은 Client Security Solution 6.0 프로그램이 설치된 경우에만 사용 가능합니다. 이 기능을 사용하려면 Client Security 6.0 Setup wizard를 완료하고 컴퓨터에 로그온할 때 암호 또는 암호구를 사용하도록 지정해야 합니다.
2. Client Security Setup 6.0 wizard 및 Client Security Solution 6.0 응용프로그램은 Windows 환경에서만 액세스 가능합니다. Client Security Solution 없이 Rescue and Recovery를 사용하려면 Rescue and Recovery 작업 공간이 암호나 암호구로 보호받지 못합니다.
3. Client Security Solution 응용프로그램은 Rescue and Recovery 작업 공간 내에서 암호 복구 옵션을 설정할 수 있게 합니다.

다음 방법을 사용하여 암호 또는 암호구로 Rescue and Recovery 작업 공간을 보호하십시오.

방법 1: Client Security Setup Wizard를 완료하지 않은 경우 다음을 수행하여 암호 또는 암호구로 Rescue and Recovery 작업 공간을 보호할 수 있습니다.

1. Windows 바탕 화면에서 **시작**을 클릭하고 **모든 프로그램**을 클릭하고 **ThinkVantage**를 선택한 후 **Client Security Solution**을 더블 클릭하십시오.
2. Client Security Solution 창이 열리면 **고급** 메뉴 항목을 클릭하십시오.
3. **보안 및 백업 환경 설정** 아이콘을 클릭하십시오. Client Security Setup Wizard가 열립니다.
4. 보안 환경을 설정하십시오. 프롬프트되면 다음 중 하나를 선택하십시오.
   - Windows 로그온 암호를 사용하여 Rescue and Recovery 작업 공간을 보호하려면 **Rescue and Recovery 작업 공간 액세스에 Windows 암호 사용** 선택란에 표시하십시오.
   - Client Security Solution 로그온 암호구를 사용하여 Rescue and Recovery 작업 공간을 보호하려면 **Rescue and Recovery 작업 공간 액세스에 Client Security Solution 암호구 사용** 선택란에 표시하십시오.
5. Client Security Solution Setup wizard를 완료한 후 **완료**를 클릭하십시오. 자세한 정보는 Client Security Setup Wizard 내의 **도움말**을 클릭하십시오.

방법 2: Client Security Setup Wizard를 완료한 경우 다음을 수행하여 암호 또는 암호구로 Rescue and Recovery 작업 공간을 보호할 수 있습니다.

1. Windows 바탕 화면에서 **시작**을 클릭하고 **모든 프로그램**을 클릭하고 **ThinkVantage**를 선택한 후 **Client Security Solution**을 더블 클릭하십시오.
2. Client Security Solution 창이 열리면 **고급** 메뉴 항목을 클릭하십시오.
3. **로그온 설정 변경**을 클릭하십시오.
4. 화면의 지시사항을 따르십시오. 자세한 정보는 Client Security Solution 응용프로그램 내의 **도움말**을 클릭하십시오.

Client Security Setup Wizard를 사용한 백업 환경 설정

Client Security Solution Setup Wizard는 임베디드 Security Chip 사용, 원하는 Windows 환경 인증 방식 선택, 중요 데이터 백업을 위한 Rescue and Recovery 사용의 선택 또는 지문 인증 사용 선택과 같은 다양한 보안 기능을 설정할 수 있는 구성 옵션을 제공합니다.

다음 절차를 완료하여 Client Security Setup wizard를 사용하십시오.

1. Windows 바탕 화면에서 **시작**을 클릭하고 **모든 프로그램**을 클릭하고 **ThinkVantage**를 선택한 후 **Client Security Solution**을 더블 클릭하십시오.
2. Client Security Solution 창이 열리면 **고급** 메뉴 항목을 클릭하십시오.
3. Client Security Solution 창이 열리면 **보안 및 백업 환경 설정**을 클릭하십시오. Client Security Setup Wizard가 열립니다.
4. 보안 환경을 설정하십시오.
5. Client Security Solution Setup wizard를 완료한 후 **완료**를 클릭하십시오. 자세한 정보는 Client Security Setup Wizard 내의 **도움말**을 클릭하십시오.

Client Security Solution에 대한 추가 정보

Client Security Solution 응용프로그램 및 해당 기능에 대한 자세한 정보는 다음 웹에 있는 *Client Security Solution User Guide*를 참고하십시오.

`http://www.ibm.com/pc/support/site.wss/`

Client Security Solution 응용프로그램이 이미 설치되어 있는 경우 다음 절차를 완료하여 User Guide의 보다 자세한 정보를 읽을 수 있습니다.

1. Windows 바탕 화면에서 **시작**을 클릭하십시오.
2. **모든 프로그램**을 선택하십시오.
3. **ThinkVantage**를 선택하십시오.
4. **Client Security Solution**을 클릭하십시오.
5. Client Security Solution 메뉴 바에서 **도움말**을 클릭하십시오.
6. **사용 설명서**를 클릭하십시오.

第 15 章 简体中文

客户端安全解决方案应用程序是一组 ThinkVantage™ Technology 工具套件，用于帮助保护对您的计算机操作系统和敏感数据的访问。客户端安全解决方案将其嵌入式芯片的硬件保护与其安全软件提供的保护整合起来。通过将专用硬件与其软件保护组合，客户端安全解决方案极大地增强了构建到您计算机操作系统中的安全功能。

本指南的读者

《*ThinkVantage 客户端安全解决方案用户指南*》用于单个最终用户以及在企业环境中工作的多个最终用户。本指南提供了有关以下范围的信息:

- 客户端安全解决方案组件
- 客户端安全解决方案安装注意事项
- 客户端安全解决方案功能

本指南对客户端安全解决方案帮助系统（提供有关在程序中如何执行特定任务的循序渐进说明）进行了补充。

附加信息

如果您是系统管理员、系统工程师、网络管理员或客户工程师，试图在大型企业中实现客户端安全解决方案，则可以通过阅读位于以下 Web 站点的 *ThinkVantage Rescue and Recovery™ and Client Security Solution Deployment Guide* 以获取详细信息:

```
http://www.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-54502
```

客户端安全解决方案组件

客户端安全解决方案用于装配有嵌入式安全芯片的计算机，该芯片有助于为计算机数据和进程提供附加的安全性级别。但是，现在可通过配置客户端安全解决方案软件来增强未装配安全芯片的计算机的安全性。

客户端安全解决方案分为以下硬件和软件组件。

- **嵌入式安全芯片**

  客户端安全解决方案用于装配有嵌入式安全芯片的计算机。嵌入式安全芯片是一种内置加密硬件技术，它为计算机提供了额外的安全性级别。安全芯片使加密和认证过程能够从易受攻击的软件转移到专用硬件的安全环境中。这样便切实地增加了安全性。

- **客户端安全安装向导**

  “客户端安全安装向导”会帮助指导您逐步完成安全选项的配置过程。该向导可帮助您启用嵌入式安全芯片、选择认证和登录方法、创建密码恢复问题、建立指纹认证（可选）以及配置其他客户端安全解决方案组件。

- **密码管理器**

客户端安全密码管理器使您能够安全而方便地管理敏感且容易忘记的应用程序和 Web 站点登录信息（例如，用户标识、密码和其他个人信息）。客户端安全密码管理器通过嵌入式安全芯片来存储所有信息，这样对您应用程序和 Web 站点的访问仍是绝对安全的。

- **PrivateDisk**

  PrivateDisk 会设置加密虚拟盘驱动器，该驱动器会自动加密您存储在该“电子保险箱”的安全界限内的任何数据。请使用您自己的虚拟驱动器来加密和存储您所有的关键数据。当数据存储在任何 PrivateDisk 卷中时，会自动进行加密。

- **客户端安全解决方案应用程序**

  客户端安全解决方案应用程序提供了单个界面以使用户能够执行基本和高级的安全功能，例如启用嵌入式安全芯片、更改口令或使用指纹软件。有关完整客户端安全解决方案功能的列表，请参阅第 15-3 页的『客户端安全解决方案功能』。

- **ThinkVantage 指纹软件**

  ThinkVantage 指纹软件使用户能够建立指纹认证。这种方便的安全功能在选定的 ThinkPad 和 ThinkCentre 型号和选件上是可用的。

在安装客户端安全解决方案之前

在安装客户端安全解决方案应用程序之前，满足以下先决条件非常重要:

- Windows XP 或 Windows 2000（Service Pack 3）。如果您要在容量大于 137 GB 的硬盘上安装该程序，则对于 Windows XP，Service Pack 1 是必需的。
- Internet Explorer 5.5（或更高版本）。
- 128 MB 内存，其中在 BIOS 中视频设置下指定的共享内存不能超过 8 MB。
- 800 MB 可用磁盘空间。

如果您具有先前版本的客户端安全解决方案、客户端安全软件或 Rescue and Recovery，请参阅第 15-5 页的『结合 Rescue and Recovery 使用客户端安全解决方案』以获取特定说明。

安装客户端安全解决方案

客户端安全解决方案应用程序可从 `http://www.pc.ibm.com/thinkvantage` Web 站点获取。下载、安装和配置客户端安全解决方案可以在数分钟内完成。

下载和安装客户端安全解决方案

请完成以下安装过程以下载并安装客户端安全解决方案程序:

1. 启动计算机并关闭任何打开的程序。
2. 转至 `http://www.pc.ibm.com/thinkvantage` Web 站点。
3. 在 Resources 部分中单击 **Support and downloads** 链接。
4. 向下滚动至 Embedded Security Subsystem and Client Security Solution 部分并单击 **Software download**。
5. 按照屏幕上的指示信息进行操作。

6. 运行安装可执行文件并按照屏幕上的指示信息进行操作。将提供您安装密码管理器和客户端安全解决方案 PrivateDisk 组件的选项。
7. 在您作出选择之后，将会提示您重新启动计算机。
8. 计算机重新启动后，“客户端安全安装向导”将会打开。如果安装向导未打开，请参阅『打开客户端安全安装向导』。
9. 完成“客户端安全安装向导”以完成配置过程。

打开客户端安全安装向导

使用“客户端安全安装向导”完成以下过程以配置客户端安全解决方案程序:

1. 从 Windows 桌面单击**开始**，单击**所有程序**，选择 **ThinkVantage**，然后双击**客户端安全解决方案**。
2. “客户端安全解决方案”窗口打开后，单击**高级**菜单项。
3. “客户端安全解决方案”窗口打开后，单击**设置安全和备份首选项**。“客户端安全安装向导”将会打开。
4. 完成“客户端安全解决方案安装向导”步骤，然后单击**完成**。有关详细信息，请在“客户端安全安装向导”中单击**帮助**。

使用客户端安全解决方案

完成以下过程以访问客户端安全解决方案应用程序:

1. 从 Windows 桌面单击**开始**。
2. 选择**所有程序**。
3. 选择 **ThinkVantage**。
4. 单击**客户端安全解决方案**。

客户端安全解决方案功能

以下信息详细说明了使用客户端安全解决方案应用程序可以完成的各种任务。

注: 如果您无法使用以下提及的某些工具，则可能是因为未安装正确的软件、您的计算机不支持该应用程序或该应用程序需要管理员或超级用户访问权。

基本功能

以下信息详细说明了使用客户端安全解决方案应用程序可以完成的基本任务。

更改口令: 更改口令工具使您能够建立新的客户端安全口令。口令必须遵守客户端安全口令需求。

配置密码恢复: 配置密码恢复工具使您能够制定用于恢复忘记的 Windows 密码或客户端安全口令的方法（视您使用的认证方法而定）。

管理登录信息: 密码管理器应用程序使您能够使用客户端安全解决方案来管理您的敏感和容易忘记的登录信息（例如，用户标识、密码和其他个人信息）。密码管理器应用程序通过嵌入式安全芯片来存储所有信息，以便您的用户认证策略控制对安全应用程序和 Web 站点的访问。这意味着不必记住和提供大量单独的密码 – 所有密码符合不同规则和有效期 – 您只需记住一个口令或提供您的指纹（如果已安装指纹软件）。

使用指纹软件: 集成的指纹阅读器使您能够登记您的指纹，并将它与您的开机密码、硬盘密码及 Windows 密码关联起来以便指纹认证可以代替密码并启用简单而安全的用户访问。指纹阅读器键盘可能由某些选定的计算机提供，也可以作为选件购买。仅有选定的 ThinkCentre 和 ThinkPad 计算机支持该选件。

保护数据: PrivateDisk 工具会生成加密虚拟盘驱动器，该驱动器会自动加密您存储在该“电子保险箱”的安全界限内的任何数据。

高级功能

以下信息详细说明了使用客户端安全解决方案应用程序可以完成的高级任务。

注: 您必须具有管理员权限以执行以下操作。

监视安全设置: 安全顾问程序工具使您能够查看计算机上当前设置的安全设置摘要。请检查这些设置以查看您当前的安全状态或增强你的系统安全性。其中包含的某些安全主题有硬件密码、Windows 用户密码、Windows 密码策略、受保护屏幕保护程序和文件共享。

注: 安全顾问程序工具仅提供安全设置的摘要和建议以帮助您增强系统安全性。并未阐述安全的所有方面，例如使用和维护反病毒和防火墙程序。许多设置需要超级用户或管理员访问权。

转移数字证书: “客户端安全证书转移向导”可指导您逐步完成将与证书关联的私钥从基于软件的 Microsoft 加密服务提供程序（CSP）转移到基于硬件的客户端安全解决方案 CSP 的过程。在转移后，由于私钥受嵌入式安全芯片的保护，所以使用证书的操作将更加安全。

建立硬件密码重置机制: 该工具可创建独立于 Windows 运行的安全环境并帮助您重置忘记的开机密码和硬盘驱动器密码。您的身份是通过回答您创建的一组问题来确定的。最好在忘记密码前尽快创建该安全环境。在硬盘驱动器上创建该安全环境且您已登记之后，才能重置忘记的硬件密码。该工具仅在选定的 ThinkCentre 和 ThinkPad 计算机上可用。

注: 在使用该工具之前，最好设置管理员或超级用户密码。如果您尚未设置管理员或超级用户密码，则您的环境将无法达到足够的安全。在完成该过程之后，您的开机密码将和硬盘驱动器密码相匹配。该过程用于帮助您完成创建安全环境的任务和在创建安全环境后重置忘记的密码。

激活嵌入式安全芯片: 该工具可启动用于激活或取消激活嵌入式安全芯片的 BIOS 设置更改。您必须重新启动计算机以使该更改生效。

更改登录设置: 该工具显示了您当前的登录设置并使管理员能够更改用户如何登录 Windows 操作系统和 ThinkVantage Rescue and Recovery 工作空间。

清除失败转移计数器: 该工具可重置认证失败计数器，该计数器监视有多少不正确的认证尝试已传至嵌入式安全芯片。在某些失败尝试之后，该芯片会自锁一段时间。锁定时间段会随失败尝试的继续而增加。

设置安全和备份首选项: “客户端安全安装向导”使您能够配置多种安全软件工具。该向导提供了配置选项使您能够设置多种安全功能（例如，启用客户端安全嵌入式安全芯片、选择您想要如何认证至 Windows 环境、选择使用 Rescue and Recovery 备份您的敏感数据或选择使用指纹认证）。

结合 Rescue and Recovery 使用客户端安全解决方案

Rescue and Recovery 程序和客户端安全解决方案应用程序都属于考虑到您的需要而开发的 ThinkVantage Technology。即它们用于单独或共同工作（视您的需要而定）。以下信息旨在帮助您设计使用这些程序的策略，并突出显示了这些程序如何相互增强。

在安装 Rescue and Recovery 程序和／或客户端安全解决方案应用程序时，需考虑一些重要的注意事项。下表提供的信息有助于为您期望的配置确定正确过程:

表 15-1. 下表提供的信息可帮助您更改 Rescue and Recovery 和客户端安全配置。客户端安全解决方案单机是指从 Web 或 CD 获取安装程序包。

已安装程序为...	而您想要...	按照该过程操作	注释
客户端安全软件 5.4x	客户端安全软件 5.4x 和 Rescue and Recovery 3.0	1. 安装 Rescue and Recovery 3.0 程序。 2. 提示时，表明您想要保留已安装的客户端安全软件 5.4x 应用程序。	使用客户端安全软件 5.4x 应用程序无法保护备份，并且 Rescue and Recovery 3.0 程序对客户端安全软件功能的任何使用都将使用客户端安全软件的模拟版本来完成。 主密码功能已添加到您的安全功能中。主密码通常在企业环境中使用。有关更多信息，请参阅第 15-1 页的『附加信息』。
客户端安全软件 5.4x	客户端安全解决方案 6.0 单机安装程序包	1. 卸载客户端安全软件 5.4x 应用程序。 2. 安装客户端安全解决方案 6.0（单机）应用程序。	• 在卸载之前，您必须解密任何加密文件并导出所有密码管理器信息。否则，这些信息将会丢失。 • 在安装客户端安全解决方案应用程序之前，您必须卸载 IBM® 文件和文件夹加密软件。
客户端安全软件 5.4x	客户端安全解决方案 6.0 和 Rescue and Recovery 3.0	1. 卸载客户端安全软件 5.4x 应用程序。 2. 安装 Rescue and Recovery 3.0 程序。（请确保已选择客户端安全解决方案 6.0 组件。）	• 在客户端安全软件 5.4x 上安装 Rescue and Recovery 3.0 而不首先卸载客户端安全软件将会导致只有 Rescue and Recovery。 • 在卸载客户端安全软件 5.4x 应用程序之前，您必须解密任何加密文件并导出所有密码管理器信息。否则，这些信息将会丢失。 • 在安装客户端安全解决方案 6.0 应用程序之前，您必须卸载 IBM 文件和文件夹加密软件。

表 15-1. 下表提供的信息可帮助您更改 Rescue and Recovery 和客户端安全配置。客户端安全解决方案单机是指从 Web 或 CD 获取安装程序包。 (续)

已安装程序为...	而您想要...	按照该过程操作	注释
Rescue and Recovery 3.0	客户端安全软件 5.4x 和 Rescue and Recovery 3.0	1. 卸载 Rescue and Recovery 3.0 程序。 2. 安装客户端安全软件 5.4x 应用程序。 3. 安装 Rescue and Recovery 3.0 程序。 4. 提示时，表明您想要保留已安装的客户端安全软件 5.4x 应用程序。	• 不能在 Rescue and Recovery 3.0 程序上安装客户端安全软件 5.4x 应用程序。 • 卸载 Rescue and Recovery 3.0 程序后会删除本地备份。
Rescue and Recovery 3.0	客户端安全解决方案 6.0 单机安装程序包	1. 卸载 Rescue and Recovery 3.0 程序。 2. 安装客户端安全解决方案 6.0（单机）应用程序。	• 卸载 Rescue and Recovery 将会删除用户文件和客户端安全解决方案注册表设置。 • 将无法再访问由客户端安全解决方案保护的 Rescue and Recovery 备份。 • 卸载 Rescue and Recovery 3.0 后会删除本地备份。 • 不能在 Rescue and Recovery 3.0 上安装客户端安全解决方案 6.0（单机）。
Rescue and Recovery 3.0	Rescue and Recovery 3.0 和客户端安全解决方案 6.0	1. 从添加/删除程序选择**修改**选项。 2. 通过添加客户端安全解决方案和任何期望的子组件来完成修改操作。	• 添加客户端安全解决方案应用程序后会删除本地备份。 • 在添加客户端安全解决方案应用程序之后，请尽快创建新的基本备份。 • 会删除客户端安全解决方案设置和数据文件。 • 不能在 Rescue and Recovery 3.0 程序上安装客户端安全解决方案 6.0（单机）应用程序。
客户端安全解决方案 6.0 单机安装程序包	客户端安全软件 5.4x	1. 卸载客户端安全解决方案 6.0（单机）应用程序。 2. 安装客户端安全软件 5.4x 应用程序。	• 在提示时删除客户端安全解决方案 6.0 数据文件和设置将不会影响客户端安全软件 5.4x 操作。

表 15-1. 下表提供的信息可帮助您更改 Rescue and Recovery 和客户端安全配置。客户端安全解决方案单机是指从 Web 或 CD 获取安装程序包。 (续)

已安装程序为...	**而您想要...**	**按照该过程操作**	**注释**
客户端安全解决方案 6.0 单机安装程序包	Rescue and Recovery 3.0	1. 卸载客户端安全解决方案 6.0 应用程序。 2. 安装 Rescue and Recovery 3.0 程序。 3. 在安装的过程中，请选择仅安装 Rescue and Recovery 程序。	在卸载客户端安全解决方案 6.0 应用程序时，您必须删除安全解决方案 6.0 文件和设置。在提示时无法除去这些内容将会终止 Rescue and Recovery 3.0 安装。
客户端安全解决方案 6.0 单机	Rescue and Recovery 3.0 和客户端安全解决方案 6.0	1. 安装 Rescue and Recovery 3.0 程序。 2. 选择您希望安装的客户端安全解决方案 6.0 应用程序的任何子组件。	• 会保留客户端安全解决方案 6.0 数据文件和设置。 • 要选择使用客户端安全解决方案 6.0 应用程序保护备份，请使用 Rescue and Recovery 程序。
Rescue and Recovery 3.0 和客户端安全解决方案 6.0	客户端安全软件 5.4x	1. 卸载 Rescue and Recovery – 客户端安全解决方案应用程序。 2. 安装客户端安全软件 5.4x 应用程序。	• 不能在客户端安全解决方案 6.0 应用程序上安装客户端安全软件 5.4x 应用程序。 • 在提示时删除数据文件和设置将不会影响客户端安全软件 5.4x 操作。 • 卸载 Rescue and Recovery 3.0 程序时，会自动卸载客户端安全解决方案 6.0 应用程序。
Rescue and Recovery 3.0 和客户端安全解决方案 6.0	Rescue and Recovery 3.0	1. 从添加/删除程序选择**修改**。 2. 除去客户端安全解决方案 6.0 应用程序。	• 除去客户端安全解决方案 6.0 应用程序后会删除本地备份。 • 卸载客户端安全解决方案 6.0 应用程序将会导致没有密码管理器或 PrivateDisk。 • 将无法再访问使用客户端安全解决方案 6.0 应用程序保护的 Rescue and Recovery 3.0 备份。请尽快创建新的备份。
Rescue and Recovery 3.0 和客户端安全解决方案 6.0	客户端安全解决方案 6.0	1. 卸载 Rescue and Recovery 3.0 程序。 2. 提示时，选择保留当前的客户端安全解决方案 6.0 设置（仅当您想要保留当前的安全配置时）。 3. 安装客户端安全解决方案 6.0（单机）应用程序。	1. 将无法再访问使用客户端安全解决方案 6.0 保护的 Rescue and Recovery 3.0 备份。 2. 卸载 Rescue and Recovery 3.0 应用程序后会删除本地备份。

Rescue and Recovery 密码和口令

您可以使用密码或口令来保护 Rescue and Recovery 工作空间，从而使关键数据免于未授权的访问。通过使用“客户端安全安装向导”设置安全首选项或通过使用客户端安全解决方案应用程序更改登录设置，您可以指定保护 Rescue and Recovery 工作空间。客户端安全解决方案应用程序还使您能够在 Rescue and Recovery 工作空间内建立密码恢复选项。

注:

1. 仅当已安装客户端安全解决方案 6.0 程序时，该功能可用。要使用该功能，您必须已完成“客户端安全 6.0 安装向导”并指定您想要使用密码或口令登录到计算机。
2. “客户端安全安装 6.0 向导”和客户端安全解决方案 6.0 应用程序都只能在 Windows 环境中访问。如果您在未使用客户端安全解决方案的情况下选择使用 Rescue and Recovery，则 Rescue and Recovery 工作空间将不受密码或口令保护。
3. 客户端安全解决方案应用程序使您能够在 Rescue and Recovery 工作空间内建立密码恢复选项。

使用以下方法可使用密码或口令来保护 Rescue and Recovery 工作空间。

方法 1: 如果您未完成“客户端安全安装向导”，请执行以下操作来使用密码或口令保护 Rescue and Recovery 工作空间:

1. 从 Windows 桌面单击**开始**，单击**所有程序**，选择 **ThinkVantage**，然后双击**客户端安全解决方案**。
2. “客户端安全解决方案”窗口打开后，单击**高级**菜单项。
3. 单击**设置安全和备份首选项**图标。“客户端安全安装向导”打开。
4. 设置您的安全首选项。提示时，选择以下其中一项:
   - 如果您想要使用 Windows 登录密码保护 Rescue and Recovery 工作空间，请选中**使用 Windows 密码获取对 Rescue and Recovery 工作空间的访问**复选框。
   - 如果您想要使用客户端安全解决方案登录口令保护 Rescue and Recovery 工作空间，请选中**使用客户端安全解决方案口令获取对 Rescue and Recovery 工作空间的访问**复选框。
5. 完成“客户端安全解决方案安装向导”，然后单击**完成**。有关更多信息，请在“客户端安全安装向导”中单击**帮助**。

方法 2: 如果您已完成“客户端安全安装向导”，请执行以下操作来使用密码或口令保护 Rescue and Recovery 工作空间:

1. 从 Windows 桌面单击**开始**，单击**所有程序**，选择 **ThinkVantage**，然后双击**客户端安全解决方案**。
2. “客户端安全解决方案”窗口打开后，单击**高级**菜单项。
3. 单击**更改登录设置**。
4. 按照屏幕上的指示信息进行操作。有关详细信息，请在客户端安全解决方案应用程序中单击**帮助**。

使用客户端安全安装向导设置备份首选项

“客户端安全解决方案安装向导”提供了配置选项使您能够设置多种安全功能（例如，启用嵌入式安全芯片、选择您想要如何认证至 Windows 环境、选择使用 Rescue and Recovery 备份您的敏感数据或选择使用指纹认证）。

完成以下过程以使用“客户端安全安装向导”：

1. 从 Windows 桌面单击**开始**，单击**所有程序**，选择 **ThinkVantage**，然后双击**客户端安全解决方案**。
2. “客户端安全解决方案”窗口打开后，单击**高级**菜单项。
3. “客户端安全解决方案”窗口打开后，单击**设置安全和备份首选项**。“客户端安全安装向导”打开。
4. 设置您的安全首选项。
5. 完成“客户端安全解决方案安装向导”，然后单击**完成**。有关详细信息，请在“客户端安全安装向导”中单击**帮助**。

关于客户端安全解决方案的更多信息

有关客户端安全解决方案应用程序及其功能的详细信息，请参阅 Web 上位于以下地址的 *Client Security Solution User Guide*:

`http://www.ibm.com/pc/support/site.wss/`

如果您已安装客户端安全解决方案应用程序，则可以通过完成以下过程从《用户指南》阅读更多详细信息:

1. 从 Windows 桌面单击**开始**。
2. 选择**所有程序**。
3. 选择 **ThinkVantage**。
4. 单击**客户端安全解决方案**。
5. 从客户端安全解决方案菜单栏单击**帮助**。
6. 单击**《 用户指南 》**。

第 16 章 Traditional Chinese

Client Security Solution 應用程式是 ThinkVantage™ Technology 工具套件，專門用來保護電腦作業系統和機密資料的存取權。Client Security Solution 整合了內嵌式晶片的硬體保護功能與安全軟體的保護功能。Client Security Solution 將軟體保護功能與專用的硬體結合在一起，因此能大幅強化電腦原本內建的安全功能。

本書適用對象

ThinkVantage Client Security Solution User's Guide 適用於個人使用者及企業環境中的使用者。本手冊提供下列各方面相關資訊：

- Client Security Solution 元件
- Client Security Solution 安裝注意事項
- Client Security Solution 功能

本手冊也是 Client Security Solution 說明系統的補充資訊，提供在程式中執行特定作業的逐步指示。

其他資訊

如果您是系統管理者、系統工程師、網路管理者或客戶服務工程師，且需要在整個大型企業中實作 Client Security Solution，您可以閱讀位於下列網站的 *ThinkVantage Rescue and Recovery™ and Client Security Solution Deployment Guide*，以取得詳細資訊：

```
http://www.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-54502
```

Client Security Solution 元件

Client Security Solution 是針對配備內嵌式安全晶片的電腦所設計的，可以爲您的電腦資料和處理提供更高層次的安全功能。不過，現在您可以配置 Client Security Solution 軟體，爲沒有配備安全晶片的電腦增加安全性。

Client Security Solution 可以分爲下列軟硬體元件：

- **內嵌式安全晶片**

  Client Security Solution 是針對配備內嵌式安全晶片的電腦所設計的。內嵌式安全晶片是內建的加密硬體技術，可以爲電腦提供更高層次的安全功能。安全晶片可以讓加密和鑑別程序從較不安全的軟體作業，轉變爲使用專用硬體的安全環境作業。明顯加強了作業的安全性。

- **Client Security 安裝精靈**

  Client Security 安裝精靈會引導您完成配置安全選項的程序。精靈會幫助您啓用內嵌式安全晶片、選擇鑑別和登入方法、建立密碼回復問題、建立指紋鑑別（選用），以及配置其他 Client Security Solution 元件。

- **密碼管理程式**

Client Security 密碼管理程式可讓您安全方便地管理機密且容易忘記的應用程式和網站登入資訊，例如使用者 ID、密碼和其他個人資訊。Client Security 密碼管理程式會透過內嵌式安全晶片儲存所有資訊，以維護存取應用程式和網站的安全性。

- **PrivateDisk**

  PrivateDisk 會設定加密的虛擬磁碟機，自動將儲存在這個「電子保險箱」安全範圍內的所有資料加密，且會使用您自己的虛擬磁碟機來加密並儲存所有重要資料。當資料儲存到任何 PrivateDisk 磁碟區時，會自動進行加密。

- **Client Security Solution 應用程式**

  Client Security Solution 應用程式提供了單一介面，可以讓使用者執行基本和進階的安全功能，例如啓用內嵌式安全晶片、變更長密碼，或使用指紋辨識軟體。如需 Client Security Solution 功能的完整清單，請參閱第 1-3 頁的『Client Security Solution 功能』。

- **ThinkVantage 指紋辨識軟體**

  ThinkVantage 指紋辨識軟體可以讓使用者建立指紋鑑別。這項方便的安全功能可用於特定的 ThinkPad 和 ThinkCentre 機型及選用設備。

安裝 Client Security Solution 之前

在安裝 Client Security Solution 應用程式之前，必須符合下列先決要件：

- 已安裝 Service Pack 3 的 Windows XP 或 Windows 2000。如果您要將這個程式安裝到容量大於 137 GB 的硬碟上，則 Windows XP 必須裝有 Service Pack 1。
- Internet Explorer 5.5（或更新版本）。
- 128 MB 的記憶體，其中用於 BIOS 視訊設定的共用記憶體不可超過 8 MB。
- 800 MB 的可用磁碟空間。

如果您有舊版的 Client Security Solution、Client Security Software 或 Rescue and Recovery，請參閱第 1-5 頁的『搭配使用 Client Security Solution 與 Rescue and Recovery』，以取得特定指示。

設定 Client Security Solution

您可以在 `http://www.pc.ibm.com/thinkvantage` 網站上取得 Client Security Solution 應用程式。只需要幾分鐘就完成下載、安裝和配置 Client Security Solution。

下載和安裝 Client Security Solution

若要下載並安裝 Client Security Solution 程式，請完成下列安裝程序：

1. 啓動電腦並關閉任何開啓的程式。
2. 連至 `http://www.pc.ibm.com/thinkvantage` 網站。
3. 按一下 Resources 區塊的 **Support and downloads** 鏈結。
4. 向下捲動到 Embedded Security Subsystem and Client Security Solution 部分，然後按一下 **Software download**。
5. 按照螢幕上的指示操作。
6. 執行安裝執行檔並按照螢幕上的指示操作。螢幕上會出現選項，讓您選擇是否要安裝 Client Security Solution 的密碼管理程式和 PrivateDisk 元件。

7. 選擇完畢後系統會提示您重新啓動電腦。
8. 當電腦重新啓動後，會開啓 Client Security 安裝精靈。如果安裝精靈沒有開啓，請參閱『開啓 Client Security 安裝精靈』。
9. 結束 Client Security 安裝精靈，以完成配置程序。

開啓 Client Security 安裝精靈

若要使用 Client Security 安裝精靈來配置 Client Security Solution 程式，請完成下列程序：

1. 在 Windows 桌面上，按一下**開始**，按一下**所有程式**，選取 **ThinkVantage**，然後連按兩下 **Client Security Solution**。
2. Client Security Solution 視窗開啓時，請按一下**進階**功能表項目。
3. 當 Client Security Solution 視窗開啓，請按一下**設定安全及備份喜好設定**。此時會開啓 Client Security 安裝精靈。
4. 完成Client Security Solution 安裝精靈，然後按一下**完成**。如需詳細資訊，請按一下 Client Security 安裝精靈中的**說明**。

使用 Client Security Solution

若要存取 Client Security Solution 應用程式，請完成下列程序：

1. 在 Windows 桌面上，按一下**開始**。
2. 選取**所有程式**。
3. 選取 **ThinkVantage**。
4. 按一下 **Client Security Solution**。

Client Security Solution 功能

下列資訊詳細說明了可使用 Client Security Solution 應用程式完成的作業。

註: 如果您無法取得以下提及的部分工具，可能是因爲您沒有安裝適當的軟體、您的電腦不支援該應用程式，或只有管理者或監督者才能存取該應用程式。

基本功能

下列資訊詳細說明了可使用 Client Security Solution 應用程式完成的基本作業。

變更長密碼: 變更長密碼工具可讓您建立新的 Client Security 長密碼。長密碼必須遵守 Client Security 長密碼要求。

配置密碼回復: 配置密碼回復工具可以根據您所使用的鑑別方式，讓您建立回復遺忘 Windows 密碼或 Client Security 長密碼的方法。

管理登入資訊: 「密碼管理程式」應用程式可讓您使用 Client Security Solution 管理機密且容易忘記的登入資訊，例如使用者 ID、密碼和其他個人資訊。「密碼管理程式」應用程式會透過內嵌式安全晶片儲存所有資訊，您可以根據使用者身份鑑別原則來控制安全應用程式和網站的存取權。也就是說，您不需要記住並提供一大堆受到不同規則和到期日限制的密碼，只需要記住一個長密碼，或提供指紋即可（安裝了指紋辨識軟體之後）。

使用指紋辨識軟體: 整合式指紋辨識器可讓您註冊指紋，並將指紋與開機密碼、硬碟密碼和 Windows 密碼建立關聯，您就能以指紋鑑別取代密碼，讓使用者存取變得更為簡單與安全。指紋辨識器鍵盤是特定電腦的配備，也可以單獨選購。只有特定的 ThinkCentre 和 ThinkPad 電腦支援這項選用設備。

保護資料: PrivateDisk 會產生加密的虛擬磁碟機，自動將儲存在這個「電子保險箱」安全範圍內的所有資料加密，

進階功能

下列資訊詳細說明了可使用 Client Security Solution 應用程式完成的進階作業。

註: 您必須具備管理者權限，才能執行下列作業：

監控安全設定: Security Advisor 工具可讓您檢視目前電腦上安全設定的摘要。檢閱這些設定，以便檢視目前的安全狀態或用來加強系統安全性。其包含的安全主題有硬體密碼、Windows 使用者密碼、Windows 密碼原則、受保護的螢幕保護程式，以及檔案共享等。

註: Security Advisor 工具僅提供安全設定和建議的摘要，可幫助您加強系統安全。此處並不會提及所有的安全觀點，例如使用與維護防毒和防火牆程式就不會提到。其中許多設定必須由監督者或管理者才能存取。

轉換數位憑證: 「Client Security 憑證傳輸精靈」會在整個傳輸過程中提供引導，協助您從軟體式 Microsoft 密碼服務提供者 (cryptographic service provider, CSP)，將與您相關的私密金鑰傳輸到硬體式的 Client Security Solution 密碼服務提供者。傳輸之後，使用憑證的作業比較安全，因為內嵌式安全晶片會保護私密金鑰。

建立硬體密碼重設機制: 這項工具會建立獨立執行於 Windows 之外的安全環境，可以幫助您重設忘記的開機密碼及硬碟密碼。在回答之前所設定的問題組後，您的身分便可建立。在遺忘密碼之前，您最好盡快建立安全環境。註冊之後，您必須在硬碟上建立安全環境，否則就無法重設忘記的硬體密碼。您只能在特定的 ThinkCentre 和 ThinkPad 電腦上使用這個工具。

註: 在使用這個工具之前，最好先設定管理者或監督者密碼。如果您尚未設定管理者或監督者密碼，使用環境就不可能像這樣安全了。當完成這個程序，您的開機密碼及硬碟密碼會進行比對。這個程序是為了協助您完成建立安全環境的作業，以便在建立安全環境後能夠重設忘記的密碼。

啓動內嵌式安全晶片: 這項工具會起始 BIOS 設定變更，以啓動或取消啓動內嵌式安全晶片。您必須重新啓動電腦，這項變更才會生效。

變更登入設定: 這項工具會顯示您目前的登入設定，讓管理者變更使用者登入 Windows 作業系統和 ThinkVantage Rescue and Recovery 工作區的方式。

清除安全防護 (fail save) 計數器: 這項工具會重設身份鑑別失敗計數器，該計數器會監控傳送到內嵌式安全晶片的鑑別嘗試錯誤次數。失敗幾次後，晶片會自我鎖定一段時間。而鎖定期間則會隨著嘗試失敗次數增加而延長。

設定安全與備份喜好設定: 您可使用 Client Security 安裝精靈來配置多種安全軟體工具。精靈會提供配置選項，讓您設定多種安全功能，例如啓用 Client Security 內嵌式安全晶片、選擇 Windows 環境中的鑑別方式、選擇使用 Rescue and Recovery 備份機密資料，或是選用指紋辨識來進行鑑別。

搭配使用 Client Security Solution 與 Rescue and Recovery

Rescue and Recovery 程式和 Client Security Solution 應用程式都是針對您的需求而開發的 ThinkVantage Technologies。也就是說，這兩個程式可以依照您的需要，共同或分別運作。下列資訊可以幫助您設計使用這些程式的策略，並進一步說明這些程式如何加強彼此的功能。

安裝 Rescue and Recovery 程式及/或 Client Security Solution 應用程式時，有一些重要的注意事項。下表提供的資訊可以幫助您判斷所需配置的正確程序：

表 1-1. 下表提供的資訊可以幫助您變更 Rescue and Recovery 和 Client Security 的配置。獨立式 Client Security Solution 表示安裝套件是從 Web 或 CD 取得。

安裝的軟體...	所需軟體...	請遵循此程序進行	註解
Client Security Software 5.4x	Client Security Software 5.4x 和 Rescue and Recovery 3.0	1. 安裝 Rescue and Recovery 3.0 程式。 2. 請在提示時指出您要保留 Client Security Software 5.4x 應用程式。	您無法使用 Client Security Software 5.4x 應用程式保護備份，且 Rescue and Recovery 3.0 程式使用的任何 Client Security Software 功能，都會使用模擬版本的 Client Security Software 來完成。 安全功能中新增了主要密碼功能。主要密碼通常用於企業環境中。如需相關資訊，請參閱第 1-1 頁的『其他資訊』。
Client Security Software 5.4x	Client Security Solution 6.0 獨立式安裝套件	1. 解除安裝 Client Security Software 5.4x 應用程式。 2. 安裝 Client Security Solution 6.0（獨立式）應用程式。	• 在解除安裝之前，您必須先解密所有加密的檔案，並匯出所有「密碼管理程式」資訊，否則，該項資訊將會遺失。 • 在安裝 Client Security Solution 應用程式之前，您必須解除安裝 IBM® File and Folder Encryption 軟體。

表 1-1. 下表提供的資訊可以幫助您變更 Rescue and Recovery 和 Client Security 的配置。獨立式 Client Security Solution 表示安裝套件是從 Web 或 CD 取得。 (繼續)

安裝的軟體...	所需軟體...	請遵循此程序進行	註解
Client Security Software 5.4x	Client Security Solution 6.0 和 Rescue and Recovery 3.0	1. 解除安裝 Client Security Software 5.4x 應用程式。 2. 安裝 Rescue and Recovery 3.0 程式。（請確定已選取了 Client Security Solution 6.0 元件）。	• 若要在 Client Security Software 5.4x 上安裝 Rescue and Recovery 3.0，但沒有先解除安裝 Client Security Software，您將僅能使用 Rescue and Recovery。 • 在解除安裝 Client Security Software 5.4x 應用程式之前，您必須先解密所有加密的檔案，並匯出所有「密碼管理程式」資訊，否則，該項資訊將會遺失。 • 在安裝 Client Security Solution 6.0 應用程式之前，您必須解除安裝 IBM File and Folder Encryption 軟體。
Rescue and Recovery 3.0	Client Security Software 5.4x 和 Rescue and Recovery 3.0	1. 解除安裝 Rescue and Recovery 3.0 程式。 2. 安裝 Client Security Software 5.4x 應用程式。 3. 安裝 Rescue and Recovery 3.0 程式。 4. 請在提示時指出您要保留 Client Security Software 5.4x 應用程式。	• Client Security Software 5.4x 應用程式無法安裝在 Rescue and Recovery 3.0 程式之上。 • 解除安裝 Rescue and Recovery 3.0 程式時，會刪除本端備份。
Rescue and Recovery 3.0	Client Security Solution 6.0 獨立式安裝套件	1. 解除安裝 Rescue and Recovery 3.0 程式。 2. 安裝 Client Security Solution 6.0（獨立式）應用程式。	• 解除安裝 Rescue and Recovery 會刪除使用者檔案和 Client Security Solution 登錄設定。 • 您將無法再存取 Client Security Solution 保護的 Rescue and Recovery 備份。 • 解除安裝 Rescue and Recovery 3.0 時，會刪除本端備份。 • Client Security Solution 6.0（獨立式）無法安裝在 Rescue and Recovery 3.0 之上。

表 1-1. 下表提供的資訊可以幫助您變更 Rescue and Recovery 和 Client Security 的配置。獨立式 Client Security Solution 表示安裝套件是從 Web 或 CD 取得。 (繼續)

安裝的軟體...	所需軟體...	請遵循此程序進行	註解
Rescue and Recovery 3.0	Rescue and Recovery 3.0 和 Client Security Solution 6.0	1. 從「新增或移除程式」中選取**修改**選項。 2. 新增 Client Security Solution 應用程式和任何需要的子元件，完成修改作業。	• 新增 Client Security Solution 應用程式後，會刪除本端備份。 • 新增 Client Security Solution 應用程式後，請盡快建立新的基礎備份。 • 程式會刪除 Client Security Solution 的設定和資料檔。 • Client Security Solution 6.0（獨立式）應用程式無法安裝在 Rescue and Recovery 3.0 程式之上。
Client Security Solution 6.0 獨立式安裝套件	Client Security Software 5.4x	1. 解除安裝 Client Security Solution 6.0（獨立式）應用程式。 2. 安裝 Client Security Software 5.4x 應用程式。	• 在收到提示時刪除 Client Security Solution 6.0 資料檔和設定，並不會影響 Client Security Software 5.4x 的作業。
Client Security Solution 6.0 獨立式安裝套件	Rescue and Recovery 3.0	1. 解除安裝 Client Security Solution 6.0 應用程式。 2. 安裝 Rescue and Recovery 3.0 程式。 3. 在安裝期間，僅選擇安裝 Rescue and Recovery 程式。	解除安裝 Client Security Solution 6.0 應用程式時，您必須刪除 Security Solution 6.0 的檔案和設定。如果在收到提示時未移除這些項目，會終止安裝 Rescue and Recovery 3.0。
Client Security Solution 6.0 獨立式	Rescue and Recovery 3.0 和 Client Security Solution 6.0	1. 安裝 Rescue and Recovery 3.0 程式。 2. 選取要安裝的任何 Client Security Solution 6.0 應用程式子元件。	• 程式會保留 Client Security Solution 6.0 的資料檔和設定。 • 若要選擇使用 Client Security Solution 6.0 應用程式來保護備份，請使用 Rescue and Recovery 程式。
Rescue and Recovery 3.0 和 Client Security Solution 6.0	Client Security Software 5.4x	1. 解除安裝 Rescue and Recovery - Client Security Solution 應用程式。 2. 安裝 Client Security Software 5.4x 應用程式。	• Client Security Software 5.4x 應用程式無法安裝在 Client Security Solution 6.0 應用程式之上。 • 在收到提示時刪除資料檔和設定，並不會影響 Client Security Software 5.4x 的作業。 • 解除安裝 Rescue and Recovery 3.0 程式時，會自動解除安裝 Client Security Solution 6.0 應用程式。

表 1-1. 下表提供的資訊可以幫助您變更 Rescue and Recovery 和 Client Security 的配置。獨立式 Client Security Solution 表示安裝套件是從 Web 或 CD 取得。 (繼續)

安裝的軟體...	**所需軟體...**	**請遵循此程序進行**	**註解**
Rescue and Recovery 3.0 和 Client Security Solution 6.0	Rescue and Recovery 3.0	1. 從「新增或移除程式」中選取**修改**。 2. 移除 Client Security Solution 6.0 應用程式。	• 移除 Client Security Solution 6.0 應用程式時，會刪除本端備份。 • 解除安裝 Client Security Solution 6.0 應用程式後，您將無法再使用「密碼管理程式」或 PrivateDisk。 • 您將無法再存取 Client Security Solution 6.0 應用程式保護的 Rescue and Recovery 3.0 備份。請盡快建立新的備份。
Rescue and Recovery 3.0 和 Client Security Solution 6.0	Client Security Solution 6.0	1. 解除安裝 Rescue and Recovery 3.0 程式。 2. 收到提示時，如果您要保留目前的安全配置，請選擇保留目前的 Client Security Solution 6.0 設定。 3. 安裝 Client Security Solution 6.0（獨立式）應用程式。	1. 您將無法再存取 Client Security Solution 6.0 保護的 Rescue and Recovery 3.0 備份。 2. 解除安裝 Rescue and Recovery 3.0 應用程式時，會刪除本端備份。

Rescue and Recovery 密碼和長密碼

您可以使用密碼或長密碼來保護 Rescue and Recovery 工作區，避免他人未經授權存取重要資料。您可以指定使用 Client Security Solution 安裝精靈來設定安全喜好設定，或使用 Client Security Solution 應用程式來變更登入設定，以保護 Rescue and Recovery 工作區。Client Security Solution 應用程式也能讓您在 Rescue and Recovery 工作區中建立密碼回復選項。

註:

1. 您必須先安裝 Client Security Solution 6.0 程式才能使用這個功能。若要使用這項功能，您必須完成 Client Security 6.0 安裝精靈，並指定您要使用密碼或長密碼登入電腦。
2. 您僅能在 Windows 環境中存取 Client Security 6.0 安裝精靈和 Client Security Solution 6.0 應用程式。如果您選擇使用 Rescue and Recovery 而不使用 Client Security Solution，則不會以密碼或長密碼來保護 Rescue and Recovery 工作區。
3. Client Security Solution 應用程式能讓您在 Rescue and Recovery 工作區中建立密碼回復選項。

請使用下列方式，用密碼或長密碼來保護 Rescue and Recovery 工作區。

方法 1：如果您還未完成 Client Security 安裝精靈，請執行下列步驟，使用密碼或長密碼來保護 Rescue and Recovery 工作區：

1. 在 Windows 桌面上，按一下**開始**，按一下**所有程式**，選取 **ThinkVantage**，然後連按兩下 **Client Security Solution**。
2. Client Security Solution 視窗開啓時，請按一下**進階**功能表項目。
3. 按一下**設定安全及備份喜好設定**圖示。此時會開啓 Client Security 安裝精靈。
4. 設定您的安全喜好設定。在收到提示時，請選取下列一項：
   - 如果您要使用 Windows 登入密碼來保護 Rescue and Recovery 工作區，請選取**使用 Windows 密碼來取得 Rescue and Recovery 工作區存取權**勾選框。
   - 如果您要使用 Client Security Solution 登入長密碼來保護 Rescue and Recovery 工作區，請勾選**使用 Client Security Solution 長密碼來取得 Rescue and Recovery 工作區存取權**勾選框。
5. 完成 Client Security Solution 安裝精靈，然後按一下**完成**。如需相關資訊，請按一下 Client Security 安裝精靈中的**說明**。

方法 2：如果您已完成 Client Security 安裝精靈，請執行下列步驟，使用密碼或長密碼來保護 Rescue and Recovery 工作區：

1. 在 Windows 桌面上，按一下**開始**，按一下**所有程式**，選取 **ThinkVantage**，然後連按兩下 **Client Security Solution**。
2. Client Security Solution 視窗開啓時，請按一下**進階**功能表項目。
3. 按一下**變更登入設定**。
4. 按照螢幕上的指示操作。如需詳細資訊，請按一下 Client Security Solution 應用程式中的**說明**。

使用 Client Security 安裝精靈設定備份喜好設定

Client Security Solution 安裝精靈提供配置選項，可讓您設定多種安全功能，例如啓用內嵌式安全晶片、選取 Windows 環境中的鑑別方式、選擇使用 Rescue and Recovery 來備份機密資料，或是選用指紋辨識來進行鑑別。

若要使用 Client Security 安裝精靈，請完成下列程序：

1. 在 Windows 桌面上，按一下**開始**，按一下**所有程式**，選取 **ThinkVantage**，然後連按兩下 **Client Security Solution**。
2. Client Security Solution 視窗開啓時，請按一下**進階**功能表項目。
3. 當 Client Security Solution 視窗開啓，請按一下**設定安全及備份喜好設定**。此時會開啓 Client Security 安裝精靈。
4. 設定您的安全喜好設定。
5. 完成 Client Security Solution 安裝精靈，然後按一下**完成**。如需詳細資訊，請按一下 Client Security 安裝精靈中的**說明**。

Client Security Solution 相關資訊

如需 Client Security Solution 應用程式及其功能的詳細資訊，請參閱以下網頁的 *Client Security Solution User Guide*：

`http://www.ibm.com/pc/support/site.wss/`

如果您已安裝 Client Security Solution 應用程式，您可以在使用手冊中閱讀更詳細的資訊，步驟如下：

1. 在 Windows 桌面上，按一下**開始**。

2. 選取**所有程式**。
3. 選取 **ThinkVantage**。
4. 按一下 **Client Security Solution**。
5. 在 Client Security Solution 功能表列上按一下**說明**。
6. 按一下**使用手冊**。

Appendix. 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 a 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.
500 Park Offices Drive, Hwy. 54
Research Triangle Park, NC 27709
U.S.A.
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 obtained 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

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

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

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

ThinkVantage™

Printed in USA